EUSERVICE

Valutazione d'impatto sulla protezione dei dati

I.C. - "G. MICALI"-LIVORNO
Prot. 0005732 del 23/06/2025
VI (Uscita)

Descrizione del Contesto

La presente valutazione d'impatto è redatta in conformità alle principali linee guida e buone prassi in materia di protezione dei dati personali, con particolare riferimento a:

- il **"Manuale sulla sicurezza nel trattamento dei dati personali"** elaborato dall'**Agenzia dell'Unione europea per la cybersicurezza (ENISA)**, pubblicato nel dicembre 2017, il quale fornisce indicazioni operative per l'adozione di misure tecniche e organizzative adeguate;
- la **metodologia proposta dalla Commission Nationale de l'Informatique et des Libertés (CNIL)**, autorità francese per la protezione dei dati, la quale costituisce un riferimento consolidato per l'elaborazione di DPIA efficaci e orientate alla gestione del rischio.

Sotto il profilo normativo, la base giuridica per l'introduzione e l'utilizzo del registro elettronico nelle istituzioni scolastiche trova fondamento nell'art. 7, comma 31, del **Decreto-Legge 6 luglio 2012, n. 95**, convertito con modificazioni dalla Legge 7 agosto 2012, n. 135, il quale stabilisce che:

> *"A decorrere dall'anno scolastico 2012/2013, le istituzioni scolastiche e i docenti adottano registri on line e inviano le comunicazioni agli alunni e alle famiglie in formato elettronico".*

Ulteriori indicazioni operative sono state fornite dal **Garante per la protezione dei dati personali** con il provvedimento del 26 marzo 2020, nel quale si ribadisce che compete alle istituzioni scolastiche e universitarie, in qualità di titolari del trattamento, la selezione degli strumenti più idonei alla didattica digitale, anche sulla base delle indicazioni provenienti dalle autorità competenti. Tale scelta deve essere condotta nel rispetto dei **principi di "privacy by design" e "by default"** (artt. 25 e 24 del Regolamento (UE) 2016/679), tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà fondamentali degli interessati.

Infine, con **Nota n. 788 del 31 gennaio 2025**, il **Ministero dell'Istruzione e del Merito (MIM)** ha richiamato l'attenzione delle istituzioni scolastiche ed educative statali sulla necessità di garantire un utilizzo corretto e conforme degli strumenti digitali. Nella medesima nota, il Ministero ha evidenziato l'obbligo, in capo al Titolare del trattamento, di procedere alla redazione di una **valutazione d'impatto (DPIA)** ai sensi degli articoli 35 e seguenti del Regolamento (UE) 2016/679, al fine di identificare preventivamente i rischi derivanti dall'impiego delle piattaforme elettroniche e definire le misure di mitigazione più adeguate.

Nel rispetto di tale indicazione ministeriale, nonché delle previsioni normative europee e nazionali in materia di protezione dei dati personali, si procede dunque alla presente valutazione d'impatto.

Finalità e base giuridica

Il trattamento dei dati personali effettuato per il tramite del sistema di Registro Elettronico trova il proprio fondamento giuridico nell'articolo 6, paragrafo 1, lettera e), nonché nel paragrafo 3, lettera b), e nell'articolo 9, paragrafo 2, lettera g), del **Regolamento (UE) 2016/679** (di seguito, anche "Regolamento" o "GDPR"), che legittimano il trattamento in quanto necessario all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare. Tali disposizioni trovano ulteriore riscontro e specificazione negli articoli 2-ter e 2-sexies del **Decreto Legislativo 30 giugno 2003, n. 196** (di seguito, anche "Codice"), come modificato dal D.lgs. 10 agosto 2018, n. 101.

Rientrano in tale ambito anche i trattamenti di categorie particolari di dati personali, laddove funzionali all'inclusione scolastica, alla personalizzazione dei percorsi educativi, ovvero all'adempimento di obblighi derivanti da norme primarie e secondarie in materia di istruzione, con specifico riferimento anche alla tutela degli studenti con disabilità o con bisogni educativi speciali.

L'utilizzo di strumenti digitali per lo svolgimento dell'attività didattica e amministrativa è, del resto, previsto da normativa settoriale specifica. In tal senso, l'articolo 7, comma 31, del **Decreto-Legge 6 luglio 2012, n. 95**, convertito con modificazioni dalla Legge 7 agosto 2012, n. 135, come si diceva, ha introdotto l'obbligo, a decorrere dall'anno scolastico 2012/2013, per le istituzioni scolastiche e per il corpo docente, di adottare registri in formato elettronico e di effettuare le comunicazioni con studenti e famiglie attraverso modalità telematiche.

Alla luce di tale quadro normativo, deve ritenersi che il trattamento dei dati personali connesso all'impiego del Registro Elettronico sia lecito anche in assenza di uno specifico consenso da parte degli interessati (studenti, genitori, docenti), in quanto riconducibile a funzioni istituzionali svolte nell'ambito dell'esercizio di compiti di interesse pubblico rilevante.

Il trattamento è finalizzato al perseguimento di scopi **determinati, espliciti e legittimi**, e viene effettuato nel rispetto del principio di limitazione delle finalità. In particolare, le attività svolte tramite il Registro Elettronico rispondono alle seguenti esigenze funzionali:

- **Gestione dell'attività didattica**: rilevazione e registrazione delle presenze, assenze, ritardi, giustificazioni, annotazioni disciplinari e osservazioni didattiche riferite al singolo studente;
- **Valutazione del rendimento scolastico**: inserimento, conservazione e comunicazione dei voti, giudizi intermedi e finali, esiti di prove scritte, orali e pratiche;
- **Comunicazione istituzionale tra scuola e famiglie**: trasmissione di avvisi, circolari, convocazioni, materiali didattici e notifiche inerenti alla carriera scolastica degli alunni;
- **Gestione amministrativa e documentale**: archiviazione digitale di atti amministrativi e documenti scolastici (es. verbali, pagelle, certificazioni), nel rispetto della normativa vigente in materia di trasparenza, digitalizzazione e conservazione;
- **Supporto agli organi collegiali**: utilizzo della piattaforma per la convocazione e verbalizzazione delle sedute degli organi scolastici (Consiglio di Classe, Collegio Docenti, Consiglio d'Istituto, ecc.);
- **Adempimento di obblighi normativi**: conformità alle disposizioni impartite dal Ministero dell'Istruzione e del Merito e agli obblighi normativi in materia di innovazione tecnologica nella pubblica amministrazione.

Tutte le predette attività si svolgono nel rispetto dei **principi generali applicabili al trattamento dei dati personali**, come sanciti dall'articolo 5 del GDPR, ed in particolare: liceità, correttezza, trasparenza, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, nonché responsabilizzazione del titolare (principio di accountability).

Con riferimento ai **fornitori della piattaforma di accesso al registro elettronico**, operanti in qualità di responsabili del trattamento ex art. 28 del GDPR, si evidenzia che il trattamento da essi effettuato deve limitarsi a quanto strettamente necessario per l'erogazione dei servizi richiesti dall'istituto scolastico, ed essere conforme alle istruzioni ricevute dal titolare.

Nel caso in cui il fornitore, per determinate attività, operi quale **titolare autonomo del trattamento**, è tenuto al pieno rispetto degli obblighi informativi previsti dall'articolo 13 del Regolamento, nonché a garantire la sussistenza di una valida base giuridica e l'adozione di misure tecniche e organizzative adeguate.

In ogni caso, risulta **illegittimo subordinare l'accesso ai servizi di didattica digitale alla prestazione di un consenso da parte dell'interessato per trattamenti non strettamente necessari**, in quanto tale consenso non potrebbe considerarsi liberamente prestato, configurandosi un indebito condizionamento, in violazione dell'articolo 7 del Regolamento e del considerando 43.

Da ultimo, si richiama quanto disposto dal **considerando 38 del GDPR**, secondo cui i minori di età devono beneficiare di una protezione rafforzata relativamente al trattamento dei dati personali che li riguardano, in ragione della loro presumibile minore consapevolezza dei rischi connessi al trattamento, delle possibili conseguenze e dei diritti a essi riconosciuti. Particolare cautela deve essere osservata in relazione all'utilizzo dei dati dei minori per finalità ulteriori rispetto a quelle didattiche, segnatamente in ambito promozionale, commerciale o profilatorio.

EUSERVICE

Dati trattati, principio di minimizzazione

Il **principio di minimizzazione dei dati** impone che i dati personali oggetto di trattamento siano:

"adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".

Tale principio vincola il titolare del trattamento a raccogliere ed elaborare **solo ed esclusivamente** quei dati che risultano **strettamente indispensabili** al raggiungimento delle **finalità determinate, esplicite e legittime** dichiarate ex art. 5, par. 1, lett. b) del GDPR. Ciò comporta il **divieto di trattare dati eccedenti**, non pertinenti o raccolti "in via precauzionale", e impone una **valutazione preventiva della necessità di ciascun dato rispetto allo scopo perseguito.**

L'applicazione concreta del principio richiede:

- la **limitazione della raccolta** iniziale dei dati;
- la **restrizione dell'accesso** ai soli soggetti autorizzati in base al principio del "need to know";
- l'**adozione di misure tecniche e organizzative** per impedire il trattamento non necessario (es. mascheramento, pseudonimizzazione, anonimizzazione);
- la **verifica periodica** della pertinenza e dell'aggiornamento dei dati detenuti.

L'utilizzo del sistema di Registro Elettronico comporta il trattamento di una pluralità di dati personali riferibili a differenti categorie di interessati, tra cui alunni, studenti, genitori o esercenti la responsabilità genitoriale, docenti, personale amministrativo e, in taluni casi, fornitori. In funzione delle attività svolte e delle specificità del sistema impiegato (sia in modalità client/server che su piattaforma web-based), i dati oggetto di trattamento possono includere informazioni di natura anagrafica, fiscale, amministrativa e contabile, nonché — in circostanze determinate e giuridicamente giustificate — dati rientranti nelle categorie particolari di cui all'articolo 9 del GDPR, nonché dati relativi a condanne penali o reati ai sensi dell'articolo 10 del medesimo Regolamento.

Il trattamento dei dati personali avviene nel rigoroso rispetto del principio di minimizzazione, sancito dall'art. 5, par. 1, lett. c) del GDPR, in forza del quale i dati raccolti devono essere adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità perseguite. In tale prospettiva, il registro elettronico è strutturato in modo da contenere esclusivamente le informazioni indispensabili per lo svolgimento delle funzioni istituzionali dell'istituto scolastico. Tra tali informazioni rientrano: dati identificativi e di contatto degli studenti e delle loro famiglie, dati relativi alla frequenza scolastica (assenze, presenze, ritardi, giustificazioni), valutazioni periodiche, giudizi finali, annotazioni didattiche e disciplinari, nonché comunicazioni ufficiali da parte dell'istituzione.

Con riguardo al trattamento di categorie particolari di dati personali, quali quelli relativi alla salute, all'origine etnica, alle convinzioni religiose o alla situazione familiare degli studenti, si precisa che tali dati devono essere trattati esclusivamente nei casi in cui risultino strettamente indispensabili per l'adempimento di obblighi giuridici o per la predisposizione di misure di supporto previste dalla normativa (es. piani didattici personalizzati, gestione delle allergie alimentari, sostegni per DSA/BES). In tali ipotesi, il trattamento avverrà con l'adozione di specifiche misure tecniche e organizzative di protezione, quali la limitazione degli accessi ai soli soggetti legittimati, l'impiego di codificazioni o tecniche di pseudonimizzazione, e l'esclusione di diciture palesi o facilmente riconducibili all'interessato.

È fatto assoluto divieto di rendere visibili o accessibili tali dati a soggetti non autorizzati, ivi compresi altri genitori o studenti.

Liceità e correttezza del trattamento

Il **principio di liceità** prevede che ogni trattamento di dati personali sia **giuridicamente giustificato**, ossia fondato su una delle **basi giuridiche previste dall'articolo 6 del GDPR** (quali, a titolo esemplificativo: consenso esplicito dell'interessato; esecuzione di

un contratto; adempimento di un obbligo legale; salvaguardia di interessi vitali; esecuzione di un compito di interesse pubblico; perseguimento del legittimo interesse del titolare).

Un trattamento è **illecito** se effettuato in assenza di una base giuridica valida, ovvero in violazione dei limiti imposti dalla norma applicabile, con conseguente responsabilità del titolare.

Il **principio di correttezza** (fairness) impone che il trattamento dei dati personali sia effettuato in **modo leale, trasparente e non discriminatorio** nei confronti dell'interessato, nel rispetto delle sue **aspettative legittime** e della **fiducia riposta nel titolare del trattamento**.

La correttezza implica, tra l'altro:

- che i dati non siano raccolti o trattati con modalità **ingannevoli o manipolative**;
- che non vengano utilizzati in modi **sproporzionati, lesivi o imprevisti** rispetto a quanto dichiarato;
- che siano rispettati i diritti e le libertà fondamentali dell'interessato, inclusi il diritto all'informazione, all'accesso, alla rettifica e all'opposizione.

L'istituzione scolastica ha assicurato il rispetto dei principi di liceità, correttezza e trasparenza del trattamento, provvedendo a rendere un'informativa chiara, completa e accessibile agli interessati, in conformità con l'articolo 13 del Regolamento (UE) 2016/679. Tale informativa è stata predisposta in un linguaggio semplice e comprensibile anche da parte degli studenti minorenni, ed è stata resa disponibile attraverso i canali di comunicazione ufficiali dell'istituto (registro elettronico, sito web istituzionale, comunicazioni via e-mail), al fine di garantire la massima diffusione e comprensione.

L'informativa descrive in modo trasparente le finalità del trattamento, i soggetti coinvolti, i tempi di conservazione, la base giuridica, nonché i diritti esercitabili da parte degli interessati. Il trattamento dei dati è stato circoscritto esclusivamente alle attività strettamente necessarie all'utilizzo del registro elettonico, nel pieno rispetto della riservatezza, della dignità e dei diritti fondamentali degli studenti, come previsto dall'articolo 1 del D.P.R. 24 giugno 1998, n. 249 (Statuto delle studentesse e degli studenti).

Con riguardo al personale docente, l'istituto ha adottato specifiche misure organizzative e tecniche finalizzate a garantire un utilizzo degli strumenti informatici conforme ai limiti previsti dalla normativa vigente. In particolare, sono state osservate le disposizioni di cui agli articoli 5 e 88, par. 2 del GDPR, all'articolo 114 del Codice in materia di protezione dei dati personali, nonché all'articolo 4 della Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori).

L'impiego delle piattaforme e dei dispositivi digitali è stato configurato in modo tale da limitarsi alle sole funzionalità necessarie allo svolgimento dell'attività didattica, evitando in ogni caso qualsiasi forma di controllo indiretto o surrettizio sull'operato del docente, o forme di interferenza nella sua libertà di insegnamento. Non è stato effettuato alcun trattamento volto a indagare aspetti della sfera privata del personale (cfr. art. 113 del Codice), né sono stati raccolti o elaborati dati eccedenti o non pertinenti rispetto alle finalità istituzionali.

Necessità e proporzionalità del trattamento

Si valuta se il trattamento dei dati proposto è necessario per le finalità del trattamento. Si tiene conto dei principi di proporzionalità e sussidiarietà.

a) Proporzionalità: la violazione della privacy e la protezione dei dati personali dell'interessato sono proporzionate alle finalità del trattamento?

b) Sussidiarietà: gli obiettivi del trattamento non possono essere raggiunti in un altro modo che sia meno dannoso per gli interessati? Sono indicate eventuali alternative?

EUSERVICE

In primo luogo si ricorda che il servizio in esame **è obbligatorio per legge.**

La finalità della norma è quella di rendere più agevole lo scambio di informazioni dalla scuola verso utenti e famiglie.

Il trattamento dei dati è quindi assolutamente necessario e inevitabile per l'elaborazione dei dati.

a) **Proporzionalità:** l'elaborazione dei dati degli studenti e delle famiglie comporta un potenziale pericolo ulteriore per la loro privacy (specie in caso di data breach). Tuttavia, l'intento della norma, porta a ritenere questo rischio proporzionato rispetto ai potenziali danni.

b) **Sussidiarietà:** l'utilizzo di un registro elettronico, potrebbe sicuramente essere sostituito dal registro cartaceo; tuttavia, e finalità perseguite dalla legge verrebbero mortificate.

Diritti degli interessati

Non vi è alcuna limitazione dei diritti degli interessati.

Il titolare si impegna, anche attraverso l'accordo con i responsabili del trattamento, ad adottare tutte le misure necessarie per garantire che gli interessati possano esercitare i loro diritti in qualsiasi momento.

Si prendono in considerazione le procedure messe in atto dal titolare per dare riscontro all'esercizio da parte degli interessati dei diritti indicati dall'art 15 e ss. GDPR. Si ricorda infatti che, ai sensi dell'art. 28 par. 3 lett. e).

Gli interessati vengono informati circa l'esercizio dei propri diritti indicati dall'art. 15 e ss. GDPR mediante apposita informativa privacy ai segni degli artt. 13 e 14 GDPR.

L'esercizio dei diritti da parte degli interessati avviene mediante l'invio di una e-mail all'indirizzo del titolare.

Misure di sicurezza adottate

Il servizio oggetto della presente valutazione è stato **qualificato presso l'Agenzia per la Cybersicurezza Nazionale (ACN)**, in conformità al **Regolamento adottato ai sensi dell'articolo 17 del Regolamento per l'erogazione dei servizi cloud alla Pubblica Amministrazione**, raggiungendo il **Livello di Qualificazione 1 (QC1)**.

Tale qualificazione costituisce **indicatore di elevata affidabilità tecnica, organizzativa e giuridica**, ed è subordinata al rispetto di stringenti requisiti in materia di **sicurezza, continuità operativa, protezione dei dati personali e trasparenza contrattuale**. In coerenza con quanto previsto dall'articolo 14 del Regolamento ACN, il servizio viene erogato tramite un'infrastruttura cloud qualificata o adeguata per il livello richiesto, assicurando così la piena conformità alle disposizioni normative in materia di **infrastrutture digitali per le pubbliche amministrazioni**.

La presenza di tale qualificazione garantisce che le **misure tecniche e organizzative adottate** siano conformi alle migliori prassi di settore, in linea con gli standard ISO/IEC 27001, 27017 e 27018, e che siano state implementate politiche di sicurezza strutturate, meccanismi di gestione del rischio, sistemi di controllo degli accessi, nonché strumenti di tracciamento e auditing conformi al principio di accountability previsto dal GDPR.

In particolare, si indicano i requisiti soddisfatti dalla piattaforma:

Requisiti per la qualificazione ACN – Livello 1 (QC1)

1. Certificazioni obbligatorie

- **ISO 9001**: Sistema di Gestione per la Qualità (SGQ), con un campo di applicazione che includa almeno le fasi di erogazione del servizio oggetto di qualifica e la prestazione del servizio di assistenza tecnica alla Pubblica Amministrazione italiana.
- **ISO/IEC 27001**: Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), esteso con:

- ISO/IEC 27017: Controlli di sicurezza per i servizi cloud.
- ISO/IEC 27018: Protezione dei dati personali nei servizi cloud pubblici.

- In alternativa, è accettata la certificazione Cloud Security Alliance – STAR Level 2.

2. Requisiti tecnici e organizzativi

- **Tracciabilità e audit**: Implementazione di sistemi di logging e auditing per garantire la tracciabilità delle operazioni.
- **Gestione degli accessi**: Controllo rigoroso degli accessi con autenticazione forte e gestione dei privilegi basata sul principio del minimo privilegio.
- **Protezione dei dati**: Adozione di misure per garantire la riservatezza, integrità e disponibilità dei dati, inclusa la cifratura dei dati in transito e a riposo.
- **Business Continuity e Disaster Recovery**: Piani documentati e testati per assicurare la continuità operativa e il ripristino in caso di incidenti.
- **Conservazione dei dati**: Politiche di retention e cancellazione dei dati conformi alla normativa vigente.

3. Requisiti contrattuali e di trasparenza

- **Service Level Agreement (SLA)**: Definizione chiara dei livelli di servizio, con indicatori di performance e penali in caso di disservizi.
- **Trasparenza dei costi**: Disponibilità di strumenti (es. dashboard) e API per la consultazione dettagliata dei costi del servizio.
- **Monitoraggio dei costi**: Sistemi di allerta per avvisare l'amministrazione nel caso in cui l'utilizzo del servizio si avvicini o superi il budget impostato.
- **Garanzie assicurative**: Coperture assicurative adeguate per garantire lo svolgimento delle attività previste dal contratto.

4. Requisiti di interoperabilità e portabilità

- **Interoperabilità**: Adozione di standard aperti per garantire l'interoperabilità con altri sistemi e servizi.
- **Portabilità dei dati**: Meccanismi per facilitare la migrazione dei dati verso altri fornitori o infrastrutture, in conformità con il principio di portabilità.

5. Obblighi di comunicazione e monitoraggio

- **Censimento delle amministrazioni**: Comunicazione semestrale ad ACN della lista delle amministrazioni che utilizzano i servizi cloud forniti.
- **Monitoraggio continuo**: Impegno a mantenere i requisiti di qualificazione per tutta la durata della validità della qualifica (36 mesi), con possibilità di verifiche da parte di ACN.

Parti coinvolte

Soggetto coinvolto	Descrizione del ruolo e delle attività connesse al trattamento
Dirigente scolastico (Utente Master)	Riveste il ruolo di **Titolare del trattamento** ai sensi dell'art. 4, par. 7, del GDPR. Supervisiona e autorizza le attività di trattamento, individua i soggetti designati, impartisce le istruzioni operative e definisce le modalità di utilizzo della piattaforma. Detiene un profilo di accesso privilegiato

Soggetto coinvolto	Descrizione del ruolo e delle attività connesse al trattamento
	("master") che consente la gestione e la configurazione generale del sistema.
Segreteria scolastica (Utenti con privilegi di modifica)	Personale autorizzato al trattamento, incaricato di svolgere operazioni amministrative, gestionali e documentali. Ha accesso a funzioni di inserimento, modifica e validazione dei dati nel registro, nel rispetto delle istruzioni fornite dal Titolare del trattamento.
Genitori / Esercenti la responsabilità genitoriale	**Interessati** ai sensi del GDPR, accedono in modalità riservata al registro elettronico per consultare le informazioni relative al percorso scolastico dei propri figli minorenni (esiti, frequenze, comunicazioni). Non effettuano operazioni di modifica.
Studenti minorenni	Anch'essi **interessati**, possono accedere al registro in modalità consultazione, secondo quanto stabilito dalla scuola. L'accesso è subordinato a criteri di gradualità e tutela, tenuto conto dell'età e del livello di consapevolezza.
Studenti maggiorenni	In qualità di **interessati**, godono di piena titolarità rispetto ai dati trattati e accedono direttamente al sistema per consultare le informazioni personali, senza intermediazione da parte dei genitori.
Amministratore di sistema	Soggetto designato dal Titolare ai sensi del **provvedimento del Garante del 27 novembre 2008**, responsabile della gestione tecnica, della sicurezza informatica e della configurazione degli accessi. Può accedere ai sistemi per fini manutentivi e diagnostici, nel rispetto del principio di necessità.
Distributore della piattaforma (Responsabile del trattamento)	**Responsabile del trattamento** ex art. 28 GDPR, designato formalmente dal Titolare. Fornisce la piattaforma tecnologica, ne cura lo sviluppo, la manutenzione e l'hosting, attenendosi esclusivamente alle istruzioni documentate ricevute dall'istituzione scolastica.
Sub-responsabili del trattamento	Soggetti terzi ai quali il Responsabile ha delegato parte delle attività, ad esempio: **data center**, fornitori cloud, sviluppatori esterni, soggetti giuridici incaricati della gestione di componenti tecniche. Sono vincolati da contratto specifico (art. 28, par. 4 GDPR) e operano sotto la responsabilità del Responsabile.

Luoghi di elaborazione dei dati

La piattaforma dichiara di trattare i dati nello spazio dell'Unione Europea e che, in caso di trasferimento Extra UE si impegna a munirsi dei meccanismi di tutela previsti dal GDPR.

EUSERVICE

Modalità di elaborazione dei dati

I dati vengono trattati in modo digitale, senza ricorrere a sistemi di profilazione o a sistemi di intelligenza artificiale

Data retention

Trattandosi di servizi SaaS, la data retention è imposta dalla scuola, unico titolare del trattamento.

EUSERVICE

Metodologia per Valutazione dell'Impatto.

L'art. 32 REG. UE N. 679/16, prevede che *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio";*

Si procederà quindi alle valutazioni di cui sopra, basandosi sui parametri di cui alle seguenti tabelle:

FUNZIONE: rischio[1] (R) = impatto (I) X Probabilità (P)

impatto					
	MOLTO ALTO	5	10	15	20
	ALTO	4	8	12	16
	MEDIO	3	6	9	12
	BASSO	2	4	6	8
	MOLTO BASSO	1	2	3	4
		IMPROBABILE	POCO PROBABILE	PROBABILE	ALTAMENTE PROBABILE

probabilità

PARAMETRI DI VALUTAZIONE DEL RISCHIO

MOLTO ALTO	In caso di danneggiamento, distruzione, perdita delle informazioni, i dati compromessi inficerebbero **informazioni particolari e/o giudiziarie** (artt. 9 e 10 del REG. UE n. 679/16), provocando una **lesione irrimediabile** per i diritti e le libertà degli interessati.
ALTO	In caso di danneggiamento o perdita del dato, le informazioni compromesse riguarderebbero dati **comuni** (art. 6 REG. UE n. 679/16) e/o dati **particolari** (art. 9 REG. UE n. 679/16) con conseguenze anche dannose per i diritti degli interessati.
MEDIO o BASSO	La tipologia di dato trattato può presentare informazioni **particolari** e/o giudiziarie e **dati comuni** (art. 6 REG. UE n. 679/16) o solo ed esclusivamente dati comuni. Le informazioni, se compromesse, possono ledere i diritti e le libertà degli interessati (i.e., furto d'identità, lesione patrimoniale, etc.).

MOLTO BASSO	La tipologia di dato trattato non presenta informazioni particolari e/o giudiziarie (artt. 9 e 10 REG. UE n. 679/16), né informazioni che possano comportare rischi per i diritti e le libertà dell'interessato se compromesse.

Si procederà a classificare l'**impatto** sui i diritti e le libertà degli interessati considerando una scala da 1 a 5 (1 = Molto Basso, 5 = Molto Alto) a fronte dell'eventuale mancanza di: Riservatezza, Integrità, Disponibilità, Resilienza, o Altre situazioni di rischio.

PARAMETRI DI VALUTAZIONE DELLA PROBABILITA'

5	ALTAMENTE PROBABILE	Esiste un'alta probabilità che i dati personali vengano compromessi poiché le misure tecniche organizzative adottate per proteggere l'informazione personale sono limitatamente presenti, o limitatamente efficaci rispetto la tipologia di dato da proteggere o sono del tutto assenti.
4	PROBABILE	Esiste una sufficiente probabilità che accada una violazione di dati personali o che questi vengano compromessi poiché le misure tecniche organizzative adottate per proteggere l'informazione personale appaiono idonee a prevenire il verificarsi di un danno. Tale idoneità è stata valutata alla luce dell'attuale livello di soluzioni di protezione (informatiche e/o analogiche) che il mercato mette a disposizione del Titolare.
2 - 3	POCO PROBABILE	Esiste una modesta probabilità che si verifichi una violazione di dati trattati poiché le misure tecniche e organizzative di difesa appaiono idonee a tutelare l'integrità delle informazioni. L'idoneità di tali misure è stata commisurata in base all'esperienza maturata dal Titolare che, nel corso degli anni di attività, ha registrato rarissimi episodi di violazione. Il verificarsi del danno ipotizzato susciterebbe grande sorpresa in azienda.
1	IMPROBABILE	Il grado di vulnerabilità del dato è pressoché inesistente e una violazione estremamente remota poiché le misure tecniche organizzative adottate a difesa delle informazioni appaiono altamente idonee a prevenire il rischio. Non sono noti episodi già verificatisi; il verificarsi del danno susciterebbe incredulità in azienda.

Nell'ambito della presente valutazione d'impatto, verrà adottato un **modello metodologico articolato in due fasi consequenziali**, finalizzato alla determinazione e ponderazione del rischio connesso al trattamento dei dati personali.
In una prima fase, si procederà all'**individuazione del rischio potenziale lordo**, mediante una ricognizione sistematica delle tipologie e delle quantità di dati personali trattati, differenziati per ciascuna attività e finalità. Tale analisi consentirà di associare, per ogni singolo trattamento, un livello teorico di impatto potenziale, inteso come la misura delle conseguenze pregiudizievoli che potrebbero derivare agli interessati in caso di perdita di riservatezza, integrità o disponibilità dei dati.

Successivamente, nella seconda fase, si effettuerà il **calcolo del rischio effettivo netto**, ovvero una stima del rischio residuo tenuto conto delle **misure tecniche e organizzative di sicurezza** adottate dal titolare del trattamento. In tale ambito, si valuterà l'effettiva efficacia delle contromisure poste in essere (le c.d. "misure tecniche operative" – MTO), nonché dei controlli attivati, al fine di determinare la **riduzione della probabilità di accadimento** delle minacce identificate nella fase precedente. Si utilizzerà la medesima matrice di rischio impiegata per l'analisi preliminare, opportunamente integrata con l'effetto mitigante delle misure applicate, al fine di ottenere una rappresentazione attendibile del livello di rischio residuo, da considerarsi accettabile o, se del caso, da sottoporre a ulteriore mitigazione.

EUSERVICE

Valutazione dei trattamenti

Ai sensi del REG. UE n. 679/16 (art. 4) per **"trattamento"**, si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

TIPOLOGIE DI DATI TRATTATI

I dati il cui trattamento giustifica l'esistenza di un sistema di protezione dati basato sulle evidenze oggettive sono principalmente "dati personali". Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.. Particolarmente importanti sono:

- i dati **comuni**. Ai sensi dell'**articolo 4, paragrafo 1, del GDPR**, per *dato personale* si intende: **"qualsiasi informazione riguardante una persona fisica identificata o identificabile"** (c.d. "interessato").
  Una persona fisica si considera **identificabile** quando può essere individuata, direttamente o indirettamente, in particolare mediante riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

- i dati rientranti in **particolari** categorie. Ai sensi dell'**articolo 9, paragrafo 1, del GDPR**, costituiscono *categorie particolari di dati personali* — precedentemente noti come *dati sensibili* —: **"i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona."**
  Il trattamento di tali dati è **vietato in via generale**, salvo che ricorra una delle **condizioni di liceità** indicate dall'articolo 9, par. 2 (es. consenso esplicito, obblighi in materia di diritto del lavoro o di assistenza sanitaria, interesse pubblico rilevante, ecc.).

- i dati relativi a condanne penali e reati: Ai sensi dell'**articolo 10 del GDPR** e dell'**articolo 2-octies del Codice**, si definiscono *dati giudiziari*: **"i dati personali relativi a condanne penali e reati o a connesse misure di sicurezza."**
  Il trattamento di tali dati è consentito solo in presenza di una **base giuridica specifica** prevista dal diritto dell'Unione o da una norma di legge nazionale, nel rispetto di **garanzie appropriate per i diritti e le libertà degli interessati**. Tali dati non possono essere oggetto di trattamento generalizzato o automatizzato da soggetti privati se non espressamente autorizzato.

***

Nell'esercizio delle sue attività il Titolare procede al trattamento di diverse tipologie di dati. La mappatura dei trattamenti è stata formalizzata nel Registro dei Trattamenti del Titolare. Il presente documento di valutazione del rischio riguarda i trattamenti principali che, a prima vista risultano capaci di esporre il Titolare del Trattamento ad un maggior rischio.

DATI PERSONALI COINVOLTI (D)

Di seguito si riporta l'individuazione delle macrocategorie di dati trattati, con particolare riferimento ai processi aziendali:

TRATTAMENTO DEI DATI UTENTE	**Cod. 01**	**COMUNI** L'Istituto Scolastico, per mezzo del registro elettronico, tratta dati comuni di tipo anagrafico e dati riconducibili alla vita scolastica dello studente (es: dati relativi al rendimento scolastico).
GESTIONE BISOGNI	**Cod.**	**PARTICOLARI/SENSIBILI**

SPECIFICI	02	L'Istituto Scolastico, per il tramite del registro elettronico, potrebbe trattare altresì i dati di carattere particolare, primi fra tutti i dati sanitari degli studenti.

INDIVIDUAZIONE DELLE MINACCE (rischio per la sicurezza del dato)

COD.	TIPOLOGIA DI MINACCE LEGATE A MISURE ORGANIZZATIVE AZIENDALI O DOVUTE A CALAMITÀ NATURALI (M)
MIN.A	Accesso all'interno della sede da parte di soggetti non autorizzati
MIN.B	Conservazione dei dati contenuti su supporti cartacei vulnerabili
MIN.C	Conservazione dei dati contenuti in supporti di memorizzazione elettronici vulnerabili
MIN.D	Rischi correlati ad ipotesi di incendio
MIN.E	Rischi correlati ad ipotesi di allagamento
MIN.F	Rischi connessi a negligenza o imprudenza del personale
MIN.G	Rischi connessi alla mancanza di indicazioni chiare e/o atti giuridici che disciplinino il trattamento dei dati.
MIN.H	**Spoofing** (Implica l'accesso in modo illegale e l'uso delle informazioni di autenticazione di un altro utente, ad esempio nome utente e password)
MIN.I	**Tampering** (Comporta la modifica non autorizzata dei dati.)
MIN.L	**Repudation** (utente esegue un'operazione non valida in un sistema in cui non è presente la possibilità di tenere traccia delle operazioni non consentite. Il non ripudio si riferisce alla capacità di un sistema di far fronte a rischi di ripudio)
MIN.M	**Information Disclosure** (Comporta l'esposizione di informazioni a individui che non hanno il permesso di accedere al sistema, ad esempio, la capacità degli utenti di leggere un file al quale non hanno ricevuto il permesso di accesso o la capacità di un intruso di leggere dati in transito tra due computer)
MIN.N	**Denial of Service** (Gli attacchi Denial of service (DoS) negano il servizio agli utenti validi, per esempio rendendo un server Web temporaneamente non disponibile o inutilizzabile)

EUSERVICE

MIN.O	**Elevation of Privilege** (Un utente senza privilegi acquisisce accesso privilegiato e ha pertanto un accesso sufficiente per compromettere o distruggere l'intero sistema. L'elevazione dei pericoli di privilegio include quelle situazioni in cui un utente malintenzionato ha violato tutte le difese di sistema e diventa parte del sistema)

INDIVIDUAZIONE RISCHIO EFFETTIVO LORDO

*Funzione: rischio effettivo lordo **(RL)** = probabilità **(p)** x impatto **(i)***

Cod. Tratt.	Minacce	Probabilità	Impatto	RL	Note	RN
Cod. 1	A	1	1	1	Anche nell'improbabile caso di accesso alla sede, il malintenzionato difficilmente potrebbe accedere ai DB, protetti da password.	1
	B	1	3	3	Rischio mitigato con misure di sicurezza e con progressivo abbandono della documentazione cartacea	3
	C	2	3	6	Il verificarsi di una violazione sarebbe un evento eccezionale in azienda e le sue conseguenze sarebbero gravi. Il rischio viene mitigato con misure di sicurezza.	3
	D	2	1	2	Il rischio di incendio non si può escludere, ma la presenza dei dati in cloud consente di escludere ripercussioni sul trattamento di dati	1
	E	2	1	2	Il rischio di allagamento non si può escludere, ma la presenza dei dati in cloud consente di escludere ripercussioni sul trattamento di dati	1
	F	3	3	9	Rischio mitigato con formazione del personale.	6
	G	1	3	3	Ogni soggetto è designato quale persona autorizzata al trattamento dati. Anche in mancanza, il personale è sensibilizzato sull'importanza della riservatezza dei dati.	3
	H	2	3	6	Rischio mitigato con misure di sicurezza.	3
	I	2	3	6	Rischio mitigato con misure di sicurezza.	3
	L	1	3	3	Il sistema tiene traccia (tramite	3

					log) delle attività effettuate sui database	
	M	1	3	3	Rischio mitigato con misure di sicurezza	4
	N	3	3	9	Rischio mitigato con misure di sicurezza	6
	O	1	3	3	Rischio mitigato con misure di sicurezza	3
Cod. 2	A	1	1	1	Anche nell'improbabile caso di accesso alla sede, il malintenzionato difficilmente potrebbe accedere ai DB, protetti da password.	1
	B	1	3	3	Rischio mitigato con misure di sicurezza e con progressivo abbandono della documentazione cartacea	3
	C	2	3	6	Il verificarsi di una violazione sarebbe un evento eccezionale in azienda e le sue conseguenze sarebbero gravi. Il rischio viene mitigato con misure di sicurezza.	3
	D	2	1	2	Il rischio di incendio non si può escludere, ma la presenza dei dati in cloud consente di escludere ripercussioni sul trattamento di dati	1
	E	2	1	2	Il rischio di allagamento non si può escludere, ma la presenza dei dati in cloud consente di escludere ripercussioni sul trattamento di dati	1
	F	3	3	9	Rischio mitigato con formazione del personale.	6
	G	1	3	3	Ogni soggetto è designato quale persona autorizzata al trattamento dati. Anche in mancanza, il personale è sensibilizzato sull'importanza della riservatezza dei dati.	3
	H	2	3	6	Rischio mitigato con misure di sicurezza.	3
	I	2	3	6	Rischio mitigato con misure di sicurezza.	3
	L	1	3	3	Il sistema tiene traccia (tramite log) delle attività effettuate sui database	3
	M	1	3	3	Rischio mitigato con misure di sicurezza	3

	N	3	3	9	Rischio mitigato con misure di sicurezza	6
	O	1	3	3	Rischio mitigato con misure di sicurezza	3

4.Conclusioni

Allo stato, le misure tecniche e organizzative attuate permettono di mitigare il rischio ad un un valore BASSO.

Pertanto, **l'Istituzione Scolastica non è obbligata a consultare l'autorità di controllo**, in quanto il rischio è stato identificato e sufficientemente attenuato (art 36 GDPR).

L'Istituzione Scolastica terrà aggiornata la presente valutazione in relazione a possibili aggiornamenti e all'esito delle implementazione di tutte le misure tecniche e organizzative preventivate.

Milano, 12.05.2025

Il Titolare del Trattamento	Firma.....
Il DPO valuta positivamente	Firma.....