Valutazione di Impatto (DPIA)
“Google Workspace for Education Fundamentals”

Sommario

Autore : DS dell'istituto scolastico

DPO: Ing. Roberto Doria di Archè Srl – dpo.arche@arche-va.it

Introduzione

Questo documento è una valutazione dell'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) dell'Istituto in intestazione. La DPIA è un'analisi delle attività di trattamento previste e descrive i dettagli delle attività di trattamento sottoposte ad analisi ed una valutazione dei rischi associati alle stesse, comprese eventuali misure che devono essere adottate per mitigare tali rischi entro limiti accettabili.
Questa DPIA viene eseguita in accordo al requisito riportato nell'Art. 35 del Regolamento Europeo UE 2016/679, che prevede che, nel caso in cui un trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento debba effettuare una valutazione di impatto del trattamento previsto, al fine di procedere o meno con l'effettuazione dello stesso. Nel caso di rischi "residui" elevati dopo l'adozione delle misure volte a mitigare gli stessi, il Titolare è tenuto a comunicare all'Autorità Garante della Privacy l'esito di tali valutazioni e, prima di procedere con l'effettuazione delle stesse, attendere il riscontro dell'Autorità Garante.

Contesto - Panoramica del trattamento

Quale è il trattamento in considerazione?

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

Google Workspace for Education Fundamentals (precedentemente Google Suite for Education) è un pacchetto di applicazioni che consente di interagire secondo modalità collaborative anche a distanza, a beneficio della didattica. In particolare:

- Google Classroom è un servizio che consente agli insegnanti di creare una classe virtuale per gestire la comunicazione, i materiali, i compiti e le scadenze con gli studenti, direttamente online.
- Google Drive è un servizio che consente di creare, archiviare, condividere e modificare documenti direttamente online, anche in modalità collaborativa e senza necessità che sul proprio computer sia installato alcun programma, semplicemente accedendo tramite il proprio account.
- Google Meet è un'applicazione di teleconferenza che permette di svolgere lezioni e riunioni da remoto.

Per poter utilizzare queste applicazioni ad ogni studente sarà assegnata una casella di posta Gmail con un indirizzo composto dal proprio cognome e nome seguito dal nome del dominio della scuola. Gli studenti potranno utilizzare le credenziali della casella di posta assegnata per accedere alla piattaforma di e-learningdi istituto e alle numerose applicazioni web utili per la didattica.
Google Workspace for Education Fundamentals (che ha sostituito G Suite for Education) costituisce un

insieme di strumenti flessibili e di facile utilizzo per l'apprendimento, la collaborazione (Classroom) e la comunicazione (Gmail e Google Meet). Questa suite permette all'Istituto di usufruire di strumenti didattici ormai praticamente essenziali.

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento, in questo caso l'Amministrazione Scolastica, rappresentata legalmente dal Dirigente Scolastico (D.S.), che assume un ruolo centrale di supervisione e guida nei confronti dell'operato dei docenti. Inoltre, è compito del D.S. quello di definire un codice di condotta interno alla scuola che regoli l'utilizzo della strumentazione elettronica utilizzata, e di sorvegliare sulla sua attuazione. Il Titolare deve inoltre nominare i responsabili esterni che trattano dati personali per conto dell'Istituto ai sensi dell'art. 28, comma 3 del GDPR.

I Docenti. Il loro ruolo centrale nella produzione di compiti e contenuti deve essere associato ad un loro controllo nei confronti di tutte quelle attività suscettibili di violazioni della privacy. I docenti sono responsabilidella documentazione accessibile ai gruppi di lavoro e vigilano sul corretto svolgimento delle operazioni. A tal fine, il Titolare si impegna ad attribuire ai docenti il compito di supervisione sulle attività didattiche su piattaforma informatica e a fornire agli stessi indicazioni sulle modalità più opportune con cui trattare i dati personali, ai fini dell'art. 2-quaterdecies del D.Lgs. 196/2003 e dell'art. 4 del Regolamento UE 2016/679.

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.

Eventuali amministratori di sistema: nominati dal DS quali responsabili del trattamento relativamente alla gestione dei sistemi informatici, collaborano con il DPO e il DS nel fornire consulenze e pareri relativamenteallo stato delle risorse informatiche dell'amministrazione.

I responsabili del trattamento, quali i provider di servizi elettronici utilizzati per la didattica (eventualmente, BYOD) devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Particolare attenzione va posta nei confronti dei fornitori di servizi cloud, ove richiesti. In questo caso, è necessario prestare particolare attenzione alle loro policy sulla cessione dei dati a organismi terzi e all'eventuale salvataggio di dati su server extra-UE. Per questo motivo, sarà necessario effettuare una valutazione preventiva dei provider di servizi Cloud sulla base della loro compliance nei confronti della normativa in essere. Inoltre, sarà necessario procedere alla nomina formale dei fornitori di tali servizi quali responsabili del trattamento ai sensi dell'Art. 28, comma 3 del GDPR.

Google Workspace for Education si configura come un Responsabile Esterno del Trattamento. In virtù dell'accordo che deve essere sottoscritto dall'Istituto si riconosce la conformità degli strumenti proposti dato che con la caduta del Privacy Shield, ovvero lo “scudo per la privacy” fra UE e USA (meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall’Unione europea) l’utilizzo dei dati da parte delle aziende americane deve essere regolamentato da certificazioni e accordi particolari. Si riconosce pertanto che Google Workspace offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate perché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. 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. In proposito Workspace di Google Cloud Italy Srl risulta essere qualificata dal 27-11-2019 (attualmente da ACN dal 19-01-2023) nella tipologia SaaS per la categoria: Servizi per la fiscalità, Servizi demografici, Servizi interni alle PA con livello di qualificazione QC1 e identificazione scheda SA-690. Dal 19 gennaio 2023 la qualificazione dei servizi cloud per la Pubblica Amministrazione diventa di competenza dell'Agenzia per la Cybersicurezza Nazionale (ACN), che subentra all'Agenzia per l'Italia Digitale (AgID). La nuova procedura di qualificazione è indicata nel Decreto direttoriale prot. N. 29 del 02/01/2023. Per garantire la continuità dei servizi qualificati già in uso dalle amministrazioni (PA) e per consentire una graduale armonizzazione della normativa nazionale, il Decreto direttoriale prevede un regime transitorio prima della gestione ordinaria della qualificazione. Decreto direttoriale Prot. N. 5489 del 08/02/2023 per la transizione di infrastrutture e servizi digitali.

Ci sono standard applicabili al trattamento?

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

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Google Workspace for Education utilizza tecnologie cloud e deve quindi contenere le informazioni necessarie per identificare univocamente alunni, docenti ed eventuali altri soggetti interessati.
Per creare l'account l'Istituto fornirà nome, indirizzo email e la password dello studente. Quando uno studente utilizza i servizi di Google, quest'ultimo potrebbe raccogliere anche le informazioni basate sull'utilizzo di tali servizi, tra cui:

- informazioni sul dispositivo, ad esempio modello di hardware, versione del sistema operativo, identificatori univoci del dispositivo e informazioni relative alla rete mobile, incluso il numero di telefono (funzione disabilitata attraverso il pannello amministrativo dall'Istituto);
- informazioni di log, tra cui dettagli di come un utente ha utilizzato i servizi Google, informazioni sugli eventi del dispositivo e indirizzo IP (protocollo Internet) dell'utente (funzione disabilitata attraverso ilpannello amministrativo dall'Istituto);
- informazioni sulla posizione ricavate tramite varie tecnologie, tra cui l'indirizzo IP, GPS e altri sensori (funzione disabilitata attraverso il pannello amministrativo dall'Istituto);
- numeri specifici delle applicazioni, come il numero di versione dell'applicazione; infine cookie o tecnologie analoghe utilizzate per acquisire e memorizzare le informazioni relative a un browser o dispositivo, come la lingua preferita e altre impostazioni.

Le attività didattiche sono quindi svolte tramite una o più piattaforme elettroniche che facilitano la condivisione dei dati e l'organizzazione del lavoro di gruppo. Tali piattaforme, che spesso fanno utilizzo di tecnologie cloud, si troveranno quindi a contenere, oltre alle informazioni necessarie per identificare univocamente alunni, docenti ed eventuali altri interessati, tutta una serie di dati e informazioni da essi prodotti, che per lo più potrebbero essere condivisi tra diverse parti in causa, specialmente durante la loro stesura nel caso di progetti di didattica cooperativa. Tali informazioni dipenderanno ovviamente dalla natura e materia didattica svolte, ma potrebbero contenere dati o informazioni ad alto rischio per la privacy degli interessati. A titolo di esempio, potrebbero contenere degli scritti che definiscono

esplicitamente l'orientamento politico, la razza o la condizione sanitaria degli interessati, che potrebbero essere di minore età. Tutti i soggetti devono quindi essere sensibilizzati perchè sia limitata la presenza di dati particolari, siano minimizzati i dati personali e sia evidenziato che i dati presenti nella piattaforma potranno essere oggetto di valutazione scolastica.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Gli account Google Workspace for Education vengono creati e gestiti dall'Istituto Scolastico e destinati all'utilizzo da parte di studenti e docenti per lo svolgimento dell'attività didattica. Saranno mantenuti attivi per la durata del corso di studi dell'alunno/a o nel caso dei docenti per la durata del rapporto di dipendenza/servizio.

Durante l'anno scolastico i servizi forniti da Google Workspace saranno utilizzati per svolgere le attività didattiche e affidare agli studenti esercitazioni e verifiche, che possono comportare la produzione di materiali/documenti/registrazioni contenenti dati personali. Tale materiale verrà conservato su server cloud e condiviso tra i vari membri della classe e/o del gruppo di lavoro. Alla fine della produzione dello stesso, si potrà procedere all'archiviazione del materiale da parte dei docenti interessati, che lo utilizzeranno anche per esprimere le loro valutazioni. Pertanto, la documentazione ottenuta si profila quale atto amministrativoendoprocedimentale e sarà compito del docente procedere all'archiviazione dei documenti nel momento incui 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 istituzionali 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 (comunque la conservazione dei documenti sul cloud non supera l'anno scolastico, i dati in questione vengono scaricati e mantenuti all'interno della struttura scolastica).

Quali sono le risorse di supporto ai dati?

Solitamente ci si avvale di servizi in cloud che permettono la condivisione e organizzazione dei compiti assegnati. Tali tecnologie possono, talvolta, basarsi su server extra-ue, e in tal caso è importante verificarne la compliance alla normativa europea sul trattamento dei dati. A causa delle qualità cross-Platform di questi servizi, essi vengono fruiti dagli interessati tramite una grande varietà di strumentazione informatica che può comprendere tablet, pc e smartphone, che a loro volta possono essere basati su diversi sistemi operativi e permettere la fruizione dei servizi tramite diversi browser o app.

Principi Fondamentali Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento prevede l'utilizzo di tecniche didattiche innovative atte allo svolgimento dell'insegnamento scolastico in modalità remota e a sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione degli studenti. Lo scopo ultimo è quello di formare gli studenti, con l'effetto collaterale di aumentarne la consapevolezza nell'uso delle tecnologie moderne e nell'utilizzo di strumentazione digitale. I dati personali relativi alle attività didattiche possono portare ad una valutazione degli studenti stessi da parte dei docenti e sono quindi suscettibili di diventare atti amministrativi scolastici.
Il Piano scolastico per la didattica digitale integrata deve essere approvato dal Collegio Docenti e indicare criteri e modalità di erogazione dell'attività scolastica, in modo integrato tra la consueta attività didattica in presenza e le attività didattiche a distanza, anche attraverso l'utilizzo degli strumenti digitali e in particolaredi Google Workspace for Education.

Quali sono le basi legali che rendono lecito il trattamento?

Come chiarito dal Garante nel Provvedimento del 26 marzo 2020, n. 64 (doc web n. 9300784 "Didattica a distanza: prime indicazioni"), in relazione alla attività di DDI, il trattamento dei dati personali da parte delle istituzioni scolastiche è necessario in quanto collegato all'esecuzione di un compito di interesse pubblico di cui è investita la scuola attraverso una modalità operativa prevista dalla normativa, con particolare riguardoanche alla gestione della fase di emergenza epidemiologica.
Il consenso dei genitori o degli alunni maggiorenni, che non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro, non è richiesto perché l'attività svolta rientra tra le attività istituzionalmente assegnate all'istituzione scolastica, ovvero di didattica nell'ambito degli ordinamenti scolastici vigenti. Pertanto, l'Istituto è legittimato a trattare tutti i datipersonali necessari al perseguimento delle finalità collegate allo svolgimento della DDI nel rispetto dei principi previsti dalla normativa di settore. In base alle disposizioni contenute negli artt. 13 e 14 del Regolamento UE 2016/679, l'Istituto si preoccupa di informare gli interessati in merito ai trattamenti dei datipersonali effettuati nell'ambito dell'erogazione dell'offerta formativa. Poiché attraverso l'utilizzo della piattaforma per l'erogazione della DDI sono trattati sia dati degli studenti che dei docenti e, in taluni casi, anche dei genitori, la Scuola fornisce a tutte queste categorie di interessati, di regola all'inizio dell'anno scolastico, anche nell'ambito di una specifica sezione dell'informativa generale o in un documento autonomo, tutte le informazioni relative a tali trattamenti.
E' bene ricordare che alla luce del D.L. 101 del 10 agosto 2018 (art. 2 - quinquies), l'età dalla quale il minore "può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione" è stata fissata a 14 anni.

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

La segreteria dell'Istituto crea gli account Google utilizzando i dati minimi necessari e si occupa della loro eliminazione al termine del ciclo di studi o del contratto di servizio per quanto riguarda i dipendenti.

L'Istituto deve predisporre le proprie informative in materia di trattamento dati personali e dare evidenza di quelle di Google Workspace per poter sensibilizzare al massimo gli interessati in merito alla pubblicazione econdivisione di dati personali. Tutti i soggetti coinvolti nell'attività didattica sono tenuti al rispetto del Pianoscolastico per la DDI e al Regolamento.
I docenti sono invitati a raccogliere (e archiviare) la quantità minima di dati personali necessaria al corretto svolgimento delle loro funzioni. Particolari restrizioni dovranno essere adottate per i dati sensibili che dovranno limitarsi a quelli strettamente necessari. Ciò nonostante, è importante far notare come un corretto giudizio sul processo formativo degli studenti passi attraverso l'attenta valutazione dell'intero processo formativo dello studente, e non soltanto dell'elaborato ottenuto nella sua fase finale. Per questo motivo, tutte le informazioni legate al processo formativo possono essere considerate pertinenti ai fini della valutazione e quindi oggetto del trattamento.

I dati sono esatti e aggiornati?

La segreteria dell'Istituto garantisce massima attenzione nel caricamento dei dati di studenti e docenti.
I dati personali contenuti nel materiale prodotto durante l'attività didattica corrispondono a quanto caricato dagli interessati, fatte salve modifiche, volute o accidentali, intervenute nei processi di collaborazione o condivisione dei documenti. Una volta terminati, gli elaborati delle prove scritte, grafiche e pratiche possono essere considerati documentazione amministrativa oggetto di valutazione scolastica. Per questo motivo, essi non possono essere modificati o cancellati neppure su richiesta degli interessati per il periodo prescritto dalla legge e comunque funzionale alla corretta valutazione da parte dei docenti e del consiglio di classe.

Qual è il periodo di conservazione dei dati?

I dati utilizzati per la creazione dell'account sono conservati per la durata del corso di studi nel caso degli alunni e per la durata del contratto di servizio/dipendenza nel caso dei docenti.

La conservazione dei dati relativi all'attività didattica è necessaria per un periodo strettamente necessario allo svolgimento dell'attività formativa. I dati verranno poi archiviati dal docente, 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 prescrivela conservazione di documentazione campione un anno ogni dieci. 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: i dati verranno scaricati e conservati presso la struttura scolastica con le stesse modalità della didattica tradizionale.

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 deve essere somministrata a docenti, alunni e genitori degli stessi tramite registro elettronico o altra modalità ritenuta idonea.
L'Istituto da massima evidenza tramite pubblicazione sul proprio sito istituzionale (eventualmente in una sezione dedicata) anche delle informative prodotte da Google in merito ai prodotti/servizi adottati, del Pianoscolastico e del Regolamento di Didattica Digitale Integrata.
Gli interessati devono venire informati delle finalità didattiche su cui il trattamento si basa e sui possibili rischi associati. E' poi importante che ai docenti ed agli studenti vengano fornite le istruzioni e le conoscenze necessarie ad un utilizzo consapevole della strumentazione, ivi compresa la protezione dei dati personali propri e altrui. L'informativa dovrà inoltre contenere un riferimento alla policy scolastica sull'utilizzo delle strumentazioni elettroniche, nella quale devono essere ben definite le responsabilità delle parti in causa. Nella policy dovrà essere chiaro che si potranno utilizzare, a scopi didattici, solamente quei servizi considerati "sicuri", per i quali il titolare provvederà a nominare i responsabili del trattamento. Inoltre, sarà necessario rendere edotti gli interessati sui diritti di accesso, rettifica e cancellazione, ponendo preventivamente attenzione sui tempi necessari al trattamento dei dati. Particolare attenzione dovrà essere posta sul fatto che, una volta prodotti, i dati non potranno essere cancellati per un anno, in quanto atti amministrativi (o che verranno utilizzati a scopo di archivio, qualora la situazione lo preveda)

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non costituisce una base giuridica idonea per il trattamento dei dati e quindi non è richiesto perché l'attività didattica svolta, sia pure in ambiente virtuale, rientra tra le finalità istituzionali della Scuola.

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

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa o all'amministrazione, tramite la modalità da loro preferita, per l'esercizio dei propri diritti

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

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa o all'amministrazione, tramite la modalità da loro preferita, per l'esercizio dei propri diritti

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

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa o all'amministrazione, tramite la modalità da loro preferita, per l'esercizio dei propri diritti

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

contratto?

Google Workspace si configura come un Responsabile Esterno del Trattamento in virtù dell'accordo che deve essere sottoscritto dall'Istituto. Si riconosce la conformità degli strumenti proposti dato che con la caduta del Privacy Shield, ovvero lo "scudo per la privacy" fra UE e USA (meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea) l'utilizzo dei dati da parte delle aziende americane deve essere regolamentato da certificazioni e accordi particolari. Si riconosce pertanto che Google Workspace offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate perché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Il contratto d'uso di Google Workspace, visualizzato e accettato in forma elettronica, descrive l'ambito dellerispettive responsabilità e specifica gli obblighi per le parti.

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

I servizi previsti si basano sull'uso di server che possono anche essere localizzati in territori extra Unione Europea. Questo fatto ha delle criticità in relazione alla sentenza C.311/18 (Schrems II) con la quale la Corte di Giustizia ha dichiarato l'invalidità della decisione di adeguatezza Privacy Shield e che ha indotto Google stessa ad individuare nelle clausole contrattuali standard la base legale del trattamento. Cadendo quindi la valutazione di conformità a priori garantita dal Privacy Schield l'Istituto è consapevole che deve verificare che le clausole contrattuali costituiscano una garanzia sufficiente per la tipologia di dati trattati. Dall'analisi condotta, riteniamo di poter affermare che il livello di protezione garantito è adeguato alla tipologia dei datitrattati limitata a quelli strettamente necessari al perseguimento delle finalità didattiche.
Si precisa che a seguito della sentenza Schrems II, intervenuta a luglio del 2020, l'Istituto scolastico ha valutato le possibili alternative all'uso della piattaforma Google G Suite (oggi Workspace for Education Fundamentals) adottata per garantire la didattica in periodo emergenziale in attuazione del dpcm dell'8 marzo 2020. Le possibilità attualmente disponibili però non permettono di garantire gli stessi servizi (creazione di caselle mail illimitate, drive illimitato, ecc.) offerti da Google Worspace for Education Fundamentals alle stesse condizioni economiche.

Rischi: Misure esistenti o pianificate

Crittografia

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

Controllo degli accessi logici

Consiste nel limitare i rischi di accesso di persone non autorizzate ai dati personali in forma digitale. L'accesso alle funzionalità della piattaforma utilizzata 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

Politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario. 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 anche pseudominimizzati, quando possibile, per quanto previsto dalla normativa vigente. I dati sensibili devono essere limitati a quelli strettamente necessari.

Lotta contro il malware

Misure volte a proteggere l'accesso a reti pubbliche (Internet) o non controllate (di partner) nonché postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati personali Il sistema scolastico è protetto da malware con modalità di protezione sia hardware che software (firewall e antivirus). Si ritiene opportuno fornire agli utilizzatori (docenti e alunni) delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Backup

Esistenza di politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità I sistemi di didattica da remoto utilizzati per il trattamento devono essere provvisti di una modalità di backup.

Manutenzione

Viene effettuata regolare manutenzione dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento del software cloud di didattica da remoto.
Si ritiene opportuno fornire agli utilizzatori (docenti e alunni) delle linee guida sull'utilizzo sicuro delle risorseelettroniche e digitali.

Contratto con il responsabile del trattamento

I responsabili del trattamento devono essere nominati tali tramite la stipula di un contratto, ai sensi degli Artt. 28 e 29 del Reg. Ue 679/2016. Google Workspace for Education si configura come un Responsabile Esterno del Trattamento. In virtù dell'accordo che deve essere sottoscritto dall'Istituto si riconosce la conformità degli strumenti proposti dato che con la caduta del Privacy Shield, ovvero lo "scudo per la privacy" fra UE e USA (meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea) l'utilizzo dei dati da parte delle aziende americane deve essere regolamentato da certificazioni e accordi particolari. Si riconosce pertanto che Google Workspace offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate perché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

Politica di tutela della privacy

Esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno

della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio). L'Istituto, in collaborazione con il DPO, ha messo in atto una serie di misure orientate all'adeguamento dellastessa alla normativa vigente. I dipendenti sono stati autorizzati al trattamento ai sensi dell'Art. 2- quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Esistenza di un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.) 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

Gestione del personale – (Formazione specifica del personale e degli interessati)

Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite somministrazione di informativa ex Art. 13 del Reg. UE 206/679. L'informativa viene somministrata a docenti, alunni e genitori degli stessi tramite registro elettronico o altra modalità ritenuta idonea.
L'Istituto da massima evidenza tramite pubblicazione sul proprio sito istituzionale (eventualmente in una sezione dedicata) anche delle informative prodotte da Google in merito ai prodotti/servizi adottati, del Pianoscolastico e del Regolamento di Didattica Digitale Integrata. Il personale e gli alunni saranno istruiti riguardo alle modalità di utilizzo dei software, così da limitare il rischio di comportamenti che possano comportare un rischio per se e per gli altri.

Rischio - Accesso illegittimo ai dati

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

Furto d'identità, Reati informatici, Uso improprio di dati personali, Ripercussioni sulla Didattica, Violazione diNorma di Legge, Danno Reputazionale, Richieste di Risarcimento. Accesso a dati personali di minori con uso improprio degli stessi

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Mancata formazione, Sottovalutazione del Rischio, Comportamento negligente, Attività Fraudolenta, Accesso ai dati da parte di amministrazioni extra unione europea. Diffusione su piattaforme social dei dati personali acceduti, Scarsa sensibilità degli studenti alla privacy dei compagni. Queste ultime minacce sono da ricollegarsi anche a fenomeni di cyber bullismo.

Quali sono le fonti di rischio?

Virus informatici, Attacchi Hacker, Errore umano, Malfunzionamento, Incidente/sinistro, Interruzione alimentazione elettrica.

Un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.

Uno studente che voglia utilizzare le informazioni per mettere in atto episodi di bullismo.
Accesso di autorità governative statunitensi su server collocati su territorio extraeuropeo.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Minimizzazione dei dati, Politica di tutela della privacy, Lotta contro il malware, Controllo degli accessi logici, Backup, Archiviazione, Manutenzione, Gestione del personale, Contratto con il responsabile del trattamento, Gestire gli incidenti di sicurezza e le violazioni dei dati personali. In particolare, la proibizione dell'uso di dati personali non necessari all'attività formativa con particolare riferimento a quelli sensibili per i quali deve essere fatta una più rigorosa valutazione di stretta necessità.

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

Trascurabile, Trascurabile per quanto concerne il trattamento dati di docenti e alunni.
Limitata. Le misure di sicurezza adottate e la limitazione dei dati personali a quelli necessari allo svolgimento dell'attività didattica riducono sensibilmente la gravità dei rischi. La natura dei dati personali trattati consente di valutare come limitata anche la gravità del rischio associato all'accesso ai medesimi da parte delle autorità governative statunitensi su server collocati al di fuori del territorio europeo. Questa eventualità è stata quella che ha fatto decadere la valutazione di idoneità a priori costituita dal privacy shield, idoneità che nel presente documento viene valutata dal titolare in relazione ai trattamenti effettivamente effettuati.

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

Trascurabile, L'attivazione di sistemi di vigilanza interna e l'adozione e attuazione del regolamento, unito ad attività di sensibilizzazione possono essere in grado di limitare violazioni ad alto impatto.
Trascurabile la probabilità di accesso alle informazioni detenute su server extraeuropei da parte di autorità governative statunitensi.

Rischio - Modifiche indesiderate dei dati

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

Uso improprio di dati personali, Valutazioni Errate, Ripercussioni sulla Didattica, Danno Reputazionale

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Comportamento negligente, Mancata formazione, Sottovalutazione del Rischio, Accesso illecito ai dati e modifica degli stessi

Quali sono le fonti di rischio?

Errore umano, Malfunzionamento, Incidente/sinistro, Attacchi Hacker

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Minimizzazione dei dati, Backup, Gestione del personale, Politica di tutela della privacy, Controllo degli accessi logici

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

Limitata, Trascurabile per quanto concerne il trattamento dati di docenti e alunni. Sebbene la violazione potrebbe portare ad una errata valutazione dell'alunno, le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.
Limitato per quanto concerne i dati dell'utente amministratore della piattaforma.

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

Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda all'alienazione della disponibilità degli stessi agli studenti interessati, alla fine della fase di elaborazione concessagli.

Rischio - Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Ripercussioni sulla Didattica, Valutazioni Errate, Danno Reputazionale

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio? Sottovalutazione del Rischio, Mancata formazione, Comportamento negligente, Attività Fraudolenta, Distruzione dei server del servizio, Perdita dell'accesso ai documenti, errore umano

Quali sono le fonti di rischio?

Attacchi Hacker, Incidente/sinistro, Errore umano, Virus informatici, Malfunzionamento, Interruzione alimentazione elettrica

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Backup, Archiviazione, Crittografia, Minimizzazione dei dati, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Politica di tutela della privacy, Controllo degli accessi logici, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Gestione del personale

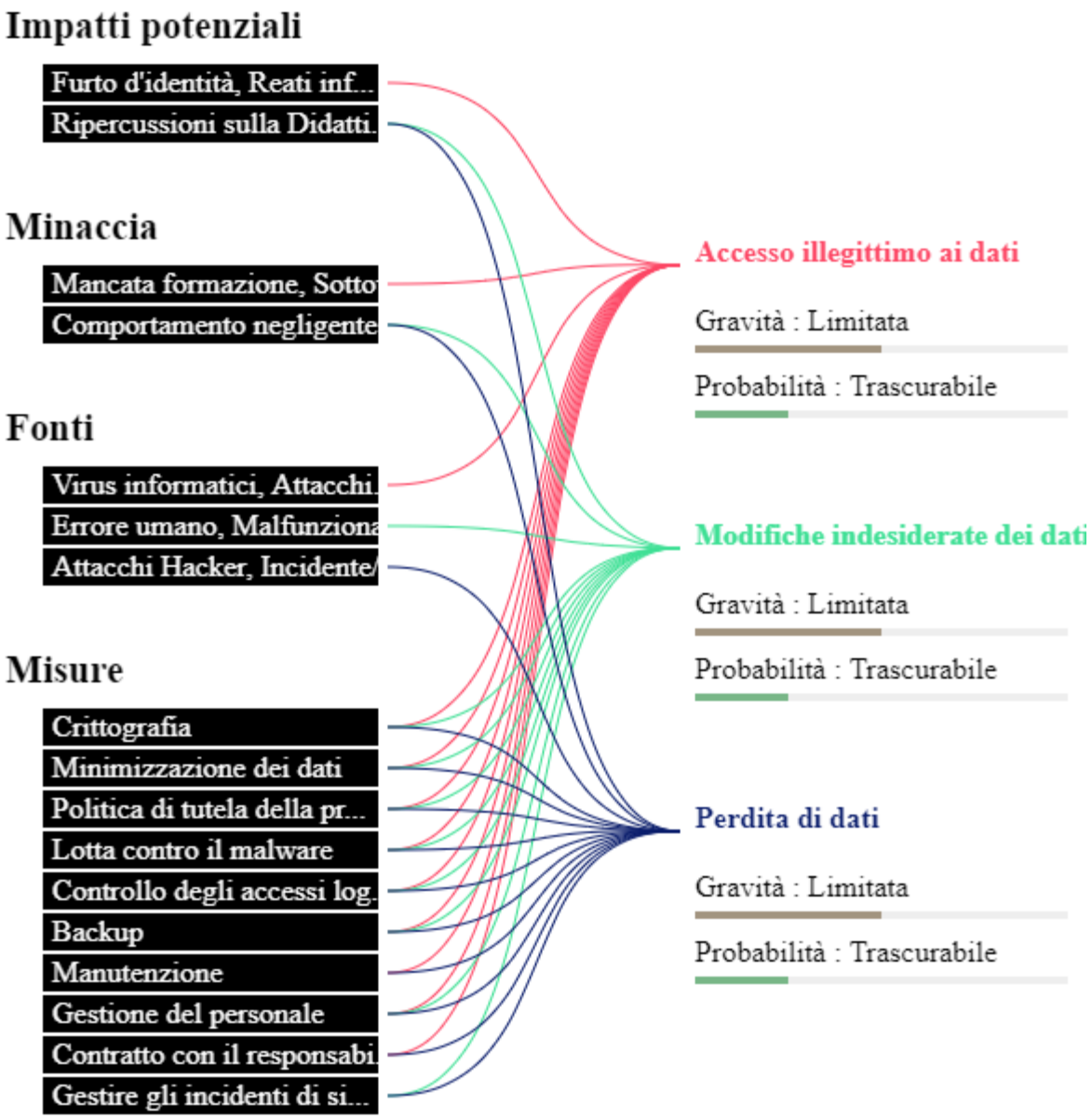
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

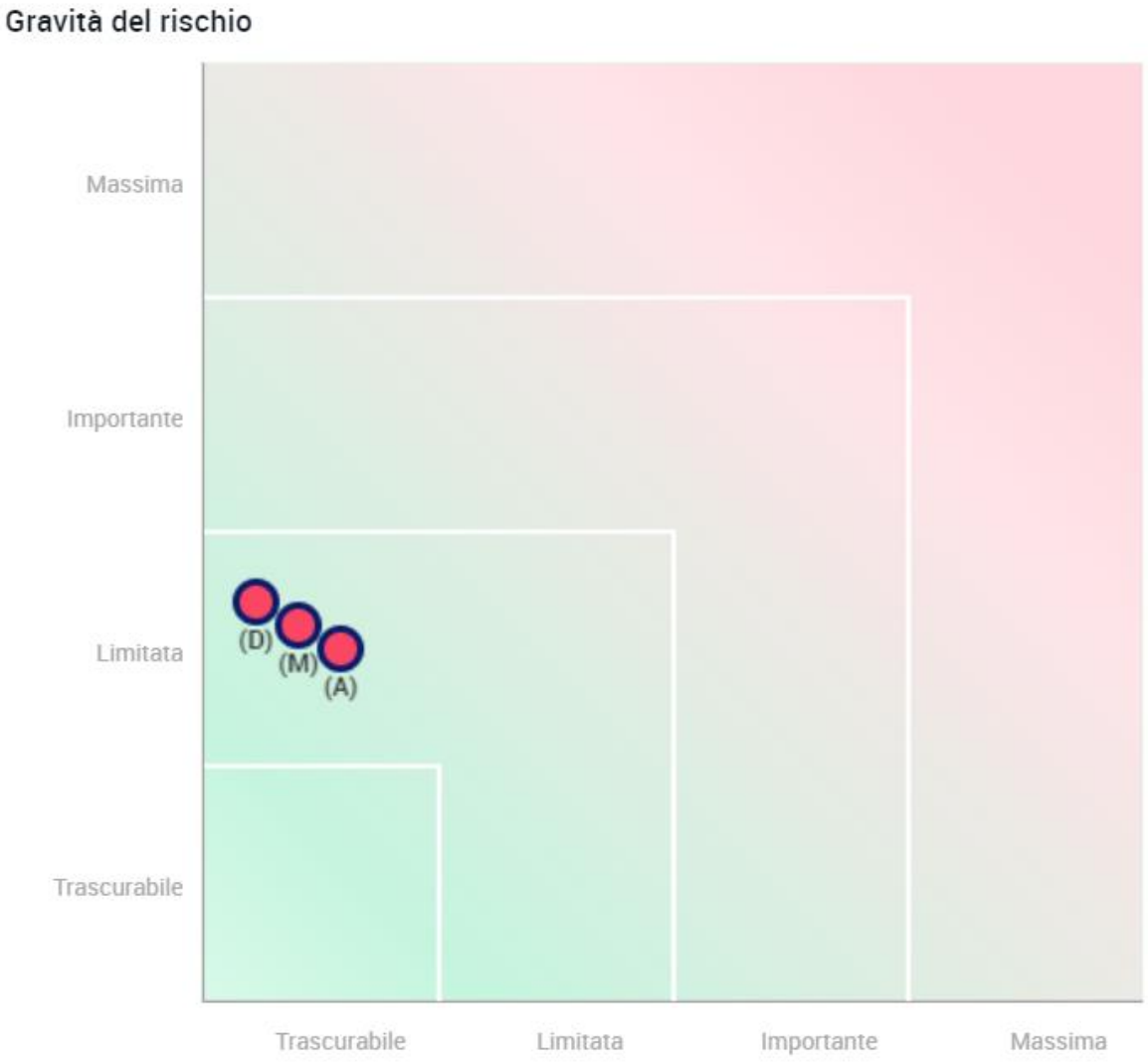
LImitato, Trascurabile per quanto riguarda il caricamento dei dati relativi alla didattica. Possibile valutazione scolastica errata dell'alunno, a causa dell'incompletezza delle informazioni a disposizione del valutatore.

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

Trascurabile, Le misure messe in campo e l'utilizzo di un software cloud minimizzano il rischio di perdita didati.

Rischi - Panoramica dei rischi





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

14/04/23

Elenco allegati:

- Allegato 1 - Guida sottoscrizione accordo Google Workspace
- Allegato 2 - Informativa Google Workspace
- Allegato 3 - ALL. A Linee Guida Didattica Digitale Integrata
- Allegato 4 - Comunicazione utilizzo Google Workspace for Education ALUNNI
- Allegato 5 - Comunicazione utilizzo Google Workspace for Education DOCENTI
- Allegato 6 – Garante Privacy 9300784-1.1
- Allegato 7 – DDI e tutela della privacy Indicazioni generali
- Allegato 8 – Scheda ACN “servizi per la fiscalità, Servizi demografici, Servizi interni alle PA liv. Qualificazione QC1 identificazione SA-690
- Allegato 9 - APPROFONDIMENTI TECNICI DI SUPPORTO PER LE ISTITUZIONI SCOLASTICHE del Ministero dell’istruzione e del merito