LICEO STATALE
VERONICA GAMBARA
LICEO LINGUISTICO - LICEO MUSICALE - LICEO DELLE SCIENZE UMANE
Via V. Gambara 3 - 25121 Brescia Tel. 030 3775004 Fax 0303776455
Cod. meccanografico BSPM020005 – C.F. 80049650171
E-mail bspm020005@istruzione.it – PEC bspm020005@pec.istruzione.it
www.liceogambara.edu.it

DPIA Data Protection Impact Assessment

(valutazione d'impatto in caso di violazione della protezione dei dati)

Adozione di piattaforme cloud nello svolgimento delle attività didattiche ed amministrative, trasferimento di dati verso paesi terzi in mancanza di decisione di adeguatezza

Introduzione

Questa valutazione si riferisce all'uso di tecnologie digitali utilizzate per l'insegnamento, per la gestione di contenuti e la condivisione di documenti nell'ambito delle attività didattiche, organizzative e amministrative dell'istituto.

Sia mediante gli strumenti digitali messi a disposizione dall'Istituto che mediante dispositivi personali compatibili con il sistema digitale adottato, gli alunni, i loro famigliari e il personale dell'istituto possono accedere alle risorse digitali gestite dall'istituto, siano esse posizionate su dispositivi interni sia su piattaforma cloud.

Per fruire di questa struttura di utilizzo e condivisione, ogni utente deve essere dotato di una identità digitale che includa:

1. credenziale di autenticazione basata su codice utente per accedere alle piattaforme di:
   - gestione delle lezioni
   - condivisione di documenti
   - videocomunicazione
   - lavoro collaborativo

2. indirizzo di posta elettronica fornita e gestita dall'Istituto (è sempre escluso l'utilizzo di caselle di posta non gestite dall'Istituto).

L'identità digitale viene gestita dall'istituto tempestivamente sia in fase di assegnazione che di revoca.

In fase di scelta degli strumenti da adottare per i vari elementi del sistema si è tenuto conto di diversi elementi:

- efficienza nella gestione del proprio ambito

- facilità d'uso
- sicurezza
- conformità con normative di riferimento
- costi

non sempre l'Istituto ha avuto la possibilità di valutare efficacemente tutti gli elementi, dovendo compiere scelte influenzate anche da altri fattori, quali la disponibilità di assistenza e di formazione, la diffusione del prodotto in ambiti simili, la dimestichezza del personale nell'uso del prodotto.

La piattaforma per la quale redigiamo questa analisi è stata adottata anche nei mesi dell'emergenza pandemica. La scelta ha anche tenuto conto delle indicazioni allora presenti sul sito istituzionale e su altri canali digitali del Ministero.

Sulla base dei criteri sopra esposti il nostro istituto ha deliberato con delibera del Consiglio di Istituto n. 51/2020 in data 22.12.2020 (prot. n. 10348 - 29/12/2020) il regolamento relativo all'utilizzo della piattaforma Google Workspace a seguito delle disposizioni contenute nei decreti, emanati ai sensi dell'art. 3 del d.l. 23 febbraio 2020, n. 6, che hanno disposto - per tutta la durata della sospensione delle attività didattiche "in presenza" nelle scuole a causa della diffusione di Covid 19 - l'attivazione di modalità di didattica a distanza.

La scelta è stata fatta valutando gli elementi sopra riportati e sulla base delle indicazioni provenienti dal Ministero dell'Istruzione che ha riportato nel suo sito l'elenco delle risorse che le scuole potevano prendere in considerazione per lo svolgimento dell'attività DAD, fra le quali era anche presente la piattaforma poi adottata dalla scuola. Si è altresì provveduto a verificare la certificazione AgID dell'applicazione adottata, condizione prevista come necessaria all'adozione di piattaforme cloud da parte della pubblica amministrazione.

A causa della situazione emergenziale in cui si è dovuto allora operare la scuola non ha effettuato alcuna valutazione di impatto sul trattamento di dati personali operati sulla piattaforma come peraltro previsto provvedimento del garante Privacy 26 marzo 2020, n.64 che, oltre a indicare come non necessaria la redazione di una DPIA, si era anche impegnato a vigilare sulle soluzioni adottate e quindi a comunicare alle scuole eventuali impedimenti all'uso delle piattaforme cloud.

Così precisava il Garante:

"La valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici)."

Una volta terminata la fase emergenziale, alla luce della sentenza che ha sospeso il trattato fra UE e USA, cosiddetto "scudo" che regolava il trasferimento dei dati personali fuori dallo spazio economico europeo (SEE), avendo assistito al nascere di dubbi sulla conformità al GDPR dei servizi basati in USA, come quello da noi scelto, abbiamo ritenuto di effettuare la presente DPIA.

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 investita la scuola (art. 6 comma 1 lettera e del GDPR).

L'obiettivo della transizione al digitale delle pubbliche amministrazioni è stato indicato fin dal 2005 con l'adozione del CAD. Da allora anche nel contesto scolastico in cui l'insegnamento di competenze digitali integrate è da considerarsi centrale nell'educazione dell'individuo in qualsiasi fascia di età, l'utilizzo consapevole di questi strumenti durante l'attività didattica è una delle metodologie che possono facilitarne l'apprendimento.

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 era il parere espresso dal Garante nel provvedimento 26 marzo 2020, n.64.

Ci sono standard applicabili al trattamento?

Primo riferimento relativo ai trattamenti in questione è costituito dal documento edito dall'European Data Protection Board (EDPD) intitolato ***"2022 Coordinated Enforcement Action Use of cloud-based services by the public sector"*** (link) nel quale sono indicate le misure di sicurezza e le azioni da intraprendere per garantire al meglio la protezione dati degli utenti durante l'utilizzo di piattaforme cloud. L'EDPD ha pubblicato in precedenza 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"*** (link) che vengono in rilievo per il trasferimento di dati all'estero.

Ulteriori indicazioni provengono dal Ministero dell'Istruzione che ha pubblicato nell'estate del 2020 le Linee Guida per la Didattica Digitale Integrata (DDI) (link) contenenti indicazioni operative per la redazione di un piano per la didattica digitale integrata da parte di ciascun istituto scolastico.

In relazione alla individuazione dei fornitori viene in rilievo la **circolare AGID n. 2 del 09/04/2018** (link) che dispone che le Pubbliche Amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati da AGID (oggi attività demandata a Agenzia per la Cybersicurezza Nazionale – ACN).

In relazione all'adozione delle piattaforme cloud da parte delle istituzioni scolastiche si è preso anche di riferimento il **Provvedimento del Garante del 26 marzo 2020 - "Didattica a distanza: prime indicazioni"** (link) nel quale si dichiara come non necessaria la valutazione di impatto, ex art. 35 del GDPR che tuttavia viene redatta nel presente documento.

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 o di attività amministrativa.

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 a 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. A questo proposito, è necessario definire delle policy che limitino l'uso sulla piattaforma di dati di natura sensibile se non è possibile garantire adeguati livelli di sicurezza.

Il LICEO VERONICA GAMBARA ha ottenuto la qualifica di "scuola virtuosa" sui temi relativi all'uso sicuro e positivo delle tecnologie digitali per essersi dotata in data 30/11/2020 di un proprio documento di ePolicy recante le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico:
https://liceogambara.edu.it/documento/certificato-scuola-virtuosa/

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 potrebbe profilare quale atto amministrativo parte di un procedimento più ampio.

In questo particolare caso, sarebbe 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 basarsi su server extra-ue e in tal caso è necessario verificarne la compliance alla normativa europea sul trattamento dei dati, come faremo in seguito. 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.

Tali strumenti devono permettere, per poter fornire una adeguata copertura delle funzionalità necessarie alla didattica digitale, i seguenti servizi:

- Uno strumento di condivisione di file e cartelle. Tale strumento deve essere sicuro, protetto da autenticazione, con funzionalità di backup o comunque di versioning dei file, e con la possibilità di selezionare in maniera semplice e sicura le regole di condivisione dei file stessi. Deve inoltre essere possibile, a livello di amministrazione della piattaforma, selezionare la limitazione dell'accesso a file o cartelle a entità interne all'amministrazione stessa.
- Uno o più strumenti di messaggistica *sincrona* e *asincrona* (ad es. mail, chat), che possano essere utilizzati da studenti, genitori e personale scolastico ai fini di garantire la comunicazione tra alunni, scuola alunni e scuola famiglia, tramite modalità e strumenti sicuri e protetti da autenticazione, su strumenti sotto il controllo scolastico.
- Uno strumento di gestione delle classi virtuali che, possibilmente, integri le funzioni di condivisione e messaggistica sopra descritte, da utilizzare per la condivisione di materiale didattico, informativo o compensativo.
- Uno strumento di editing e condivisione di documenti, fogli di calcolo e presentazioni, da utilizzare per la didattica digitale. Valgono le stesse considerazioni fatte prima per quanto riguarda le modalità di condivisione.
- Condivisione eventuale di calendari a livello scolastico o di classe, per finalità di migliore comunicazione scuola-famiglia.

Trasferimento dati extra UE

E’ previsto il trasferimento di dati al di fuori dell'Unione europea?

Si. Google Workspace ha dei datacenter collocati in Europa dove normalmente risiedono i dati per i clienti europei ma non si può escludere che dati e documenti possano essere portati in data center al di fuori dell’UE. Si rileva inoltre che dati personali sono comunque trasferiti fuori dall’UE per la fornitura dei servizi in transito nei sistemi o in forma di dati di telemetria. (N.B. le scuole che hanno acquistato la versione PLUS possono dichiarare la collocazione dei server in territorio europeo. E’ comunque il caso di rilevare che anche in questo caso alcuni dati personali potrebbero uscire dalla UE in transito nei sistemi o come dati di telemetria).

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

No. In base alla legislazione attuale il trattamento dei dati operati nel territorio statunitense non garantisce un livello di protezione equivalente o comunque adeguato al GDPR. Ciò a seguito della sentenza Schrems II del 16 luglio 2020 che ha comportato l’invalidità del Privacy Shield che costituiva la decisione di adeguatezza in base alla quale, fino a tale data, avveniva il trasferimento dei dati verso gli Stati Uniti.

Per quali aspetti il grado di protezione non è equivalente a quello garantito dal GDPR?

La decisione di invalidità presa dalla Corte di Giustizia dell’Unione Europea (CGUE) in relazione all’adeguatezza della protezione fornita dal Privacy Shield deriva dalla legislazione statunitense che consente al Governo di accedere ai fini della sicurezza nazionale ai dati personali trasferiti dall’UE, con limitazioni alla protezione dei dati personali ed in violazione dei diritti fondamentali delle persone. Tali controlli possono avvenire senza che i cittadini europei possano opporsi o far valere i propri diritti in sede giudiziaria nei confronti delle autorità statunitensi.

Si rileva che non è invece in discussione la sicurezza intrinseca della piattaforma Google che possiede innumerevoli certificazioni per i principali standard internazionali riconosciuti. Google Workspace è anche presente nel Cloud Marketplace gestito dall’Agenzia per la Cybersicurezza nazionale nell’elenco SaaS (Software as a Service) con codice SA-690.

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

I trattamenti operati da Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) dove oltre ad attestare la conformità ed il rispetto delle disposizioni del GDPR, viene dichiarato all’articolo 10 che nel caso in cui il trasferimento di dati personali avvenga verso un paese non coperto da una decisione di adeguatezza, allo stesso si applicano le clausole contrattuali tipo, previste dall’articolo 46 GDPR. Analoga rassicurazione viene

fornita nelle FAQ di Google su privacy e sicurezza dove si afferma che Google Workspace for Education può essere utilizzato in conformità con il GDPR. Il nostro Emendamento sul trattamento dei dati è progettato per soddisfare i requisiti di adeguatezza e sicurezza del GDPR; inoltre, la Commissione europea ha creato delle clausole contrattuali tipo per consentire in particolare il trasferimento dei dati personali dall'Europa. I clienti possono aderire all'Emendamento sul trattamento dei dati e alle clausole contrattuali tipo.

La valutazione concreta dell'effettivo rispetto del GDPR nei trattamenti operati sulla piattaforma Google è resa complessa dalle dimensioni della nostra amministrazione che, pur supportata dal proprio DPO, non può contare su personale interno con adeguate competenze tecniche. Gli istituti scolastici non hanno poi alcun potere contrattuale nei confronti delle multinazionali del settore per cui è difficile entrare nel merito di certi aspetti contrattuali ed ancor meno è possibile, ove necessarie, definire condizioni personalizzate (c.d. tailored) sulle garanzie e responsabilità delle parti relativamente a tutti i processi di trattamento dati gestiti da Google. Come detto nel documento di EDPB "2022 Coordinated Enforcement Action Use of cloud-based services by the public sector" (link), è invece auspicabile un intervento di gruppo che permetta una contrattazione collettiva che garantisca una maggiore equità nel potere contrattuale delle parti. In questo senso riteniamo possa svolgere un ruolo fondamentale il Responsabile della Transizione Digitale per le scuole italiane, ruolo ricoperto dal Direttore Generale dei sistemi informativi del Ministero dell'Istruzione, che potrebbe avviare le interlocuzioni eventualmente necessarie con Microsoft e Google al fine di chiarire alcuni aspetti dei trattamenti operati sulle piattaforme.

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 costituita dall' esecuzione di un compito di interesse pubblico di cui è investita la scuola (art. 6 comma 1 lettera e del GDPR).

L'uso della piattaforma oggetto di analisi è finalizzato al perseguimento delle finalità istituzionali di istruzione e formazione. Altro utilizzo del medesimo strumento è finalizzato a condurre la transizione digitale imposta alle PA dal D. Lgs 82/2005 (CAD), dal PNSD, dai piani triennali per l'informatica nelle PA e dal PNRR. L'uso delle piattaforme digitali per il perseguimento delle finalità istituzionali e per condurre la transizione digitale dell'amministrazione è stabilito nel Piano Triennale dell'Offerta Formativa (PTOF) redatto dall'istituto (verificare).

E' possibile perseguire l'interesse pubblico con altri strumenti?

Volendo prima di tutto garantire la tutela dei diritti degli interessati, anche alla luce del dibattito aperto da associazioni di attivisti che hanno preso di mira l'uso delle piattaforme cloud da parte delle pubbliche amministrazioni italiane, abbiamo valutato la possibilità di rinunciare all'uso della piattaforma per il conseguimento delle finalità di interesse pubblico di pertinenza delle istituzioni scolastiche. E' però anni che i vari piani triennali per l'informatica nelle PA, in attuazione del Codice dell'Amministrazione Digitale, inducono le pubbliche amministrazioni ad un uso sempre più diffuso e capillare dell'informatica con

particolare riferimento ad applicazioni e piattaforme cloud (secondo il paradigma cloud first). Questo processo ha avuto una repentina accelerata con le misure emergenziali di contenimento del Covid 19 che hanno portato alla diffusione anche nel contesto scolastico dei nuovi strumenti di comunicazione e di lavoro collaborativo sia per condurre attività in smart working che per condurre le quotidiane attività didattiche. Negli ultimi anni il nostro istituto, costretto dall'emergenza, ha rivisto la propria organizzazione e le proprie procedure alla luce dell'impiego delle nuove tecnologie telematiche e del cloud entrati a far parte della quotidiana attività di alunni, docenti e personale scolastico. Oggi gli strumenti telematici e la piattaforma cloud sono utilizzati in affiancamento e di supporto alla ordinaria attività didattica in presenza in tutte le discipline per favorire nuove modalità di apprendimento. L'uso di tali strumenti ha poi una valenza educativa e formativa per l'uso consapevole di applicazioni da parte dei futuri cittadini che devono vedere garantiti i propri diritti nella società digitale verso cui stiamo andando. Al fine di favorire l'uso delle nuove tecnologie la scuola ha infine prodotto delle profonde revisioni alle proprie procedure ed organizzazione nelle quali hanno oggi un ruolo centrale l'uso di caselle elettroniche istituzionali assegnate dalla scuola, la videocomunicazione e strumenti per il lavoro collaborativo. Il nostro istituto si trova oggi ad un punto del processo di transizione al digitale, promosso dalla normativa vigente ed incentivato anche dal finanziamento del PNRR, da cui non è possibile tornare indietro. Le nuove tecnologie e la piattaforma cloud adottata sono quindi oggi necessarie al perseguimento degli interessi pubblici e la scuola non può rinunciare ad esse senza rinunciare a perseguire le proprie finalità istituzionali.

Esistono possibili alternative alla piattaforma adottata?

Valutato che non è possibile rinunciare all'utilizzo di strumenti cloud per la conduzione delle attività scolastiche passiamo a considerare se esistono delle soluzioni alternative a quella adottata dalla scuola che possano garantire maggiori livelli di sicurezza nel trattamento dei dati personali. Il contesto attuale nel settore dei servizi cloud è tuttavia dominato dalle multinazionali statunitensi mentre l'Europa svolge oggi un ruolo solo secondario. Le soluzioni alternative in qualche modo paragonabili a quella adottata dal nostro istituto sono quindi di altre multinazionali statunitensi con i medesimi problemi legati alla sentenza Schrems II e non esistono soluzioni equiparabili di fornitori europei.

Anche in ambito open source non esistono ambienti integrati per la didattica ed il lavoro collaborativo che forniscano la stessa ricchezza di strumenti e la semplicità d'uso e di gestione garantiti dalla piattaforma adottata. C'è poi da rilevare che la nostra scuola non ha fra il proprio personale le competenze necessarie per allestire e gestire correttamente del software in ambito open source. L'assenza di competenze informatiche specifiche renderebbe verosimilmente l'ambiente open source allestito estremamente insicuro ed esposto a incidenti non potendo garantire livelli di sicurezza paragonabili a quelli possibili sulla piattaforma già adottata.

Quali misure supplementari sono state adottate?

Valutata l'inesistenza di possibili soluzioni alternative che diano maggiori garanzie di adeguatezza si ritiene di dover adottare il principio di minimizzazione del rischio stabilito anche dal recente report di EDPB (Use of cloud-based services by the public sector

Adopted - 17 January 2023 - link). In pratica vedremo di seguito le misure supplementari adottate per ridurre il rischio associato all'uso della piattaforma per poi valutare se l'entità del rischio residuo è al di sotto di una soglia che si può ritenere accettabile.

Si precisa che in questa sede si sono prese in considerazione misure di sicurezza supplementari attuabili in un contesto scolastico e quindi ignorate soluzioni tecniche troppo complesse da implementare e da gestire in assenza di personale tecnico specializzato.

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

- **Coinvolgimento del DPO: nella presente valutazione è stato coinvolto direttamente il DPO**
- Corretta attribuzione dei ruoli: sono state adottate misure organizzative tali da garantire concretamente la gestione del rischio attraverso l'individuazione di specifici ruoli e responsabilità.
- Valutazione dei dati da trattare: anche la scelta dei dati personali oggetto di trattamento sulla piattaforma cloud è stata valutata alla luce dei principi di necessità (per i dati sensibili) e di riduzione del rischio (per i dati personali comuni).
- Valutazione dei servizi necessari: per la minimizzazione dei rischi si è anche valutato di limitare l'uso delle applicazioni da utilizzare nella piattaforma.
- Anonimizzazione, cifratura e pseudonimizzazione: per garantire adeguati livelli di protezione si sono prese in considerazione tecniche di anonimizzazione, cifratura e pseudonimizzazione.
- Definire regolamenti e disposizioni specifiche per l'uso delle piattaforme: l'istituto ha formato un coerente corpo documentale con informative, disciplinari e regolamenti atti a gestire il trattamento dei dati personali sulla piattaforma cloud e sui sistemi informatici dell'istituto in generale.

E' stato coinvolto il DPO nella valutazione dei rischi?

Si. Il DPO ha fornito supporto ed assistenza nella redazione del presente documento come dell'altra documentazione prodotta per l'uso della piattaforma nel rispetto della normativa.

Sono stati attribuiti correttamente ruoli e responsabilità?

La complessità delle azioni e dei possibili risvolti in termini di violazione dei Dati Personali 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 e di tutte le parti che fruiscono del servizio. Inoltre, è compito del D.S. quello di definire un codice di condotta interno alla scuola che regoli l'utilizzo della strumentazione elettronica e la piattaforma utilizzate, e di sorvegliare sulla sua attuazione.

- I docenti: Il loro ruolo centrale nella produzione di compiti e contenuti deve essere associato ad un'attività di controllo nei confronti di tutte quelle attività suscettibili di violazioni della privacy e dei dati personali. 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. I docenti hanno funzioni di supervisione delle modalità di utilizzo della piattaforma relativamente alle attività didattiche da loro gestite.
- Il consiglio di classe: Delibera sulla valutazione finale in fase di scrutini. Potrebbe quindi essere necessario allo stesso l'accesso ai documenti prodotti in modalità digitale, ivi inclusi i dati personali.
- Il Responsabile della Protezione dei Dati (RPD/DPO): 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: i provider dei servizi in cloud utilizzati 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. A seguito di tale valutazione il fornitore del servizio deve essere nominato responsabile del trattamento ai sensi dell'Art. 28, comma 3 del GDPR. Secondo quanto previsto dal Regolamento servizi cloud AGID, che mira a garantire "i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione", le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati, la cui lista aggiornata può essere trovata sul c.d. "Cloud Marketplace" dell'AGID. Dal 2 gennaio 2023 con il Decreto direttoriale n. 29 del 2 gennaio 2023, tale compito è stato affidato all'Agenzia per la Cybersicurezza nazionale, e il processo di certificazione è attualmente in una fase transitoria che durerà fino a gennaio 2024.
- 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.

E' stato applicato un principio di minimizzazione dei dati personali trattati?

Con l'obiettivo di ridurre i rischi associati si è limitato il trattamento ai dati necessari per il conseguimento delle finalità sopra richiamate. In particolare per ogni utente la scuola ha caricato soltanto il nome ed il cognome a cui è stato poi attribuita una casella istituzionale costituita da nome.cognome@dominio.scuola. Si intende disabilitare la possibilità di aggiungere ulteriori informazioni da parte dell'utente proprietario del profilo quali telefono, email alternative e foto (misura che suggeriamo comunque di adottare).

Il principio di minimizzazione dei dati personali dovrà essere tenuto in considerazione anche da tutti gli utenti che dovranno evitare di inserire nei documenti caricati sulla piattaforma dati personali non necessari e non pertinenti con la finalità del documento. Particolarmente rigorosi nel rispetto di tale principio devono essere i docenti nel momento in cui affidano dei compiti agli alunni o svolgono le attività didattiche, amministrative e collegiali di propria competenza. Le disposizioni relative alla minimizzazione dei dati personali da utilizzare nella redazione di relazioni, verbali ed altri documenti sono presenti nell'autorizzazione al trattamento dei dati personali formalizzata al personale nello svolgimento delle proprie funzioni.

Sono state adottate particolari misure per il trattamento di dati sensibili?

Per il trattamento dei dati sensibili sono state date agli utenti indicazioni di stretta necessità dell'informazione prima del suo inserimento in un documento da caricare nella piattaforma cloud. Per quanto riguarda gli alunni, i docenti sono stati invitati a valutare attentamente l'opportunità di proporre ad essi attività che prevedono il trattamento di dati ed informazioni sensibili e di valutare possibili alternative all'uso della piattaforma. Il principio di stretta necessità del dato sensibile dovrà anche essere utilizzato da tutto il personale nella redazione della documentazione di propria competenza. La scuola intende valutare se proibire dall'a.s. 2023/24 l'uso della piattaforma cloud per la redazione e la condivisione di determinati documenti quali, ad esempio, il Piano Educativo Individualizzato (PEI) o il Piano Didattico Personalizzato (PDP). Prima di prendere misure più drastiche, ed anche più onerose, la scuola ha deciso di consentire la redazione e lo scambio dei PEI in forma pseudonimizzata a seguito dell'associazione di un codice riservato per ogni alunno che necessita della redazione del documento. Analogo codice dovrà essere utilizzato anche in altra documentazione che faccia riferimenti all'alunno con necessità di sostegno e per il quale debba essere garantita riservatezza.

E' stato applicato un principio di minimizzazione anche in relazione alle applicazioni utilizzate?

Si. Anche nella scelta dei servizi e delle applicazioni utilizzate si sono tenuti presenti i principi di necessità e di minimizzazione per ridurre i possibili rischi associati al loro uso. Al termine di tale valutazione si è deciso di attivare le seguenti applicazioni:

- Caselle di posta elettronica
- Sistema di videoconferenza (*Meet*)
- *Documenti*, *Fogli* di calcolo e *Presentazioni*
- *Classroom* per la gestione delle lezioni e dei compiti
- Strumenti per il lavoro collaborativo
- *Moduli* per sondaggi e iscrizioni ad attività scolastiche ed extrascolastiche
- Calendari per la condivisione di impegni e appuntamenti comuni
- Rubriche e gruppi per la condivisione di contatti
- *Sites* per la creazione di siti web
- Spazio di archiviazione condivisa (*Drive*)
-

Come ulteriore misura di contenimento dei rischi si è limitata la comunicazione delle caselle degli alunni con le caselle di posta elettronica a quelle realizzate nel dominio associato alla scuola

Sono state adottate tecniche di anonimizzazione, pseudonimizzazione e cifratura per la protezione dei dati personali?

Come detto più sopra nella relativa sezione, sono state adottate tecniche di anonimizzazione e di pseudonimizzazione per la protezione dei dati sensibili (in particolare per la redazione dei PEI). Si è anche presa in considerazione l'opportunità di procedere alla pseudonimizzazione dei dati personali identificativi caricati sulla piattaforma. In particolare si è valutata la possibilità di caricare nella piattaforma non il nome e cognome dell'utente ma il codice di pseudonimizzazione ad esso associato. Adottando tale soluzione la casella associata all'utente non sarà più nome.cognome@dominio.scuola ma codice-utente@dominio.scuola. In tal modo, tuttavia, si complica notevolmente la gestione della piattaforma e diventa complessa la comunicazione email, fatto che comporta un sensibile aumento del rischio di errori che possono condurre anche a rilevati violazioni dei dati personali (si pensi ai problemi che possono nascere da errori nella digitazione del destinatario di una comunicazione o alla perdita della chiave che associa un codice ad un determinato utente). Al termine della valutazione del rischio condotta si ritiene che adottare tecniche di pesudonimizzazione del nome e cognome degli utenti e delle caselle email ad esse associate comporti non una diminuzione ma un sensibile aumento del rischio associato. Si rileva peraltro che il fornitore è senz'altro autorizzato ad accedere a tali dati nel ruolo di responsabile del trattamento e che il rischio che si deve considerare a seguito della sentenza Schrems II è la possibilità che il governo degli Stati Uniti possa, per motivi di sicurezza nazionale, accedere ai dati caricati sulla nostra piattaforma scolastica, evento possibile a causa della vigente legislazione statunitense ma evidentemente assai remoto in termini di probabilità.

L'estrema improbabilità di tale evento ci induce anche a rinunciare a tecniche di crittografia lato client che permetterebbero di tenere nascosti i dati caricati sulla piattaforma agli occhi del fornitore e quindi al governo degli Stati Uniti che chiedesse l'accesso. Anche in questo la soluzione tecnica e le procedure farraginose che ne deriverebbero, poco attuabili in un contesto scolastico, aumenterebbero a dismisura i rischi di violazione di dati personali invece di diminuirli (si pensi soltanto alla difficoltà di gestione delle chiavi di decodifica e dei problemi che potrebbero derivare dalla loro perdita).

E' stata fornita agli utente idonea informativa e sono state portate a conoscenza di essi le procedure di utilizzo della piattaforma?

Si. Tutti gli utenti registrati sulla piattaforma hanno ricevuto specifica informativa privacy per i trattamenti di dati personali operati sulla piattaforma cloud adottata dalla scuola. In essa gli interessati sono stati informati della nomina di Google a responsabile del trattamento e che nell'uso della piattaforma potrà occorrere il trasferimento di dati personali al di fuori dello Spazio Economico Europeo. Sono state fornite a tutti gli utenti disposizioni specifiche per l'uso corretto della piattaforma e tali da garantire la sicurezza e la protezione dei dati personali in essa trattati.

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 di monitoraggio specifico, relativo alla probabilità massima di accesso annuale accettabile. Tale numero è stato calcolato considerando accettabile una probabilità del 50% che un accesso avvenga ogni 40 anni, e corrisponde ad una probabilità di accesso annuale dell’1,48%.

Qual è la 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 effettiva 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 e calcolando un numero di account iscritti a Google Workspace nel 2021 di circa 3'000'000'000, sono state effettuate due valutazioni di rischio:

- La prima riguarda le probabilità di accesso delle agenzie di sicurezza USA sulla base del Foreign Intelligence Surveillance Act (FISA) e delle National Security Letters (NSLs), e restituisce una probabilità di accesso dello 0,0009% annuo, arrotondato per eccesso.
- La seconda, effettuata sul numero di accessi a livello mondiale (il quale include tutte le richieste legittime dei governi sulla popolazione residente nei propri stati di nazionalità, e tutte le richieste di governi Europei o di stati per i quali esiste una decisione di adeguatezza), restituisce una probabilità di accesso di circa lo 0,027% per quanto riguarda il singolo account, a livello mondiale.

Non è stato possibile reperire informazioni sul numero di account enterprise attivi nel mondo per effettuare una analisi su un campione più ristretto. Perciò, la valutazione è stata effettuata su un campione mondiale, consci del fatto che il campione potrebbe non essere rappresentativo della popolazione scolastica Europea, ma non ci si aspetta errori statistici tali da far si che le probabilità sopra considerate superino il valore massimo di soglia accettabile.

Il rischio associato al trasferimento dei dati al di fuori dell’UE è ritenuto accettabile?

Nell’analisi condotta la probabilità massima di accesso non autorizzato annuale accettabile (KPI) è stata fissata all’1,48% (probabilità del 50% che avvenga un accesso non autorizzato ogni 40 anni). Dai valori statistici forniti da Google risultano probabilità di accesso di 0,027% calcolate nelle condizioni più svantaggiose, abbondantemente al di sotto del rischio accettabile stabilito. Al fine di verificare e garantire nel tempo che questo rischio continui a mantenersi accettabile, si prevede di verificarne la validità con cadenza annuale, sulla base dei report pubblicati dal fornitore Responsabile del Trattamento.

Quali conclusione sulla valutazione del rischio associato al trasferimento extra UE dei dati personali?

La sentenza Schrems II ha determinato l'invalidità del Privacy Shield e con esso la decadenza della decisione di adeguatezza sul trasferimento negli Stati Uniti dei dati personali dei cittadini europei.

Con la sua sentenza la Corte di Giustizia dell'Unione Europea (CGUE) ha stabilito che i requisiti del diritto interno degli Stati Uniti non garantiscono un livello di protezione dei dati equivalente a quello europeo a causa della legislazione che consente alle autorità pubbliche degli Stati Uniti di accedere ai dati personali trasferiti dall'UE ai fini della sicurezza nazionale con limitazioni alla protezione dei dati personali ed in violazione dei diritti fondamentali delle persone. Tali controlli possono avvenire senza che i cittadini europei possano opporsi o far valere i propri diritti in sede giudiziaria nei confronti delle autorità statunitensi.

A seguito della sentenza Schrems II e del dibattito che si è aperto sul tema, abbiamo quindi ritenuto necessario valutare i rischi associati all'uso della piattaforma adottata dalla scuola, limitatamente al trasferimento dei dati personali negli Stati Uniti che ne consegue, rilevandoli assolutamente contenuti e praticamente nulli. E' infatti assolutamente improbabile che il governo degli Stati Uniti, per motivi di sicurezza nazionale, possa essere interessato ai dati personali caricati sulla piattaforma utilizzata dal nostro istituto per svolgere la propria attività istituzionale. Anche le conseguenze di un simile atto, già improbabile, sarebbero nulle ove gli utenti, adeguatamente informati, si fossero attenuti alle disposizioni impartite dalla scuola per l'uso della piattaforma.

L'entità insignificante del rischio concreto associato al trasferimento di dati personali su server statunitensi ci ha indotto a non adottare tecniche particolarmente complesse, ed incompatibili con un contesto scolastico, per la riduzione di un rischio già abbondantemente al di sotto di una soglia accettabile ove tali tecniche comporterebbero invece un innalzamento del rischio di incidenti con conseguente violazione dei dati personali.

Di maggior rilievo sono invece i rischi associati all'uso della piattaforma cloud in sé, indipendentemente dalla collocazione geografica dei server o del fornitore, e relativi al trattamento di dati personali, anche sensibili e di minorenni, su sistemi informatici complessi. Per la gestione di tali rischi nel trattamento di dati personali necessari per il conseguimento di finalità istituzionali, si sono adottati i principi di necessità e di minimizzazione stabiliti dal GDPR. Nel prosieguo del documento la valutazione di impatto per l'uso della piattaforma cloud che prende in considerazione tutti i rischi associati ai trattamenti operati e non solo quelli relativi al trasferimento extra UE.

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 digitale 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 all'utilizzo di piattaforme e servizi digitali, con l'effetto collaterale di aumentarne la consapevolezza nell'uso dell'ambito tecnologico, lato fruizione e lato produzione. Tale consapevolezza è utile fin dalle classi di ordine inferiore e diventa necessaria a orientarsi nella scelta del futuro percorso di studio e/o professionale da intraprendere per gli studenti degli istituti superiori. In questo processo è importante l'utilizzo di software e attrezzature dedicati fra i quali abbiamo deciso di puntare su strumenti molto diffusi e spesso già utilizzati dagli studenti e dal personale scolastico. 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.

Gli stessi strumenti adottati per condurre l'attività didattico/formativa devono essere utilizzati anche per favorire la comunicazione fra le varie componenti scolastiche per finalità organizzative ed amministrative. Da qui l'uso di sistemi di videocomunicazione, email e di condivisione documenti e risorse anche nello svolgimento delle attività dei vari organi collegiali, delle commissioni e più in generale del personale scolastico che allo scopo è stato dotato dall'amministrazione scolastica di una casella email istituzionale.

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)
- Legge 13 Luglio 2015, n. 107 (Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti – PNSD).
- D. L. 179/2012 convertito con L. 221/2012
- D.L. 95/2012 (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 necessità, possano garantire lo svolgimento dell'attività didattica a distanza. Il CAD offre invece la base normativa per l'uso delle tecnologie informatiche e telematiche per lo svolgimento delle attività organizzative ed amministrative dell'amministrazione.

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), viene in rilievo 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 stringente per i dati particolari di cui all'art. 9 del GDPR (dati sensibili) che dovranno essere trattati solo se strettamente necessari, e comunque utilizzando degli strumenti di minimizzazione e protezione dei dati (ad es. pseudonimizzazione).

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 fornire adeguate informazioni agli utenti e 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 soluzioni di backup e di cronologia delle modifiche (versioning).

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 o amministrativa prevista. 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 a personale, alunni e genitori degli stessi tramite una combinazione più completa possibile dei canali disponibili alla scuola, che includono, a titolo esemplificativo e non esaustivo:

- L'utilizzo delle modalità di comunicazione scuola famiglia messe a disposizione dal registro elettronico.
- La pubblicazione nella sezione privacy del sito web istituzionale;
- 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);

Gli interessati sono stati informati sulle modalità di trattamento e sui possibili rischi associati anche in relazione al possibile trasferimento dei dati personali al di fuori dell'UE. Durante il processo didattico stesso verranno forniti agli studenti le conoscenze necessarie ad un utilizzo consapevole della piattaforma anche per garantire la protezione dei dati personali propri e altrui.

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 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 trattamenti operati da Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) dove sono specificati gli obblighi del fornitore individuato responsabile del trattamento. E' tuttavia da rilevare lo scarso potere contrattuale detenuto dalla scuola nei confronti del fornitore e l'importanza che potrebbe avere il coinvolgimento diretto del Responsabile della Transizione Digitale delle istituzioni scolastiche, ruolo assunto dal Direttore Generale dei sistemi informativi del Ministero dell'Istruzione, che potrebbe avviare le interlocuzioni eventualmente necessarie con i fornitore al fine di chiarire alcuni aspetti dei trattamenti operati sulle piattaforme

Per quanto riguarda la valutazione dell'affidabilità dei servizi presi in esame, si è provveduto a verificare che il fornitore è inserito nel c.d. Cloud Marketplace gestito dall'agenzia all'**Agenzia per la Cybersicurezza nazionale** nell'elenco SaaS (Software as a Service) con codice **SA-690** (Google Workspace)**.**

Per quanto riguarda la gestione dei subresponsabili, le problematiche relative al controllo su di essi risultano particolarmente complesse da gestire. Non è infatti alla portata del singolo istituto scolastico entrare nel merito dell'operato di ciascun subresponsabile né di richiedere delle modifiche in tal senso. Se si ritenesse necessario un approfondimento di questo aspetto sarebbe opportuno l'intervento del Responsabile della Transizione Digitale.

Rischi

Misure esistenti o pianificate

Crittografia

Il fornitore cripta i dati per impostazione predefinita. I dati sono protetti con più livelli di sicurezza che includono tecnologie di crittografia all'avanguardia, come i protocolli HTTPS e Transport Layer Security. Non si è ritenuto opportuno adottare tecniche di cifrature client side.

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

Sebbene il fornitore debba predisporre le soluzioni tecniche atte a garantire la reperibilità e l'integrità dei dati caricati sulla piattaforma è opportuno che la scuola valuti ulteriori misure di salvaguardia dei dati e dei documenti.

Manutenzione

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware e software scolastici. Allo scopo è stato individuato un amministratore di sistema che garantisce anche la gestione e la sicurezza dei sistemi informatici. Il fornitore della piattaforma cloud garantisce il corretto funzionamento e la sicurezza dei propri sistemi.

Contratto con il responsabile del trattamento

I trattamenti operati da Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) dove vengono specificati gli obblighi del fornitore individuato responsabile del trattamento.

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. Specifiche istruzioni e regolamenti sono stati emessi dall'istituto per la tutela dei dati personali nell'uso della piattaforma cloud.

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 degli incidenti che coinvolgono dati personali. Emessa anche una circolare per il personale che deve essere in grado di riconoscere un data breach quando interviene e che deve sapere cosa fare all'occorrenza.

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

Il rischio: Il primo rischio che andiamo a valutare è l'accesso illegittimo ai dati che può intervenire a seguito di azioni accidentali o dolose. Le fonti del rischio sono le seguenti:

- errori nell'indicazione dell'indirizzo del destinatario di una comunicazione
- errato uso del campo CC al posto di quello CCN
- errori nella concessione dei permessi di accesso ai documenti al momento del caricamento sulla piattaforma
- azioni dolose da parti di utenti della piattaforma o di estranei per accedere a dati ed informazioni di terze persone

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
- minimizzazione dei dati

- pseudonimizzazione e anoniomizzazione
- manutenzione
- politiche di tutela della privacy
- formazione
- procedure per la gestione degli incidenti

Stima gravità del danno: La gravità del danno per l'accesso illegittimo ai dati personali comuni possiamo ritenerla **limitata** (livello 2 su una scala di 4). Più grave l'accesso illegittimo ai dati di natura sensibile quando questo, ad esempio, coinvolge documenti di programmazione dell'attività didattica/educativa (PDP/PEI) legati a particolari condizioni dell'alunno. In tal caso la venuta a conoscenza di tutti gli alunni della classe di situazioni personali e di salute particolari di un proprio compagno può comportare in questo e nella sua famiglia un notevole disagio. 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 già adottate la probabilità del rischio può essere valutata come **limitata** (livello 2 su una scala di 4). Per mantenere la probabilità di rischio ad un livello contenuto la scuola si impegna a portare avanti attività formative e di sensibilizzazione di tutti gli utenti della piattaforma.

Stima gravità del rischio:

Gravità del rischio = Danno x Probabilità

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

Modifiche indesiderate dei dati

Il rischio: Il secondo rischio che andiamo a valutare è la modifica indesiderata di dati. Le fonti del rischio sono le seguenti:

- errore umano
- azione volontaria di un utente della piattaforma o di un soggetto esterno

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: La gravità del rischio per modifiche indesiderate ai dati personali comuni possiamo ritenerla **limitata** (livello 2 su una scala di 4). Fra le eventualità più gravi da considerare è che la violazione potrebbe portare ad una errata valutazione dell'alunno. Tuttavia le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

Stima probabilità del rischio: A seguito delle misure di sicurezza già adottate la probabilità del rischio può essere valutata come **trascurabile** (livello 1 su una scala di 4). Per mantenere la probabilità di rischio ad un tale livello la scuola si impegna a portare avanti attività formative e di sensibilizzazione di tutti gli utenti e dei docenti in particolare che devono vigilare sul corretto uso della piattaforma. Gli utenti, ed il personale scolastico in particolare, devono anche essere sensibilizzati sulle misure di sicurezza da adottare per tenere riservate le proprie credenziali ed evitare così un accesso indebito ai sistemi da parte di terzi.

Stima gravità del rischio:

Gravità del rischio = Danno x Probabilità

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

Perdita di dati

Il rischio: Il terzo rischio che andiamo a valutare è la perdita di dati. Le fonti del rischio sono le seguenti:

- errore umano
- azione volontaria di un utente della piattaforma o di un soggetto esterno
- guasti ed altre cause accidentali

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: La gravità del rischio per modifiche indesiderate ai dati personali comuni possiamo ritenerla **limitata** (livello 2 su una scala di 4). Fra le eventualità più gravi da considerare è la perdita di documenti soggetti a valutazione da parte del docente o quella di documenti redatti dal personale scolastico.

Stima probabilità del rischio: A seguito delle misure di sicurezza già adottate la probabilità del rischio può essere valutata come **trascurabile** (livello 1 su una scala di 4). Per mantenere la probabilità di rischio ad un tale livello la scuola si impegna a portare avanti attività formative e di sensibilizzazione di tutti gli utenti della piattaforma.

Stima gravità del rischio:

Gravità del rischio = Danno x Probabilità

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

Valutazione gravità del rischio

A seguito dell'analisi condotta abbiamo quindi ricavato le seguenti valutazioni:

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

Quelle condotte sono delle valutazioni sommarie volte a stimare l'entità dei rischi connessi all'uso della piattaforma cloud. L'analisi condotta evidenzia come i rischi, valutati in relazione alla probabilità ed alla entità del danno, sono al di sotto di una soglia accettabile considerate le misure di contenimento del rischio già adottate. Non si ritiene quindi di dover fare analisi più approfondite sui rischi volte a stimare questi in modo più puntuale e alla ulteriore riduzione del rischio residuo.

Conclusioni

Gli organi collegiali del nostro istituto hanno deliberato in merito all'utilizzo delle moderne tecnologie informatiche e telematiche nello svolgimento delle proprie attività istituzionali 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.

In tale occasione il nostro istituto ha deciso per l'adozione della piattaforma 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.

A seguito della sentenza Schrems II che ha causato la caduta del Privacy Shield e del più recente dibattito aperto da gruppi di attivisti sull'uso delle piattaforme statunitensi da parte dei cittadini europei, abbiamo ritenuto di fare la presente valutazione di impatto per l'utilizzo di applicazioni cloud nello svolgimento delle attività didattiche ed amministrative e per il trasferimento di dati verso paesi extra UE.

E' importante rilevare che l'uso di qualunque strumento informatico comporta dei rischi per i dati personali trattati e che l'obiettivo non può essere quello di conseguire il rischio zero (a meno che non si voglia rinunciare allo strumento, cosa che abbiamo evidenziato non essere possibile) ma quello di contenere i rischi al di sotto di una soglia accettabile. Si evidenzia che non è in discussione la sicurezza intrinseca della piattaforma adottata dalla scuola che possiede innumerevoli certificazioni per i principali standard internazionali riconosciuti e che è presente nel Cloud Marketplace gestito dall'Agenzia per la

Cybersicurezza nazionale. Il fatto che non siano in discussione la sicurezza e l'affidabilità della piattaforma Google lo dimostra anche il provvedimento 26 marzo 2020, n.64 nel quale il Garante aveva ritenuto non necessaria la redazione della DPIA da parte delle scuole e non aveva espresso alcun parere contrario all'adozione delle piattaforme cloud. Questo è peraltro ciò che emerge dalla DPIA condotta nel presente documento che ha valutato alfine i rischi associati all'uso della piattaforma come al di sotto di una soglia accettabile, viste le misure di sicurezza adottate.

Particolare evidenza nel presente documento si è voluta dare alla valutazione di impatto per il trasferimento di dati verso paesi extra UE a seguito delle azioni intraprese da gruppi di attivisti che contestano alle scuole l'uso delle piattaforme delle multinazionali statunitensi. A conclusione di tale analisi possiamo concludere che anche in questo caso le misure di sicurezza adottate dall'istituto sono tali da contenere i rischi associati al trasferimento all'estero di dati personali al di sotto di una soglia accettabile. Si rileva peraltro che il rischio specifico evidenziato dalla sentenza Schrems II è quello del potenziale accesso del governo USA ai dati presenti nei server di aziende statunitensi, in violazione del GDPR, evento che nel nostro caso specifico può essere valutato come trascurabile sia in termini di probabilità dell'evento che per i possibili danni conseguenti.

Al termine di tale analisi riteniamo che l'uso della piattaforma cloud adottata dall'istituto garantisca la tutela dei dati personali nel rispetto del GDPR.

Il Collegio dei docenti nella seduta del 17 giugno 2023 si è espresso dal punto di vista didattico con delibera a favore del mantenimento di utilizzo della piattaforma Google Workspace.

Il presente documento è stato approvato dal Consiglio di Istituto con delibera n. 47 del 29.6.2023.