Liceo Scientifico Statale "Filolao"
Via Acquabona snc – 88900 – Crotone (KR)
Tel. 0962 27808 – CF. 81005270798 - Codice meccanografico: KRPS010005
E- mail: krps010005@istruzione.it - PEC:krps010005@pec.istruzione.it - https://filolao.edu.it/
PAGO IN RETE

REGISTRO DELL'ATTIVITA' DI TRATTAMENTO (Art. 30 GDPR)

sullo stato di attuazione della Privacy con particolare riguardo alle banche dati informatizzate, cartacee e in cloud nonché analisi dei rischi connessi

In appendice:

Analisi dei rischi DPIA per:

- Banche dati in uso (informatiche e cartacee)
- Dati esternalizzati (protocollo e registro elettronico)
- Banca Dati SIDI Miur
- Microsoft 365 con Teams
- Google Workspace for Education

Premessa

Il/La sottoscritta Dirigente Scolastico Prof.ssa Maria Rosaria Iaccarino nella sua qualità di legale rappresentante pro tempore dell'Istituto di cui in intestazione in qualità di Titolare del trattamento dei dati dell'istituzione scolastica, coadiuvato dal DPO pro tempore

valutato il Principio di responsabilizzazione (accountability), previsto dall'art. 5 in forza del quale è rimesso al titolare del trattamento il compito di assicurare, e, soprattutto, di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (liceità del trattamento, correttezza, trasparenza, pertinenza, necessità)

valutato l'obbligo previsto all'art. 32 del Reg. 2016/679 di attuare misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, ritiene utile e fondamentale "fotografare" lo stato della sicurezza dati digitali (informatici) e analogici (cartacei), con la descrizione delle norme comportamentali e degli accorgimenti adottati in maniera di sicurezza e salvaguardia dati, in conformità a quanto descritto nel Manuale di Gestione Documentale, redatto sulla base dell'art. 5 c.1 DPCM 03/12/2013, nonché di annotare nel **Registro Accountability,** cronologicamente le misure di sicurezza adottate, atta a comprovare il suo diligente operato, e la congruità delle scelte effettuate volte a migliore la sicurezza e la salvaguardia dei dati.

Valutazione di impatto del trattamento (D.P.I.A., *Data Protection Impact Assesment*), presente in appendice, descrive il trattamento, ne valuta la necessità e la proporzionalità e gli eventuali rischi connessi all'utilizzo di banche dati, per i diritti e le libertà delle persone derivanti dal trattamento.

Un approfondimento particolare è stato compiuto sulle piattaforme di collegamento audio-video sincrono (Microsoft e Google), che per la loro natura intrinseca di Multinazionali, con allocazioni delle infrastrutture IT in territorio Europeo ed extraeuropeo (spesso USA) hanno suscitato un appassionato dibattito circa i presupposti giuridici, previsti dal GDPR 679/2016, in materia di trattamento dati.

Va tenuto presente che la Corte di Giustizia dell'Unione Europea (CGUE), con sentenza del 16 luglio 2020, nella trattazione del caso C 311/18, noto alle cronache come "Schrems II" ha dichiarato nei confronti degli Stati Uniti non applicabile il principio di adeguatezza, previsto dall'art. 45 del GDPR; invalidando, conseguentemente, la Decisione 2016/1250 della Commissione Europea, base giuridica per i trasferimenti di dati personali dei cittadini europei negli USA.

In assenza di un nuovo pronunciamento degli organi giuridici della Comunità Europea, il trasferimento dei dati transfrontalieri di cittadini Europei, non potendo avvenire più sulla base dell'art. 45 del GDPR (Principio di adeguatezza), avviene sulla base dell'art. 46 [1]del GDPR

[1] Art.46 **Trasferimento soggetto a garanzie adeguate**
1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.
2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:
a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) le norme vincolanti d'impresa in conformità dell'articolo 47;
c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, par. 2;
d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Introduzione

Il 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679 noto anche come GDPR (General Data Protection Regulation) che è diventato direttamente applicabile dal 25 maggio 2018.

All'art. 30 del GDPR è stabilito che ogni titolare deve tenere un **registro delle attività di trattamento** svolte sotto la propria responsabilità che contiene le informazioni relative ai dati del titolare, le finalità del trattamento, alle categorie degli interessati e dei dati trattati, le categorie dei destinatari, le misure di sicurezza tecniche ed organizzative.

L'importanza del registro dei trattamenti è evidenziata dal Garante che la considera come attività prioritaria per la pianificazione e gestione dell'attività di protezione delle persone con riguardo al trattamento dei dati. L'Autorità sta valutando di mettere a disposizione il modello di un registro sul proprio sito. Anche il Ministero dell'Istruzione dell'Università e della Ricerca nella sua nota 563 del 22/05/2018 ha anticipato la fornitura della bozza di un registro dei trattamenti specificatamente rivolto alle amministrazioni scolastiche.

In ottemperanza alle disposizioni dell'art. 30 del GDPR il presente documento costituisce una stesura in continuo aggiornamento del registro delle attività dell'istituto in intestazione

1. Nome e dati del titolare del trattamento e del RPD

1.1 Il titolare del trattamento:
DATI DELL'ISTITUZIONE SCOLASTICA
Liceo Scientifico Statale "Filolao"
Via Acquabona snc – 88900 – Crotone (KR)
E- mail: krps010005@istruzione.it - PEC:krps010005@pec.istruzione.it
Tel. 0962 27808

1.2 Il responsabile della protezione dati (RPD):
DATI DI CONTATTO DPO
AZSoluzioni.com di A. Zanghì
Via Arabia Saudita 9 – 88900 Crotone
Email az@azsoluzioni.com Pec antonino.zanghi@legalmail.it
Cell. 3483723759 – TEL. 0962982480

2. Indicazioni relative ai dati trattati

In questa parte del documento vengono fornite informazioni essenziali in merito ai dati personali trattati, con riferimento alla natura ed alla classificazione;

Natura dei dati trattati

La natura dei dati soggetti al trattamento da parte della scuola è la seguente:

- Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati
- Documenti prodotti dalle famiglie anche riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
- Documentazione riguardante il personale docente e non docente anche con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari.
- Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi
- Dati contabili e fiscali

Nel trattamento dei **dati di natura sensibile e giudiziaria**, così come definiti dall'art. 4 lettere d) ed e), verrà osservato il documento redatto da codesto istituto dal titolo "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dall'Istituto scolastico".

BANCHE DATI ATTIVATE

Le banche dati attivate sono quelle sottoindicate in ragione del software utilizzato, nell'ambito dei processi di informatizzazione dell'attività di segreteria, nonché del collegamento con le banche dati Sidi:

- Gestione Alunni
- Gestione Personale
- Protocollo Informatico
- Inventario dei Beni
- Magazzino
- Rapporti con enti pubblici ed imprese
- Fornitori
- Bilancio Gestionale
- Elaborazione cedolini Stipendi
- Registro di classe
- Registro degli insegnanti
- Registro infortuni alunni e dipendenti

FINALITÀ PERSEGUITA CON IL TRATTAMENTO DEI DATI

Nell'ambito della propria funzione istituzionale l'Istituto scolastico tratta dati personali relativi a studenti, personale dipendente a tempo indeterminato e determinato e fornitori con le seguenti finalità:

- Garanzia del servizio scolastico
- Gestione e formazione del personale
- adempimenti assicurativi
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori
- attività strumentali alle precedenti

Affidamento dei dati a terzi per il trattamento:

Tutti i dati di cui l'Ente Scolastico dispone sono esclusivamente trattati presso gli Uffici dell'Istituto e la piattaforma in cloud di gestione documentale messa a disposizione di un fornitore esterno, con il quale è stato siglato un rapporto trattamento dati esterno, nonché con la Banca dati SIDI del Miur.
L'eventualità che i dati possano essere comunicati a terzi potrà verificarsi unicamente nell'ambito dell'attività istituzionale dell'Istituto. Tali casi sono elencati nell'informativa, che viene consegnata agli interessati e pubblicata nell'apposita sezione del sito web e, qualora si verificasse un'evenienza non contemplata nella stessa, in seguito ad esplicito consenso richiesto agli interessati

MODALITÀ DI TRATTAMENTO E CONSERVAZIONE

La conservazione delle banche dati in possesso avviene, in questi anni di transizione digitale con due modalità:

1) Cartaceo
2) Informatizzato

1) ***MODALITÀ CARTACEA:***

I dati in possesso della scuola sono conservati nell'archivio cosiddetto di "deposito" in locali e armadi dotati di chiusura a chiave ai quali hanno accesso esclusivamente le persone incaricate.

Ai fini di garantire una tracciabilità della documentazione, che per ragioni di ufficio viene movimentata (prelevata e riposta) è posto all'entrata un apposito Registro degli Accessi in cui viene registrata l'attività.

Alcuni dati personali non sensibili possono essere riposti in armadi senza serratura ospitati in locali vigilati e sotto il controllo dei collaboratori scolastici anche dopo l'orario di chiusura degli uffici.

L'Istituzione Scolastica attua come, disposto dall'art. 4 punto 5 del GDPR la pseudonimizzazione dei dati in suo possesso.

2) ***MODALITA' INFORMATIZZATA***

Il controllo degli accessi alle varie postazioni di lavoro viene effettuato, dagli incaricati al trattamento dati, appositamente nominati con lettera di incarico, mediante l'adozione di un sistema di autenticazione che permette l'identificazione indiretta dell'operatore autorizzato al trattamento dei dati con Login e Password. Quest'ultima, conosciuta unicamente dall'operatore, deve contenere almeno 8 caratteri, una lettera maiuscola, un numero ed un carattere speciale. Viene sostituita ogni tre mesi.

E' custodita, in busta chiusa, dal custode delle password, nell'evenienza, che in assenza dell'operatore si renda necessario l'utilizzo della postazione.

Elenco dei trattamenti di dati personali

1		2		3	4	5
Identificativo del Trattamento		**Natura dei dati trattati** S	G	**Struttura di riferimento**	**Altre strutture concorrenti al trattamento**	**Descrizione degli strumenti utilizzati**
Breve Descrizione						
Trat.1	Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.	S	G	Dirigente Scolastico, DSGA Assistenti Amministrativi	Collaboratori del D.S., Collaboratori scolastici, RSPP e addetti SPP, Medico Competente (se nominato)	Documenti cartacei, registri e strumenti elettronici, Terminali per la rilevazione delle presenze, collegati in cloud
Trat.2	DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)		Documenti cartacei e strumenti informatici
Trat.3	Organismi collegiali e commissioni istituzionali	S		Dirigente Scolastico, DSGA e Assistenti Amministrativi	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei e strumenti informatici
Trat.4	Attività propedeutiche all' avvio dell'anno scolastico	S	G	Dirigente Scolastico, DSGA e Assistenti Amministrativi	Collaboratori del D.S., Docenti, Collaboratori scolastici,	Documenti cartacei, registri e strumenti informatici
Trat.5	Attività educativa, didattica e formativa, di valutazione	S	G	Dirigente Scolastico, DSGA e Assistenti Amministrativi	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei, registri e strumenti informatici

Trat.6	Rapporti scuola – famiglie : gestione del contenzioso	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati), Docenti,		Documenti cartacei e strumenti informatici
Trat.7	Fornitori e clienti			Dirigente Scolastico, DSGA e Assistenti Amministrativi	Collaboratori del D.S., Docenti nelle commissioni, Membri di organi Collegiali, Collaboratori scolastici,	Documenti cartacei e strumenti informatici
Trat.8	Gestione finanziaria e contabile			Dirigente Scolastico, DSGA e Assistenti Amministrativi	Collaboratori del D.S.	Documenti cartacei, registri e strumenti elettronici
Trat.9	Gestione Istituzionale			Dirigente Scolastico, DSGA e Assistenti Amministrativi	Collaboratori del D.S.	Documenti cartacei, registro protocollo, e strumenti elettronici
Trat.10	Gestione sito web dell'istituto			Dirigente Scolastico, Incaricati sito web	Azienda esterna	Documenti cartacei e strumenti elettronici
Trat.11	Verifica certificazione verde COVID-19 di cui all'art. 9, comma 2, del medesimo D.L. n. 52 (convertito, con modifi cazioni, dalla L. n. 87 del 17/6/2021) attraverso l'App "VerificaC19" o altra piattaforma apposita messa a disposizione dal MIUR di concerto con il Ministero della Sanità. (Fino al termine del periodo emergenza)			Dirigente Scolastico	DSGA, Ass.ti Amm.vi, su apposita nomina del DS per verifica su piattaforma Sidi Collaboratori Scolastici per verifica visitatori con apposita APP C19	Documenti cartacei e strumenti elettronici

3. Struttura organizzativa funzionale al trattamento dati

Si riporta di seguito una sintetica descrizione della struttura organizzativa funzionale al trattamento dei dati con i riferimenti agli incarichi conferiti, ai trattamenti operati ed alle relative responsabilità:

PERSONALE	TRATTAMENTI OPERATI	COMPITI DELLA STRUTTURA:
Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:		
Collaboratori del DS	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Trat.1, Trat.5 (dati sensibili). Se membri di commissione Trat.2 (dati sensibili o giudiziari).	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Trat.3, Trat.4, Trat.5, Trat.7, Trat.8, Trat.9, Trat.10 Tr .3 anche dati sindacali. In casi eccezionali: Trat.1, Trat.5 (dati sensibili). Se membri di commissione Trat.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc,)
Collaboratori sc. e personale ausiliario	Tutti, ma con attività di supporto. Tr .3 anche dati sindacali. In casi eccezionali: Trat.1, Trat.5 (dati sensibili).	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni,
	Se membri di commissione Trat.2 (dati sensibili o giudiziari).	docenti e familiari
Membri ESTERNI di Organi Collegiali	Trat.3 e tutti gli altri (tranne Trat.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:		
Incaricato del Backup periodico	Tutti, ma limitatamente alla funzione	Esegue il backup almeno settimanale degli archivi informatici contenenti dati personali.

Custode delle passwords	Tutti i trattamenti informatici , ma limitatamente alla funzione	Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 o 6 mesi, a seconda dei casi) riceve una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente
Tecnico interno/esterno della Manutenzione del Software [se incaricato]	Tutti, ma limitatamente alla funzione	Manutenzione del software e piccoli interventi sull'hardware
R.S.P.P. e Addetti al S.P.P. (se esistono), R.L.S.	I trattamenti relativi all'applicazione della normativa sulla sicurezza (attualmente Testo unico DLgs. 81/08) o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Trat.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Trat.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Trat.3 Organismi collegiali e commissioni istituzionali Trat.4 Attività propedeutiche all' avvio dell'anno scolastico Trat.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
RLS – rappresentante dei lavoratori per la sicurezza	Diritto di consultazione di tutti i documenti e materiali informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza	Contributo all'applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica ecc.
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap [se esistenti] creazione e gestione del sito web [se esistente]	tutti i trattamenti informatizzati e non relativi all'attività Trat.4 Attività propedeutiche all' avvio dell'anno scolastico Trat.5 Attività educativa, didattica e formativa, di valutazione	Gestione di alunni con handicap didattico grave

Personale incaricato della gestione del sito web [se esistente]	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti funzioni: Trat.11 Gestione sito web dell'istituto	gestione del sito web dell'Istituto
RESPONSABILI INTERNI DI TRATTAMENTO:		
RESPONSABILE DI TRATTAMENTI: Direttore Servizi Generali Amm.vi	Tutti i trattamenti, limitatamente alla gestione amministrativo contabile e alla gestione delle attività dei Collaboratori Scolastici.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
INCARICATI ESTERNI:		
Medico competente ai sensi del Dlgs 81/2008 [se nominato]	I trattamenti relativi all'applicazione della normativa 81/2008 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Trat.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Trat.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Trat.3 Organismi collegiali e commissioni istituzionali Trat.4 Attività propedeutiche all' avvio dell'anno scolastico Trat.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale

RSPP o Addetto al S.P.P. ai sensi del Dlgs 81/2008. [se esistenti]	I trattamenti relativi all'applicazione della normativa 81/2008 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Trat.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Trat.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Trat.3 Organismi collegiali e commissioni istituzionali Trat.4 Attività propedeutiche all' avvio dell'anno scolastico Trat.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
Incaricato Tecnico Esterno della Manutenzione Hardware e Software [se nominato]	tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione del software dei computers e delle reti
Incaricato Tecnico Esterno della Manutenzione dell'Hardware [se incaricato]	tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione dell'hardware dei computers e delle reti
Docente o animatore Figura esterna [se nominata]	i seguenti trattamenti non informatici: Trat.4 - Attività propedeutiche all' avvio dell'anno scolastico Trat.5 - Attività educativa, didattica e formativa, di valutazione, rigorosamente nei limiti relativi alle funzioni	Attività di animazione a favore degli alunni della scuola
Incaricato esterno per la creazione e gestione del sito web [se esistente]	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti attività: Trat.11 Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto

RESPONSABILI ESTERNI:		
RESPONSABILE ESTERNO DEL TRATTAMENTO: organizzazione per la manutenzione del Software [se esistente]	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione	Manutenzione del software
RESPONSABILE ESTERNO DEL TRATTAMENTO: organizzazione per la manutenzione dell'Hardware [se esistente]	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione	Manutenzione dell'hardware dei computers e Reti lan
RESPONSABILE ESTERNO DEL TRATTAMENTO: organizzazione di Docenti o Animatori Esterni [se esistente]	I seguenti trattamenti informatici e no: Trat.4 - Attività propedeutiche all' avvio dell'anno scolastico Trat.5 - Attività educativa, didattica e formativa, di valutazione, rigorosamente nei limiti relativi alle funzioni	Gestione di attività teatrali o ludiche o di animazione in favore degli alunni dell'Istituto Scolastico
RESPONSABILE ESTERNO DEL TRATTAMENTO: organizzazione per la creazione e gestione del sito web [se esistente]	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti funzioni: Trat.11 Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto
RESPONSABILE ESTERNO DEL TRATTAMENTO: organizzazione Agenzia	tutti i trattamenti informatici e no, rigorosamente nei limiti relativi alle funzioni:	Organizzazione di visite con finalità d'istruzione e viaggi
viaggi, Gestori di trasporti (Qualora vi sia un trattamento dati significativo rispetto ai dati puramente identificativi) [se esistente]	Trat.5 - attività educativa, didattica e formativa, di valutazione, ma limitatamente a pochissimi dati Trat.1 – gestione del personale, in quanto accompagnatori, ma limitatamente a pochissimi dati	
RESPONSABILE ESTERNO DEL TRATTAMENTO: Ente di certificazione di qualità [se esistente	tutti i trattamenti informatici e no, rigorosamente nei limiti relativi alle funzioni	Verifica delle condizioni che consentono l'ottenimento del marchio di qualità
AMMINISTRATORI DI SISTEMA ED ASSIMILATI		
Amministratore del sistema informatico	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione	Gestione del sistema informatico dell'istituto

Le banche dati utilizzate sono cartacee e informatiche.

1. **LA SICUREZZA DEI DATI (PRIVACY BY DESIGN e PRIVACY BY DEFAULT)**

Alla luce dei rischi individuati, l'istituzione Scolastica si è posta come obiettivo quello di mettere in atto le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio.

In particolare, l'Istituzione Scolastica innanzitutto tratta i dati rispettando i principi esplicitamente indicati nell'art. 5 del Reg. 2016/679 ossia:

- **Liceità, correttezza, trasparenza: ogni trattamento è esplicitamente indicato nell'informativa;**
- **Limitazione delle finalità: le finalità sono quelle di utilità sociale con attività prevalente nel settore della formazione;**
- **Minimizzazione dei dati e, dove possibile, pseudonimizzazione: i dati trattati sono soltanto quelli necessari per l'erogazione del piano formativo;**
- **Esattezza dei dati: i dati sono inseriti direttamente dall'Istituzione Scolastica**
- **Limitazione della conservazione: il tempo di conservazione dei dati è in genere quello della durata necessaria all'espletamento del compito istituzionale.**
- **L'istituzione Scolastica tratta anche, in talune occasioni, dati sensibili e per questi prevede un esplicito consenso, nonché dati giudiziari esclusivamente per fini istituzionali precisi.**
- **Integrità e riservatezza attraverso le misure adottate per la protezione dei dati stessi.**

La prima e fondamentale misura per garantire la sicurezza dei dati è l'informativa privacy: l'informativa ex art. 13 del Regolamento 2016/679 continua a rappresentare il fulcro per poter trattare i dati di una persona fisica.

Quando il consenso al trattamento dei dati è necessario, si sottopone alla controparte una esplicita richiesta che viene, successivamente, archiviata.

PUBBLICITÀ GDPR

A tal proposito l'Istituzione Scolastica provvede a pubblicizzare sul proprio sito web, in apposita sezione, brochure informative, le informative alunni e genitori, dipendenti e fornitori nonché i dati del responsabile protezione dati DPO

DATI CARTACEI

ARCHIVIO CARTACEO CORRENTE

Stato degli archivi cartacei correnti (personale e alunni)

Gli archivi cartacei correnti, costituti da parte della documentazione, relativa al personale attualmente in forza all'Istituzione Scolastica e agli studenti frequentanti, per ragioni organizzative, sono ubicato nelle stanze della segreteria, in appositi contenitori (Armadi e porta contenitori a cartelle sospese) dotati di regolare chiusura a chiave.

Sono posti, in modo tale, che si possa rilevare, a vista, da parte degli addetti (assistenti e collaboratori) il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

Al termine dell'anno scolastico la documentazione cartacea prodotta viene collocata nei fascicoli di ognuno, posti, nell'archivio storico.

ARCHIVIO CARTACEO DI DEPOSITO

Pseudonimizzazione:
Si rileva che la documentazione degli archivi cartacei ai sensi dell'art.4 comma 5 del GDPR "Il trattamento dei dati personali" deve essere conservato " in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"..

REGISTRO DEGLI ACCESSI
Per l'archivio cartaceo di deposito è presente un registro degli accessi allo scopo di avere una tracciabilità del trattamento dati cartacei, che vengono prelevati e, successivamente, riposti.

SISTEMI DI STAMPA CENTRALIZZATI E LOCALI
L'ubicazione di stampanti centralizzate e locali è messa in essere in maniera tale da non consentire ad estranei di leggere od asportare eventualmente documenti; l'area interessata è controllata a vista per impedirne l'accesso alle persone estranee.

L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici.

CRITERI E PROCEDURE ADOTTATI PER ASSICURARE L'INTEGRITÀ DEI DATI
Relativamente ai supporti cartacei, i criteri di protezione dei dati sono le seguenti:

2. Qualsiasi documento in entrata/uscita dell'istituzione Scolastica appartenente a alunni/genitori/fornitori/dipendenti/ecc. è posto in apposite cartelline non trasparenti, raccoglitori o buste;

3. Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione in armadi o cassettiere, che dopo l'orario di lavoro sono chiuse a chiave;

4. L'archivio cartaceo corrente, relativi ai dipendenti (docenti e ATA) e agli alunni, è custodito all'interno di armadi e raccoglitori chiusi a chiave, la cui disponibilità è esclusiva degli incaricati al trattamento dati.

DATI ELETTRONICI
Personal Computer segreteria amministrativa
I dati di tipo informatico vengono gestiti da PC e sono protetti tramite l'utilizzo di passwords: le passwords sono costituite da 8 caratteri alfanumerici (almeno un carattere maiuscolo e un carattere speciale) e hanno validità di 90 giorni. A termine di tale periodo sono reimpostate.

Personal Computer DSGA
Il DSGA conosce, in esclusiva, la password del proprio PC che utilizza in modo che possa accedere ai documenti, per i quali è incaricato del trattamento.

Personal Computer Assistenti Amministrativi
Ogni assistente amministrativo conosce, in esclusiva, la password del proprio PC che utilizza in modo che ognuno, a seconda delle mansioni svolte all'interno della Istituzione Scolastica, possa accedere solo ai documenti, per i quali è incaricato del trattamento.

a. **Gestione delle Password**
   Le password dei Personal Computer sono custodite in buste chiuse, consegnate al Gestore delle password, e, all'occorrenza, potranno essere aperte per accedere al PC dell'assistente amministrativo momentaneamente assente.
   L'interessato viene messo a conoscenza dell'avvenuta apertura della busta e, al suo ritorno, dovrà provvedere a ripristinare le condizioni originarie.
b. **Salvataggio dati**
   Il salvataggio dei dati avviene in maniera periodica e programmata con sistema NAS o, in alternativa, in maniera manuale con dischi esterni o chiavette USB.
   Tale salvataggio riguarda le cartelle documenti dei singoli client e il database gestionale (Sissi) e, eventualmente, la cartella condivisa se presente.
   È auspicabile l'utilizzo, di un sistema in cloud per un doppio backup dati, allo scopo di aumentare la sicurezza e l'integrità dei dati.
   L'amministratore di sistema, se nominato, verifica che il backup sia andato a buon fine. E si occupa della manutenzione "spicciola" o del riavvio per malfunzionamento.

CRITERI E PROCEDURE DA ADOTTARE PER ASSICURARE L'INTEGRITÀ DEI DATI

Sito Internet

Il sito internet risponde alle norme di legge in particolare in tema di cookies e informativa da pubblicare.

Computer e supporti informatici:

1. I computer sono sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti, ecc.;
2. L'integrità dei dati è garantita mediante idonee procedure di salvataggio periodico (backup).
3. L'introduzione di password all'accensione del personal computer determinerà un livello di sicurezza, circa i dati contenuti nei PC, ritenuto più che soddisfacente. L'introduzione di dette password inibirà ad estranei l'uso dei personal computer, attraverso i quali, si accede alla posta elettronica;
4. In merito a messaggi e-mail inviati a più destinatari, quale mittente è indicata l'istituzione Scolastica con il suo indirizzo e-mail, ed in Ccn i destinatari (che in tal modo non possono individuare gli indirizzi e-mail degli altri destinatari, attraverso la funzione di proprietà) salvo richieste esplicite di utenti;
5. Nei messaggi di posta inviati viene digitata la seguente dicitura: "*in ottemperanza al Reg. UE 2016/679 le informazioni contenute in questo messaggio di posta elettronica sono destinate esclusivamente agli individui e agli enti ai quali risulta indirizzato. Il suo contenuto (inclusi gli allegati) sono confidenziali e riservati: qualora non fosse tra i destinatari originari la esortiamo a non utilizzare, rivelare, trasmettere, copiare né stampare il suo contenuto; qualora avesse ricevuto questo messaggio di posta elettronica per errore, è pregato di avvisarci inviando un messaggio di posta elettronica all'indirizzo del mittente, e quindi cancellare e distruggere il messaggio dal Suo sistema*";
6. I supporti magnetici (penne usb, dischi esterni, ecc) contenenti dati, possono essere riutilizzati esclusivamente previa formattazione irreversibile, in modo da impedire le letture dei dati precedenti;
7. Al fine di condividere documenti tra più operatori è utilizzata una cartella condivisa, piuttosto che pen drive USB o dischi dati esterni, al fine di ridurre notevolmente il rischio di virus e malware.
8. Tutti i giorni, in orario di chiusura, i personal computer saranno spenti o posti in modalità stand-by. Dunque, per la riattivazione è necessaria la password.
9. I Personal Computer ed il PC Server sono dotati di antivirus professionale, con
   - Protezione anti-ransomware

- Protezione dal furto degli account
- Protezione dagli attacchi attraverso le applicazioni
- Neutralizzazione dei rootkit
- Prevenzione degli attacchi via rete

NOMINA RESPONSABILI

1. **Nomina DSGA**
   Con riferimento alle Banche dati cartacee ed informatiche in possesso della Istituzione Scolastica, con riferimento all'articolo 28, che stabilisce che i "trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto; nella nostra fattispecie è stata nominato come responsabile la DSGA Carmine Lepera;
2. **Nomina Responsabile trattamento dati esterno per Segreteria Digitale e Registro elettronico**
   Con riferimento all'utilizzo di servizi in cloud per il protocollo informatico digitale, conservazione sostitutiva e registro elettronico il GDPR, all'articolo 28, stabilisce che i "trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto.
   Nello stesso tempo, ai sensi del GDPR, qualora "un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".
   Alla luce di quanto sopra, il Dirigente Scolastico, Titolare del trattamento ha nominato la ditta fornitrice con apposito atto sottoscritto tra le parti.
3. **Nomina Responsabile trattamento dati esterno per attività di manutenzione hardware e software**
   Con riferimento all'attività di manutenzione delle attrezzature hardware e dei software utilizzati, in particolare quelle in uso negli uffici amministrativi, in forza dell'art. 28 del GDPR, è stato nominato, il legale rappresentante della/e ditta/e a cui si esternalizzano i servizi, per il tempo necessario alla riparazione delle attrezzature affidate, responsabile del trattamento dati, per i contenuti presenti negli archivi di massa (dischi interni, supporti magnetici esterni, sistemi di archiviazione, ecc.) delle attrezzature informatiche.
4. **Nomina Responsabile trattamento dati esterno per attività didattiche su piattaforme esterne**
   Con riferimento all'attività didattica secondo le necessità qualora sia necessario procedere all'utilizzo di piattaforme didattiche esterne (GSuite, Office 365, ecc) si è provveduto alla stipula di contratti per trattamento dati

NOMINA INCARICATI

1. **Nomina Incaricati**
   Il Dirigente Scolastico, con apposita lettera di incarico collettiva ha nominato gli assistenti amministrativi quali incaricati del trattamento con l'avvertimento che dovranno essere osservate per il trattamento Dati una serie di direttive specifiche individuate e dettagliatamente elencate dal titolare/responsabile. **Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.**
2. **Nomina Medico Competente**
   Qualora ci si avvalga, per la sorveglianza sanitaria dei dipendenti, dei servizi professionali di un medico specialista, quest'ultimo sarà nominato con apposita lettera di incarico per trattamento della banca dati con informazioni sensibili
3. **Nomina "Unità Organizzativa Collaboratori Scolastici"**
   Per la parte che loro compete, i collaboratori scolastici tutti, (sia a tempo determinato che quelli a tempo indeterminato) definiti, nel loro complesso, in "Unità organizzativa collaboratori Scolastici" vengono nominati incaricati del trattamento per la parte "circoscritta" della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti nonché, infine, sulla vigilanza dei locali in cui viene effettuato il trattamento dei dati personali.
4. **Nomina "Unità Organizzativa Docenti"**
   Per la parte che loro compete, i docenti tutti (sia a tempo determinato che quelli a tempo indeterminato) definiti, nel loro complesso "Unità organizzativa docenti" vengono nominati incaricati del trattamento dati

per la parte relativa alla "didattica" in occasione della tenuta di documenti e registri, di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia, specie per i rapporti con famiglie e alunni in situazione di disagio psico-sociale; ricezione di certificati medici relativi allo stato di salute degli alunni, documentazione alunni disabili, documentazione mensa/intolleranze, documentazione DSA e BES, ecc.

Attrezzature Informatiche per la Didattica

Le attrezzature informatiche utilizzate per la didattica non custodiscono al loro interno alcuna banca dati. L'eventuale utilizzo dei docenti dei PC delle LIM nelle aule, di tablet o altro device per la registrazione delle attività didattiche nel Registro elettronico, non comporta alcun immagazzinamento di dati in essi, essendo un collegamento in cloud attraverso un normale browser.

Smaltimento rifiuti apparecchiature elettroniche e misure di sicurezza dei dati personali

Viste le disposizioni del Garante contenute nel provvedimento **n° 287 del 09/12/2008** dal titolo "*Rifiuti di apparecchiature elettroniche e misure di sicurezza dei dati personali*", nello smaltimento dei PC in disuso verranno adottate specifiche misure che garantiscano l'impossibilità di accedere ai dati contenuti nei supporti di memoria. Tale misura, non necessaria nei PC utilizzati per lo svolgimento dell'attività didattica e non contenenti dati personali, è rigorosamente adottata per i PC utilizzati per lo svolgimento dell'attività amministrativa.

Formazione del personale

Il **titolare ed il responsabile del trattamento dei dati personali** valutano, per ogni persona cui hanno affidato un incarico o una responsabilità, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.

CONCLUSIONI

Il sottoscritto dirigente scolastico è impegnato inoltre a perfezionare le misure già adottate tramite:

- Analisi e valutazione continua e sistematica delle misure adottate;
- Valutazione dell'applicazione del nuovo Regolamento europeo e adeguamento alle direttive di attuazione di volta in volta emanate dal Garante della Privacy;
- Responsabilizzazione massima di tutti gli operatori anche tramite interventi formativi ed informativi;

APPENDICE A

ANALISI RISCHIO DATI INFORMATIZZATI

1. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI INFORMATIZZATI

In questa sezione vengono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati e valutate le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Verranno presi in considerazione i seguenti eventi:

1. **COMPORTAMENTO DEGLI OPERATORI:**
   - Sottrazione di credenziali di autenticazione
   - Carenza di consapevolezza, disattenzione o incuria
   - Comportamenti sleali o fraudolenti
   - Errore materiale

2. **EVENTI RELATIVI AGLI STRUMENTI:**
   - Azione di virus informatici o di programmi suscettibili di recare danno
   - Spamming o tecniche di sabotaggio
   - Malfunzionamento, indisponibilità e degrado degli strumenti
   - Accessi esterni non autorizzati
   - Intercettazione di informazioni in rete

3. **EVENTI RELATIVI AL CONTESTO FISICO-AMBIENTALE:**
   - Ingressi non autorizzati a locali/aree ad accesso ristretto
   - Sottrazioni di strumenti contenente dati
   - Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali,..), nonché dolosi, accidentali o dovuti ad incuria
   - Guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.) ▪ Errori umani nella gestione della sicurezza fisica

Una volta individuati gli eventi potenzialmente dannosi per la sicurezza dei dati verrà valutata l'IMPATTO SULLA SICUREZZA, cioè verranno descritte le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutata la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'vento (in termini: alta/media/bassa).
In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare. L'analisi dei rischi è esplicitata nelle tabelle seguenti.

Tabella 1 (analisi dei rischi in base all'evento: *comportamento degli operatori*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Comportamento degli operatori	Sottrazione di credenziali di autenticazione		X		ALTO
	Carenza di consapevolezza, disattenzione o incuria		X		MEDIO
	Comportamenti sleali o fraudolenti		X		ALTO
	Errore materiale		X		MEDIO
	Altro evento				

Tabella 2 (analisi dei rischi in base agli: *eventi relativi agli strumenti*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	X			ALTO
	Spamming o tecniche di sabotaggio		X		MEDIO
	Malfunzionamento, indisponibilità e degrado degli strumenti	X			BASSO
	Accessi esterni non autorizzati		X		BASSO
	Intercettazione di informazioni in rete	X			ALTO
	Altro evento				

Tabella 3 (analisi dei rischi in base agli: *eventi relativi al contesto fisico-ambientale*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Eventi relativi al contenuto fisico o ambientale	Ingressi non autorizzati a locali/aree ad accesso ristretto		X		BASSO
	Sottrazioni di strumenti contenente dati		X		BASSO
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria		X		BASSO
	Guasto a sistemi complementari (impianto elettrico, condizionatore ecc.)	X			BASSO
	Errori umani nella gestione della sicurezza fisica		X		BASSO
	Altro evento				

APPENDICE B

ANALISI RISCHIO DATI CARTACEI

2. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI CARTACEI

In questa sezione vengono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati e valutate le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento .
Verranno presi in considerazione i seguenti eventi:

4. **COMPORTAMENTO DEGLI OPERATORI:**

   - Sottrazione di chiavi di accesso
   - Carenza di consapevolezza, disattenzione o incuria
   - Comportamenti sleali o fraudolenti
   - Errore materiale

5. **EVENTI RELATIVI AGLI STRUMENTI:**

   - Mancata custodia di documentazione cartacea sulle scrivanie da lavoro
   - Accessi esterni non autorizzati

6. **EVENTI RELATIVI AL CONTESTO FISICO-AMBIENTALE:**

   - Ingressi non autorizzati a locali/aree ad accesso ristretto
   - Sottrazioni di fascicoli contenenti dati
   - Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali,...), nonché dolosi, accidentali o dovuti ad incuria
   - Guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
   - Errori umani nella gestione della sicurezza fisica

Una volta individuati gli eventi potenzialmente dannosi per la sicurezza dei dati verrà valutata l'IMPATTO SULLA SICUREZZA, cioè verranno descritte le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutata la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'vento (in termini: alta/media/bassa).
In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare. L'analisi dei rischi è esplicitata nelle tabelle seguenti.

Tabella 1 (analisi dei rischi in base all'evento: *comportamento degli operatori*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Comportamento degli operatori	Sottrazione di credenziali di autenticazione		X		ALTO
	Carenza di consapevolezza, disattenzione o incuria		X		MEDIO
	Comportamenti sleali o fraudolenti		X		ALTO
	Errore materiale		X		MEDIO
	Altro evento				

Tabella 2 (analisi dei rischi in base agli: *eventi relativi agli strumenti*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Eventi relativi agli strumenti	Mancata custodia di documentazione cartacea sulle scrivanie da lavoro		X		ALTO
	Accessi esterni non autorizzati		X		BASSO
	Altro evento				

Tabella 3 (analisi dei rischi in base agli: *eventi relativi al contesto fisico-ambientale*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Eventi relativi al contenuto fisico o ambientale	Ingressi non autorizzati a locali/aree ad accesso ristretto		X		BASSO
	Sottrazioni di fascicoli		X		BASSO
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria		X		BASSO
	Guasto a sistemi complementari (impianto elettrico, condizionatore ecc.)	X			BASSO
	Errori umani nella gestione della sicurezza fisica		X		BASSO
	Altro evento				

APPENDICE C

Sicurezza piattaforme in cloud
SEGRETERIA DIGITALE E REGISTRO ELETTRONICO

ESTRATTI DELLE POLICY IN ALLEGATO

1. Madisoft Spa

Madisoft S.p.A. , è impegnata costantemente a pianificare e monitorare le proprie azioni per la gestione dei dati e dei processi interni nell'ottica della salvaguardia dell'integrità e della disponibilità delle informazioni stesse…"
"In quest'ottica Madisoft ha certificato il proprio sistema di gestione integrato ISO 9001 Qualità e ISO 27001 Sicurezza delle informazioni."

Tipologia dei dati gestiti dalla Madisoft SpA
I dati gestiti dalla Madisoft SpA riguardano i dati contenuti negli archivi delle scuole fruitrici del servizio Nuvola In riferimento a quest'ultimi, la natura dei dati varia in base alle caratteristiche del servizio attivato dalla scuola.

GRADO DI SICUREZZA e Modalità di gestione dei dati e di erogazione del servizio
"Per quanto riguarda la gestione dei servizi e dei dati, Madisoft SpA garantisce vari livelli di ridondanza: sia le applicazioni che il database dell'infrastruttura principale sono replicati in maniera sincrona su un server della stessa infrastruttura (ossia i dati vengono specularmente memorizzati sui due server) e su un server dell'infrastruttura secondaria. Madisoft SpA effettuata a intervalli regolari copie di back-up.
La Madisoft SpA è inoltre dotata di uno strumento di monitoraggio continuo degli applicativi web che fornisce in tempo reale, indicatori sulle prestazioni degli stessi, inclusi eventuali picchi di carico."

Modalità di sicurezza nella trasmissione dei dati
"I dati viaggiano sulla rete criptati, secondo il protocollo SSL (Secure Sockets Layer) che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche. La connessione è protetta a crittografia 256-bit. La connessione utilizza TLS 1.2. La connessione è crittografata utilizzando AES_256_CBC, con SHA1 per l'autenticazione dei messaggi e DHERSA come meccanismo principale di scambio delle chiavi."

ALLOCAZIONE DEI DATI - WEB FARM Europea -
Amazon web services Inc. – Relativamente all'erogazione tecnica dei servizi IT
Sede Legale: 410 Terry Ave North Seattle , WA 98109-5210 , US Luogo del Trattamento: **South Dublin Data Center** - Parkview, Greenhills Rd, Tymon North, Dublin 24, Ireland

BANCA DATI SIDI MIUR

Responsabile della protezione dei dati

Il Responsabile per la protezione dei dati personali del Ministero dell'Istruzione è stato individuato, con D.M. 215 del 4 agosto 2022, nella Dott.ssa Alessia Auriemma – Dirigente Ufficio III - Protezione dei dati personali del Ministero - della DGPOC E-mail: rpd@istruzione.it

Responsabile del trattamento

Responsabile del trattamento dei dati è la **Società Generale d'Informatica S.P.A. (Sogei)**, in quanto affidataria dei servizi infrastrutturali, di gestione e sviluppo applicativo del sistema informativo del Ministero dell'Istruzione. Sogei opera attraverso un data center di proprietà costituito da un Ced primario di 4.000 metri quadri e da un Ced secondario interrato di oltre 4.000 metri quadrati. Gestisce quasi 200 banche dati e oltre 900 servizi Ict.

Finalità del trattamento e base giuridica

I dati personali forniti sono trattati unicamente per finalità strettamente connesse e necessarie alla fruizione del Sito e dei Servizi richiesti, ovvero per finalità funzionali allo svolgimento di ricerche, analisi economiche e statistiche, invio di materiale informativo e di aggiornamenti su iniziative e programmi del Ministero dell'Istruzione.

La base giuridica del trattamento è individuata nell'esecuzione dei compiti di interesse pubblico o connessi all'esercizio dei compiti istituzionali posti in capo ai Titolari, ai sensi dell'art. 6 par. 1, lett. c) ed e) del Regolamento UE 679/2016.

Dati oggetto di trattamento

Durante la sola navigazione sul Sito non sono registrati dati personali dell'utente da parte dei Titolari del trattamento. Nell'ambito dell'utilizzo dei singoli servizi offerti nel Sito, possono essere trattati dati personali per specifiche finalità di trattamento come indicato nelle specifiche informative all'uopo dedicate.

Obbligo di conferimento dei dati

La sola navigazione sul Sito non comporta l'obbligo di conferire dati personali da parte degli utenti. L'utilizzo di specifici servizi offerti all'interno del Sito può, tuttavia, richiedere il conferimento dei dati personali da parte dell'utente. In tali casi, sarà specificato, tramite apposita informativa rilasciata al momento dell'accesso allo specifico servizio, se il conferimento sarà obbligatorio o facoltativo. Laddove il conferimento sarà obbligatorio, l'eventuale rifiuto di conferirli può comportare l'impossibilità di utilizzare il relativo servizio. L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo Sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva.

Modalità del trattamento

Il trattamento dei dati personali è compiuto tramite l'utilizzo di strumenti elettronici o comunque automatizzati, nell'ambito del sistema informativo del Ministero dell'Istruzione e nel rispetto delle regole di riservatezza e di sicurezza previste dalla normativa vigente. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti e accessi non autorizzati.

Destinatari del trattamento

I dati personali, eventualmente conferiti, potranno essere comunicati, nel rispetto della normativa vigente, a società esterne incaricate dal Ministero dell'Istruzione al fine di svolgere servizi di varia natura, quali a titolo esemplificativo, la manutenzione e l'assistenza del Sito e dei relativi servizi
I dati personali non sono in alcun modo diffusi.

Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali

Non sono previsti trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali.

Periodo di conservazione dei dati personali

Ai sensi dell'art. 5, par. 1, lett. e) del Regolamento UE n. 679/2016, al fine di garantire un trattamento corretto e trasparente, i dati sono conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, conformemente a quanto previsto dagli obblighi di legge.

GOOGLE LLC (Prodotti e piattaforme in cloud)

La società Google llC effettua il trattamento dati personali di coloro che usufruiscono dei servizi offerti :

- Google Cloud Platform
- Google Workspace
- Cloud Identity

In ottemperanza a quanto indicato nel documento Data processing Addendum (CDPA), presente nella documentazione allegata, espressamente all'art. 10 [2]viene detto che qualora il trasferimento dei dati

[2] **10. Trasferimenti di dati**

10.1 *Strutture per l'archiviazione e l'elaborazione dei dati* . Fatti salvi gli impegni di Google sulla posizione dei dati ai sensi dei Termini specifici del servizio e del resto della presente Sezione 10 (Trasferimenti di dati), i Dati del cliente possono essere elaborati in qualsiasi Paese in cui Google o i suoi Sub-responsabili hanno strutture.

10.2 *Trasferimenti europei limitati* . Le parti riconoscono che la Legge europea sulla protezione dei dati non richiede SCC o una soluzione di trasferimento alternativa affinché i Dati personali del cliente vengano elaborati o trasferiti in un Paese adeguato. Se i Dati personali del cliente vengono trasferiti in qualsiasi altro paese e ai trasferimenti si applica la Legge europea sulla protezione dei dati (come certificato dal Cliente ai sensi della Sezione 10.3 (Certificazione da parte di clienti non EMEA) se il suo indirizzo di fatturazione è al di fuori dell'area EMEA) ("Trasferimenti europei limitati ") , Poi:

UN. se Google ha adottato una Soluzione di trasferimento alternativa per qualsiasi Trasferimento europeo limitato, Google informerà il Cliente della soluzione pertinente e si assicurerà che tali Trasferimenti europei limitati siano effettuati in conformità con essa; e/o

B. se Google non ha adottato, o informa il Cliente che Google non sta più adottando, una Soluzione di Trasferimento Alternativa per eventuali Trasferimenti Europei Limitati, allora:

io. se l'indirizzo di Google si trova in un Paese adeguato:

A. le SCC (da responsabile a responsabile, esportatore di Google) si applicheranno in relazione a tali trasferimenti europei limitati da Google ai sub-responsabili; E

B. inoltre, se l'indirizzo di fatturazione del Cliente non si trova in un Paese adeguato, si applicheranno le SCC (da Responsabile a Titolare) (indipendentemente dal fatto che il Cliente sia titolare e/o responsabile del trattamento) in relazione a tali Trasferimenti europei limitati tra Google e il Cliente ; O

ii. se l'indirizzo di Google non si trova in un Paese adeguato, si applicheranno le SCC (da titolare a responsabile) e/o le SCC (da titolare a responsabile) (a seconda che il Cliente sia titolare e/o responsabile del trattamento) in relazione a tali Restrizioni Trasferimenti europei tra Google e il Cliente.

10.3 *Certificazione da parte di clienti non EMEA* . Se l'indirizzo di fatturazione del Cliente è al di fuori dell'area EMEA e il trattamento dei Dati personali del Cliente è soggetto alla Legge europea sulla protezione dei dati, il Cliente certificherà in quanto tale e identificherà l'autorità di vigilanza competente tramite la Console di amministrazione per Google Cloud Platform o Google Workspace e Cloud Identity , a seconda del caso.

10.4 *Misure e informazioni supplementari* . Google fornirà al Cliente le informazioni relative ai Trasferimenti limitati in Europa, incluse le informazioni sui Controlli di sicurezza aggiuntivi e altre misure supplementari per proteggere i Dati personali del Cliente:

UN. come descritto nella Sezione 7.5.1 (Revisioni della Documentazione sulla Sicurezza);

B. nella documentazione dei Servizi, disponibile su https://cloud.google.com/docs ; E

C. nel sito web Google Cloud Trust and Security, disponibile all'indirizzo https://cloud.google.com/security .

10.5 *Risoluzione* . Se il Cliente conclude, in base all'uso attuale o previsto dei Servizi, che la Soluzione di trasferimento alternativa e/o le SCC, a seconda dei casi, non forniscono tutele adeguate per i Dati personali del Cliente, allora il Cliente può rescindere immediatamente il Contratto applicabile per comodità notificandolo Google.

10.6 *Informazioni sul centro dati* . Le ubicazioni dei data center di Google sono descritte in:

UN. https://cloud.google.com/about/locations/ per Google Cloud Platform; E

B. https://www.google.com/about/datacenters/locations/ per Google Workspace e Cloud Identity.

avvenga verso un paese non coperto dalla cosiddetta clausola di adeguatezza[3] allo stesso si applicano gli SCC, clausole contrattuali tipo, previste dall'art. 46[4] del GDPR.

---

[3] **Decisioni di adeguatezza (art. 45)**

La Commissione europea può stabilire, valutati gli elementi indicati nell'art. 45, par. 2 del Regolamento UE 2016/679 e sulla base di un procedimento che prevede il parere del Comitato europeo per la protezione dei dati, che il Paese terzo (ma anche un territorio o un settore specifico al suo interno) o l'organizzazione internazionale garantiscano un livello di protezione adeguato e che pertanto è possibile trasferirvi dati personali. Il Regolamento prevede un'attività di monitoraggio da parte della Commissione mediante riesame delle decisioni a cadenza periodica, almeno ogni quattro anni. Tale attività può concludersi con una modifica della decisione o in altre circostanze con la sospensione o persino con la sua revoca, (art. 45, paragrafi 3-5 del Regolamento UE 2016/679).

Di seguito sono riportate le decisioni sinora adottate ai sensi della Direttiva 95/46/CE in materia di adeguatezza, in vigore fino a quando non vengano modificate, sostituite o abrogate dalla stessa Commissione (art. 45, par. 9 del Regolamento UE 2016/679).

- Decisione di esecuzione (UE) 2021/1773 della Commissione del 28 giugno 2021 a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito
- Andorra
- Argentina
- Australia PNR
- Canada
- Faer Oer
- Giappone
- Guernsey
- Isola di Man
- Israele
- Jersey
- Nuova Zelanda
- Svizzera
- Uruguay
- USA Privacy Shield*
- USA PNR

*La Corte di giustizia dell'Unione europea (CGUE) si è pronunciata il 16 luglio 2020 (c.d. "Sentenza Schrems II") in merito al regime di trasferimento dei dati tra l'Unione europea e gli Stati Uniti invalidando la decisione di adeguatezza del **Privacy Shield**, adottata nel 2016 dalla Commissione europea in seguito alla decadenza dell'accordo **Safe Harbor.** Nella stessa sentenza la CGUE ha inoltre ritenuta valida la decisione 2010/87 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi. Il Comitato Europeo per la Protezione dei Dati (EDPB) ha predisposto delle FAQ relative alla sentenza Schrems II e ai suoi effetti. **PER APPROFONDIMENTI:** https://www.garanteprivacy.it/temi/privacy-shield

[4] **Articolo 46**

Trasferimento soggetto a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) le norme vincolanti d'impresa in conformità dell'articolo 47;
c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale;
b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

4. L'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 63 nei casi di cui al paragrafo 3 del presente articolo.

5. Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46/CE restano in vigore

La piattaforma Google Workspace for Education può essere utilizzata in piena conformità con il GDPR

Google Workspace e Cloud Identity adottano l'Addendum per il trattamento dei dati Cloud o ATDC (in precedenza denominato Emendamento sul trattamento dei dati o ETD), che incorpora clausole contrattuali tipo (SCC), come metodo per soddisfare i requisiti di sicurezza, contrattuali e per il trasferimento di dati ai sensi delle leggi dell'Unione Europea, del Regno Unito e della Svizzera in materia di protezione dei dati.

Come attivare l'Addendum sul trattamento dei dati Cloud (ATDC)

È necessario attivare l'Addendum per il trattamento dei dati Cloud (ATDC) soltanto se il Contratto Google Workspace o Cloud Identity non incorpora già l'ATDC (o l'ETD) mediante riferimento. Se non si ha la certezza che tale contratto incorpori già l'ATDC (o l'ETD) mediante riferimento, consigliamo di attivare l'ATDC, in quanto contiene importanti impegni relativi alla conformità e la sua attivazione non farà alcuna differenza anche se di fatto fosse già incorporato nel contratto (o se vi fosse già incorporato l'ETD).

PER PROCEDERE ALL'ATTIVAZIONE:

1. Accedere alla **Console di amministrazione Google**.

   Utilizzare un account con privilegi di super amministratore.

2. Nella Console di amministrazione, vai al Menu ->**Account** -> **Impostazioni account** -> **Aspetti legali e conformità**.
3. In **Termini di servizio aggiuntivi per sicurezza e privacy**, sotto **Addendum per il trattamento dei dati Cloud al Contratto Google Workspace o Cloud Identity**, fare clic su **Leggi e accetta**.

Nel documento Google Cloud e il Regolamento generale sulla protezione dei dati (GDPR), in nota, si legge che nel caso in cui i dati personali vengano trasferiti fuori dall'UE in paesi terzi, non coperti da decisioni di adeguatezza, come disposto dall'art.46 del GDPR, Google LLC a fronte dei contratti per il trattamento dati si impegna a mantenere un meccanismo che faciliti questi trasferimenti secondo quanto stabilito dal GDPR[5]

Ulteriore Sicurezza lato Client

Crittografia lato Client, a secondo del tipo di contratto di acquisto del servizio Google è possibile rafforzare ulteriormente la sicurezza dal lato client cercando di abbassare l'entità del rischio attraverso la pseudonimizzazione e cifratura dal lato client . Tale servizio viene offerto dai seguenti partner di Google:

---

fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo.

[5] **Trasferimento internazionale dei dati**
Il regolamento GDPR prevede vari meccanismi per facilitare il trasferimento dei dati personali al di fuori dell'UE. Questi meccanismi sono mirati a fornire un livello adeguato di protezione o ad assicurare l'implementazione di misure di salvaguardia appropriate al momento del trasferimento dei dati personali in un paese terzo.
L'adeguato livello di protezione può essere confermato da decisioni di adeguatezza come quelle che supportano la legge giapponese sulla protezione dei dati personali (APPI, Act on the Protection of Personal Information) e la legge federale svizzera sulla protezione dei dati (LPD).
Nel caso in cui i dati personali vengano trasferiti fuori dall'UE in paesi terzi non coperti da decisioni di adeguatezza, ci impegniamo a fronte dei nostri contratti per il trattamento dei dati a mantenere un meccanismo che faciliti questi trasferimenti secondo quanto stabilito dal GDPR. Nel 2017, le autorità europee competenti per la protezione dei dati personali hanno confermato la conformità delle nostre clausole contrattuali tipo, dichiarando che i nostri impegni contrattuali per Google Workspace e Google Cloud rispettano i requisiti previsti per inquadrare giuridicamente il trasferimento dei dati personali dall'UE a paesi terzi che non forniscono protezione adeguata.

- FlowCrypt
- Fortanix
- FutureX
- Stormshield
- Thales
- Virtru

Le chiavi create, forniscono strumenti, che soddisfano le specifiche di Google relative alle funzionalità sia di gestione delle chiavi sia di controllo degli accessi.

Il partner terzo, detiene la chiave per la decodifica dei file criptati e altri contenuti e Google non può in alcun modo accedere a questi file o decifrarli senza questa chiave.

INDICE DEGLI ARGOMENTI

IL DIRIGENTE SCOLASTICO
Prof.ssa Maria R. Iaccarino