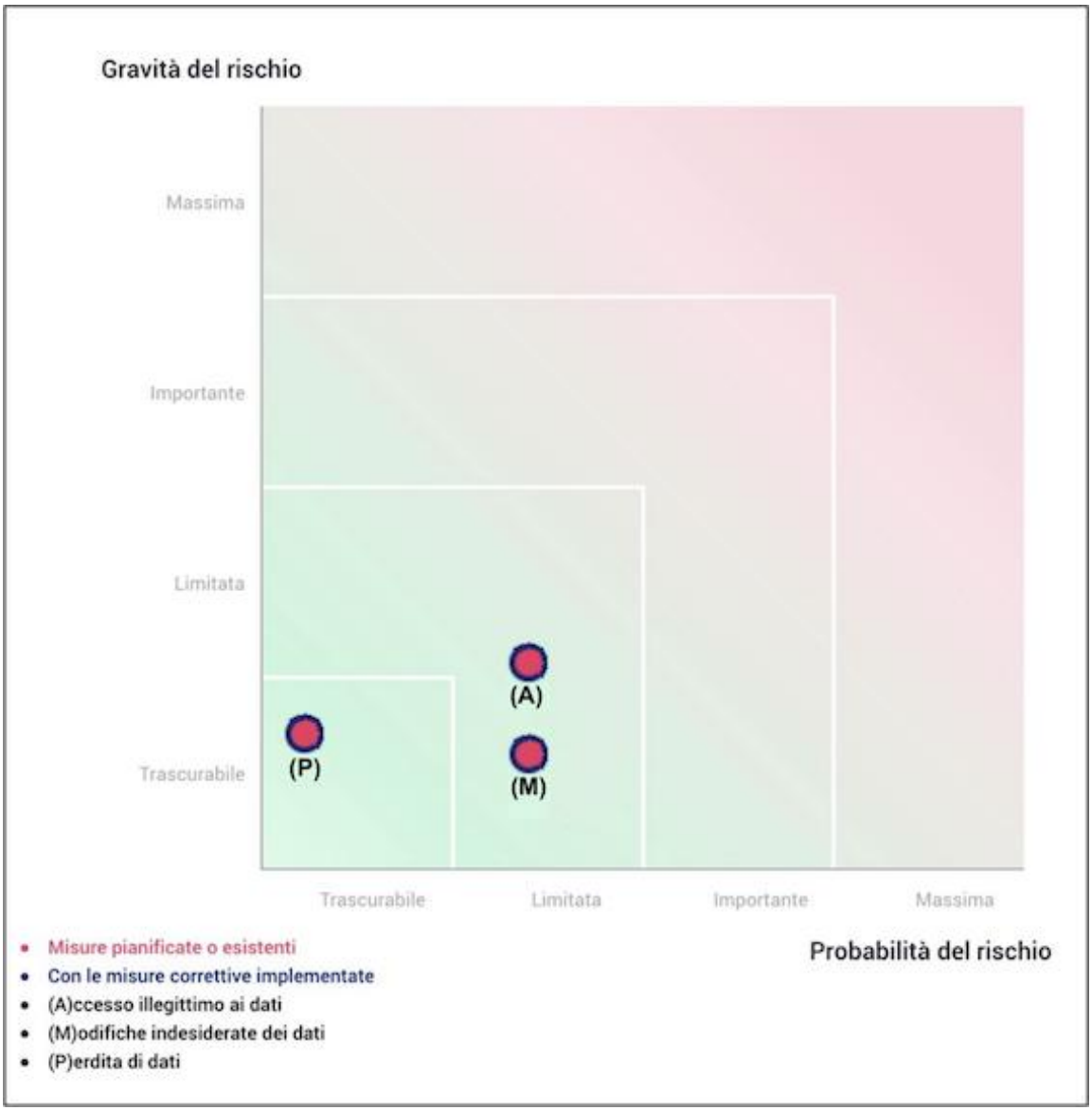
I S T I T U T O C O M P R E N S I V O S T A T A L E D I R U F I N A
Via P. Calamandrei, 5 – Rufina (FI) 50068- Tel.: 0558398803
FIIC83000L@istruzione.it - pec: FIIC83000L@pec.istruzione.it
C.F.:80019690488- COD. MECC.: FIIC83000L – COD. UNIVOCO UFF.: UFNXXT
sito web: www.istitutocomprensivorufina.edu.it

ISTITUTO COMPRENSIVO DI RUFINA
Prot. 0002003 del 13/05/2025
IV (Uscita)

DPIA relativa all'utilizzo del Registro Elettronico nel contesto scolastico

Dati riassuntivi della DPIA

Mappa dei rischi


Gravità del rischio
Massima
Importante
Limitata
Trascurabile
(A)
(P)
(M)
Trascurabile
Limitata
Importante
Massima
Probabilità del rischio
Misure pianificate o esistenti
Con le misure correttive implementate
(A)ccesso illegittimo ai dati
(M)odifiche indesiderate dei dati
(P)erdita di dati

Opinione del D.P.O. e degli interessati

Nome del DPO/RPD

NetSense S.r.l.

Posizione del DPO/RPD

Il trattamento può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Il trattamento dei dati trova fondamento giuridico in basi legittime previste dal GDPR, quali l'adempimento di obblighi legali da parte dell'istituzione scolastica (art. 6, par. 1, lett. c) e l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri (art. 6, par. 1, lett. e).

Più specificamente, l'uso del Registro Elettronico è previsto dall'art. 7, comma 31, del D.L. n. 95/2012, il quale dispone che: «A decorrere dall'anno scolastico 2012-2013 le istituzioni scolastiche e i docenti adottano registri online e inviano le comunicazioni agli alunni e alle famiglie i formato elettronico».

Si sottolinea che, in ottemperanza agli articoli 2-ter e 2-sexies del codice privacy italiano, il consenso degli interessati non è necessario per i trattamenti effettuati dalle pubbliche amministrazioni, fatto salvo che tali trattamenti siano effettuati nel rispetto della normativa vigente.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Nell'attuale contesto educativo, in costante evoluzione, l'integrazione delle tecnologie digitali sta trasformando profondamente l'approccio tradizionale all'insegnamento e all'apprendimento. In questo scenario, l'Istituto si propone come promotore dell'adozione delle migliori soluzioni offerte dal mercato, nel pieno rispetto delle normative vigenti.

Numerose suite software oggi disponibili consentono agli insegnanti di rispondere in modo efficace alle esigenze dell'apprendimento personalizzato, di preparare gli studenti alle competenze richieste nel XXI secolo e di favorire la creazione di una comunità educativa interconnessa e dinamica.

Tra questi strumenti, un ruolo centrale è ricoperto dal Registro Elettronico, il cui uso è previsto dall'art. 7, comma 31, del D.L. n. 95/2012, il quale dispone che: «A decorrere dall'anno scolastico 2012-2013 le istituzioni scolastiche e i docenti adottano registri online e inviano le comunicazioni agli alunni e alle famiglie i formato elettronico».

Il Registro Elettronico rappresenta ad oggi una risorsa fondamentale per:

(i) gestire le attività didattiche da parte dei docenti (ad esempio: registrazione di assenze, voti, giudizi, annotazioni sulle lezioni);

(ii) consentire alle famiglie la consultazione delle attività scolastiche svolte dagli studenti e dalle studentesse (come compiti assegnati, lezioni, assenze, voti);

(iii) garantire la trasmissione di comunicazioni istituzionali da parte del Ministero e delle Istituzioni scolastiche alle famiglie e agli studenti, anche in riferimento alla Nota MIM n. 788 del 31 gennaio 2025.

Tuttavia, l'utilizzo del Registro Elettronico da parte delle istituzioni scolastiche comporta potenziali rischi in relazione al trattamento dei dati personali e, in alcuni casi, dei dati particolari degli studenti e delle famiglie. Per quanto tale trattamento avvenga per finalità istituzionali e sia strettamente connesso all'erogazione del servizio scolastico, risulta cruciale individuare piattaforme adeguate e stabilire linee guida per minimizzare il rischio di violazione della privacy degli studenti.

La presente Valutazione dell'Impatto della Protezione dei Dati (DPIA) è condotta proprio per analizzare i rischi e le contromisure da implementare nell'impiego del registro elettronico.

Quali sono le responsabilità connesse al trattamento?

Data la complessità delle azioni e delle potenziali conseguenze relative alle violazioni della privacy, è fondamentale stabilire una collaborazione attiva tra le diverse parti coinvolte. Queste parti includono, ai sensi del Regolamento Europeo 679/2016 (GDPR):

Il Titolare del Trattamento: In questo caso, l'Amministrazione Scolastica rappresentata dal Dirigente Scolastico in carica. Il Dirigente assume un ruolo centrale di supervisione e guida nei confronti delle

altre parti coinvolte. La sua responsabilità principale è garantire una gestione adeguata dei dati e dei sistemi informatici. A tal fine, sovrintende alla definizione e all'attuazione delle procedure, sviluppa un codice di condotta interno e vigila sull'osservanza delle regole.

I Responsabili del Trattamento ai sensi dell'art. 28 del GDPR: In accordo con quanto previsto dall'articolo 28 del GDPR, il Titolare del Trattamento deve nominare responsabili esterni che tratteranno i dati personali per conto dell'Istituto. Questi soggetti, scelti tra quelli che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR e a garantire la tutela dei diritti dell'interessato, hanno la responsabilità di trattare i dati in modo sicuro e conforme alle disposizioni normative. Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati, la cui lista aggiornata può essere trovata sul sito dell'AGID. Nel caso in questione il Responsabile esterno è indicato nella informativa sul trattamento dei dati fornita agli interessati ai sensi degli articoli 13 e 14 del GDPR.

I docenti: essi, autorizzati dal DS per l'uso del sistema, svolgono un ruolo cruciale nell'assicurare il rispetto degli standard di sicurezza per la tutela dei dati personali degli studenti e della loro privacy nell'uso della Registro Elettronico. I docenti sono chiamati a gestire le attività didattiche (ad esempio: registrazione di assenze, voti, giudizi, annotazioni sulle lezioni), le comunicazioni e le interazioni online con la massima riservatezza e consapevolezza delle modalità di condivisione dei dati, degli strumenti di sicurezza forniti dall'applicazione e delle pratiche che minimizzino il rischio di accessi non autorizzati. Inoltre, i docenti hanno la responsabilità di informare gli studenti e di promuovere la consapevolezza sulla privacy digitale.

I Referenti del Registro Elettronico: docenti designati dal DS ai sensi dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali (Dlgs 196/2003 e s..mm.ii.) quali soggetti che operano sotto la sua autorità a cui sono attribuiti i compiti di gestire e supervisionare l'utilizzo del sistema di registrazione elettronica, assicurando che vengano rispettate le normative e le procedure interne. Tra i principali compiti del referente si annoverano: 1. Gestione e supervisione dell'utilizzo del registro elettronico (monitorare l'accesso e l'utilizzo del registro da parte di docenti, studenti e famiglie); 2. Supporto agli utenti (offrire assistenza in caso di difficoltà tecniche o problematiche relative all'uso della piattaforma); 3. Gestione delle credenziali e degli accessi (gestire gli account degli utenti nel sistema, monitorare l'aggiornamento delle credenziali e risolvere eventuali problemi di accesso, in vista della piena integrazione del sistema basato su SPID); 4. Verifica e controllo della qualità dei dati (assicurarsi che i dati registrati - assenze, voti, valutazioni, annotazioni - siano corretti e completi, effettuando controlli periodici per evitare errori nei dati inseriti e garantire la precisione delle informazioni); 5. Collaborazione con il personale amministrativo (garantire che i dati e le informazioni nel registro siano coerenti con le altre piattaforme gestionali della scuola).

Il Responsabile della Protezione dei Dati (RPD, anche denominato 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.

La collaborazione attiva tra queste parti è cruciale per garantire il rispetto delle normative sulla privacy e la protezione dei dati personali all'interno dell'ambiente scolastico. La designazione dei responsabili esterni ed interni e il coinvolgimento del Dirigente Scolastico nella supervisione e

nell'attuazione delle procedure rappresentano passi fondamentali per gestire efficacemente la complessità delle sfide legate alla privacy nell'era digitale.

Ci sono standard applicabili al trattamento?

Ci sono diversi standard e normative applicabili al trattamento dei dati personali nel contesto del Registro Elettronico, soprattutto in relazione alla protezione dei dati sensibili degli studenti e del personale scolastico. Questi includono:

1. Regolamento Generale sulla Protezione dei Dati (GDPR): Il GDPR (Regolamento UE 2016/679) è la normativa principale che disciplina il trattamento dei dati personali nell'Unione Europea. Esso impone obblighi specifici ai titolari e ai responsabili del trattamento dei dati, inclusi quelli che gestiscono il Registro Elettronico. Le scuole, come titolari del trattamento, devono garantire la sicurezza, la riservatezza e la protezione dei dati degli studenti e del personale. Devono anche fornire trasparenza riguardo alle modalità di trattamento e rispettare i diritti degli interessati, come il diritto all'accesso, alla rettifica e alla cancellazione dei dati.

2. ISO/IEC 27001 - Sistema di gestione della sicurezza delle informazioni: Questo standard internazionale fornisce un quadro per gestire la sicurezza delle informazioni, utile per i fornitori di servizi cloud che gestiscono i dati del Registro Elettronico. L'adozione di questo standard implica che il fornitore abbia implementato politiche, procedure e misure tecniche per garantire la protezione dei dati contro accessi non autorizzati, alterazioni o perdite.

3. ISO/IEC 27018 - Protezione dei dati personali nei cloud: Questo standard si concentra specificamente sulla protezione dei dati personali trattati nel cloud, un aspetto cruciale per i fornitori di Registro Elettronico che offrono soluzioni basate su cloud. Fornisce linee guida su come gestire i dati personali, inclusi i dati degli studenti, con particolare attenzione alla privacy e alla sicurezza nel contesto del cloud computing.

4. Normative nazionali: A livello nazionale, il trattamento dei dati personali è regolato dalla Legge 675/1996 (abrogata, ma ancora rilevante per alcuni aspetti storici) e dalla Legge 196/2003, aggiornata dal Decreto Legislativo 101/2018, che adegua la normativa italiana al GDPR. Inoltre, l'Autorità Garante per la Protezione dei Dati Personali fornisce linee guida specifiche per l'uso dei dati personali nelle scuole e nelle pubbliche amministrazioni.

5. Direttive e regolamenti specifici: l'Agenzia per la Cybersicurezza Nazionale (ACN) ha introdotto regolamenti specifici per le infrastrutture digitali e i servizi cloud destinati alla pubblica amministrazione, imponendo requisiti di sicurezza e qualificazione per i fornitori privati. Questi requisiti garantiscono elevati livelli di qualità e affidabilità dei servizi, promuovendo al contempo la competitività nel mercato del cloud computing per le pubbliche amministrazioni.

In sintesi, il trattamento dei dati all'interno del Registro Elettronico deve rispettare una combinazione di normative europee, standard internazionali di sicurezza informatica e regolamenti nazionali, tutti volti a garantire la protezione dei dati personali e la sicurezza delle informazioni sensibili.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Le piattaforme di Registro Elettronico online consentono di svolgere attività caratterizzate da un alto grado di condivisione di informazioni e di collaborazione di gruppo. Ne nasce un trattamento sistematico di dati personali di studenti, famiglie, docenti e personale scolastico, il quale deve avvenire nel rispetto dei principi sanciti dal Regolamento (UE) 2016/679 (GDPR) e dal Codice in materia di protezione dei dati personali (D.lgs. 196/2003, come modificato dal D.lgs. 101/2018).

Nel Registro Elettronico, basato su tecnologie cloud, sono memorizzati di fatto dati identificativi degli studenti, degli insegnanti e di altri partecipanti, oltre a una vasta gamma di informazioni prodotte durante il loro lavoro; tutte informazioni che, a scelta dell'utente, possono essere condivise con altri utenti, specialmente durante la creazione di attività collaborative nell'ambito dell'istruzione.

I dati trattati sono:

Dati anagrafici e identificativi

- Nome, cognome, codice fiscale, data e luogo di nascita degli studenti, delle famiglie e dei docenti;
- Dati di contatto (indirizzo e-mail).

Dati scolastici

- Presenze/assenze;
- Voti, giudizi, valutazioni intermedie e finali;
- Annotazioni sul comportamento, sugli apprendimenti, sul rendimento scolastico.

Dati particolari (ex dati sensibili)

- Informazioni che possono riguardare lo stato di salute (es. giustificazioni per assenze per malattia), disabilità, bisogni educativi speciali (BES/DSA), o situazioni familiari particolari.

Questi dati richiedono particolari cautele nel trattamento, come previsto dall'art. 9 del GDPR.

In considerazione della natura dei dati trattati con il Registro Elettronico, è fondamentale sensibilizzare tutti gli utenti, sia il personale amministrativo dell'istituto sia quello docente, sull'importanza di limitare al minimo indispensabile la presenza di dati sensibili (applicando il principio della minimizzazione dei dati personali) e di porre estrema attenzione nella condivisione dei dati in attività collaborative.

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

L'impiego del registro elettronico comporta, come già accennato nelle precedenti sezioni del presente documento, il trattamento sistematico di dati personali di studenti, famiglie e docenti. Tale trattamento deve avvenire nel rispetto dei principi sanciti dal Regolamento (UE) 2016/679 (GDPR)

e dal Codice in materia di protezione dei dati personali (D.lgs. 196/2003, come modificato dal D.lgs. 101/2018).

Di seguito si fornisce una descrizione funzionale delle principali fasi che compongono il ciclo di vita dei dati personali trattati attraverso il registro elettronico.

Raccolta dei dati

I dati personali vengono acquisiti per finalità determinate, esplicite e legittime, quali la gestione amministrativa, didattica e disciplinare dell'istituzione scolastica. In questa fase, è necessario fornire agli interessati un'informativa chiara e completa prodotta ai sensi degli articoli 13 e 14 del GDPR.

Registrazione e archiviazione

I dati raccolti vengono inseriti all'interno del registro elettronico, in cloud, in modo sicuro, adottando misure tecniche e organizzative adeguate per garantirne l'integrità, la riservatezza e la disponibilità.

Utilizzo dei dati

I dati vengono trattati esclusivamente per le finalità per cui sono stati raccolti. L'accesso ai dati è limitato al personale autorizzato, in base a specifici profili di autorizzazione, nel rispetto del principio di minimizzazione.

Conservazione dei dati

I dati personali saranno conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati. In sintesi:

- Dati didattici (valutazioni, assenze, note disciplinari): Termine di conservazione: 5 anni scolastici (salvo casi particolari), data la necessità di documentare il percorso scolastico e rispondere a eventuali richieste o contenziosi.

- Dati amministrativi (iscrizione, anagrafica, certificazioni): termine di conservazione: 10 anni, come previsto per gli atti amministrativi generali.

- Conservazione a lungo termine: alcuni dati/documenti (ad esempio voti finali, titoli conseguiti) devono essere versati in conservazione digitale permanente, come previsto dalle Linee Guida AgID.

Aggiornamento e verifica

I dati devono essere costantemente aggiornati e verificati affinché risultino esatti e pertinenti. In caso di variazione delle informazioni o delle finalità del trattamento, è necessario aggiornare la documentazione relativa, incluso il registro dei trattamenti.

Cancellazione o anonimizzazione

Una volta esaurite le finalità del trattamento, i dati devono essere cancellati in modo sicuro o resi anonimi, secondo modalità che ne impediscano la ricostruzione. Tale attività deve essere effettuata in conformità alle disposizioni normative e alle policy interne dell'istituto scolastico.

Documentazione e monitoraggio

Ogni fase del trattamento deve essere tracciabile e documentata all'interno del registro dei trattamenti previsto dall'art. 30 del GDPR. I tracciamenti saranno utilizzati nelle operazioni di supervisione e monitoraggio condotte dal Titolare del trattamento.

Quali sono le risorse di supporto ai dati?

Di solito, si utilizzano servizi basati su cloud per agevolare la condivisione e l'organizzazione dei compiti assegnati. Nel caso del Registro Elettronico, queste tecnologie devono fare affidamento su server situati all'interno dell'Unione Europea, ed è di fondamentale importanza verificare che rispettino la normativa europea in materia di gestione dei dati.

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

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento dei dati effettuato mediante il registro elettronico risultano specifici, espliciti e legittimi, in conformità con quanto previsto dall'art. 5 del Regolamento (UE) 2016/679 (GDPR).

Specificità e finalità

Il trattamento dei dati personali attraverso il registro elettronico persegue finalità chiaramente definite, tra cui:

- la registrazione delle valutazioni scolastiche;
- la rilevazione delle assenze, dei ritardi e delle uscite anticipate;
- la gestione delle comunicazioni tra scuola e famiglie;
- la documentazione di eventuali provvedimenti disciplinari;
- la redazione di pagelle, attestati e documentazione relativa agli scrutini.

Tali finalità sono esplicitamente indicate nel Regolamento d'Istituto e nell'informativa sul trattamento dei dati personali fornita agli interessati.

Legittimità del trattamento

Le basi giuridiche per il trattamento sono riportate nel successivo paragrafo.

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento dei dati trova fondamento giuridico in basi legittime previste dal GDPR, quali l'adempimento di obblighi legali da parte dell'istituzione scolastica (art. 6, par. 1, lett. c) e l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri (art. 6, par. 1, lett. e).

Più specificamente, l'uso del Registro Elettronico è previsto dall'art. 7, comma 31, del D.L. n. 95/2012, il quale dispone che: «A decorrere dall'anno scolastico 2012-2013 le istituzioni scolastiche

e i docenti adottano registri online e inviano le comunicazioni agli alunni e alle famiglie i formato elettronico».

Si sottolinea che, in ottemperanza agli articoli 2-ter e 2-sexies del codice privacy italiano, il consenso degli interessati non è necessario per i trattamenti effettuati dalle pubbliche amministrazioni, fatto salvo che tali trattamenti siano effettuati nel rispetto della normativa vigente.

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

Nell'ambito dell'utilizzo del registro elettronico, il trattamento dei dati personali avviene nel rispetto dei principi di adeguatezza, pertinenza e limitazione rispetto alle finalità del trattamento, come previsto dall'art. 5, par. 1, lett. c) del Regolamento (UE) 2016/679 (GDPR). Ciò implica che i dati raccolti e registrati saranno strettamente necessari allo svolgimento delle attività istituzionali della scuola e rilevanti rispetto alle specifiche finalità didattiche, amministrative e organizzative perseguite.

Non saranno trattati dati eccedenti o non coerenti con gli scopi dichiarati; sono attività categoricamente escluse lo (i) svolgimento di iniziative commerciali o di marketing, (ii) trasferimento di dati a soggetti terzi, oltre ovviamente al Responsabile del Trattamento, fornitore del servizio, (iii) messa a disposizione di contenuti non essenziali (i.e., mini-games, oroscopo, chat), (iv) esposizione di banner pubblicitari o rinvio a siti di terze parti contenenti proposte commerciali di qualunque categoria merceologica (i.e. acquisto di libri, di materiale scolastico, etc.).

L'accesso alle sole informazioni indispensabili per l'espletamento delle proprie funzioni sarà limitato al personale autorizzato e alle famiglie, queste ultime suddivise per classi di riferimento e assegnatarie di una room virtuale privata.

Infine, la conservazione dei dati è definita secondo tempi proporzionati e compatibili con le finalità perseguite, evitando l'archiviazione prolungata o indiscriminata di informazioni personali (si veda quanto indicato nel paragrafo del presente documento relativo al ciclo di vita del trattamento dei dati).

I dati sono esatti e aggiornati?

Nel contesto del trattamento dei dati personali tramite il registro elettronico, l'istituzione scolastica deve garantire il rispetto del principio di esattezza e aggiornamento dei dati, ai sensi dell'art. 5, par. 1, lett. d) del Regolamento (UE) 2016/679 (GDPR).

A tal fine, i dati inseriti nel sistema informativo sono oggetto di verifica, controllo e aggiornamento continuo da parte del personale autorizzato e dei Referenti del RE, al fine di assicurarne la rispondenza alla situazione reale dello studente e alla corretta gestione delle attività scolastiche. In particolare, le informazioni relative a valutazioni, presenze, assenze, comportamenti e dati anagrafici sono registrate tempestivamente, e possono essere rettificate su richiesta degli interessati o su iniziativa della scuola in caso di errori accertati. Sono altresì adottate misure organizzative e tecniche per evitare l'utilizzo di dati inesatti o obsoleti, adoperate principalmente

durante i collegi di classe e in fase di scrutinio, contribuendo così alla trasparenza e all'affidabilità del processo educativo e amministrativo.

Qual è il periodo di conservazione dei dati?

I dati personali sono oggetto di conservazione per un periodo di tempo non superiore a quello strettamente necessario al raggiungimento delle finalità per le quali vengono trattati, nel rispetto dei principi di limitazione della conservazione e proporzionalità. In particolare:

- Dati di natura didattica (quali valutazioni, assenze e annotazioni disciplinari): vengono conservati per un periodo pari a cinque anni scolastici, salvo specifiche eccezioni. Tale durata è giustificata dalla necessità di documentare il percorso formativo dello studente e di fornire riscontro in caso di richieste ufficiali o contenziosi.

- Dati amministrativi (inclusi dati anagrafici, documentazione di iscrizione e certificazioni): sono conservati per un periodo di dieci anni, in conformità alla normativa generale in materia di atti amministrativi.

- Conservazione a lungo termine: taluni documenti e dati rilevanti (ad esempio, valutazioni finali e titoli di studio conseguiti) sono destinati alla conservazione digitale permanente, secondo quanto stabilito dalle Linee Guida dell'Agenzia per l'Italia Digitale (AgID) in materia di conservazione dei documenti informatici.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

All'inizio dell'anno scolastico, gli interessati vengono informati del trattamento dei dati attraverso la presentazione di una apposita informativa redatta in conformità agli articoli 13 e 14 del Regolamento UE 2016/679. Tale informativa viene resa disponibile agli studenti, ai loro genitori e ai docenti mediante un utilizzo il più ampio possibile dei mezzi di comunicazione a disposizione della scuola, che comprendono, a titolo esemplificativo, ma non esaustivo:

- la pubblicazione sulla sezione privacy del sito WEB;

- la divulgazione di una circolare;

- la messa a disposizione durante le fasi di iscrizione e in tutte le fasi di compilazione della documentazione amministrativa propedeutiche all'inizio dell'anno scolastico;

- eventuali aggiornamenti della informativa potranno anche essere resi disponibili grazie all'utilizzo delle modalità di comunicazione tra scuola e famiglia rese disponibili dallo stesso registro elettronico.

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

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

Ove applicabile: come si ottiene il consenso degli interessati?

La base giuridica per il trattamento non è costituita dal consenso dell'interessato, ai sensi degli articoli 2-ter e 2-sexies del Codice in materia di protezione dei dati personali (D.lgs. 196/2003, come modificato dal D.lgs. 101/2018).

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

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati hanno la possibilità di contattare l'amministrazione utilizzando il metodo di comunicazione di loro scelta per esercitare tali diritti.

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

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati hanno la possibilità di contattare l'amministrazione utilizzando il metodo di comunicazione di loro scelta per esercitare tali diritti.

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

Nella selezione dei servizi digitali impiegati in ambito scolastico, è essenziale prevedere la stipula di un contratto d'uso con i fornitori e la formale designazione di un Responsabile del Trattamento, in conformità a quanto previsto dal Regolamento (UE) 2016/679 (GDPR). Tali atti, anche qualora siano accettati o sottoscritti in modalità elettronica, devono esplicitare con chiarezza le reciproche responsabilità e specificare in modo dettagliato gli obblighi a carico di ciascuna delle parti coinvolte.

Nel caso specifico del Registro Elettronico, i contenuti del contratto stipulato con il fornitore del servizio, nonché gli aspetti relativi alla sua nomina a Responsabile del Trattamento, sono redatti in maniera trasparente e conforme ai principi di liceità, correttezza e responsabilizzazione sanciti dal GDPR.

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

Non è previsto alcun trasferimento di dati personali verso Paesi non appartenenti all'Unione Europea o allo Spazio Economico Europeo. Tale esclusione garantisce che i dati rimangano sotto giurisdizione europea, in conformità con i requisiti del Regolamento (UE) 2016/679 (GDPR), evitando rischi connessi all'inadeguatezza dei livelli di protezione nei Paesi terzi.

Rischi

Misure esistenti o pianificate

Controllo e gestione degli account di accesso

L'accesso alle funzionalità del Registro Elettronico deve essere disciplinato mediante un sistema strutturato di gestione degli account, che preveda l'assegnazione di profili autorizzativi differenziati protetti da credenziali individuali (username e password). Tali account devono poter essere attivati e disattivati a cura dei Referenti del Registro Elettronico, appositamente designati dal Dirigente scolastico in conformità a quanto disposto dall'art. 2-quaterdecies del D.lgs. 196/2003, come modificato dal D.lgs. 101/2018.

In merito al Controllo e alla gestione degli account di accesso, ai Referenti del Registro Elettronico competono le seguenti attività:

- la definizione dei profili di autorizzazione, assicurando un'adeguata segmentazione delle funzionalità (es. attività didattiche, gestionali, amministrative), con l'obiettivo di limitare l'accesso degli utenti esclusivamente ai dati strettamente necessari per lo svolgimento delle rispettive mansioni;

- la revoca tempestiva dei privilegi di accesso in caso di cessazione del ruolo o del diritto all'utilizzo delle risorse, al fine di prevenire accessi non autorizzati;

- la revisione periodica, almeno annuale, delle autorizzazioni con l'obiettivo di individuare eventuali account inattivi, aggiornare i privilegi concessi e mantenere l'allineamento tra i profili di accesso e le funzioni effettivamente ricoperte.

Minimizzazione dei dati

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

Lotta contro il malware

I sistemi informatici utilizzati nel contesto scolastico sono protetti contro le minacce informatiche, inclusi i malware, attraverso una combinazione di misure di sicurezza hardware e software. Tali misure comprendono l'adozione di firewall e programmi antivirus, finalizzati a rilevare e prevenire

potenziali attacchi informatici. Inoltre, è essenziale fornire agli utenti – che comprendono studenti, docenti e personale scolastico – adeguate linee guida per l'uso sicuro delle risorse elettroniche e digitali. Si sottolinea, altresì, che l'uso dei software essenziali per l'attività didattica, resi disponibili tramite il Registro Elettronico, non comporta un rischio incrementato di infezione da malware.

Manutenzione dei sistemi hardware in uso a scuola

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici. Il responsabile del trattamento (il fornitore del servizio) garantisce inoltre il corretto funzionamento del software cloud da remoto.

Backup dei dati presenti nella piattaforma

Al fornitore del registro elettronico sarà imposta l'adozione di tecniche per garantire la sicurezza e l'integrità dei dati attraverso strategie di backup efficaci. Una pratica consolidata è la regola del 3-2-1, che prevede la conservazione di almeno tre copie dei dati su due supporti differenti, con una copia archiviata in una località separata. Questa metodologia riduce il rischio di perdita di dati dovuta a guasti hardware, disastri naturali o attacchi informatici.

Inoltre, è fondamentale che la trasmissione dei dati avvenga tramite crittografia (protocollo HTTPS). La crittografia garantisce che, in caso di attacco man-in-the-middle, i dati rimangano illeggibili e protetti.

È altresì essenziale definire assieme al fornitore obiettivi chiari di Recovery Point Objective (RPO) e Recovery Time Objective (RTO), stabilendo la frequenza dei backup e i tempi massimi accettabili per il ripristino dei dati in caso di incidente.

La combinazione di queste tecniche contribuisce a garantire la protezione, l'affidabilità e la disponibilità dei dati gestiti attraverso registri elettronici in cloud, assicurando la continuità operativa e la conformità alle normative vigenti in materia di protezione dei dati.

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

Una volta esaurite le finalità del trattamento (si veda la sezione del presente documento relativa ai tempi di conservazione), i dati devono essere cancellati in modo sicuro o resi anonimi, secondo modalità che ne impediscano la ricostruzione. Tale attività deve essere effettuata in conformità alle disposizioni normative e alle policy interne dell'istituto scolastico.

Tracciabilità delle operazioni effettuate online

La piattaforma di Registro Elettronica adottata integra in maniera nativa i più moderni sistemi di tracciabilità delle operazioni effettuate dagli utenti, nel rispetto della loro privacy: i log di tracciamento sono accessibili esclusivamente su richiesta delle autorità giudiziarie.

Continuo monitoraggio e risoluzione delle vulnerabilità del sistema

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

Contratto con il responsabile del trattamento

Il Responsabile del Trattamento, fornitore della piattaforma di Registro Elettronico, è nominato responsabile del trattamento ai sensi dell'Art. 28 del Reg. Ue 679/2016. Ciò avviene tramite la stipula di un opportuno contratto tra le parti, sottoscritto anche in formato elettronico.

Politica di tutela della privacy: misure tecniche ed organizzative da adottare

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

Formazione specifica del personale e degli interessati

Il personale e le famiglie saranno informati e 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.

Sicurezza dei canali informatici

Di seguito alcune misure di sicurezza associate ai canali informatici del Registro Elettronico che l'istituto ha preso in esame per la stesura della presente DPIA:

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

SPID: L'abilitazione futura dell'accesso via SPID consentirà di garantire un adeguato livello di sicurezza, impedendo o limitando l'accesso al Registro medesimo a soggetti non autorizzati. A tal fine è importante che, progressivamente, l'identità digitale diventi la preponderante modalità di accesso al registro.

Protezione Anti-Phishing: il sistema include filtri anti-phishing per rilevare e bloccare tentativi di phishing e di attacchi di spear-phishing.

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

Sicurezza dell'hardware e del servizio

I meccanismi di sicurezza dell'hardware e, più in generale, della fornitura del servizio sono implementati dal fornitore del servizio cloud e includono politiche di sicurezza rigorose per garantire la protezione e l'integrità dei dati sensibili gestiti dalle istituzioni scolastiche. Queste politiche includono misure come la selezione di data center conformi agli standard di sicurezza internazionali,

tra cui la certificazione ISO/IEC 27002, che stabilisce le best practices per la gestione della sicurezza delle informazioni.

Inoltre, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha introdotto regolamenti specifici per le infrastrutture digitali e i servizi cloud destinati alla pubblica amministrazione, imponendo requisiti di sicurezza e qualificazione per i fornitori privati. Questi requisiti garantiscono elevati livelli di qualità e affidabilità dei servizi, promuovendo al contempo la competitività nel mercato del cloud computing per le pubbliche amministrazioni.

In sintesi, le politiche di sicurezza hardware adottate dai fornitori di servizi cloud per registri elettronici sono fondamentali per garantire la protezione dei dati sensibili nel settore educativo. La conformità a standard internazionali e a regolamenti specifici, unitamente a una rigorosa verifica delle misure di sicurezza implementate, contribuiscono a salvaguardare l'integrità e la riservatezza delle informazioni gestite.

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

L'amministrazione scolastica aderisce scrupolosamente alle disposizioni normative vigenti in materia di gestione delle violazioni dei dati personali (c.d. "data breach"). In conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR), l'istituto utilizza le procedure operative dettagliate dal Garante per la Protezione dei Dati Personali per la gestione e la notifica di tali violazioni. In caso di incidente che possa compromettere la riservatezza, l'integrità o la disponibilità dei dati personali trattati, il personale è tenuto a informare tempestivamente il Responsabile della Protezione dei Dati (DPO). Il DPO, in collaborazione con il dirigente scolastico, valuterà l'entità dell'incidente e, se necessario, notificherà l'evento all'Autorità Garante per la Protezione dei Dati Personali entro 72 ore dalla scoperta della violazione, come previsto dall'articolo 33 del GDPR. Qualora la violazione comporti un rischio elevato per i diritti e le libertà degli interessati, l'amministrazione provvederà a informare direttamente gli interessati senza ingiustificato ritardo, ai sensi dell'articolo 34 del GDPR. Tali misure sono adottate per garantire la massima trasparenza e tutela nei confronti degli studenti, del personale docente e non docente, assicurando al contempo la conformità alle normative sulla protezione dei dati personali.

Rischi

Accesso illegittimo ai dati (A)

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

Violazione della privacy: gli interessati potrebbero vedere le proprie informazioni personali e sensibili esposte a terzi non autorizzati, il che potrebbe violare la loro privacy.

Perdita di dati, anche appartenenti a categorie particolari (ex sensibili): il rischio di perdere dati sensibili o di proprietà potrebbe avere conseguenze finanziarie o legali per gli interessati.

Violazione dei regolamenti sulla protezione dei dati: un accesso illegittimo potrebbe portare a una violazione delle leggi sulla protezione dei dati, con possibili conseguenze legali o sanzioni.

Danno alla reputazione: una violazione della sicurezza potrebbe danneggiare la reputazione degli interessati, sia a livello personale che professionale.

Quali sono le principali minacce e le fonti del rischio?

Phishing: gli attaccanti possono utilizzare messaggi di phishing per indurre gli utenti a condividere le proprie credenziali, consentendo loro di accedere in modo fraudolento ai dati.

Violazione delle credenziali: le credenziali degli utenti, come password o chiavi di accesso, possono essere compromesse o rubate, consentendo l'accesso non autorizzato.

Attacchi di forza bruta: gli attaccanti possono tentare di indovinare le password degli account utilizzando attacchi di forza bruta o dizionario.

Vulnerabilità del software: le vulnerabilità nel software utilizzato per l'accesso al Registro Elettronico possono essere sfruttate per ottenere accesso non autorizzato.

Accesso fisico non autorizzato: qualcuno potrebbe ottenere fisicamente un dispositivo utilizzato per accedere al Registro Elettronico e accedere ai dati.

Accesso a causa di errori umani: gli errori umani, come la configurazione errata delle autorizzazioni, possono aprire la porta a accessi non autorizzati.

Attacchi mirati (Spear Phishing): gli attaccanti possono condurre attacchi mirati a specifici utenti o organizzazioni, cercando di ottenere le loro credenziali.

Malware: l'installazione di malware nei dispositivi degli utenti può consentire agli attaccanti di monitorare le attività e ottenere l'accesso ai dati.

Accesso da dispositivi smarriti o rubati: se dispositivi contenenti l'accesso al Registro Elettronico vengono smarriti o rubati, ciò potrebbe portare all'accesso non autorizzato ai dati.

Accesso da parte di ex dipendenti o utenti precedentemente autorizzati: ex dipendenti o utenti con accesso precedentemente autorizzato potrebbero utilizzare le loro credenziali per accedere illegittimamente ai dati.

Formazione carente del personale: la condivisione errata dei dati tra il personale che non appartengono allo stesso gruppo di lavoro è una fonte del rischio concreta.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo e gestione degli account di accesso e futura integrazione con i sistemi di identità digitale SPID tenendo anche in considerazione la piattaforma di autenticazione messa a disposizione dal Ministero, la c.d. «Gateway delle identità» o «eID Gateway», la quale agevola l'integrazione con i sistemi «Entra con SPID» e «Entra con CIE». Il «Gateway delle identità» supporta anche l'utilizzo dello SPID Minori, consentendo agli alunni e agli studenti minorenni di poter utilizzare i servizi sia tramite SPID che CIE.

Minimizzazione dei dati: raccogliere e trattare solo i dati strettamente necessari per le finalità previste, riducendo al minimo le informazioni personali gestite.

Lotta contro il malware: implementare software antivirus e antimalware aggiornati per prevenire infezioni e accessi non autorizzati.

Manutenzione dei sistemi hardware in uso a scuola: garantire il corretto funzionamento e l'aggiornamento delle apparecchiature per prevenire malfunzionamenti e vulnerabilità.

Backup dei dati presenti nella piattaforma: eseguire copie di sicurezza periodiche dei dati per garantire il recupero in caso di perdita o attacco informatico.

Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati: cancellare regolarmente i documenti non più necessari per evitare trattamenti prolungati e inutili dei dati personali.

Tracciabilità delle operazioni effettuate online: registrare e monitorare le attività svolte sulla piattaforma per garantire trasparenza e responsabilità.

Continuo monitoraggio e risoluzione delle vulnerabilità del sistema: effettuare controlli costanti per individuare e correggere eventuali punti deboli nella sicurezza.

Contratto con il responsabile del trattamento: stipulare accordi formali con soggetti terzi che trattano dati per conto della scuola, definendo responsabilità e obblighi.

Politica di tutela della privacy: definire e adottare misure tecniche e organizzative per garantire la protezione dei dati personali.

Formazione specifica del personale e degli interessati: educare il personale scolastico e gli utenti sull'importanza della protezione dei dati e sulle buone pratiche da adottare.

Gestione online dei dispositivi mobili che hanno accesso alla piattaforma: controllare e proteggere i dispositivi mobili (es. tablet, smartphone) utilizzati per accedere ai dati scolastici.

Sicurezza dei canali informatici: utilizzare connessioni protette (es. HTTPS, VPN) per evitare intercettazioni e accessi non autorizzati.

Sicurezza dell'hardware: proteggere fisicamente gli strumenti informatici da furti, danni o usi impropri.

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali: predisporre procedure per identificare, segnalare e risolvere rapidamente eventuali problemi di sicurezza o violazioni.

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

Limitata.

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

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

Limitata.

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

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

Rischi

Modifiche indesiderate dei dati (M)

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

Violazione della privacy: gli interessati potrebbero vedere le proprie informazioni personali e sensibili esposte a terzi non autorizzati, il che potrebbe violare la loro privacy.

Corruzione dei Dati: i dati potrebbero essere corrotti o danneggiati, rendendoli inutilizzabili o non affidabili.

Errore nei documenti o comunicazioni: le modifiche non autorizzate potrebbero influire sulla correttezza di documenti, comunicazioni o rapporti.

Perdita di dati, anche appartenenti a categorie particolari (ex sensibili): le modifiche indesiderate potrebbero portare alla perdita di dati importanti o sensibili.

Violazione dei regolamenti sulla protezione dei dati: un accesso illegittimo potrebbe portare a una violazione delle leggi sulla protezione dei dati, con possibili conseguenze legali o sanzioni.

Danno alla reputazione: una violazione della sicurezza potrebbe danneggiare la reputazione degli interessati, sia a livello personale che professionale.

Interruzione delle attività: il recupero da una violazione potrebbe richiedere tempo e risorse, interrompendo le normali attività degli interessati.

Quali sono le principali minacce e le fonti del rischio?

Phishing: gli attaccanti possono utilizzare messaggi di phishing per indurre gli utenti a condividere le proprie credenziali, consentendo loro di accedere in modo fraudolento ai dati.

Violazione delle credenziali: le credenziali degli utenti, come password o chiavi di accesso, possono essere compromesse o rubate, consentendo l'accesso non autorizzato.

Attacchi di forza bruta: gli attaccanti possono tentare di indovinare le password degli account utilizzando attacchi di forza bruta o dizionario.

Vulnerabilità del software: le vulnerabilità nel software utilizzato per l'accesso al Registro Elettronico possono essere sfruttate per ottenere accesso non autorizzato.

Accesso fisico non autorizzato: qualcuno potrebbe ottenere fisicamente un dispositivo utilizzato per accedere al Registro Elettronico e accedere ai dati.

Accesso a causa di errori umani: gli errori umani, come la configurazione errata delle autorizzazioni, possono aprire la porta a accessi non autorizzati.

Attacchi mirati (Spear Phishing): gli attaccanti possono condurre attacchi mirati a specifici utenti o organizzazioni, cercando di ottenere le loro credenziali.

Malware: l'installazione di malware nei dispositivi degli utenti può consentire agli attaccanti di monitorare le attività e ottenere l'accesso ai dati.

Accesso da dispositivi smarriti o rubati: se dispositivi contenenti l'accesso al Registro Elettronico vengono smarriti o rubati, ciò potrebbe portare all'accesso non autorizzato ai dati.

Accesso da parte di ex dipendenti o utenti precedentemente autorizzati: ex dipendenti o utenti con accesso precedentemente autorizzato potrebbero utilizzare le loro credenziali per accedere illegittimamente ai dati.

Formazione carente del personale: la condivisione errata dei dati tra il personale che non appartengono allo stesso gruppo di lavoro è una fonte del rischio concreta.

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

Controllo e gestione degli account di accesso e futura integrazione con i sistemi di identità digitale SPID tenendo anche in considerazione la piattaforma di autenticazione messa a disposizione dal Ministero, la c.d. «Gateway delle identità» o «eID Gateway», la quale agevola l'integrazione con i sistemi «Entra con SPID» e «Entra con CIE». Il «Gateway delle identità» supporta anche l'utilizzo dello SPID Minori, consentendo agli alunni e agli studenti minorenni di poter utilizzare i servizi sia tramite SPID che CIE.

Minimizzazione dei dati: raccogliere e trattare solo i dati strettamente necessari per le finalità previste, riducendo al minimo le informazioni personali gestite.

Lotta contro il malware: implementare software antivirus e antimalware aggiornati per prevenire infezioni e accessi non autorizzati.

Manutenzione dei sistemi hardware in uso a scuola: garantire il corretto funzionamento e l'aggiornamento delle apparecchiature per prevenire malfunzionamenti e vulnerabilità.

Backup dei dati presenti nella piattaforma: eseguire copie di sicurezza periodiche dei dati per garantire il recupero in caso di perdita o attacco informatico.

Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati: cancellare regolarmente i documenti non più necessari per evitare trattamenti prolungati e inutili dei dati personali.

Tracciabilità delle operazioni effettuate online: registrare e monitorare le attività svolte sulla piattaforma per garantire trasparenza e responsabilità.

Continuo monitoraggio e risoluzione delle vulnerabilità del sistema: effettuare controlli costanti per individuare e correggere eventuali punti deboli nella sicurezza.

Contratto con il responsabile del trattamento: stipulare accordi formali con soggetti terzi che trattano dati per conto della scuola, definendo responsabilità e obblighi.

Politica di tutela della privacy: definire e adottare misure tecniche e organizzative per garantire la protezione dei dati personali.

Formazione specifica del personale e degli interessati: educare il personale scolastico e gli utenti sull'importanza della protezione dei dati e sulle buone pratiche da adottare.

Gestione online dei dispositivi mobili che hanno accesso alla piattaforma: controllare e proteggere i dispositivi mobili (es. tablet, smartphone) utilizzati per accedere ai dati scolastici.

Sicurezza dei canali informatici: utilizzare connessioni protette (es. HTTPS, VPN) per evitare intercettazioni e accessi non autorizzati.

Sicurezza dell'hardware: proteggere fisicamente gli strumenti informatici da furti, danni o usi impropri.

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali: predisporre procedure per identificare, segnalare e risolvere rapidamente eventuali problemi di sicurezza o violazioni.

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

Trascurabile.

Le misure di sicurezza implementate, in particolar modo quello legato al backup dei dati, e la limitazione dei dati personali a quelli strettamente necessari per le attività didattiche riducono significativamente la gravità dei potenziali rischi.

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

Limitata.

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

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

Rischi

Perdita di dati (P)

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

Corruzione dei Dati: i dati potrebbero essere corrotti o danneggiati, rendendoli inutilizzabili o non affidabili.

Interruzione delle attività: il recupero da una violazione potrebbe richiedere tempo e risorse, interrompendo le normali attività degli interessati.

Perdita di dati, anche appartenenti a categorie particolari (ex sensibili): l'evento potrebbe portare alla perdita di dati importanti o sensibili.

Violazione dei regolamenti sulla protezione dei dati: la perdita di dati potrebbe portare a una violazione delle leggi sulla protezione dei dati, con possibili conseguenze legali o sanzioni.

Danno alla reputazione: una violazione della sicurezza potrebbe danneggiare la reputazione degli interessati, sia a livello personale che professionale.

Interruzione delle attività: il recupero da una violazione potrebbe richiedere tempo e risorse, interrompendo le normali attività degli interessati.

Quali sono le principali minacce e le fonti del rischio?

Phishing: gli attaccanti possono utilizzare messaggi di phishing per indurre gli utenti a condividere le proprie credenziali, consentendo loro di accedere in modo fraudolento ai dati.

Violazione delle credenziali: le credenziali degli utenti, come password o chiavi di accesso, possono essere compromesse o rubate, consentendo l'accesso non autorizzato.

Attacchi di forza bruta: gli attaccanti possono tentare di indovinare le password degli account utilizzando attacchi di forza bruta o dizionario.

Vulnerabilità del software: le vulnerabilità nel software utilizzato per l'accesso al Registro Elettronico possono essere sfruttate per ottenere accesso non autorizzato.

Accesso fisico non autorizzato: qualcuno potrebbe ottenere fisicamente un dispositivo utilizzato per accedere al Registro Elettronico e accedere ai dati.

Accesso a causa di errori umani: gli errori umani, come la configurazione errata delle autorizzazioni, possono aprire la porta a accessi non autorizzati.

Attacchi mirati (Spear Phishing): gli attaccanti possono condurre attacchi mirati a specifici utenti o organizzazioni, cercando di ottenere le loro credenziali.

Malware: l'installazione di malware nei dispositivi degli utenti può consentire agli attaccanti di monitorare le attività e ottenere l'accesso ai dati.

Accesso da dispositivi smarriti o rubati: se dispositivi contenenti l'accesso al Registro Elettronico vengono smarriti o rubati, ciò potrebbe portare all'accesso non autorizzato ai dati.

Accesso da parte di ex dipendenti o utenti precedentemente autorizzati: ex dipendenti o utenti con accesso precedentemente autorizzato potrebbero utilizzare le loro credenziali per accedere illegittimamente ai dati.

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

Controllo e gestione degli account di accesso e futura integrazione con i sistemi di identità digitale SPID tenendo anche in considerazione la piattaforma di autenticazione messa a disposizione dal Ministero, la c.d. «Gateway delle identità» o «eID Gateway», la quale agevola l'integrazione con i sistemi «Entra con SPID» e «Entra con CIE». Il «Gateway delle identità» supporta anche l'utilizzo dello SPID Minori, consentendo agli alunni e agli studenti minorenni di poter utilizzare i servizi sia tramite SPID che CIE.

Minimizzazione dei dati: raccogliere e trattare solo i dati strettamente necessari per le finalità previste, riducendo al minimo le informazioni personali gestite.

Lotta contro il malware: implementare software antivirus e antimalware aggiornati per prevenire infezioni e accessi non autorizzati.

Manutenzione dei sistemi hardware in uso a scuola: garantire il corretto funzionamento e l'aggiornamento delle apparecchiature per prevenire malfunzionamenti e vulnerabilità.

Backup dei dati presenti nella piattaforma: eseguire copie di sicurezza periodiche dei dati per garantire il recupero in caso di perdita o attacco informatico.

Tracciabilità delle operazioni effettuate online: registrare e monitorare le attività svolte sulla piattaforma per garantire trasparenza e responsabilità.

Continuo monitoraggio e risoluzione delle vulnerabilità del sistema: effettuare controlli costanti per individuare e correggere eventuali punti deboli nella sicurezza.

Contratto con il responsabile del trattamento: stipulare accordi formali con soggetti terzi che trattano dati per conto della scuola, definendo responsabilità e obblighi.

Politica di tutela della privacy: definire e adottare misure tecniche e organizzative per garantire la protezione dei dati personali.

Formazione specifica del personale e degli interessati: educare il personale scolastico e gli utenti sull'importanza della protezione dei dati e sulle buone pratiche da adottare.

Gestione online dei dispositivi mobili che hanno accesso alla piattaforma: controllare e proteggere i dispositivi mobili (es. tablet, smartphone) utilizzati per accedere ai dati scolastici.

Sicurezza dei canali informatici: utilizzare connessioni protette (es. HTTPS, VPN) per evitare intercettazioni e accessi non autorizzati.

Sicurezza dell'hardware: proteggere fisicamente gli strumenti informatici da furti, danni o usi impropri.

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali: predisporre procedure per identificare, segnalare e risolvere rapidamente eventuali problemi di sicurezza o violazioni.

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

Trascurabile.

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

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

Trascurabile.

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

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

Panoramica dei principi, misure e rischi analizzati

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Diritto di accesso e diritto alla portabilità dei dati
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

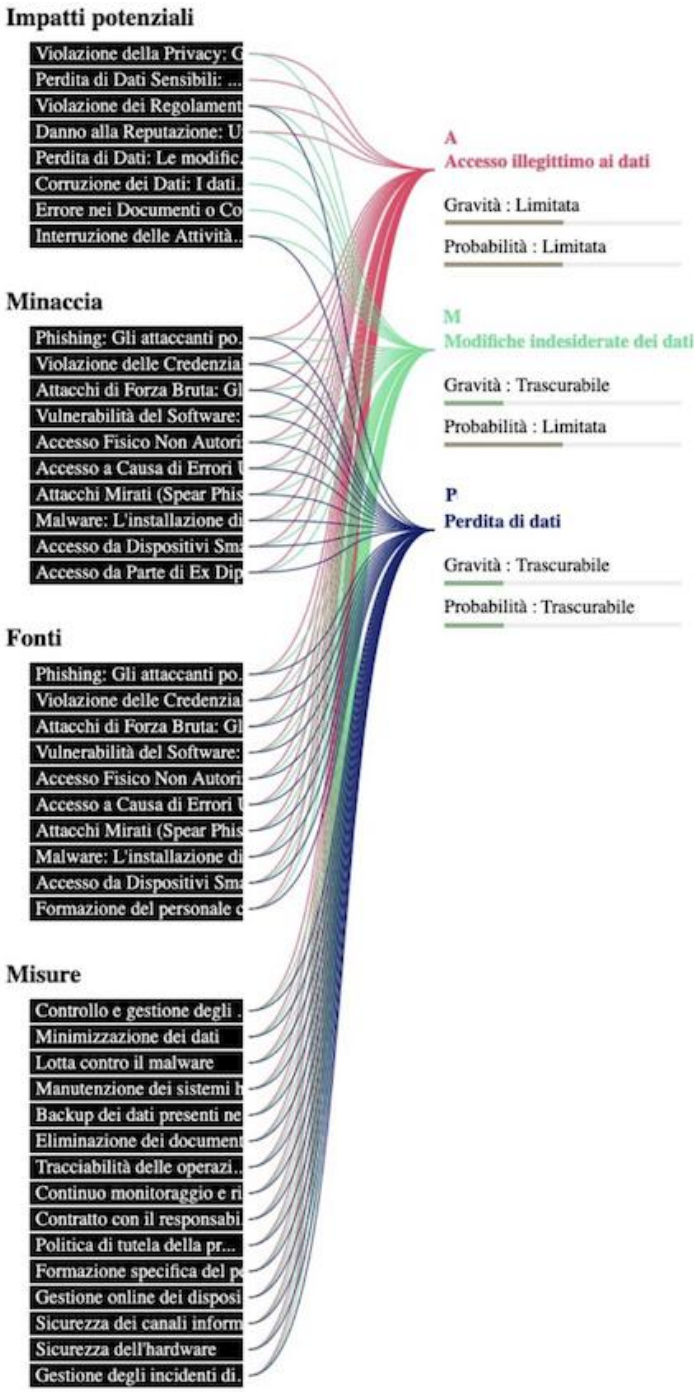
Misure esistenti o pianificate

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

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Panoramica dei rischi analizzati

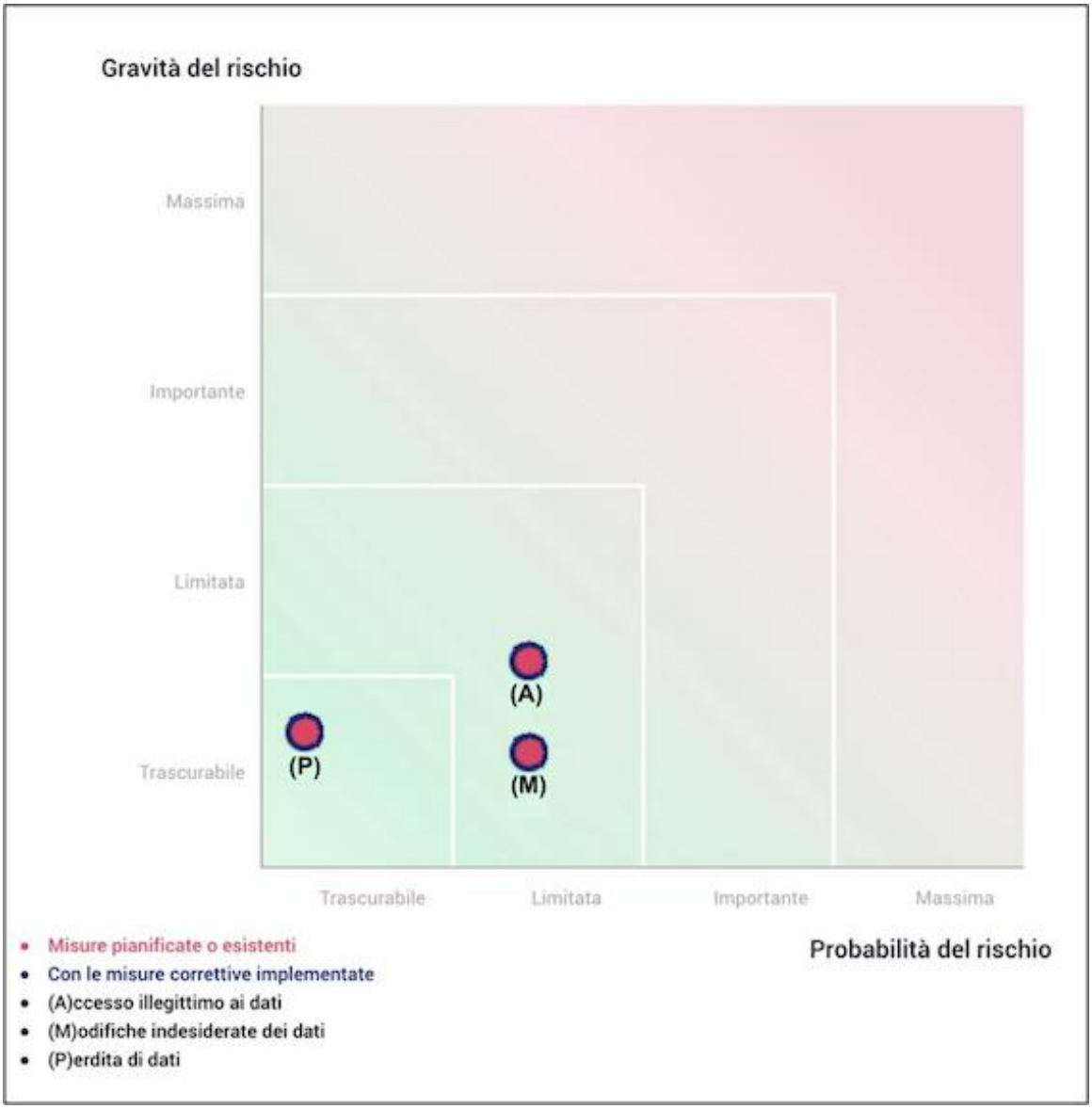


Panoramica dei piani di azione

Sezione	Titolo	Commento sul piano di azione	Data stimata di implementazione	Soggetto responsabile
Misure esistenti o pianificate				
	Controllo e gestione degli account di accesso		Inizio a.s. riferimento	Referente del RE
	Minimizzazione dei dati	always on		Docenti
	Lotta contro il malware	always on		Responsabile del Trattamento
	Manutenzione dei sistemi hardware in uso a scuola	always on		Animatore Digitale, personale tecnico e ditte esterne incaricate
	Backup dei dati presenti nella piattaforma	always on		Responsabile del Trattamento
	Eliminazione dei documenti nell'ottica di ridurre il ciclo di vita del trattamento dei dati		Inizio a.s. riferimento	
	Tracciabilità delle operazioni effettuate online	always on		Responsabile del Trattamento
	Continuo monitoraggio e risoluzione delle vulnerabilità del sistema	always on		Responsabile del Trattamento
	Contratto con il responsabile del trattamento		Inizio a.s. riferimento	Dirigente Scolastico
	Politica di tutela della privacy: misure tecniche ed organizzative da adottare		Inizio a.s. riferimento	Dirigente Scolastico
	Formazione specifica del personale e degli interessati		Inizio a.s. riferimento	Dirigente Scolastico
	Sicurezza dei canali informatici	always on		Responsabile del Trattamento

	Sicurezza dell'hardware	always on		Animatore Digitale, personale tecnico e ditte esterne incaricate
	Gestione degli incidenti di sicurezza e dele violazioni dei dati personali	always on		Dirigente Scolastico, Referente del RE
Accesso illegittimo ai dati				
	Accesso illegittimo ai dati	always on		Dirigente Scolastico, Referente del RE
Modifiche indesiderate dei dati				
	Modifiche indesiderate dei dati	always on		Dirigente Scolastico, Referente del RE
Perdita di dati				
	Perdita di dati	always on		Dirigente Scolastico, Referente del RE

Mappa dei rischi



Data: si veda segnatura di protocollo

Il Titolare del Trattamento
Il Dirigente Scolastico
Dott.ssa Paola Gallo

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 e ss.mm.ii. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa