# DPIA

## PER UTILIZZO DELLA PIATTAFORMA GOOGLE WORSKSPACE FOR EDU

**AUTORE:**

Dott.ssa Simona Urso

**REDATTORE:**

Dott.ssa Simona Urso

**VALIDATORE:**

Dott. Lorenzo Casali (Ufficio del D.P.O.)

**D.P.O.:**

Referente: Dott. Massimo Zampetti

### PARERE DEL DPO

I rischi di violazione e/o difformità rispetto all'utilizzo di servizi e applicativi che comportano il trasferimento di dati personali in territori extra-EU sono residui in considerazione delle misure di sicurezza supplementari implementate dall'Istituto Scolastico. La configurazione di strumenti di autotutela "lato client" dimostrano di poter colmare le difformità al GDPR nell'applicazione, da parte della Big Tech Google, delle sole *clausole contrattuali standard (CCS).*

### RICHIESTA DEL PARERE DEGLI INTERESSATI

Non è stato chiesto il parere degli interessati.

### MOTIVAZIONE DELLA MANCATA RICHIESTA DEL PARERE DEGLI INTERESSATI

Non si è ritenuto necessario richiedere un parere agli interessati dato l'interesse dell'Istituto di fornire uno strumento utile e complementare della didattica ordinaria anche alla luce dei suggerimenti del Ministero dell'Istruzione e del Merito all'utilizzo di piattaforme multimediali durante la pandemia da Covid-19. Qualora vi fossero pareri contrapposti da parte dell'utenza, l'amministrazione si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto degli stessi.

## DETTAGLI DELLA DPIA

La tabella seguente mostra le informazioni di base della DPIA:

**TABELLA 1**

| | |
|---|---|
| **DESCRIZIONE E SCOPO DELLA DPIA** | La presente valutazione di impatto è effettuata dall'istituto scolastico allo scopo di valutare l'impatto sui diritti e libertà dell'utenza scolastica, dovuti ai rischi relativi al trattamento dei dati personali degli stessi nell'utilizzo dei servizi/applicativi integrati nella piattaforma multimediale di Google Workspace |
| **PERSONE INTERESSATE E TIPOLOGIE DI DATI PERSONALI TRATTATI** | La valutazione di impatto (DPIA) è effettuata per le seguenti tipologie di "interessati" e di relativi dati personali:<br>Alunni (dati personali "comuni" nome e cognome, e-mail) ed eventuali contenuti quali foto/audio/video in occasione di progetti/attività di didattica.<br>Personale scolastico (dati personali "comuni" nome e cognome, e-mail) ed eventuali progetti di foto/audio/video in occasione di progetti/attività. |
| **FINALITÀ DEL TRATTAMENTO** | I dati degli alunni e del personale scolastico sono oggetto di trattamento al fine di attivare gli account e utilizzare gli applicativi/servizi integrati nella piattaforma multimediale solo ed esclusivamente per finalità di didattica. |
| **MINIMIZZAZIONE E AGGIORNAMENTO DEI DATI** | I dati raccolti sono adeguati, rilevanti e limitati a quanto necessario in relazione alle finalità del trattamento. I dati sono costantemente aggiornati in base alle eventuali modifiche riscontrate. Gli amministratori della Google Workspace assicurano un controllo sulla gestione degli account, intervenendo con limitazioni e/o disattivazioni. |
| **PERIODO DI CONSERVAZIONE DEI DATI** | I dati sono conservati per il tempo necessario a consentire lo svolgimento dell'attività di didattica durante l'intero ciclo scolastico. Al termine del ciclo, gli account e i relativi dati presenti negli stessi saranno oggetto di cancellazione permanente, previa concessione di un intervallo di tempo idoneo a garantire la portabilità dei propri dati. |
| **MODALITÀ DI INFORMAZIONE ADOTTATA** | Informativa condivisa su registro elettronico e disponibile sulla pagina privacy policy del sito web istituzionale. È stato, inoltre, approvato un Regolamento, deliberato al Consiglio d'istituto, sull'utilizzo della piattaforma multimediale a scopo di integrazione degli strumenti a disposizione della didattica ordinaria. |
| **DESTINATARI DEI DATI TRATTATI** | I dati personali sono trattamenti unicamente per l'erogazione dei contenuti didattici. Non sono previsti destinatari di dati diversi dal gestore della piattaforma stessa. |
| **COMUNICAZIONE DATI AL DI FUORI DELL'UE** | Google Workspace dispone di data center presenti sia in Europa sia in USA. Il trasferimento transfrontaliero di dati personali è supportato dall'accettazione da parte del Titolare di clausole contrattuali standard (CCS) che a seguito della sentenza "*Schrems II*" costituiscono l'unica base giuridica di legittimità, in assenza del "Privacy Shield" USA-EU. Le misure di sicurezza supplementari attivate dall'Istituto consentono di superare le potenziali difformità in sede di applicazione delle sole CCS. |

## VALUTAZIONE PRELIMINARE

Il Titolare del trattamento, con il supporto del Responsabile per la protezione dati, ha effettuato una analisi preliminare sulla necessità o meno di condurre una **Valutazione di Impatto (DPIA – "Data Protection Impact Assessment") sulla protezione dei dati personali,** adottando come guida la Tabella 2 seguente, tratta dai "criteri da considerare secondo il Gruppo di Lavoro Art. 29 (WP 29)"

**TABELLA 2**

Criteri da considerare secondo il gruppo di lavoro art. 29 (wp 29) quando si identifica un rischio elevato (che richiede l'impegno di una pia)

| I TRATTAMENTI SONO RIFERITI AI SEGUENTI CRITERI? | SI | NO |
|---|---|---|
| 1. Valutazione o punteggio, inclusa la profilazione e la previsione | | X |
| 2. Processo decisionale automatizzato con effetto significativo legale o simile | | X |
| 3. Monitoraggio sistematico (es. videosorveglianza su larga scala) | | X |

| | | |
|---|---|---|
| 4. Dati sensibili, giudiziari, etc. | | X |
| 5. Dati trattati su larga scala | X | |
| 6. Set di dati che sono stati abbinati o combinati | | X |
| 7. Dati riguardanti soggetti vulnerabili (minori) | X | |
| 8. Uso innovativo o applicazione di soluzioni tecnologiche o organizzative (es: riconoscimento facciale, ecc...) | | X |
| 9. Quando l'elaborazione in sé "impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto (es: selezione clienti banca per concessione finanziamento) | | X |

**Il Gruppo di Lavoro Art. 29 suggerisce di effettuare una DPIA se almeno 2 (due) dei criteridi cui sopra sono soddisfatti.** La valutazione preliminare conferma quindi che almeno due criteri della tabella precedente sono soddisfatti, pertanto il Titolare del trattamento, con il supporto del Responsabile per la protezione dei dati, ha ritenuto di effettuare una esaustiva **Valutazione di Impatto (DPIA) sulla protezione dei dati personali**, con l'impegno di rivederla periodicamente (in caso di variazione significativa dei dati trattati o del loro trattamento o almeno con cadenza annuale).

## CONTESTO

### PANORAMICA DEL TRATTAMENTO

### QUALE È IL TRATTAMENTO IN CONSIDERAZIONE?

Questa DPIA è stata redatta al fine di valutare i rischi connessi all'utilizzo di applicativi e servizi integrati nella piattaforma multimediale Google Workspace for Edu (Google Gmail, Google Drive, Google Calendar, Google Sites, Google Meet).

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 alla rete internet (sia domestica sia d'Istituto).

La fruizione di tali servizi/applicativi consente la condivisione e collaborazione di documentazione che persegue le finalità di didattica e che si integrano agli strumenti digitali già presenti in istituto, come per esempio il registro elettronico e altri spazi digitali debitamente autorizzati (librerie digitali ecc...).

L'utilizzo di meccanismi di condivisione e cooperazione facenti uso di tecnologie cloud, però, è associabile ad un rischio connesso al trattamento dei dati personali degli alunni. Si rende perciò necessaria l'identificazione di piattaforme e policy di utilizzo volte a minimizzare la possibilità di violazioni della privacy degli studenti.

### QUALI SONO LE RESPONSABILITÀ CONNESSE AL TRATTAMENTO?

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

- Il titolare del trattamento, in questo caso l'Amministrazione Scolastica, rappresentata legalmente dal Dirigente Scolastico (D.S.), che assume un ruolo centrale di supervisione e guida nei confronti dell'operato dei docenti. Inoltre, è compito del D.S. quello di definire un codice di condotta interno alla scuola che regoli l'utilizzo della strumentazione elettronica utilizzata, e di sorvegliare sulla sua attuazione.

- I docenti. Il loro ruolo centrale nella produzione di materiale didattico e contenuti multimediali deve essere associato ad un loro controllo nei confronti di tutte quelle attività suscettibili di potenziale violazione della riservatezza. Al loro ruolo di amministratori, spesso unici, di tutta la documentazione accessibile ai gruppi di lavoro va associata la responsabilità del controllo delle regole di utilizzo prescritte, e la vigilanza sul corretto svolgimento delle operazioni. A tal fine, il titolare si impegna ad attribuire ai docenti il compito di supervisione sulle attività didattiche su piattaforma informatica e a fornire agli stessi indicazioni sulle modalità più opportune con cui trattare i dati personali, ai fini dell'Art. 2-quaterdecies del D.Lgs. 196/2003.

- Il consiglio di classe: Delibera sulla valutazione finale in fase di scrutini. Potrebbe quindi essere necessario allo stesso l'accesso ai documenti presenti sulla piattaforma informatica, ivi inclusi i dati personali.

- Il Responsabile della Protezione dei Dati (RPD) ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.

- I responsabili del trattamento, quali i provider di servizi elettronici utilizzati per la didattica (eventualmente, BYOD) devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Particolare attenzione va posta nei confronti dei fornitori di servizi cloud, ove richiesti. In questo caso, è necessario prestare particolare attenzione alle loro policy sulla cessione dei dati a organismi terzi e all'eventuale salvataggio di dati su server extra-UE. Per questo motivo, sarà necessario effettuare una valutazione preventiva dei provider di servizi Cloud sulla base della loro compliance nei confronti della normativa in essere. Inoltre, sarà necessario procedere alla nomina formale dei fornitori di tali servizi quali responsabili del trattamento ai sensi dell'Art. 28, comma 3 del GDPR. Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati, la cui lista aggiornata può essere trovata sul sito dell'AGID.

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

## CI SONO STANDARD APPLICABILI AL TRATTAMENTO?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al problema in esame. L'European Data protection Board (EDPB) ha però recentemente pubblicato le "Raccomandazioni 01/2020" relative alle misure tecniche e organizzative che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", che specificano, inoltre, i comportamenti da seguire riguardo al trasferimento di dati all'estero. In linea di principio, le misure supplementari applicate possono avere carattere contrattuale, tecnico o organizzativo. La combinazione di misure diverse in modo che si sostengano e si basino l'una sull'altra può migliorare il livello di protezione e può quindi contribuire a raggiungere gli standard dell'Unione.

## DATI, PROCESSI E RISORSE DI SUPPORTO

### Quali sono i dati trattati?

Google Workspace 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 e-mail 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 il pannello amministrativo dall'Istituto);
- informazioni sulla posizione ricavate tramite varie tecnologie, tra cui l'indirizzo IP, GPS e altri sensori (funzione disabilitata attraverso il controllo dell'amministratore della piattaforma);
- 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.

La didattica utilizza, inoltre, gli strumenti di collaborazione digitale per il perseguimento di finalità didattiche e formative. Nel caso specifico gli strumenti hardware, anche di proprietà degli studenti e del persole docente, vengono utilizzati con l'intento di svolgere compiti didattici o per l'accesso a materiale formativo.

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

Tali informazioni dipenderanno ovviamente dalla natura e materia didattica svolte, ma potrebbero contenere dati o informazioni ad alto rischio per la privacy degli interessati. A titolo di esempio, potrebbero contenere degli scritti che definiscono esplicitamente l'orientamento politico, l'etnia e/o la condizione di informazioni sanitarie degli interessati.

È quindi importante sensibilizzare tutti gli utenti (alunni e docenti) sulla necessità di limitare allo stretto indispensabile la presenza di dati personali particolari e di attuare comunque misure efficaci in ossequio al principio di minimizzazione dei dati personali, anche comuni. Infine, è importante far notare che i dati presenti nelle piattaforme potranno essere oggetto di valutazione scolastica.

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

Gli account Google Workspace for Edu 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 amministrativo endoprocedimentale e sarà 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 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?**

Ferma restando la preferenza per le attività scolastiche svolte in presenza, come fu affermato dal DL 11/2021 sulla scorta di quanto sostenuto dal Comitato Tecnico Scientifico nel verbale n. 34 del 12/07/2021, vi era la necessità, durante il contesto pandemico, di sviluppare anche una Didattica Digitale Integrata con strumentazione e metodologie idonee in ossequio al Piano Nazionale per la Scuola Digitale, pilastro fondamentale della cd Buona Scuola (legge 107/2015). Le istituzioni scolastiche dovevano promuovere, all'interno dei Piani Triennali dell'Offerta Formativa e in collaborazione con il Ministero, azioni coerenti con le finalità, i principi e gli strumenti previsti nel PNSD (L. 107/2015, art. 1, commi 56 e 57 in particolare). Il PTOF dell'Istituto rappresentava quindi uno strumento importante per mettere a sistema le finalità, i principi e gli strumenti previsti nel PNSD. Il Piano scolastico per la didattica digitale integrata veniva approvato dal Collegio Docenti indicando i 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 particolare di Google Workspace.

Al termine del contesto pandemico, l'Istituto scolastico ha provveduto a sospendere quasi totalmente l'utilizzo di sessioni di lezione da remoto, pur continuando ad utilizzare applicativi/servizi della Google Workspace come strumenti complementari della didattica ordinaria. L'utilizzo della Google Workspace e in particolare del Drive, del Calendar e della Gmail ha consentito di efficientare il servizio di didattica, consentendo sia ai docenti sia agli alunni di condividere materiale di lezione e comunicare attraverso una rete chiusa e sottoposta a stringenti controlli da parte del team digitale. Sebbene i protocolli di comunicazione ufficiale tra scuola e famiglie restino il registro elettronico e le PEO istituzionali, la piattaforma multimediale Google Workspace si è dimostrata utile, anche in virtù dell'esperienza vissuta durante la pandemia da Covid-19, a fornire uno spazio digitale di condivisione del materiale didattico. L'Istituto ha operato inoltre una scelta sui servizi necessari e pertinenti alla didattica, impedendo al contempo l'apertura degli account degli studenti con dominio istituzionale (es. *nomestudente@istituto.edu.it*) verso l'esterno (salvo casi eccezionali derivati da esigenze di didattica) e bloccando servizi/applicativi del tutto eccedenti e/o inutilizzati in ambiente scolastico (es. servizi di geolocalizzazione, download di applicativi non autorizzati su Google Play...).

**Quali sono le basi legali che rendono lecito il trattamento?**

Il trattamento è stato effettuato inizialmente sulla base del DPCM dell'8 marzo 2020 e successive modifiche ed aggiornamenti che prevedevano l'attivazione di strumenti per lo svolgimento delle attività didattiche a distanza in sostituzione o ad integrazione dell'attività didattica in presenza.

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 era 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 riguardo anche alla gestione della fase di emergenza epidemiologica.

Ad oggi, in virtù del Regolamento d'Istituto, la piattaforma multimediale Google Workspace si dimostra necessaria in quanto il suo utilizzo è correlato all'esecuzione di un compito di interesse pubblico di cui è investita la scuola attraverso una modalità operativa prevista dal regolamento d'Istituto. In sostanza, seguiti i suggerimenti del Ministero dell'Istruzione e del Merito che durante il contesto pandemico si era espresso favorevolmente all'utilizzo di piattaforme a supporto della didattica digitale integrale, l'Istituto scolastico ha ritenuto utile garantire un proseguo delle attività di didattica anche al termine della DDI, attraverso servizi digitali e applicativi presenti nella Google Workspace, sempre e solo con l'obiettivo di garantire un servizio di istruzione qualitativamente migliore rispetto al semplice registro elettronico. In base alle disposizioni contenute negli artt. 13 e 14 del Regolamento UE 2016/679, l'Istituto ha provveduto ad informare gli interessati in merito ai trattamenti dei dati personali effettuati nell'ambito dell'erogazione dell'offerta formativa. Poiché attraverso l'utilizzo della piattaforma sono trattati sia dati degli alunni sia 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. Il consenso dei genitori per l'apertura di un account e per l'utilizzo di servizi autorizzati dall'Istituto a supporto della didattica ordinaria, non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro e non è richiesto. L'Istituto approvando il Regolamento d'istituto all'utilizzo della piattaforma multimediale Google

Workspace assicura a tutta l'utenza scolastica lo stesso diritto all'istruzione, attivando gli account ad inizio del ciclo scolastico e dimostrando il perseguimento di un interesse istituzionale volto a fornire un supporto didattico maggiormente efficace. Pertanto, l'Istituto si ritiene legittimato a trattare i dati personali necessari al perseguimento delle finalità collegate allo svolgimento della didattica nel rispetto dei principi previsti dal Regolamento.

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

I docenti sono invitati a raccogliere (e archiviare) la quantità minima di dati personali necessaria al corretto svolgimento delle loro funzioni. Particolari restrizioni dovranno essere adottate per i dati personali particolari che dovranno limitarsi a quelli strettamente necessari. L'Istituto adotta misure di sicurezza supplementari volte a garantire una tutela della riservatezza adeguata (*vedi misure di sicurezza*).

Ciononostante, è importante far notare come un corretto giudizio sul processo formativo degli studenti passi attraverso l'attenta valutazione dell'intero processo formativo dello studente, e non soltanto dell'elaborato ottenuto nella sua fase finale. Per questo motivo, tutte le informazioni legate al processo formativo possono essere considerate pertinenti ai fini della valutazione e quindi oggetto del trattamento.

**I dati sono esatti e aggiornati?**

La procedura di raccolta e conservazione dei dati prevede la creazione spesso cooperativa di contenuti; perciò, potrebbe presentarsi il caso in cui un elaborato venga deliberatamente modificato da eventuali collaboratori durante il suo processo di creazione. In tal caso, è preferibile utilizzare uno strumento che tenga traccia delle modifiche apportate alla documentazione, tramite ad esempio soluzioni di backup e di cronologia delle modifiche.

Una volta terminati, gli elaborati delle prove scritte, grafiche e pratiche possono essere considerati documentazione amministrativa oggetto di valutazione scolastica. Per questo motivo, essi non possono essere modificati o cancellati neppure su richiesta degli interessati per il periodo prescritto dalla legge e comunque funzionale alla corretta valutazione da parte dei docenti e del consiglio di classe.

**Qual è il periodo di conservazione dei dati?**

La conservazione dei dati è necessaria per un periodo strettamente necessario allo svolgimento dell'attività di didattica. successivamente ad essa, i dati verranno archiviati sulla repository digitale dell'Istituto scolastico, e la documentazione prodotta verrà resa inaccessibile agli interessati, salvo richiesta scritta di accesso o cancellazione degli interessati. La piattaforma multimediale e il correlato servizio di cloud (Google Drive) viene gestito unicamente per la gestione di materiale di supporto alla didattica. Eventuali documenti contenenti dati personali particolari (ad. es. PDP, PEI) sono sottoposti a misure di pseudonimizzazione durante la fase di redazione, ovvero conservati con adeguate tecniche di cifratura attivate.

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.

Gli account abilitati all'utenza scolastica sono soggetti ad eliminazione al termine del periodo di utilità a seconda della categoria di interessati. Per il personale scolastico si considera un intervallo di tempo indicativo di 30/60 gg per consentire

la portabilità dei dati prima della cancellazione definitiva. Per gli studenti al termine del ciclo scolastico si concede un periodo indicativo di 30gg per salvare i propri documenti per poi procedere alla cancellazione definitiva.

## MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

### Come sono informati del trattamento gli interessati?

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

- La pubblicazione sul sito web, nella sezione privacy policy;
- L'utilizzo delle modalità di comunicazione scuola/famiglia messe a disposizione dal registro elettronico (opzione di spunta di presa visione attivata).

Gli interessati sono informati delle finalità didattiche su cui il trattamento si basa e sui possibili rischi associati. È 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 contiene inoltre un riferimento alla policy scolastica sull'utilizzo delle strumentazioni elettroniche, nella quale vengono definite le responsabilità delle parti in causa. Nella policy si evidenzia quali servizi e applicativi utilizzare, a scopi didattici ovvero i servizi considerati "sicuri" e "pertinenti", per i quali l'istituto provvede a nominare i responsabili del trattamento.

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

### Ove applicabile: come si ottiene il consenso degli interessati?

La base legale del trattamento non è il consenso dell'interessato.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

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

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

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

La piattaforma Google Workspace for Edu si basa su server che possono anche essere localizzati negli Stati Uniti d'America. Questo fatto ha delle criticità in relazione alla recente sentenza C.311/18 (Schrems II) con la quale la Corte di Giustizia ha dichiarato l'invalidità della decisione di adeguatezza Privacy Shield e che ha indotto Google stessa ad individuare nelle clausole contrattuali standard (CCS) la base legale del trattamento. Cadendo quindi la valutazione di conformità a priori garantita dal privacy Schield (Accordo Scudo USA-EU) l'Istituto scolastico è consapevole che spetta a lui verificare che le clausole contrattuali standard costituiscano una garanzia sufficiente per la tipologia di dati trattati. Dall'analisi condotta nella sezione successiva, riteniamo di poter affermare che il livello di protezione garantito è adeguato alla tipologia dei dati trattati limitata a quelli strettamente necessari al perseguimento delle finalità didattiche.

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

Una prima opzione considerata è stata quella di optare per la versione a pagamento (Education Standard e Education plus) che consente di mantenere i dati trattati dalla piattaforma all'interno dei confini dell'Unione Europea. Questa soluzione, tuttavia, non garantisce una perfetta compliance alle disposizioni del GDPR circa la tutela dei diritti degli interessati in quanto, a seguito dell'approvazione del "Clarifying Lawful Overseas Use of Data" (c.d. *Cloud Act)* voluto dall'amministrazione USA durante il mandato del presidente Donald Trump, le autorità statunitensi, forze dell'ordine e agenzie di intelligence possono acquisire dati informatici dagli operatori di servizi di cloud computing a prescindere dalla località i cui i dati si trovano.

Una seconda opzione è stata la valutazione di servizi equivalenti forniti da altre società che utilizzassero server posti sul territorio europeo. La ricerca ha dato esito negativo in considerazione dei prezzi prospettati.

È stata infine valutata la possibilità di attrezzarsi in modo autonomo, con i server in locale. Tale soluzione è risultata percorribile solo in parte, soprattutto per la gestione di file estremamente sensibili.

**RISCHI**

**Misure esistenti o pianificate**

**Crittografia**

I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, al fine di garantire la minimizzazione del rischio di acceso agli stessi. Il personale scolastico è stato avvertito della necessità di implementare misure di sicurezza supplementari, tra le quali la cifratura di documenti con informazioni e dati particolari attraverso strumenti di protezione "lato client" sia sui documenti in formato .pdf sia sui documenti della suite di MS Office presenti sul Google Drive.

**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 personali particolari devono essere limitati a quelli strettamente necessari. Il personale scolastico è stato istruito sull'utilizzo di modalità di pseudonimizzazione dei contenuti di testo e-mail, delle informazioni riportate sul Calendar e di quanto conservato sul Drive. È stata inoltre raccomandata la rimozione di immagini profilo sugli account nominali che rendano identificabili

direttamente/indirettamente gli utenti. Infine, si stanno valutando piani di intervento al fine di pseudonimizzare gli account già attivati e quelli di futura creazione.

**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**

L'Istituto provvede all'implementazione di politiche di disaster recovery al fine di prevenire rischi di perdita di disponibilità di documentazione contenente dati personali e in uso per finalità di natura istituzionale.

**Manutenzione**

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento della piattaforma multimediale implementata.

**Contratto con il responsabile del trattamento**

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

**Politica di tutela della privacy**

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

**Gestire gli incidenti di sicurezza e le violazioni dei dati personali**

L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalità di gestione di tali fenomeni.

**Modalità di restrizione degli account**

Gli account attivati dall'Istituto scolastico sono sottoposti a limitazioni che comporta una restrizione all'uso di applicativi e servizi non pertinenti al contesto scolastico. Permane inoltre un controllo dell'amministratore della Google Workspace per l'implementazione di misure di sicurezza ulteriori o configurazioni che si rendono necessarie per limitare maggiormente i rischi di utilizzo improprio (es. geolocalizzazione, accesso al Google Play store).

**Navigazione internet**

Al fine di garantire una minimizzazione dei dati di navigazione è stato raccomandato l'utilizzo di modalità di navigazione in incognito differenti a seconda del browser di ricerca utilizzato (Microsoft Edge, Google Chrome, Mozilla Firefox, Safari)

**Formazione specifica del personale e degli interessati**

Il personale e gli alunni saranno informati e istruiti riguardo alle modalità di utilizzo dei servizi, così da limitare il rischio di comportamenti che possano comportare un rischio per sé e per gli altri. L'istituto ha inoltre approvato un Regolamento che include netiquette e condizioni d'uso della piattaforma.

**ACCESSO ILLEGITTIMO AI DATI**

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

Accesso a dati personali di minori con uso improprio degli stessi

**Quali sono le principali minacce che potrebbero concretizzare il rischio?**

Accesso ai dati da parte di amministrazioni e autorità extra-EU. Diffusione su spazi digitali non autorizzati di dati personali contenuti in documenti condivisi sulla piattaforma. Manomissioni, intrusioni e attacchi informatici. Cyberbullismo.

**Quali sono le fonti di rischio?**

Un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Un utente (studente) che voglia utilizzare le informazioni per mettere in atto episodi di bullismo. Accesso di autorità governative statunitensi su server collocati su territorio extraeuropeo.

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

Tutte le misure esistenti o pianificate individuate. In particolare, la proibizione dell'uso di dati personali non necessari all'attività formativa con particolare riferimento a quelli sensibili per i quali deve essere fatta una più rigorosa valutazione di stretta necessità.

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

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

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

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

**MODIFICHE INDESIDERATE DEI DATI**

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

Potrebbe limitare le possibilità di intervento dell'amministrazione o dell'autorità giudiziaria.

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

Accesso illecito ai dati e modifica degli stessi

**Quali sono le fonti di rischio?**

Errore umano, Fonti umane interne, che intervengano nella modifica dei dati Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? Tutte le misure esistenti o pianificate individuate.

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

Limitata, Sebbene la violazione potrebbe portare ad una errata valutazione dell'alunno, le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

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

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

**PERDITA DI DATI**

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

Problematiche nella valutazione degli studenti da parte dei docenti e dell'amministrazione.

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

Distruzione dei server del servizio, Perdita dell'accesso ai documenti, errore umano

**Quali sono le fonti di rischio?**

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

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

Tutte le misure esistenti o pianificate individuate.

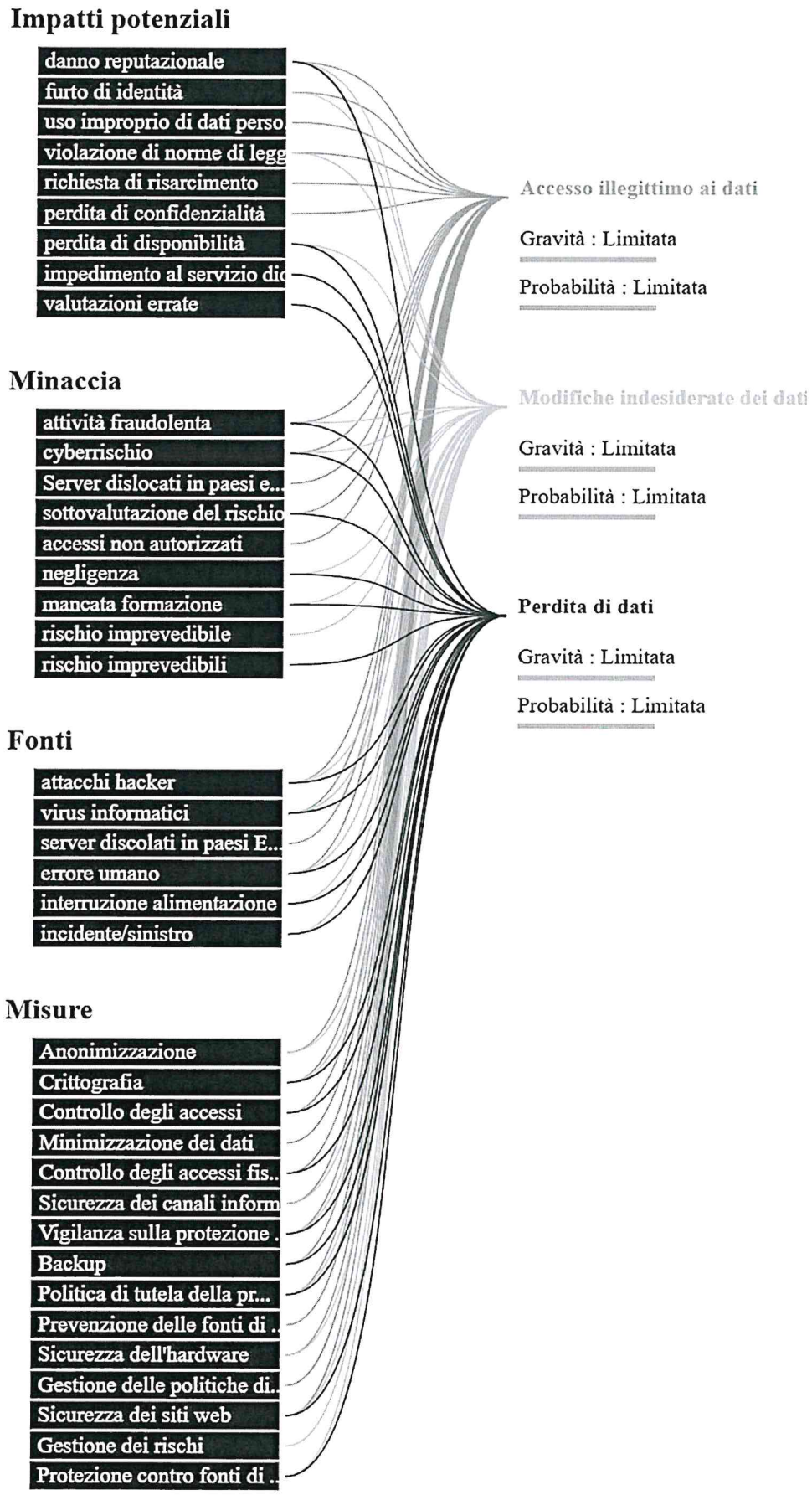
**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**

Limitata per quanto riguarda il caricamento dei dati relativi alla didattica in virtù delle misure di sicurezza supplementari implementate.

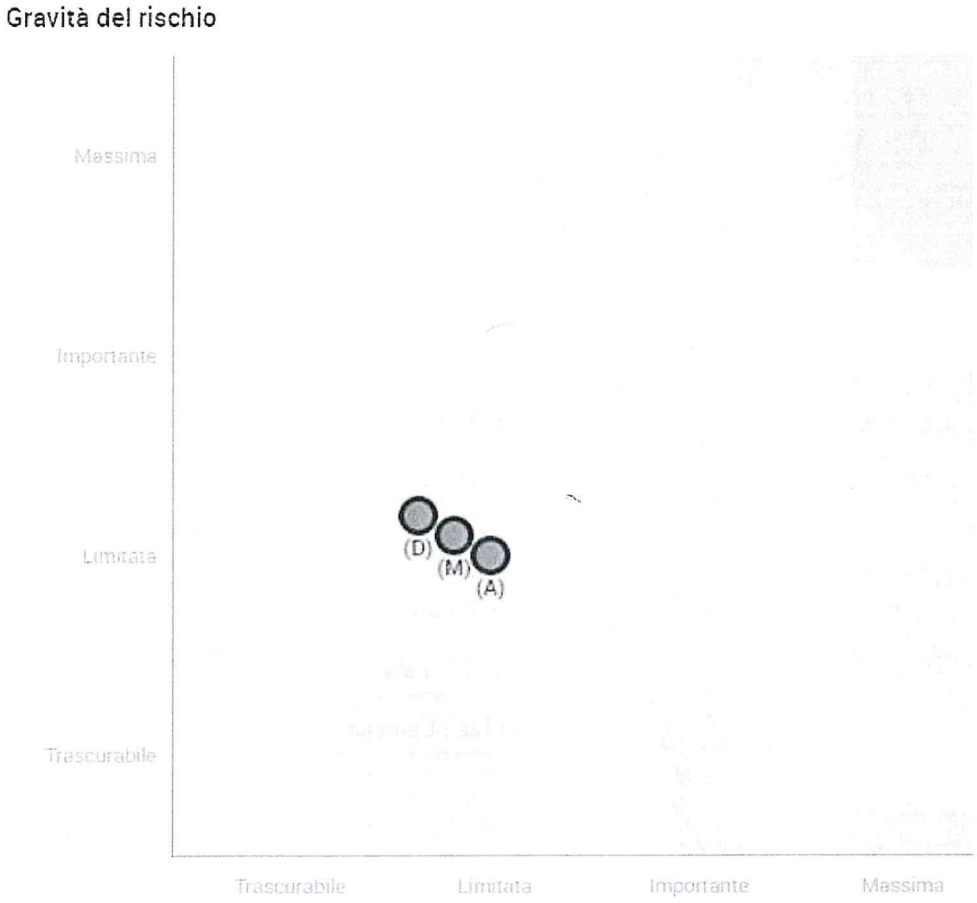
**Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**

Limitata. Le misure di sicurezza messe in campo e l'utilizzo di servizi/applicativi per soli fini di didattica minimizzano il rischio di perdita di disponibilità, di accesso illegittimo e perdita di riservatezza dei dati personali trattati.

## RISCHI - PANORAMICA DEI 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