ISTITUTO COMPRENSIVO PAGANICA
Via del Rio 67100 PAGANICA (AQ)
https://www.icpaganica.edu.it
e-mail: aqic84600q@istruzione.it pec: aqic84600q@pec.istruzione.it
Cod. Fisc. 93105530666 Cod. Mecc. AQIC84600Q
Codice Univoco: UFQDF5 Tel 0862 689583

D. P. I. A.

(Data Protection Impact Assessment)

DOCUMENTO DI VALUTAZIONE DI IMPATTO SULLA PRIVACY

Ex art.35 GDPR R.E.679/2016

Nel presente documento viene sintetizzata e descritta l'attività di **analisi e valutazione dei rischi** che l'Istituto Scolastico ha preliminarmente avviato e portato a conclusione, ai fini della predisposizione del modello organizzativo in materia di protezione dei dati personali.

Paganica (AQ), 14 gennaio 2022

CAP. I Premessa normativa e regolamentare

Art. 1 FONTI

a. GDPR art.35

b. Linee Guida Gruppo 29

c. Linee Guida Garante della Privacy

Art. 2 INDICAZIONI TERMINOLOGICHE

a. Trattamento:

b. RISCHIO: scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità.

c. Gestione del rischio: insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio

d. Diritti e Libertà: nel contesto giuridico della protezione dei dati vanno intesi come riferiti in primo luogo al DIRITTO ALLA PRIVACY, ma possono riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione, il diritto alla segretezza della corrispondenza etc.

Art. 3 VALUTAZIONE DEI RISCHI

In relazione a tutti i trattamenti di dati personali effettuati dalle scuole, le Istituzioni Scolastiche devono obbligatoriamente eseguire una valutazione dei rischi, per analizzare quali sono i rischi per gli interessati (docenti, alunni, famiglie, etc.), legati ai trattamenti effettuati. La valutazione dei rischi serve per adottare le misure di sicurezza (antivirus, procedure di gestione password, controllo accessi, ecc.). La valutazione dei rischi deve essere effettuata anche in relazione alle piattaforme digitali usate dalle scuole, compreso il Registro Elettronico, per tutte le attività ivi svolte (registrazione voti, consegne compiti, messaggistica, annotazioni presenze-assenze, annotazioni disciplinari etc.);

Art. 4 VALUTAZIONE D'IMPATTO

L'art.35 del Regolamento UE 2016/679 (GDPR) prescrive per alcuni trattamenti la non sufficienza della valutazione dei rischi e la necessità di un processo più approfondito e complesso ovvero la valutazione di impatto. In particolare l'art.35 recita che "se un trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali"

Art. 5 INDIVIDUAZIONE DEI CASI DI TRATTAMENTO SOGGETTI A DPIA

a. Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'art.35 paragrafo 3 fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basato su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art.9 § 1, o di dati relativi a condanne penali e a reati di cui all'art.1013;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

b. Il Gruppo di Lavoro Articolo 29 (WP29) per la Protezione dei Dati del 4 aprile 2017, ha adottato alcune Linee Guida in materia, fatte proprie dal Comitato Europeo per la protezione dei dati il 25 maggio 2018. Queste Linee Guida hanno individuato Nove Criteri da considerarsi indicatori ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato" tale da richiedere la valutazione d'impatto:

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone
3. Monitoraggio sistematico degli interessati
4. Dati sensibili o dati aventi carattere altamente personale
5. Trattamento dei dati su larga scala
6. Creazione di corrispondenze o combinazioni di insiemi di dati;
7. Dati relativi a interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
9. Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"

Il WP29 ha evidenziato che al ricorrere di due o più dei predetti criteri è da ritenersi sussistente l'indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è richiesta una valutazione di impatto

c. Secondo le Linee Guida del WP29 la DPIA è particolarmente importante e consigliabile quando viene introdotta una nuova tecnologia di trattamento dei dati

d. Nei casi in cui non è chiaro se sia richiesta obbligatoriamente una valutazione d'impatto sulla protezione dei dati o meno, il WP29 raccomanda di effettuarla comunque , in quanto detta valutazione è uno strumento utile che assiste i Titolari del trattamento a rispettare la legge in materia di protezione dei dati

Art. 6 ATTIVITA' SOGGETTE A VALUTAZIONE D'IMPATTO SECONDO IL GARANTE DELLA PRIVACY

Il Garante della Privacy italiano, a completamento del Documento prodotto dal WP29, con il Provvedimento n.467 dell'11 ottobre 2018 ha redatto un elenco di attività che andrebbero sottoposte a valutazione d'impatto:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate

anche on line o attraverso app , relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato”

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi)
3. Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuate anche on line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web , tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti d i metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnlogico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti)
5. Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)
7. Trattamenti effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es.IoT, sistemi di intelligenza artificiale, utilizzo di assistenti vocali on line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità (come ad esempio il WiFi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248 rev.01
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l’incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)

10. Trattamenti di categorie particolari di dati ai sensi dell'art.9 oppure di dati relativi a condanne penali e a reati di cui all'art.10 interconnessi con altri dati personali raccolti per finalità diverse
11. Trattamenti sistematici di dati biometrici, tenendo conto in particolare del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza dell'attività di trattamento

Art. 7 OBBLIGHI DEL TITOLARE, DEL RESPONSABILE DEL TRATTAMENTO E DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

a. Spetta al Titolare garantire l'effettuazione della DPIA (art.35 paragrafo 2 GDPR). La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia la responsabilità ultima dell'adempimento ricade sul titolare del trattamento

b. Il titolare deve consultarsi con il Responsabile della Protezione dei Dati (DPO/RPD), ove designato (art.35 paragrafo 2); tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA.

c. Il DPO deve monitorare lo svolgimento e l'osservanza della DPIA (art.39 paragrafo 1 lettera C)

d. Se il trattamento è svolto, in tutto o in parte, da un responsabile, quest'ultimo deve assistere il titolare nella conduzione della DPIA fornendo ogni informazione necessaria conformemente con l'art.28 paragrafo 3 lettera f

e. Il titolare "raccoglie le opinioni degli interessati o dei loro rappresentanti.. se del caso (art.35 paragrafo 9 GDPR). A giudizio del WP29:

- Per la raccolta delle opinioni in oggetto si possono individuare molteplici modalità, in rapporto al contesto: per esempio uno studio generico relativo a finalità e mezzi del trattamento; un quesito rivolto ai rappresentanti del personale; un questionario inviato ai futuri clienti del titolare;
- Qualora la decisione assunta in ultima analisi dal titolare si discosti dall'opinione degli interessati, è bene che il titolare documenti le motivazioni che hanno condotto alla prosecuzione o meno del progetto;
- Il titolare dovrebbe documentare anche le motivazioni della mancata consultazione degli interessati, qualora decida che quest'ultima non sia opportuna

Art. 8 OGGETTO E CONTENUTO DELLA DPIA

a. Il GDPR (art.35§7 e considerando84 e 90) definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati:
   - una descrizione dei trattamenti previsti e delle finalità del trattamento
   - una valutazione della necessità e proporzionalità dei trattamenti
   - una valutazione dei rischi per i diritti e le libertà degli interessati
   - le misure previste per affrontare i rischi e dimostrare la conformità al presente regolamento

b. nel valutare l'impatto di un trattamento va tenuto conto (art.35§8 GDPR) del rispetto di un codice di condotta (art.40), al fine di dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessato

c. Una singola DPIA può riguardare una sola operazione di trattamento dei dati oppure può essere utilizzata per valutare molteplici operazioni di trattamento che sono simili in termini di rischi presentati, purchè siano adeguatamente considerate la specifica natura, portata, contesto e finalità del trattamento. Si può far riferimento, quindi, a tecnologie simili utilizzate per raccogliere lo stesso tipo di dati per le medesime finalità.

d. La DPIA deve stabilire chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati

e. Il Titolare del Trattamento deve indicare con chiarezza nella DPIA le esigenze e le ragioni di necessità o opportunità che hanno determinato la predisposizione della valutazione d'impatto con riferimento ai diritti e alle libertà che si intendono tutelare, condividendo tutte le informazioni utili allo scopo, fatte salve le informazioni coperte da segreto (d'ufficio, di Stato, professionale, industriale etc.)

Art. 9 PROCESSI METODOLOGICI DELLA DPIA CONFORME AL GDPR

a. Le Linee Guida WP29 suggeriscono diverse metodologie per effettuare una DPIA (es. ISO/IEC 29134 "Privacy Impact Assesment-Methodology; ISO 3100025 etc.), in conformità all'art. 90 GDPR che elenca alcuni elementi comuni dei processi di gestione del rischio che devono essere considerati nella effettuazione della DPIA, proponendo i seguenti criteri che i titolari del trattamento devono declinare nell'ambito della DPIA in conformità a quanto richiesto nel precedente art.6 sub a):

La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento (art.35§7 lett.a), prevede:

- la descrizione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento
- la registrazione di dati personali, dei destinatari e del periodo di conservazione dei dati personali
- la descrizione funzionale del trattamento
- l' individuazione delle risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea)
- considerazione del rispetto dei codici di condotta (art.35§8

La valutazione della necessità e proporzionalità dei trattamenti (art.35§7 lett.b) e d), prevede l'indicazione ed esplicitazione di

- finalità determinate, esplicite e legittime (art.5§1 lett.B)
- liceità del trattamento (art.6)
- dati personali adeguati, pertinenti e limitati a quanto necessario (art.5§1 lett.C)
- limitazione della conservazione (art.5§1 lett.e)
- misure che contribuiscono ai diritti degli interessati

- informazioni fornite all'interessato (artt.12,13 e 14)
- diritto di accesso e portabilità dei dati (art.15 e 20)
- diritto di rettifica e alla cancellazione (artt.16, 17 e 19)
- diritto di opposizione e di limitazione di trattamento (artt.18, 19 e 21)
- rapporti con i responsabili del trattamento (art.28
- garanzie riguardanti trattamenti internazionali (Capo V)
- consultazione preventiva (art.36)

la valutazione dei rischi per i diritti e le libertà degli interessati, deve considerare

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- i comportamenti degli operatori
- gli strumenti utilizzati per il trattamento dei dati
- gli eventi relativi al contesto
- l'origine, la natura, la particolarità e la gravità dei rischi
- le fonti di rischio
- la stima della probabilità e della gravità
- le minacce che potrebbero determinare l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati
- le aspettative degli interessati con particolare riguardo agli impatti potenziali per i diritti e le libertà degli interessati stessi in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati

Le misure previste per affrontare i rischi e dimostrare la conformità al presente regolamento.

b. Il Regolamento consente ai Titolari un margine di flessibilità nello stabilire la struttura e la forma della valutazione di impatto in modo da consentire l'inclusione nelle prassi lavorative in essere

c. Il WP29 incoraggia lo sviluppo di quadri DPIA settoriali , in quanto essi possono attingere a conoscenze specifiche di settore. In tal modo la DPIA può essere indirizzata alle specificità di un particolare tipo di operazione di trattamento (es.particolari tipi di dati, beni aziendali etc.) e gestire i rischi che possono derivare qualora il trattamento venga effettuato nell'ambito di particolari settori, o utilizzando particolari tecnologie, o configurandosi come operazioni di trattamento particolarmente complesse e invasive della privacy

Art. 10 TEMPISTICA, PUBBLICITÀ E VANTAGGI DELLA DPIA

a. La DPIA dovrebbe essere condotta "prima di procedere al trattamento" (art.35, paragrafo 1 e paragrafo 10 considerando 80 e 93), coerentemente con i principi della privacy by design e by default (art.25 e considerando 78). Dovendosi considerare uno strumento di ausilio nel processo decisionale relativo al trattamento, l'effettuazione della DPIA dovrebbe collocarsi

quanto più a monte possibile nella fase di progettazione di un trattamento, anche qualora non tutte le operazioni di tale trattamento siano state già delineate

b. La DPIA è un processo continuativo e non una tantum, pertanto è suscettibile di continuo aggiornamento nel corso dell'intero ciclo di vita di un determinato trattamento, in modo che sia garantita la dovuta considerazione dell'evoluzione delle tematiche di privacy e protezione dei dati, dovute anche ai cambiamenti tecnologici e degli orientamenti di giurisprudenza e dottrina e delle soluzioni individuate che ne promuovano l'osservanza

c. La pubblicazione della DPIA non costituisce un obbligo formale ai sensi del Regolamento ed è quindi rimessa alla discrezionalità del titolare. E' consentito ai Titolari valutare l'opportunità di rendere pubbliche almeno parti della DPIA, quali una sintesi o le conclusioni, anche al fine di accountability e promozione della fiducia nelle attività di trattamento svolte dai Titolari, secondo un approccio responsabile e trasparente. Invero, la pubblicazione della DPIA appare particolarmente indicata se il trattamento produce effetti su una parte della popolazione, il che vale soprattutto nel caso sia un' Autorità Pubblica a condurre la DPIA

d. La DPIA può essere seguita, periodicamente o a fine trattamento, da un processo di follow up che si compendia nelle seguenti attività

- Preparazione del report
- Pubblicazione
- Attuazione delle misure o dei piani di gestione dei rischi
- Review e/o audit della valutazione d'impatto
- Documentazione della valutazione d'impatto

e. L'utilità e il vantaggio della effettuazione della DPIA consiste nel fatto che essa consente principalmente di:

- Identificare gli impatti, i rischi e le responsabilità sulla privacy
- Fornire input per progettare per la tutela della privacy
- Revisionare i rischi per la privacy di un nuovo sistema di informazione e valutarne l'impatto e la probabilità
- Fornire la base per la fornitura di informazioni sulla privacy
- Mantenere gli aggiornamenti successivi con funzionalità aggiuntive
- Condividere e mitigare i rischi con le parti interessate, fornendo le informazioni relative alla conformità
- Identificare in anticipo e precocemente i problemi e l'eventuale contenzioso, riducendo i costi del tempo di gestione, le spese legali e potenziali mediatici o d'interesse pubblico
- Evitare o ridurre il rischio di incidenti o errori costosi e/o imbarazzanti sulla privacy, che possono incidere negativamente sull'immagine e il dato reputazionale del Titolare
- Fornire la prova che l'organizzazione ha agito in modo appropriato nel tentativo di prevenire il verificarsi di violazioni o lasciare vuoti di tutela, escludendo ipotesi di culpa in organizzando o fattispecie riconducibili a ipotesi di colpe omissive
- Conoscere in anticipo le insidie alla privacy di un processo, di un sistema informatico o un programma

- Aiutare un'organizzazione a creare consapevolezza, a stabilire responsabilità, trasparenza e
- visibilità, a guadagnare la fiducia del pubblico, degli stakeholder, anticipando e rispondendo in anticipo alle preoccupazioni del pubblico sulla privacy, in un contesto di Rendicontazione Sociale

CAP. II Disposizioni preliminari alla valutazione di impatto

Art. 1 Indicazione del Titolare del trattamento, del DPO e dei responsabili

a. Il titolare del Trattamento dei dati è l'Istituto Comprensivo "Paganica" di Paganica (AQ) in persona della Dirigente Scolastica Giovanna CARATOZZOLO

b. Il Responsabile della Protezione dei dati (DPO) è l'ing. Bruno Martini

Art. 2 Adempimenti del Titolare e del DPO

b. Prima di procedere alla elaborazione della presente Valutazione d'Impatto, La Dirigente Scolastica ha provveduto, ai sensi dell'art.35§2, a consultarsi con il Responsabile della Protezione dei Dati (DPO/RPD) designato.

c. Il DPO monitorerà lo svolgimento e l'osservanza della DPIA (art.39 paragrafo 1 lettera C), attraverso atti di interlocuzione, analisi e consultazione diffusa con i responsabili della conduzione della DPIA, ovvero il personale Docente e il personale di Segreteria, nonché con specifiche figure dell'Organigramma della Scuola, preposte allo svolgimento di incarichi che rivestono una rilevante importanza ai fini della osservanza e gestione del rischio del trattamento dei dati nella DAD: in particolare la DSGA, e l'Animatore Digitale

d. Il DPO ha provveduto ad assistere il titolare nella conduzione della DPIA fornendo ogni informazione necessaria, conformemente con l'art.28 paragrafo 3 lettera f, assunta dai docenti e dal personale di segreteria, nonché dalle predette figure preposte

Art. 3 Individuazione degli indici di opportunità-obbligatorietà della DPIA nell'ambito dei Nove Criteri

La necessità di procedere alla effettuazione della DPIA è scaturita dall'obbligo di dover attivare modalità e procedure di Didattica a Distanza, sia on line che off line, a seguito dei DPCM che si sonno susseguiti a far tempo dal 05 Marzo 2020 per far fronte all'emergenza COVID 19. L'attivazione delle procedure e modalità di svolgimento della DAD ha determinato il ricorso, sistematico ed ordinario, a strumenti digitali afferenti alle tecnologie informatiche della comunicazione.

L'utilizzo massivo e quotidiano dei suddetti strumenti digitali ha determinato l'elevazione del rischio della protezione dei dati che vengono trattati nell'espletamento della Didattica a distanza, configurando la ricorrenza di alcuni dei Nove Criteri individuati da WP29, conformemente al Regolamento Europeo 679/2016-GDPR, che rendono obbligatoria o quanto meno necessaria la Valutazione di Impatto del rischio, come d'altronde prescritto dalle vigenti leggi che ha espressamente previsto che le Istituzioni Scolastiche attuino la valutazione di impatto.

Nello specifico sono stati individuati dal DPO e dal Titolare del Trattamento i seguenti criteri-indice di rischiosità (cfr.: CAP. 1 Art.3 p.B):

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale…l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (criterio 1)
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone (criterio 2)
3. Monitoraggio sistematico degli interessati (criterio 3)
4. Dati sensibili o dati aventi carattere altamente personale (criterio 4)
5. Dati relativi a interessati vulnerabili (criterio 7)
6. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative (criterio 8)

Art. 4 Soggetti coinvolti, esigenze e diritti che si intendono tutelare

a. I soggetti coinvolti nel trattamento dei dati sono individuati nelle persone:

- dei docenti, che effettuano le attività di Didattica a Distanza
- degli alunni, che fruiscono della prestazione lavorativa dei docenti
- dei genitori, tutori legali e/o affidatari degli alunni, che in quanto esercenti la potestà parentale, sono obbligati a svolgere adempimenti di carattere negoziale tecnico-giuridico per consentire l'attuazione della DAD (es. iscrizione a piattaforme, ritiro di password, accesso a piattaforme e Registro Elettronico) e legittimati a svolgere compiti di vigilanza-controllo (cosiddetto parental control), per favorire la correttezza metodologica e deontologica dello scambio pedagogico-didattico attraverso il mezzo digitale, secondo le regole che di seguito saranno indicate (ad esempio allestimento di setting e spazi adeguati e conformi, coadiuvazione tecnica, interlocuzioni di carattere organizzativo-amministrativo con le figure preposte etc.)

b. Le esigenze che si intendono tutelare, sono connesse essenzialmente

- alla difficile gestione e organizzazione degli spazi e dei tempi disponibili per l'attuazione della DAD che devono essere conciliati con le impellenze di vita quotidiana e con gli impegni dei diversi componenti del nucleo familiare (ad esempio esiguità degli ambienti domestici che abbiano caratteristiche consone alla mediazione didattica digitale protetta; sussistenza di più membri del nucleo familiare che versano nella necessaria condizione di avvalersi di strumenti digitali, come genitori o coniugi che effettuano smartworking, fratelli-sorelle o figli impegnati altrettanto in attività di Dad;
- alla insufficienza o inappropriatezza degli strumenti telematici di cui si dispone, dei servizi di connettività, del bagaglio di formazione e competenza nell'uso e padronanza delle strumentazioni digitali, che possono produrre sintomi di ansia, stress, sensazioni di inadeguatezza e complessi di inferiorità
- al carico emotivo-psicologico determinato dalla situazione emergenziale che ha comportato l'improvviso cambiamento delle proprie abitudini, anche di vita scolastica, sia per i docenti che per gli alunni e i genitori, con effetti plausibili di destabilizzazione e disorientamento professionale e di posizione di ruoli;

c. I diritti che si intendono tutelare sono essenzialmente quelli connessi alla tutela

DELLA PRIVACY:

- Diritto di riservatezza di dati sensibili che afferiscono alla persona o agli ambienti ad essa contigui e familiari (es. condizioni di salute, uso di farmaci e/o presidi sanitari, tipologia e caratteristiche degli ambienti domestici e/o privati, condizioni igienico-sanitarie legate all'ambiente in cui il contatto comunicativo viene fatto avvenire, credo religioso, opinioni politiche, titoli professionali, frequentazioni di terzi, condizioni di affinità e parentela, stili e tenore di vita, abitudini alimentari scansione del tempo di vita quotidiana etc.);
- Diritto di riservatezza di dati connessi alla valutazione in tutte le sue tipologie (es. voti, osservazioni formative, commenti e contributi di carattere valutativo, annotazioni di carattere educativo-disciplinare etc.), per quanto riguarda gli alunni;
- Diritto di riservatezza di dati connessi al rendimento e alla prestazione professionale (es. efficacia di scelte metodologiche, capacità di conduzione di video lezioni o altre prestazioni didattiche, disinibizione e disinvoltura nella comunicazione, proprietà di linguaggio, intelligenza emotiva etc.
- Diritto di riservatezza di dati connessi alla diligenza nell'esercizio della potestà parentale e nell'adempimento dell'obbligo genitoriale di assistenza materiale e morale (es. capacità di gestire i tempi del proprio figlio, capacità di responsabilizzare il proprio figlio, adeguatezza e capacità di assistenza e vigilanza in adempimenti di carattere tecnico-giuridico, competenze digitali, condizioni economiche)
- Diritto alla segretezza della corrispondenza

DI ALTRI DIRITTI E LIBERTA' FONDAMENTALI

- Diritto allo studio
- Diritto alla libertà d'insegnamento
- Diritto alla salute
- Diritto alla sicurezza nei luoghi di lavoro
- Libertà di movimento

1 METODOLOGIA DI VALUTAZIONE DEI RISCHI

1.1 Valutazione degli impatti sugli interessati

Per ciascun processo e tipologia di dato trattato deve essere effettuata un'analisi dei possibili **impatti sugli interessati** identificando un valore qualitativo secondo la seguente scala di valutazione:

ID	Impatto	Descrizione
4	**Altissimo**	Dati particolarmente delicati dal punto di vista della legislazione vigente in materia di privacy (es. dettaglio sullo stato di salute delle persone, abitudinisessuali, problemi di salute, ecc.) o idonei a rivelare aspetti particolarmente intimi della sfera personale di un individuo e/o dei suoi congiunti. Rientrano intale categoria anche i trattamenti di dati per i quali una loro indisponibilità o violazione dell'integrità potrebbe comportare gravi violazioni per la dignitàdell'individuo o rischi per la vita delle persone coinvolte.
3	**Alto**	Dati delicati dal punto di vista della legislazione vigente in materia di privacy (es.sensibili, biometrici, giudiziari, ecc.) o idonei a rivelare aspetti intimi della sfera personale di un individuo e/o dei suoi congiunti. Rientrano in tale categoria anche i trattamenti di dati per i quali una loro indisponibilità o violazione dell'integrità potrebbe comportare gravi disagi per la vita delle personecoinvolte.
2	**Medio**	Dati personali il cui impatto in caso di violazione potrebbe avere conseguenze non trascurabili per gli interessati (es. dati anagrafici, dati sulle abitudini, ecc.) siain termini di riservatezza che di disponibilità ed integrità legate all'impossibilità o alla limitazione per l'erogazione di servizi contrattualizzati con gli stessi interessati
1	**Basso**	Dati personali in grado di identificare solo per via indiretta l'interessato attraverso id non direttamente riconducibili all'interessato separati da riferimentianagrafici e di contatto e la cui disponibilità ed integrità non risulta critica per erogare un servizio o processo contrattualizzato

1.2 Valutazione della probabilità di accadimento

Per ciascun processo e tipologia di dato trattato deve altresì essere effettuata un'analisi della **probabilità di accadimento di eventi di rischio sugli interessati** identificando un valore qualitativo secondo la seguente scala di valutazione:

ID	Probabilità	Descrizione
3	**Alto**	Eventi di violazione di aspetti di riservatezza, integrità e disponibilità verificatisicon frequenza pari ad almeno una volta negli ultimi 2 anni, oppure; Assenza di misure di sicurezza di base (es. misure idonee di sicurezza) o mancato adempimento di misure prescritte in apposti provvedimenti in materia di protezione dei dati personali da parte delle Autorità competenti
2	**Medio**	Eventi di violazione di aspetti di riservatezza, integrità e disponibilità verificatisicon frequenza pari ad almeno una volta negli ultimi 5 anni, oppure; Presenza di misure di base (es. misure minime, ecc.) ed adempimento di provvedimenti prescrittivi in materia di privacy relativi al trattamento, masenza ulteriori misure proattive atte a limitare i rischi (es. crittografia, pseudonimizzazione, ...)
1	**Basso**	Eventi di violazione di aspetti di riservatezza, integrità e disponibilità verificatisicon frequenza pari ad almeno una volta negli ultimi 10 anni, oppure; Presenza di misure di base (es. misure minime, ecc.) ed adempimento di provvedimenti prescrittivi in materia di privacy relativi al trattamento, e diulteriori misure proattive atte a limitare i rischi (es. crittografia, pseudonimizzazione, ...)

1.3 Valutazione del rischio del processo di trattamento

Dall'incrocio dei parametri di *Impatto* e *Probabilità* sulla base della seguente matrice, si ricava un indice di rischio del processo di trattamento:

			Basso	Medio	Alto	Altissimo
			1	2	3	4
	Alto	3	2 - Medio	2 - Medio	3 - Alto	4 - Altissimo
Probabilità	Medio	2	1 – Basso	2 - Medio	2 - Medio	3 - Alto
	Basso	1	1 – Basso	2 - Medio	2 - Medio	2 - Medio

I valori di rischio rilevati vanno confrontati con le misure di cui è prevista l'attuazione per contrastare gli eventi potenziali identificati per i diritti e le libertà degli interessati e

garantire la *compliance*.

1.4 Valutazione delle misure di trattamento del rischio

Se il valore del sistema di controllo di cui si prevede l'attuazione assume un valore almeno pari alla classe di rischio del processo, si può ritenere che i rischi rilevati siano ragionevolmente sotto controllo ed il processo di trattamento possa essere avviato/continuato.

In caso contrario occorre determinare misure di controllo che consentano di elevare l'efficacia del sistema di controllo.

Di seguito è riportata la scala di valutazione del sistema di misure che si intende adottare:

4 – Misure ad Altissima Efficacia	L'insieme di controlli implementati nell'area di processo sono in lineacon le migliori pratiche disponibili sul mercato
3 – Misure ad Alta Efficacia	È presente un sistema di controllo in linea con le buone pratiche organizzative e tecniche mediamente presenti sul mercato e pertanto presente alcune aree di potenziale vulnerabilità a fronte di minacce evolute (es. attacchi mirati)
2 – Misure ad Efficacia Media	È presente un sistema di controllo minimale, che consente dicontrastare le minacce note e derivanti da vulnerabilità ampiamente conosciute
1 – Misure inefficaci	Non sono presenti misure di controllo o sono inefficaci per contrastarei rischi rilevati e garantire la conformità del trattamento

2 ANALISI DEI PROCESSI DI TRATTAMENTO

In considerazione dell'attività svolta, i dati abitualmente trattati dall'Istituto Scolastico sono strettamente connessi allo svolgimento della funzione istituzionale e pertanto tali dati riguardano:

a) Gestione dati dipendenti/collaboratori/consulenti
b) Gestione dei dati relativi agli alunni e alle loro famiglie
c) Gestione dati fornitori

Per ogni processo di trattamento nel seguito si è pertanto proceduto a fornire:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle

finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati

Si procederà successivamente alla disamina delle misure per affrontare i rischi attualmenteadottate e di quelle da adottare.

2.1 Gestione dati dipendenti/collaboratori/consulenti nell'ambito rapporto lavorativo e/o di collaborazione

2.1.1 Descrizione processo di trattamento

Il trattamento in esame riguarda la gestione dei dati dei dipendenti - collaboratori - consulenti, di natura personale, sensibile e giudiziaria con lo scopo di dare corretta esecuzione al rapporto di lavoro e/o collaborazione.

L'istituto Scolastico gestisce tali dati al fine di consentire ai dipendenti/ collaboratori/consulenti l'esercizio di tutti i diritti di legge e previsti dai CCNL con riferimento alle funzioni espletate, nella qualità di datore di lavoro, nonché di controllare nei limiti di legge l'attività svolta dai dipendenti. Pertanto il trattamento di tali dati avviene per finalità specifiche, esplicite e legittime e legislativamente e contrattualmente previste.

I dati personali sono gestiti su base cartacea e informatizzata e dovrebbero essere trattati per tutta la durata del rapporto di lavoro e successivamente all'eventuale risoluzione del rapporto per il tempo previsto dalla normativa fiscale e lavoristica ai fini della prescrizione dei relativi diritti.

L'accesso a tali dati è consentito limitatamente alla Dirigente Scolastica, Collaboratori del DS, DSGAe ai soggetti facenti parte dell'unità organizzativa "segreteria".

2.1.2 Necessità e proporzionalità dei trattamenti

La base legale che legittima il trattamento di tali dati si fonda sull'esecuzione del contratto di lavoro e/o collaborazione stipulato con la Pubblica Amministrazione.
I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati. I dati sono accurati e costantemente mantenuti aggiornati nell'ambito della gestione del rapporto contrattuale.

I dati dovrebbero essere trattati per tutta la durata del rapporto di lavoro e successivamente all'eventuale risoluzione del contratto per il tempo previsto dalla normativa fiscale e giuslavoristica ai fini della prescrizione dei relativi diritti.

2.1.3 Valutazione dei rischi per i diritti e le libertà degli interessati (rischio intrinseco)

Nel caso di violazione o illecito trattamento di questa tipologia di dati, l'impatto sugli interessati avrebbe un livello MEDIO, in quanto l'eventuale violazione o trattamento illecito o indisponibilità potrebbe avere conseguenze non trascurabili per gli interessati sia

in termini di riservatezza che di disponibilità ed integrità legate all'impossibilità o alla limitazione per l'erogazione di servizi contrattualizzati con gli stessi interessati.

Considerata anche la non elevata probabilità di accadimento (tenuto conto dei dati storici) e delle misure di sicurezza adottate il rischio intrinseco connesso al processo di trattamento in oggetto è stato nel complesso valutato **MEDIO**.

2.2 Gestione dei dati relativi agli alunni e alle loro famiglie

2.2.1 Descrizione processo di trattamento

Il trattamento in esame riguarda la gestione dei dati degli alunni e delle loro famiglie di natura personale, sensibile e giudiziaria con lo scopo di dare corretta esecuzione alla funzione istituzionale svolta dall'Istituzione Scolastica.

L'istituto Scolastico gestisce tali dati al fine di consentire agli alunni e alle loro famiglie o esercenti la potestà l'esercizio di tutti i diritti di legge connessi all'espletamento della funzione istituzionale educativa e didattica svolta dall'Istituto Scolastico. Pertanto il trattamento di tali dati avviene per finalità specifiche, esplicite e legittime e legislativamente e contrattualmente previste.

I dati personali sono gestiti su base cartacea e informatizzata e dovrebbero essere trattati per tutta la durata del periodo di iscrizione dell'alunno alla scuola nonché limitatamente all'esecuzione degli obblighi di legge anche successivamente alla fine della frequenza dell'Istituto.

L'accesso a tali dati è consentito limitatamente alla Dirigente Scolastica, collaboratori del DS, docenti, DSGA e soggetti facenti parte dell'unità organizzativa "segreteria"

2.2.2 Necessità e proporzionalità dei trattamenti

La base legale che legittima il trattamento si fonda sugli obblighi di legge connessi all'espletamento della funzione istituzionale.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati. I dati sono accurati e costantemente mantenuti aggiornati nell'ambito della gestione del rapporto istituzionale.

I dati dovrebbero essere trattati per tutta la durata del periodo di iscrizione dell'alunno alla scuola nonché limitatamente all'esecuzione degli obblighi di legge anche successivamente alla fine della frequenza dell'Istituto.

2.2.3 Valutazione dei rischi per i diritti e le libertà degli interessati (rischio intrinseco)

Nel caso di violazione o illecito trattamento di questa tipologia di dati, l'impatto sugli interessati avrebbe un livello ALTO, in quanto l'eventuale violazione o trattamento illecito

o indisponibilità avrebbe la conseguenza di rilevare aspetti intimi della sfera personale di un individuo e/o dei suoi congiunti. Il rischio si potrebbe definire di alto livello poiché in questo caso trattasi di dati non solo di natura comune ma anche di natura sensibile e giudiziaria. Pertanto l'eventuale loro violazione potrebbe comportare danni di rilevante entità in capo agli alunni e anche alle loro famiglie e congiunti, riducendo drasticamente la sfera di libertà personale degli stessi.

Considerata anche la non elevata probabilità di accadimento (tenuto conto dei dati storici) e delle misure di sicurezza adottate il rischio intrinseco connesso al processo di trattamento in oggetto è stato nel complesso valutato **MEDIO**.

2.3 Gestione dati fornitori

2.3.1 Descrizione processo di trattamento

Il trattamento in esame riguarda la gestione dei dati aziendali dei fornitori e personali (identificativi) dei loro rappresentanti legali e referenti ai fini della gestione delle procedure di acquisto di beni e servizi.

L'Istituto Scolastico è pertanto in possesso dei dati identificativi aziendali e personali dei fornitori ai fini della sottoscrizione e gestione del contratto e del rapporto di fornitura anche con riferimento alla verifica e controllo iniziale e periodico dei requisiti di legge per la stipula di contratti con la PA. Pertanto il trattamento di tali dati avviene su base di legge e di contratto per finalità specifiche, esplicite e legittime.

I dati personali sono gestiti su base cartacea e informatizzata e dovrebbero essere trattati per tutta la durata della fornitura e successivamente all'eventuale risoluzione del contratto per il tempo previsto dalla normativa fiscale e tributaria ai fini della prescrizione dei relativi diritti.

L'accesso a tali dati è consentito limitatamente alla Dirigente Scolastica, collaboratori del DS, DSGAe soggetti facenti parte dell'unità organizzativa "segreteria".

2.3.2 Necessità e proporzionalità dei trattamenti

La base legale che legittima il trattamento si fonda sull'esecuzione del contratto di fornitura stipulato tra le parti.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati. I dati sono accurati e costantemente mantenuti aggiornati nell'ambito della gestione del rapporto contrattuale.

I dati dovrebbero essere trattati per tutta la durata della fornitura e successivamente all'eventuale risoluzione del contratto per il tempo previsto dalla normativa fiscale e tributaria ai fini della prescrizione dei relativi diritti.

2.3.3 Valutazione dei rischi per i diritti e le libertà degli interessati (rischio intrinseco)

Nel caso di violazione o illecito trattamento di questa tipologia di dati, l'impatto sugli interessati avrebbe un livello BASSO in quanto trattasi di dati di natura comune e coincidenti per la maggior parte con dati di natura pubblica (dati presenti su visure camerali…); pertanto l'eventuale loro violazione non arrecherebbe danni di rilevante entità alle aziende coinvolte.

Considerata anche la non elevata probabilità di accadimento (tenuto conto dei dati storici) e delle misure di sicurezza adottate il rischio intrinseco connesso al processo di trattamento in oggetto è stato nel complesso valutato **BASSO**.

3 INDIVIDUAZIONE DELLE MISURE PER AFFRONTARE I RISCHI

3.1 Misure fisiche

Allo stato attuale le misure fisiche adottate sono riconducibili per la gran parte dei trattamenti individuati all'utilizzo di archivi cartacei accessibili ai soli soggetti autorizzati.
Ai fini della *compliance* al GDPR si rende necessaria l'implementazione di una disciplina degli accessi agli archivi, delle forme di protezione da accessi non consentiti e dei tempi di utilizzabilità econservazione dei dati.

3.2 Misure informatiche

Sotto il profilo dell'infrastruttura informatica invece, la stessa risulta sotto il profilo progettuale dotata di sistemi di sicurezza adeguati al trattamento dei dati contenuti.
Ai fini della *compliance* al GDPR si rende necessaria l'implementazione di una serie di *good practices* ai fini della *privacy* e della sicurezza dei dati gestiti.
La politica di accesso alla rete e le comunicazioni da e per la struttura deve essere regolata mediante un accesso condizionato al fine di ridurre il rischio di furti e data breach.
La conservazione dei dati deve essere sia sulle Postazioni di lavoro informatizzate che sui server (operativi e di Backup) protetta al fine di ridurre il rischio di furti e *data breach*.
Deve essere adottata una politica di mantenimento dei dati (*policy backup*) atta a conservare i datinecessari e sottoposti ad obbligatorietà, tutti i dati non necessari devono essere distrutti; tutte le attività di monitoraggio devono essere inserite in apposito registro (*registro dei log*).
Tale gestione impone il rilascio di informativa apposita al personale che deve essere informato dell'eventualità che lo svolgimento di tali attività in abbinamento ai dati di controllo e accesso alle varie applicazioni potrebbe costituire una forma di profilazione e/o controllo a distanza dell'attività dei dipendenti sottoposta alle regole e limitazioni di cui all'art. 4 dello Statuto dei Lavoratori.
Si dovrà tenere un registro delle attività di assistenza tecnica remota e assegnare ad ogni soggetto abilitato al collegamento credenziali specifiche secondo una politica adatta al livello di sicurezza interessato; tutti gli accessi dall'esterno della rete locale dovranno avvenire attraverso l'uso di connessioni protette e criptate e le credenziali devono essere attribuite dall'amministrazione di sistema secondo procedura comunicata alla direzione.

3.3 Altre misure specifiche GDPR

Per affrontare i rischi rilevati vengono identificate inoltre le seguenti ulteriori misure in considerazione degli specifici adempimenti introdotti per effetto dell'entrata in vigore del GDPR:

- Provvedere alla **nomina del personale impegnato nel processo ed autorizzato al trattamento** dei dati personali, formalizzando le istruzioni a cui attenersi per il trattamentoei dati personali nell'espletamento delle proprie mansioni;
- Provvedere ad impartire **formazione di base** in maniera documentata e dimostrabile al **personale coinvolto nel processo** sulle corrette modalità di trattamento dei dati personali, con riferimenti a casistiche potenzialmente a rischio;
- **Adozione del registro dei trattamenti, delle procedure di Data breach, del regolamento diutilizzo degli strumenti informatici e del Manuale Privacy.**

Non risulta inoltre essere necessario ricorrere ad una P.I.A. in quanto il GDPR prevede come obbligatoria tale documentazione "*in tutti i casi in cui un trattamento di dati può presentare un rischio elevato per i diritti e le libertà delle persone"*. Alla luce della tipologia dei dati sopra evidenziati e delle ulteriori condizioni individuate dal Regolamento non risulta necessaria la redazione di tale documento.

4 DATA PROTECTION OFFICER

Alla luce delle risultanze del presente Documento di valutazione dei rischi e della tipologia di dati trattati e del rischio connessi al trattamento di tali dati, l'Istituzione scolastica ritiene che sia necessaria la nomina del Data Protection Officer.

Infatti, ai sensi dell'art. 37 del GDPR il DPO, anche detto Responsabile della Protezione dei Dati (RPD), deve essere designato quando:

a. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico – eccetto le autorità giurisdizionali;
b. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

I trattamenti posti in essere da questa Istituzione Scolastica rientrano nei casi previsti dal GDPR anche alla luce delle linee guida in materia sia del Gruppo di Lavoro Articolo 29 che del Garante per la protezione dei dati personali.

5 AGGIORNAMENTI DEL DOCUMENTO

Il presente Documento di valutazione dei rischi verrà periodicamente aggiornato ogni volta

in cui l'organizzazione dell'Istituzione scolastica dovesse subire delle modifiche importanti e radicalinonché ogni volta in cui verranno poste in essere attività che andranno ad incidere in maniera decisiva e importante sulla tipologia dei dati trattati.
In ogni caso annualmente si effettuerà un'attività di controllo delle informazioni contenute nel presente Documento anche al fine di verificare la necessità di modificare eventuali misure di sicurezza adottate.

Firmato
La Dirigente Scolastica
Prof.ssa Giovanna CARATOZZOLO