Ministero dell'Istruzione, dell'Università e della Ricerca

ISTITUTO COMPRENSIVO VIA ADUA - SEVESO

Scuola primaria "C. Collodi" - Scuola primaria "E. Toti" - Scuola secondaria primo grado "Don A. Giussani"Via Adua n. 41/43 – 20822 Seveso (MB)-
C.M.: MBIC86300B – C.F. 83011280159 -☎ 0362/502894 - @: mbic86300b@istruzione.it - mbic86300b@pec.istruzione.it

Valutazione del rischio e misure di sicurezza per i dati personali

La valutazione dei rischi qui svolta è stata redatta in conformità con le indicazioni fornite dall'ENISA (European Union Agency for Network and Information Security) nell'elaborato "Handbook on Security of Personal Data Processing".

Step 1: Definizione dell'operazione di trattamento e del suo contesto

1. **Descrizione del trattamento dei dati personali.**

Trattamento di dati di alunni e docenti per attivazione della didattica a distanza

2. **Quali sono le tipologie di dati personali trattati?**

Dati anagrafici, dati di contatto, credenziali di accesso alle piattaforme, indirizzo ip di collegamento, immagini e dati audio, commenti vocali, opinioni e commenti.

3. **Qual è la finalità del trattamento?**

Svolgimento delle funzioni istituzionali relative all'istruzione e alla formazione degli alunni e alle attività amministrative ad esse strumentali con riferimento ai servizi connessi alla didattica e per assicurare il regolare svolgimento del percorso didattico e l'attuazione del PTOF di Istituto.

4. **Quali sono gli strumenti utilizzati per il trattamento dei dati personali?**

Il trattamento avviene attraverso strumenti elettronici e piattaforme collegati tramite rete internet

5. **Quali sono le categorie di soggetti interessate?**

Alunni, genitori / tutori, personale scolastico

6. **Chi sono i destinatari dei dati?**

Fornitori della piattaforma per la didattica a distanza

Personale scolastico e utilizzatori della piattaforma

7. **Dove avviene il trattamento dei dati personali?**

I dati personali sono normalmente conservati su server ubicati all'interno dell'Unione Europea da parte dei fornitori dei servizi di formazione a distanza.

Step 2: Comprensione e valutazione dell'impatto

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

N.	DOMANDA	VALUTAZIONE
I.1. **Perdita di riservatezza**	**Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	Basso Medio X Alto Molto Alto I dati trattati nella piattaforma Classroom non comporta impatti rilevanti sui diritti e le libertà Degli interessati
I.2. **Perdita di integrità**	**Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività -**	Basso Medio X Alto Molto Alto

	potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.	La modifica non autorizzata di questi dati potrebbe ostacolare la corretta gestione della DAD con complicazioni tali da non permettere la fruizione del servizio
I.3. **Perdita di disponibilità**	**Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	Basso Medio X Alto Molto Alto Il blocco della piattaforma può essere superato senza grosse difficoltà con una nuova registrazione del'utente alla piattaforma.

Essendo il risultato complessivo della valutazione dell'impatto il più alto identificato, l'impatto complessivo valutato risulta essere **MEDIO**. Punti 2

Step 3: Definizione di possibili minacce e valutazione della loro probabilità

In questa fase, lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia).

Per semplificare questo processo, sono state definite una serie di domande di valutazione che mirano a sensibilizzare l'organizzazione del titolare sull'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce). In tale prospettiva, le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

- Risorse di rete e tecniche (hardware e software)
- Processi / procedure relativi all'operazione di trattamento dei dati
- Diverse parti e persone coinvolte nell'operazione di trattamento
- Settore di operatività e scala del trattamento

Qui vi sono una serie di domande relative alla valutazione della probabilità di occorrenza di una minaccia di cui occorre valutare se la probabilità di accadimento è:

BASSA: è improbabile che la minaccia si materializzi;

MEDIA: c'è una ragionevole possibilità che la minaccia si materializzi;

ALTA: la minaccia potrebbe materializzarsi.

A. RISORSE DI RETE E TECNICHE

1	**Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?**	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.	SI (si accede alle piattaforme per la didattica a distanza e al registro elettronico tramite internet)
2	**È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?**	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.	NO (le piattaforme non sono collegate a sistemi di elaborazione interna di dati. Tutti i dati salvati sulla piattaforma rimangono al suo interno). SI (il registro elettronico è un sistema interno di trattamento di dati personali che si può accedere tramite internet).
3	**Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?**	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).	SI (il registro elettronico è interconnesso con il SIDI). NO (le piattaforme esterne non siano interconnesse ad altri sistemi).

4	**Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?**	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).	NO (possono accedere sia al registro che alle piattaforme solo i soggetti autorizzati e dotati di password; inoltre tutti gli utenti devono rispettare i regolamenti e le norme di sicurezza imposte).
5	**Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?**	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.	NO (tutti i sistemi dal registro elettronico alle piattaforme devono essere implementati secondo le raccomandazioni del GDPR e il fornitore dei servizi deve garantire alla scuola l'adesione alle attuali norme in materia di trattamento dei dati).

VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: BASSA punti 1

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

6	**I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?**	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.	NO (i ruoli e le autorizzazioni sono chiari e definiti nessuno può entrare nel sistema se non autorizzato e può visualizzare determinati dati in base ai permessi dati dalla scuola).
7	**L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?**	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche	NO (la scuola ha predisposto regole e istruzioni).

		per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	
8	**I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?**	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.	SI (nei limiti consentiti dalla scuola e vista l'emergenza che stiamo vivendo da covid-19 che ha obbligato le scuole alla chiusura e all'attivazione della didattica a distanza).
9	**I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?**	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.	SI (nei limiti consentiti dalla scuola e vista l'emergenza che stiamo vivendo da covid-19 che ha obbligato le scuole alla chiusura e all'attivazione della didattica a distanza).
10	**Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?**	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali.	NO (solitamente tutte le operazioni compiute all'interno del registro elettronico vengono tracciate.).

VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: BASSA punti 1

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

11	**Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?**	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	NO (tutti i dipendenti e gli utenti sono monitorati e definiti).
12	**Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza**	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere	SI (dai soggetti esterni alla scuola che forniscono il registro elettronico e le piattaforme).

	parte (responsabile del trattamento)?	introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	
13	**Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?**	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.	NO (definiti dalla scuola. Tutto il personale scolastico è stato inoltre autorizzato al trattamento dei dati).
14	**Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?**	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	NO (il personale è stato formato e istruito).
15	**Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?**	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.	NO (il personale è stato formato e istruito).

VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: BASSA

D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO

16	**Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?**	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è	NO (il settore dell'istruzione non è esposto a particolari attacchi informatici)

		un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.	
17	**La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?**	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	NO
18	**Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?**	Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.	NO
19	**Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?**	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	SI (i dati degli alunni e del personale della scuola).
20	**Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?**	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.	NO (la scuola segue le best practice suggerite dal Ministero dell'istruzione e dall'AGID).

VALUTAZIONE DELLA PROBABILITA' DI ACCADIMENTO DI UNA MINACCIA: BASSA punti 1

Step 4: Valutazione del rischio

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi.

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilevante, la valutazione finale del rischio è **BASSO**. (punti 5)

Indipendentemente dal risultato finale di questo esercizio, la scuola dovrebbe sentirsi libera di adeguare il livello di rischio ottenuto, tenendo conto delle caratteristiche specifiche dell'operazione di trattamento dei dati (che sono state omesse durante il processo di valutazione) e fornendo un'adeguata giustificazione per tale adeguamento.

Step 5: Misure di sicurezza

Si veda l'Allegato A delle indicazioni elaborate da Enisa che riporta l'elenco delle misure tecniche e organizzative proposte per livello di rischio BASSO.