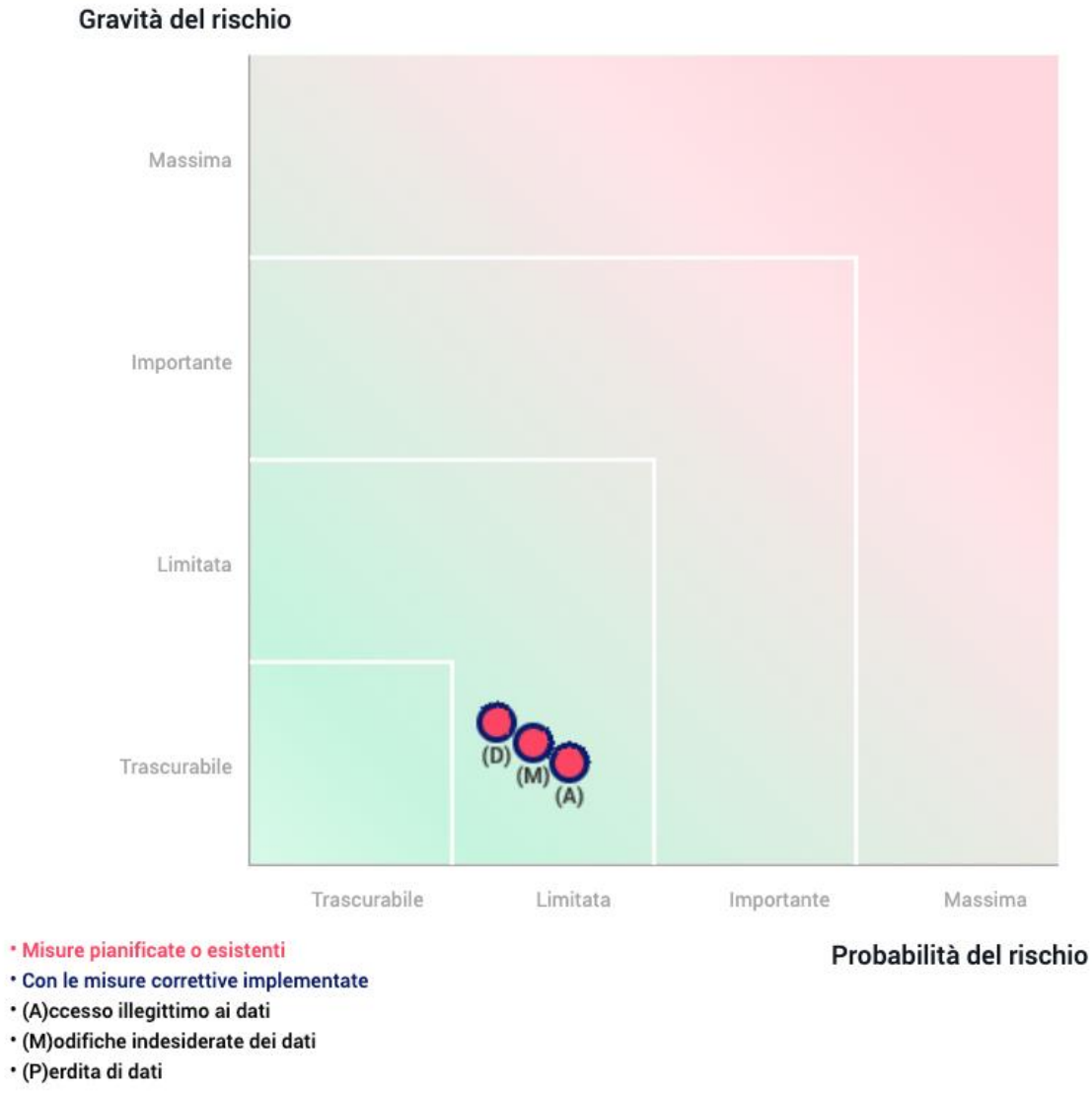
Istituto Comprensivo "don Lorenzo Milani"
Via Pietro Mascagni – 20871 Vimercate (MI)
Tel. 039/667522
c.f. 87004970155 – codice univoco UFJXIC
e-mail:mbic8ex001@istruzione.it -mbic8ex001@pec.istruzione.it
www.icsdonmilanivimercate.edu.it
M.I.

DPIA relativa all'utilizzo di Google Workspace in ambiente scolastico

Dati riassuntivi della DPIA

Mappa dei rischi



Nome del DPO/RPD

NetSense S.r.l.

Posizione del DPO/RPD

Il trattamento può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

In conformità con le dichiarazioni del Garante per la protezione dei dati personali e del Ministero, l'uso di piattaforme didattiche online come Google Workspace for Education e simili non richiede la redazione di alcuna valutazione dell'impatto sulla protezione dei dati, *a condizione che vengano attivati solamente i servizi indispensabili per l'istruzione*. Attraverso l'utilizzo di tali piattaforme per servizi didattici essenziali, infatti, l'Istituto non effettua trattamenti su vasta scala di dati personali o il monitoraggio sistematico degli utenti.
Tuttavia, in virtù della novità nell'impiego delle piattaforme di apprendimento *online* nel contesto educativo e delle possibili minacce che ne possono derivare, l'istituto ha preso l'iniziativa di implementare questa valutazione di impatto sulla protezione dei dati (DPIA) e altri documenti quali regolamenti, comunicazioni e procedure operative. Tali documenti sono stati elaborati per definire le misure tecniche e organizzative atte a ridurre al minimo i potenziali rischi per le informazioni personali dei soggetti coinvolti.

Contesto

Panoramica del trattamento

Qual è il trattamento in considerazione?

Nell'attuale contesto educativo in continua evoluzione, in cui l'integrazione delle tecnologie digitali sta rivoluzionando l'approccio tradizionale all'insegnamento e all'apprendimento, è imperativo che le istituzioni educative si adattino alle nuove sfide e alle opportunità presenti. L'integrazione di suite software nelle pratiche didattiche permette agli insegnanti di affrontare le necessità dell'apprendimento personalizzato, di preparare gli studenti per le competenze richieste nel XXI secolo e di creare una comunità di apprendimento interconnessa e dinamica.

In questo scenario, tra le diverse piattaforme disponibili, emerge Google Workspace for Education come una risorsa chiave per creare un ambiente di apprendimento innovativo, flessibile e collaborativo. Questo insieme di strumenti offre un assortimento completo di applicazioni specificamente progettate per le istituzioni scolastiche, consentendo agli educatori di sfruttare al massimo le potenzialità delle moderne tecnologie mediante l'utilizzo congiunto di mezzi di comunicazione, collaborazione e archiviazione.

L'approccio educativo nell'utilizzo di piattaforme online per l'istruzione, tra cui Google Workspace, implica che gli studenti accedano a processi di apprendimento tramite dispositivi informatici, compresi i loro dispositivi personali, come *tablet, smartphone* e computer connessi in rete. L'accesso a questi processi, mediante credenziali personali assegnate dagli istituti, è possibile sia in ambienti scolastici che domestici e coinvolge l'utilizzo di tecnologie online per condividere e collaborare, mirando a raggiungere obiettivi sia individuali che di gruppo.

Tuttavia, l'uso di metodi di condivisione e collaborazione basati su piattaforme *cloud* comporta potenziali rischi in relazione al trattamento dei dati personali degli studenti. Pertanto, risulta cruciale individuare piattaforme adeguate e stabilire linee guida per minimizzare il rischio di violazione della privacy degli studenti. La presente Valutazione dell'Impatto della Protezione dei Dati (DPIA) è condotta proprio per analizzare i rischi e le contromisure da implementare nell'impiego delle metodologie di insegnamento a distanza mediante l'utilizzo di strumenti digitali, in particolare il caso di Google Workspace for Education.

Quali sono le responsabilità connesse al trattamento?

Data la complessità delle azioni e delle potenziali conseguenze relative alle violazioni della *privacy,* è fondamentale stabilire una collaborazione attiva tra le diverse parti coinvolte. Queste parti includono:

1. **Il Titolare del Trattamento**: in questo caso, l'Amministrazione Scolastica rappresentata dal Dirigente Scolastico in carica. Il Dirigente assume un ruolo centrale di supervisione e guida nei confronti delle altre parti coinvolte. La sua responsabilità principale è garantire una gestione adeguata dei dati e dei sistemi informatici. A tal fine, sovrintende alla definizione e all'attuazione delle procedure, sviluppa un codice di condotta interno e vigila sull'osservanza delle regole.

2. **Responsabili del Trattamento ai sensi dell'art. 28 del GDPR**: in accordo con quanto previsto dall'articolo 28 del GDPR, il Titolare del Trattamento deve nominare responsabili esterni che tratteranno i dati personali per conto dell'Istituto. Questi soggetti, scelti tra quelli che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR e a garantire la tutela dei diritti dell'interessato, hanno la responsabilità di trattare i dati in modo sicuro e conforme alle disposizioni normative. Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati, la cui lista aggiornata può essere trovata sul sito dell'AGID. Nel caso in questione il Responsabile esterno è la Google LLC con sede in Mountain View in California (USA).

3. **I docenti**: essi svolgono un ruolo cruciale nell'assicurare il rispetto degli standard di sicurezza per la tutela dei dati personali degli studenti e della loro *privacy* nell'uso della piattaforma Google workspace. I docenti sono chiamati a gestire i materiali didattici, le comunicazioni e le interazioni online con la massima riservatezza e consapevolezza delle modalità di condivisione dei dati, degli strumenti di sicurezza forniti dalle applicazioni e delle pratiche che minimizzino il rischio di accessi non autorizzati. Inoltre, i docenti hanno la responsabilità di informare gli studenti sul corretto utilizzo delle piattaforme e di promuovere la consapevolezza sulla privacy digitale.

4. **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.

5. **Amministratori di sistema:** persone fisiche designate dal DS ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali (Dlgs 196/2003 e s..mm.ii.) quali soggetti che operano sotto la sua autorità a cui sono attribuiti specifici compiti e funzioni connessi al trattamento relativamente alla gestione dei sistemi informatici.

La collaborazione attiva tra queste parti è cruciale per garantire il rispetto delle normative sulla *privacy* e la protezione dei dati personali all'interno dell'ambiente scolastico. La designazione dei responsabili esterni e il coinvolgimento del Dirigente Scolastico nella supervisione e nell'attuazione delle procedure rappresentano passi fondamentali per gestire efficacemente la complessità delle sfide legate alla privacy nell'era digitale

Ci sono standard applicabili al trattamento?

Attualmente non sono stati individuati standard, certificazioni o codici di condotta pertinenti alla questione in esame. Di conseguenza, al fine di stabilire le misure tecniche ed organizzative da implementare per rispettare i principi del Regolamento, è essenziale far riferimento, oltre alle direttive stabilite dalla normativa vigente, anche alle seguenti linee guida:

- 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";* sono raccomandazioni emesse dallo European Data Protection Board (EDPD) che specificano i comportamenti da seguire riguardo al trasferimento di dati all'estero;

- Il *Provvedimento del Garante* per la protezione dei dati personali del 26 marzo 2020 - "Didattica a distanza: prime indicazioni".

- Le "*Linee Guida per la Didattica Digitale Integrata (DDI)",* emesse nell'estate 2020 dal Ministero dell'Istruzione; sono linee guida che forniscono indicazioni operative riguardo la dotazione, da parte degli istituti scolastici, di un Piano scolastico per la didattica digitale integrata da allegare al proprio Piano Triennale per l'Offerta Formativa. La circolare AGID n. 2 del 9 aprile 2018, che impone alle Pubbliche amministrazioni di avvalersi esclusivamente di servizi *cloud* abilitati (la lista aggiornata, disponibile sul sito dell'AGID, include tra i servizi SaaS qualificati anche la Google Workspace).

- Il documento *"Didattica Digitale Integrata e tutela della privacy: indicazioni generali"*, prodotto nel Settembre 2020 dal Ministero dell'Istruzione congiuntamente con l'ufficio del Garante per la protezione dei dati personali.

E' utile sottolineare che:

a) parte della sopracitata documentazione, pur essendo stata prodotta durante la situazione emergenziale da pandemia di *Covid-19*, assume caratteri del tutto generali e mantiene la sua valenza anche alla data di stesura del presente documento;

b) in conformità con le dichiarazioni del Garante per la protezione dei dati personali e del Ministero, l'uso di piattaforme didattiche online come Google Workspace e altre (non specificate in questo testo) non richiede la redazione di alcuna valutazione dell'impatto sulla protezione dei dati, come previsto dall'articolo 35 del *Regolamento Generale sulla Protezione dei Dati (GDPR*), a condizione che vengano attivati solamente i servizi indispensabili per l'istruzione. Attraverso l'utilizzo di tali piattaforme per i loro servizi didattici essenziali, infatti, l'Istituto non effettua trattamenti su vasta scala di dati personali o il monitoraggio sistematico degli utenti.

Malgrado ciò che è stato precedentemente evidenziato, in virtù della novità nell'impiego delle piattaforme di apprendimento *online* nel contesto educativo e delle possibili minacce che ne possono derivare, l'istituto ha preso l'iniziativa di implementare questa valutazione di impatto sulla protezione dei dati (DPIA) e di emanare altri documenti quali regolamenti, comunicazioni e procedure operative. Tali documenti sono stati elaborati per definire le misure tecniche e organizzative atte a ridurre al minimo i potenziali rischi per le informazioni personali dei soggetti coinvolti.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Le piattaforme online quali Google Workspace for Education consentono di svolgere attività didattiche caratterizzate da un alto grado di condivisione di informazioni e di collaborazione di gruppo. Queste piattaforme, spesso basate su tecnologie *cloud*, memorizzano di fatto dati identificativi degli studenti, degli insegnanti e di altri partecipanti, oltre a una vasta gamma di informazioni prodotte durante il loro lavoro; tutte informazioni che, a scelta dell'utente, possono essere condivise con altri utenti, specialmente durante la creazione di progetti collaborativi nell'ambito dell'istruzione.

Le informazioni presenti nelle piattaforme possono variare a seconda della materia didattica, ma potrebbero includere dati o informazioni sensibili che riguardano, ad esempio, l'orientamento politico, l'etnia o la salute degli interessati, spesso minori. È pertanto fondamentale sensibilizzare tutti gli utenti, sia gli studenti che gli insegnanti, sull'importanza di limitare al minimo indispensabile la presenza di dati sensibili e di applicare il principio della minimizzazione dei dati personali, inclusi quelli comuni.

Qual è il ciclo di vita del trattamento dei dati?

L'intero ciclo di vita dei dati attraversa diverse fasi, ciascuna delle quali comporta dei rischi potenziali. In particolare, gli studenti saranno registrati ai servizi di condivisione e organizzazione didattica tramite l'utilizzo di uno o più dispositivi di loro proprietà o forniti in comodato dalla scuola. Per quanto riguarda questa piattaforma specifica, la scuola si occuperà di creare gli *account* per docenti e studenti, che verranno utilizzati per le attività didattiche.

Durante le attività didattiche, questi servizi verranno utilizzati per stimolare la produttività dello studente, attraverso l'assegnazione di compiti ed obiettivi da raggiungere talvolta anche in gruppo.

Tutto il materiale didattico prodotto verrà archiviato su server cloud e condiviso tra i membri del team. In qualsiasi momento i docenti interessati potranno archiviarlo per accedervi eventualmente anche in un secondo momento.

È importante notare che, in conformità con la normativa in vigore e in situazioni di ordinaria frequenza scolastica, i sistemi di eLearning non possono essere utilizzati per esprimere valutazioni sull'operato degli studenti. Di conseguenza, a differenza del periodo di emergenza durante la pandemia di *Covid-19*, i documenti ottenuti non costituiscono atti amministrativi. Questo semplifica il processo di eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati.

Quali sono le risorse di supporto ai dati?

Di solito, si utilizzano servizi basati su *cloud* per agevolare la condivisione e l'organizzazione dei compiti assegnati. Queste tecnologie possono, in alcune occasioni, fare affidamento su server situati al di fuori dell'Unione Europea, ed è di fondamentale importanza verificare che rispettino la normativa europea in materia di gestione dei dati.

Gli utenti accedono a tali servizi utilizzando una vasta gamma di dispositivi informatici, tra cui tablet, computer e smartphone, che possono a loro volta essere basati su diversi sistemi operativi e consentire l'accesso ai servizi tramite vari browser o applicazioni.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici, espliciti e legittimi in quanto l'impiego di approcci didattici innovativi, spesso basati sull'utilizzo di sistemi online, sono necessari a promuovere una comprensione consapevole delle tecnologie digitali e a potenziare la capacità critica nell'uso delle fonti informative da parte degli studenti. L'obiettivo principale consiste nell'istruire gli studenti, con l'effetto collaterale di migliorare la loro competenza nell'uso delle moderne tecnologie e dell'attrezzatura digitale. La base giuridica sulla quale si opera il trattamento è indicata nel prossimo paragrafo del presente documento.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica per il trattamento in esame risiede nella lettera e) del Regolamento EU 679/2016 (GDPR) "trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", ai sensi di quanto specificato dal codice privacy italiano all'art. 2-ter. Nello specifico, la norma a cui si fa riferimento nasce dal Piano nazionale per la scuola digitale (PNSD), il principale strumento di programmazione del processo di trasformazione digitale della scuola italiana, introdotto dall'articolo 1, commi 56-59, della legge 13 luglio 2015, n. 107. Il Piano in vigore è stato adottato con decreto del Ministro dell'istruzione, dell'università e della ricerca 27 ottobre 2016, n. 851. Esso si compone complessivamente di 35 azioni, suddivise in tre ambiti di intervento:

- Connettività: azioni per garantire l'accesso alla rete Internet da parte di tutte le istituzioni scolastiche, degli studenti e del personale scolastico
- Ambienti e Strumenti: azioni finalizzate a dotare le istituzioni scolastiche di ambienti di apprendimento innovativi, basati sull'utilizzo delle tecnologie digitali
- Competenze e Contenuti: azioni destinate a promuovere e potenziare le competenze digitali degli studenti e a favorire lo sviluppo di contenuti di qualità per la didattica digitale
- Formazione e accompagnamento: azioni destinate a supportare l'innovazione didattica e digitale attraverso percorsi di accompagnamento alle istituzioni scolastiche e di formazione per il personale scolastico.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti vengono mantenuti in linea con i principi di adeguatezza, rilevanza e limitazione, garantendo che siano raccolti solo i dati necessari per gli scopi specifici del trattamento. In particolare:

- Per quanto riguarda gli account utente, vengono registrati solo il nome e il cognome dell'utente come informazioni di identificazione
- Secondo il principio di privacy-by-design, l'uso dell'autenticazione a due fattori viene evitato, per cui non sono necessari il numero di cellulare, l'indirizzo email personale o dispositivi personali per accedere al sistema
- Gli insegnanti ricevono istruzioni specifiche su come raccogliere la quantità minima di dati personali necessaria per svolgere le loro funzioni nel contesto della produzione di materiale didattico. In particolare, vengono applicate restrizioni rigorose quando si tratta di dati sensibili, assicurandosi di raccoglierne solo quelli strettamente indispensabili.

I dati sono esatti e aggiornati?

L'Amministratore designato dal Dirigente Scolastico, conformemente all'Articolo 2-quaterdecies del *Codice privacy* italiano, è responsabile di assicurare che i dati identificativi degli *account* degli studenti e dei docenti nella piattaforma Google Workspace for Education siano accurati e aggiornati. Questa aggiornamento può avvenire anche in risposta a segnalazioni da parte degli utenti stessi.

La procedura di raccolta e conservazione dei dati nei materiali didattici spesso coinvolge una collaborazione nella loro creazione. Pertanto, potrebbe verificarsi il caso in cui uno degli autori apporti modifiche intenzionali durante il processo di creazione. In tali situazioni, è possibile fare affidamento su strumenti che tengono traccia delle modifiche apportate alla documentazione, come backup e cronologia delle modifiche.

Qual è il periodo di conservazione dei dati?

La conservazione dei dati è limitata al periodo strettamente necessario per condurre le attività formative. Ai sensi della normativa vigente, i sistemi online possono essere utilizzati solo come strumenti di supporto alla didattica, che non può essere svolta a distanza. Per questo motivo, i dati o i materiali creati, poiché non sono considerati documenti amministrativi, possono essere eliminati al termine delle attività formative.

Di solito, questi dati vengono cancellati alla fine dell'anno scolastico, a meno che l'attività programmata si svolga su più anni scolastici e richieda un qualche tipo di trattamento sui dati raccolti negli anni precedenti.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

All'inizio dell'anno scolastico, gli interessati vengono informati del trattamento dei dati attraverso la presentazione di una apposita informativa redatta in conformità all'Articolo 13 del Regolamento UE 2016/679. Tale informativa viene resa disponibile agli studenti e ai loro genitori mediante un utilizzo il più ampio possibile dei mezzi di comunicazione a disposizione della scuola, che comprendono, a titolo esemplificativo, ma non esaustivo:

- La pubblicazione sulla sezione privacy del sito WEB
- La divulgazione di una circolare
- La messa a disposizione durante le fasi di iscrizione e in tutte le fasi di compilazione della documentazione amministrativa propedeutia all'inizio dell'anno scolastico.
- L'utilizzo delle modalità di comunicazione tra scuola e famiglia rese disponibili tramite il registro elettronico.

L'informativa contiene una sezione che istruisce gli interessati sui diritti di accesso, correzione e cancellazione, fornendo informazioni preventive sui tempi necessari per il trattamento dei dati.

Gli interessati ricevono informazioni sulle finalità didattiche alla base del trattamento dei dati e sui potenziali rischi associati. Docenti, studenti e famiglie ricevono le istruzioni e le conoscenze necessarie per un utilizzo responsabile degli strumenti, compresa la protezione dei dati personali propri e di altri.

Ove applicabile: come si ottiene il consenso degli interessati?

La base giuridica per il trattamento *non* è costituita dal consenso dell'interessato.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio di tali diritti.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati hanno la possibilità di contattare l'Amministrazione utilizzando il metodo di comunicazione di loro scelta per esercitare tali diritti.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati hanno la possibilità di contattare lAamministrazione utilizzando il metodo di comunicazione di loro scelta per esercitare tali diritti.

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

La selezione dei servizi utilizzati nelle scuole include la presenza di un contratto d'uso con i fornitori e la designazione di un Responsabile del trattamento, entrambi potenzialmente visualizzati e accettati in formato elettronico. Questi documenti delineano le rispettive responsabilità e dettagliano gli obblighi delle parti coinvolte.

Nel caso specifico di Google Workspace for Education i contenuti del contratto e dell'*addendum* per il rispetto dei principi del *Regolamento Europeo 679/2016* sono definiti con doverosa chiarezza.

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

I servizi offerti dalla Google Workspace for Education si basano sull'uso di server che possono anche essere localizzati nel territorio degli Stati Uniti d'America. Nel luglio 2023 la Commissione Europea ha emesso, in accordo con le autorità statunitensi, la decisione di adeguatezza denominata Data Privacy Framework, volta a tutelare i diritti dei cittadini europei garantendo un adeguato livello di protezione per i dati personali trasferiti dall'UE alle aziende statunitensi. Questo accordo ha cancellato gli effetti della sentenza C.311/18 (Schrems II) con la quale la Corte di Giustizia aveva dichiarato l'invalidità della precedente decisione di adeguatezza Privacy Shield.

Rischi

Misure esistenti o pianificate

Controllo e gestione degli *account* di accesso

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, designato dal Dirigente ai sensi dell'art. 2-quaterdecis del codice privacy italiano.

L'amministratore della piattaforma dovrà:

- definire i profili di autorizzazione nei sistemi separando le attività e le aree di responsabilità per limitare l'accesso degli utenti ai soli dati strettamente necessari per portare a termine i rispettivi compiti;

- rimuovere le autorizzazioni di accesso non appena un utente cessi di essere abilitato ad accedere a una risorsa locale o IT;

- realizzare una revisione annuale delle abilitazioni per identificare ed eliminare gli account non utilizzati e riallineare i privilegi concessi alle funzioni di ciascun utente.

Minimizzazione dei dati

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

Lotta contro il *malware*

I sistemi scolastici sono resi sicuri da minacce informatiche, tra cui il *malware*, grazie a un mix di protezioni hardware e software. Queste contengono l'utilizzo di firewall e programmi antivirus per scoprire e impedire possibili minacce informatiche. Inoltre, è fondamentale fornire agli utenti, che includono studenti, insegnanti e personale scolastico, linee guida per l'uso sicuro delle risorse elettroniche e digitali.

È importante notare che l'uso dei *software* strettamente necessari per l'istruzione forniti dalla suite Google Workspace for Education non comporta un rischio maggiore di infezione da *malware*.

Manutenzione dei sistemi hardware in uso a scuola

Viene effettuata regolarmente un'attività di manutenzione nei confronti dei sistemi *hardware* scolastici. Il responsabile del trattamento (Google stessa) garantisce inoltre il corretto funzionamento del *software cloud* di didattica da remoto.

Backup dei dati presenti nella piattaforma

La piattaforma Google Workspace for Education integra in maniera nativa i più moderni sistemi di replica e backup dei dati. E' importante comunque sottolineare che i dati ivi contenuti non sono vitali per l'attività didattica che, per legge, è sempre condotta in presenza.

Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati

I dati personali, a parte quelli identificativi dell'*account*, dovranno essere cancellati alla fine dell'anno scolastico.

Tracciabilità delle operazioni effettuate *online*

La piattaforma Google Workspace for Education integra in maniera nativa i più moderni sistemi di tracciabilità delle operazioni effettuate dagli utenti, nel rispetto della loro *privacy*: i *log* di tracciamento sono accessibili esclusivamente da parte dell'amministratore della piattaforma.

Continuo monitoraggio e risoluzione delle vulnerabilità del sistema

Il Responsabile del Trattamento, fornitore della piattaforma Google Workspace for Education, mantiene una vigilanza costante e opera in modo continuo per individuare e risolvere eventuali vulnerabilità che possono emergere nel tempo.

Contratto con il responsabile del trattamento

Google deve essere nominato responsabile del trattamento ai sensi dell'Art. 28 del *Reg. Ue 679/2016.* Ciò avviene tramite la stipula di un opportuno contratto tra le parti, sottoscritto in formato elettronico.

Politica di tutela della p*rivacy*: misure tecniche ed organizzative da adottare

Il Dirigente Scolastico ha messo in atto una serie di misure tecniche ed organizzative descritte nel regolamento di utilizzo della Google workspace. Egli ha inoltre istruito i docenti, sensibilizzato le famiglie verso il corretto utilizzo della piattaforma e ha nominato un Amministratore della piattaforma ai sensi dell'Art. 2-quaterdecies del *D.Lgs. 196/2003*.

Formazione specifica del personale e degli interessati

Il personale e gli alunni saranno informati e istruiti riguardo alle modalità di utilizzo dei *software*, così da limitare il rischio di comportamenti che possano comportare un rischio per sé e per gli altri.

Gestione *online* dei dispositivi mobili che hanno accesso alla piattaforma

L'approccio educativo nell'utilizzo di piattaforme *online* per l'istruzione, tra cui Google Workspace, implica che gli studenti accedano a processi di apprendimento tramite dispositivi informatici, compresi i loro dispositivi personali, come *tablet, smartphone e computer* connessi in rete. Con la gestione dei dispositivi mobili, è possibile applicare politiche di sicurezza a tutti i dispositivi che accedono a Google Workspace da remoto.

Per quanto riguarda i dispositivi concessi in comodato d'uso dall'istituto, questi dovranno essere dotati di antivirus, anti *malware* e *software firewall* e devono essere costantemente manutenuti da personale specializzato.

Sicurezza dei canali informatici

Di seguito alcune misure di sicurezza associate ai canali informatici di Google Workspace for Education che l'istituto ha preso in esame per la stesura della presente DPIA:

Crittografia: Google Workspace utilizza crittografia per proteggere i dati in transito. Questo significa che le informazioni vengono criptate durante la trasmissione per impedire a terzi non autorizzati di accedervi.

Autenticazione a Due Fattori (2FA): L'abilitazione dell'autenticazione a due fattori, sebbene renda più difficile l'accesso non autorizzato richiedendo un secondo passaggio di verifica oltre alle credenziali di accesso standard, non viene implementata per i motivi esposti nei paragrafi precedenti.

Protezione *Anti-Phishing*: Google Workspace include filtri *anti-phishing* per rilevare e bloccare tentativi di *phishing* e di attacchi di *spear-phishing.*

Firewall e Protezione Antivirus: L'uso di firewall e software antivirus aiuta a proteggere da *malware* e minacce online.

Sicurezza dell'*hardware*

Con la gestione dei dispositivi mobili integrata nella piattaforma, è possibile applicare politiche di sicurezza ai dispositivi che accedono a Google Workspace for Education da remoto.

Gestione degli incidenti di sicurezza e delle 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.

Rischi

Accesso illegittimo ai dati

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

Violazione della *Privacy*: gli interessati potrebbero vedere le proprie informazioni personali e sensibili esposte a terzi non autorizzati, il che potrebbe violare la loro *privacy*. Perdita di Dati Sensibili: Il rischio di perdere dati sensibili o di proprietà potrebbe avere conseguenze finanziarie o legali per gli interessati.
Violazione dei Regolamenti sulla Protezione dei Dati: un accesso illegittimo potrebbe portare a una violazione delle leggi sulla protezione dei dati, con possibili conseguenze legali o sanzioni.
Danno alla Reputazione: una violazione della sicurezza potrebbe danneggiare la reputazione degli interessati, sia a livello personale che professionale.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Phishing: gli attaccanti possono utilizzare messaggi di *phishing p*er indurre gli utenti a condividere le proprie credenziali, consentendo loro di accedere in modo fraudolento ai dati.
Violazione delle Credenziali: le credenziali degli utenti, come password o chiavi di accesso, possono essere compromesse o rubate, consentendo l'accesso non autorizzato.
Attacchi di Forza Bruta: gli attaccanti possono tentare di indovinare le *password* degli *account* utilizzando attacchi di forza bruta o dizionario.
Vulnerabilità del *Software*: le vulnerabilità nel software utilizzato per l'accesso a Google Workspace for Education possono essere sfruttate per ottenere accesso non autorizzato.
Accesso Fisico Non Autorizzato: qualcuno potrebbe ottenere fisicamente un dispositivo utilizzato per accedere a Google Workspace e accedere ai dati.
Accesso a Causa di Errori Umani: gli errori umani, come la configurazione errata delle autorizzazioni, possono aprire la porta ad accessi non autorizzati.
Attacchi Mirati (*Spear Phishing*): gli attaccanti possono condurre attacchi mirati a specifici utenti o organizzazioni, cercando di ottenere le loro credenziali.
Malware: l'installazione di *malware* nei dispositivi degli utenti può consentire agli attaccanti di monitorare le attività e ottenere l'accesso ai dati.
Accesso da Dispositivi Smarriti o Rubati: se dispositivi contenenti l'accesso a Google Workspace vengono smarriti o rubati, ciò potrebbe portare all'accesso non autorizzato ai dati.
Accesso da Parte di Ex Dipendenti o Utenti Autorizzati: ex dipendenti o utenti con accesso precedentemente autorizzato potrebbero utilizzare le loro credenziali per accedere illegittimamente ai dati.

Quali sono le fonti di rischio?

Phishing: gli attaccanti possono utilizzare messaggi di *phishing* per indurre gli utenti a condividere le proprie credenziali, consentendo loro di accedere in modo fraudolento ai dati.
Violazione delle Credenziali: le credenziali degli utenti, come password o chiavi di accesso, possono essere compromesse o rubate, consentendo l'accesso non autorizzato.
Attacchi di Forza Bruta: gli attaccanti possono tentare di indovinare le password degli account utilizzando attacchi di forza bruta o dizionario.
Vulnerabilità del Software: le vulnerabilità nel software utilizzato per l'accesso a Google Workspace for Education possono essere sfruttate per ottenere accesso non autorizzato.
Accesso Fisico Non Autorizzato: qualcuno potrebbe ottenere fisicamente un dispositivo utilizzato per accedere a Google Workspace e accedere ai dati.
Accesso a Causa di Errori Umani: gli errori umani, come la configurazione errata delle autorizzazioni, possono aprire la porta a accessi non autorizzati.
Attacchi Mirati (Spear Phishing): gli attaccanti possono condurre attacchi mirati a specifici utenti o organizzazioni, cercando di ottenere le loro credenziali.
Malware: l'installazione di malware nei dispositivi degli utenti può consentire agli attaccanti di monitorare le attività e ottenere l'accesso ai dati.
Accesso da Dispositivi Smarriti o Rubati: se dispositivi contenenti l'accesso a Google Workspace vengono smarriti o rubati, ciò potrebbe portare all'accesso non autorizzato ai dati.
Formazione del personale carente.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo e gestione degli account di accesso, Minimizzazione dei dati, Lotta contro il *malware*, Manutenzione dei sistemi hardware in uso a scuola, Backup dei dati presenti nella piattaforma, Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati, Tracciabilità delle operazioni effettuate *online,* Continuo monitoraggio e risoluzione delle vulnerabilità del sistema, Contratto con il responsabile del trattamento.
Politica di tutela della *privacy*: Misure tecniche ed organizzative da adottare, Formazione specifica del personale e degli interessati, Gestione online dei dispositivi mobili che hanno accesso alla piattaforma, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestione degli incidenti di sicurezza e delle violazioni dei dati personali.

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

Trascurabile. Le misure di sicurezza implementate e la limitazione dei dati personali a quelli strettamente necessari per le attività didattiche riducono significativamente la gravità dei potenziali rischi.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata. L'implementazione di sistemi di vigilanza interna e l'applicazione del regolamento di istituto, insieme a iniziative di formazione e sensibilizzazione degli utenti, possono contribuire a ridurre le violazioni con conseguenze significative.

La probabilità di una violazione ai sistemi di sicurezza del Responsabile del Trattamento (Google) è considerata trascurabile.

La probabilità di accesso da parte delle autorità governative statunitensi alle informazioni archiviate su server al di fuori dell'Europa è considerata trascurabile.

Il Dirigente Scolastico

Dott.ssa Mariateresa Chieli

documento firmato digitalmente

Vimercate, 17 Aprile 2024

Firmato da:
DIRIGENTE SCOLASTICO
Dott.ssa MARIATERESA CHIELI
17/04/2024 13:03:58