

Data Protection Impact Assessment
Istituto Istruzione Superiore
“Vanvitelli Stracca Angelini” di Ancona

Indice

1. Panoramica	4
Introduzione	4
Contesto	4
Schema di riepilogo	5
2. Processo di valutazione dei trattamenti	7
Flusso operativo	7
Mappatura dei Dati	8
Risorse coinvolte nel processo di trattamento dei dati	9
Internal IT	9
External IT	9
Not IT Assessment	9
(Sistemi di trattamento non informatizzati)	9
Gestione degli accessi ai trattamenti	9
Identificazione e autenticazione	10
Controllo accessi	10
Gestione dei supporti e dei documenti cartacei	10
Gestione delle risorse umane	10
Formazione	10
Funzioni e obblighi	10
Conseguenze per violazioni	11
Acquisizione dati personali	11
3. Necessità e proporzionalità del trattamento	13
Contesto generale che giustifica il trattamento e la valutazione d'impatto	13
Interessi legittimi	13
4. Rischi e Correttivi	14
Metodologia di valutazione del rischio	14
Minacce ai dati personali	14
Rischi connessi alla violazione della riservatezza o dell'integrità dei dati	15

Rischi connessi alla perdita di dati personali	17
Rischi connessi all'esercizio dei diritti conferiti dal GDPR	19
Misure relative alla sicurezza e controlli esistenti o pianificati	22
5. Informazioni di supporto	23
Codici di condotta	24
Certificazioni	24
Richieste degli interessati	24
Consultazione con il responsabile della protezione dei dati (DPO)/Indicazione dei remedies	24
6. Conclusioni	
Valutazione finale	24
Rischio residuale	25

1. Panoramica

Introduzione

La valutazione d'impatto sulla protezione dei dati (DPIA, acronimo di Data Protection Impact Assessment) rappresenta l'output del processo di analisi del trattamento dei dati personali per l'IIS "Vanvitelli Stracca Angelini" di Ancona. Questo documento è quindi un'analisi delle attività di trattamento attualmente gestite e delle relative valutazioni. Esso evidenzia i dettagli dell'attività di elaborazione stessa e fornisce una valutazione dei rischi associati al trattamento, suggerendo eventualmente le misure che possono essere adottate per mitigarli, anche grazie ad un'eventuale consultazione preliminare con il Responsabile per la Protezione dei Dati (RDP) competente.

Il titolare del trattamento elabora la DPIA ai sensi dell'articolo 35 del GDPR, laddove il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche (l'interessato).

Questo documento, nelle sue varie parti:

- valuta i rischi per la privacy personale nei processi;
- identifica le misure, le salvaguardie e i meccanismi esistenti o pianificati per garantire la protezione dei dati personali;
- identifica, ove ve ne sia necessità, il corretto bilanciamento tra i diritti alla privacy dell'individuo e quelli di raccolta ed elaborazione dei dati per finalità legittime dell'Istituzione scolastica e dell'interessato

Contesto

Il trattamento dei dati personali è realizzato per mezzo delle operazioni indicate all'art. 4 Codice Privacy e all'art. 4 n. 2) GDPR e precisamente: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione dei dati. I dati personali sono sottoposti a trattamento sia cartaceo che elettronico e/o automatizzato.

Il trattamento riguarda le seguenti categorie di dati:

- degli studenti e dei genitori (o tutori);
- dei fornitori e dei referenti commerciali;
- dei dipendenti (personale docente ed ATA)

I dati relativi a studenti, docenti e dipendenti riguardano: anagrafiche (nome, cognome, recapiti telefonici, residenza, e-mail), curriculum vitae, coordinate bancarie per pagamento degli stipendi; quest'ultimi sono acquisiti per consenso degli interessati al momento della sottoscrizione del contratto di lavoro e sono destinati all'amministrazione dell'istituzione scolastica per le attività di gestione del rapporto d'impiego.

I dati relativi ai referenti commerciali delle imprese fornitrici riguardano: anagrafiche, indicazione della azienda di appartenenza e tutti i dati necessari per l'esercizio del rapporto commerciale. Tali dati sono acquisiti per consenso degli interessati al momento della sottoscrizione del contratto commerciale.

Schema di riepilogo

Tavola di Riferimento con le Informazioni Chiave		
(a)	Titolare del trattamento	IIS "Vanvitelli Stracca Angelini" Ancona Dirigente Scolastico pro-tempore
(b)	Responsabile del trattamento	Il Responsabile del Trattamento interno è una figura che coincide solitamente con la figura del DSGA o eventualmente con un Collaboratore del Dirigente.
(c)	Incaricati al trattamento	a vario titolo: personale docente (per gli alunni delle proprie classi) personale ATA (in particolare assistenti amministrativi della segreteria didattica, con responsabilità sul trattamento dei dati degli alunni, assistenti amministrativi della segreteria del personale con riferimento al trattamento dei dati del personale docente/ATA)
(d)	Descrizione del Trattamento	Trattamento dati studenti Trattamento commerciale Trattamento dipendenti
(e)	Scopo del Trattamento	Esecuzione attività didattica Esecuzione contratti commerciali Esecuzione contratti lavorativi
(f)	Contesto, ambito e background	Ambito educativo e formativo (dati relativi agli studenti) Ambito commerciale (dati relativi ai referenti) Ambito lavorativo (dati relativi ai dipendenti). Acquisiti contestualmente alla stipula dei contratti, con consenso.
(g)	Soggetti coinvolti nel trattamento e relative mansioni	Titolare del trattamento Responsabili esterni Incaricati
(h)	Tipologia di dati personali	Anagrafici relativi agli studenti. Anagrafici relativi ai referenti aziendali Anagrafici, codici malattia, presenze relativi ai dipendenti
(i)	Categorie speciali di dati	Assenti
(l)	Destinatari dei dati personali	Amministrazione e dirigenza, interni all'azienda Consulenti esterni, Enti e/o Associazioni nell'ambito di Cultura e Spettacolo.

Il trattamento ha finalità legate all'esecuzione delle attività espletate dall'Istituzione Scolastica e non eccede tale finalità. L'Istituto non effettua alcun tipo di profilazione e la gestione del trattamento viene esplicitata nell'Informativa privacy presente sul sito istituzionale. I dati raccolti, sia come singolo record che come aggregati, non eccedono la portata strettamente necessaria alla finalità, dunque sono minimizzati, *by default*, le eventuali integrazioni richieste hanno esclusivamente relazione allo scopo definito.

Attualmente i dati hanno un periodo di archiviazione indefinito, ma viene proposto, tra i remedies di limitarne l'archiviazione ai soli fini legali (creditizi o fiscali) i dati vengono aggiornati con regolarità nell'interesse delle imprese clienti o del lavoratore.

2. Processo di valutazione dei trattamenti

Flusso operativo

Le operazioni di elaborazione previste nel processo di valutazione dei trattamenti possono essere suddivise in sei fasi:



1. Pianificazione della Valutazione

Sono individuate le funzioni dell'Istituto e le persone che possono rendere disponibili le conoscenze, le prassi e la documentazione presenti, per quanto riguarda il trattamento dei dati e le esigenze tecniche e normative del GDPR. E si stabilisce un piano di attività per lo svolgimento del processo di valutazione.

2. Raccolta e analisi dei dati

In questa fase vengono raccolte tutte le informazioni necessarie a mappare i sistemi informativi ed il flusso di gestione documentale presenti. L'obiettivo è che lo sforzo di adeguamento alle linee guida del GDPR comporti un complessivo miglioramento degli asset informativi e tecnici.

3. Stesura e redazione della DPIA

In base alle risultanze delle interviste ed all'analisi dei dati viene aggiornata la DPIA.

4. Revisione di gruppo

Il documento finale viene revisionato alla presenza del Titolare del Trattamento, del Responsabile IT e quindi sottoposto anche alla verifica del RPD/DPO.

5. Redazione dei report

Una volta terminata la valutazione, si procede alla redazione di report, che costituiranno parte integrante di un processo di revisione atto a garantire che l'analisi del rischio venga effettuata correttamente, innescando un processo di revisione e aggiornamento continuo.

6. Condivisione dei risultati

A revisioni concluse i risultati sono condivisi tra il titolare e chi è intervenuto nel processo.

Mappatura dei Dati

In questa sezione della DPIA è presentata una mappatura di tutti i dati personali presenti nei contesti dell'Istituzione Scolastica.

Le attività di archiviazione sono effettuate, per i dati digitali, con il software gestionale, gestito dall'azienda esterna Axios; i dati cartacei, invece, sono conservati in archivio, sito nei locali degli uffici amministrativi, il cui accesso è ristretto ai soli autorizzati.

Dati gestione Studenti:

- Nome, Cognome, Recapiti telefonici, Indirizzi residenza email, Coordinate bancarie per pagamento borse di studio.
- Destinati a: Segreteria Studenti

Dati gestione Dipendenti:

- Nome, Cognome, Recapiti telefonici, Indirizzi residenza email, Coordinate bancarie per pagamento stipendi, Curriculum Vitae
- Destinati a: Amministrazione

Dati gestione commerciale referenti clienti e fornitori

- Nome, Cognome, Recapiti telefonici, indirizzi email, Azienda di appartenenza.
- Destinatari: Amministrazione

Archiviati su:

- Software gestionale cloud-based, accessibile via browser web, gestito dalla azienda esterna Axios.
- Armadio in archivio cartaceo negli uffici amministrativi (restrizione degli accessi all'archivio ai soli autorizzati)

Risorse coinvolte nel processo di trattamento dei dati

Questa sezione della DPIA contiene un elenco delle risorse attraverso le quali avviene l'elaborazione dei dati personali, sia interni che esterni.

Internal IT

(Sistemi IT interni all'azienda/Ente)

Postazioni PC dei dipendenti, per elaborazione dati ed accesso al sw gestionale.

Software gestionale cloud-based, accessibile via browser web, gestito dalla azienda esterna Axios

n. 1 PC Ufficio DS

n. 1 PC Ufficio DSGA

n. 6 PC Ufficio della segreteria amministrativa e del personale

n. 5 PC Ufficio della segreteria didattica

External IT

(Sistemi IT esterni all'azienda/Ente)

Il dominio www.istvas.edu.it è un sito ospitato su un server esterno la cui gestione tecnica e operativa è affidata al provider di hosting specializzato, Register.it

Il sito web non ha sezioni con accesso protetto tramite login e password.

Not IT Assessment

(Sistemi di trattamento non informatizzati)

Archivio cartaceo presso gli uffici amministrativi dell'Istituzione Scolastica riguardanti anche anni scolastici precedenti. L'istituzione scolastica sta progressivamente digitalizzando i fascicoli degli alunni e del personale rendendoli "fascicoli elettronici"

Gestione degli accessi ai trattamenti

In questa sezione vengono descritte le misure, regole, procedure e norme per la gestione degli accessi ai trattamenti.

Identificazione e autenticazione

I PC sono dotati di password, le credenziali vengono attribuite ai singoli dipendenti.

Controllo accessi

Ai dipendenti vengono attribuite le credenziali per l'accesso al Software gestionale cloud-based, accessibile via browser web, con protocollo HTTPS, ed altresì le credenziali per l'accesso all'archivio documenti che si trova nel server interno alla scuola.

Gestione dei supporti e dei documenti cartacei

Archivi documentali cartacei in locali ad accesso ristretto.

Gestione delle risorse umane

In questa sezione vengono descritte le procedure di gestione delle risorse umane coinvolte nel trattamento dei dati personali: politiche di formazione, funzioni e obblighi ed eventuali previsioni sanzionatorie per i trasgressori.

Formazione

Viene effettuato un intervento di formazione in favore di tutto il personale in materia di privacy e gestione documentale, in ottemperanza a quanto sancito dal GDPR 679/2016.

Funzioni e obblighi

Tutto il personale è formalmente “Incaricato al trattamento dei dati”:

- I docenti sono incaricati al trattamento dei dati relativamente agli alunni delle classi in cui prestano servizio;
- Il personale della segreteria didattica ha l’incarico relativo al trattamento dei dati degli alunni dell’intera istituzione scolastica; la segreteria del personale ha l’incarico al trattamento dei dati relativi il personale dell’istituzione scolastica;
- Il dirigente scolastico nella sua qualità di rappresentante legale pro-tempore dell’Istituzione Scolastica “Titolare del trattamento” con l’obbligo di segnalare eventuali DATA BREACH alle autorità competenti (Garante privacy) ed effettuare la valutazione dei rischi.

Conseguenze per violazioni

Segnalazione al Garante Privacy

Sanzioni disciplinari ai sensi del CCNL Scuola e della normativa.

Acquisizione dati personali

Questa sezione descrive in dettaglio i tipi di informazioni personali che l'Ente raccoglie dagli interessati:

I soggetti interessati vengono informati del trattamento, tramite il rimando all'Informativa e con il consenso inserito a tergo del contratto (commerciale e di lavoro). Il consenso viene firmato contestualmente al contratto. Su richiesta espressa, i dati vengono concessi ai fini della portabilità. Il diritto alla cancellazione viene concesso su apposita richiesta, salvo finalità legali o fiscali che lo rendano illegittimo. Non sono definite durate massime del tempo di vita dei dati. Alcuni dati in archivio cartaceo potrebbero aver superato il tempo di vita massimo stimato e andrebbero eliminati.

Studenti

- Nome, Cognome
- Indirizzo
- Indirizzo Email
- Numeri di telefono fisso e cellulare
- Codice Fiscale

Genitori degli studenti (o tutori)

- Nome, Cognome
- Indirizzo
- Indirizzo Email
- Numeri di telefono fisso e cellulare
- Codice Fiscale

Dipendenti (docenti e personale ATA):

- Nome, Cognome
- Indirizzo
- Indirizzo Email
- Numeri di telefono fisso e cellulare
- Dati finanziari
- Codice Fiscale o Partita IVA
- Curriculum Vitae
- Orari di entrata e uscita del dipendente

Referenti Commerciali:

- Nome, Cognome
- Indirizzo
- Azienda per cui lavora e posizione aziendale
- Numeri di telefono fisso e cellulare
- Codice Fiscale o Partita IVA

L'eventuale collezione di dati appartenenti alle cosiddette categorie particolari di dati personali (Art. 9 Reg. UE 679/2016) è indicata nel riquadro seguente:

Assenti.

3. Necessità e proporzionalità del trattamento

La validità di quanto dedotto durante il processo di valutazione è direttamente connesso all'integrità e alla completezza delle informazioni raccolte nello svolgimento dello stesso.

Contesto generale che giustifica il trattamento e la valutazione d'impatto

Considerata la natura dei dati raccolti, il contesto, l'ambito e le finalità legittime dei trattamenti, tenuto conto delle indicazioni contenute nei "considerando dal 47 al 51" del *Regolamento (UE) 2016/679*, la valutazione d'impatto viene effettuata al fine di ridurre ulteriormente il rischio di eventuali minacce all'integrità dei diritti e le libertà degli interessati. La raccolta dei dati è limitata a quelli necessari per l'esecuzione delle attività dell'Istituzione Scolastica.

Interessi legittimi

L'Istituto gestisce trattamenti come descritto in **Sezione 1** e **Sezione 2**. I trattamenti dei dati personali sono funzionali all'ottenimento degli interessi legittimi e non vengono usati per altri fini.

L'Istituto ha pertanto un legittimo interesse:

I trattamenti descritti e mappati nella DPIA sono conformi con le indicazioni del considerando 47 (GDPR) e non sussistono altre finalità oltre quelle relative alla corretta esecuzione delle attività e dei contratti commerciali e di lavoro, stipulati dal titolare del trattamento

Come datore di lavoro, l'Istituto raccoglie i dati del personale e dei partner esterni al fine di:

- Offrire una corretta esecuzione dei rapporti contrattuali
- Migliorare le capacità personali
- Rispondere alle esigenze di conformità normativa
- Garantire la produttività e retribuzione del personale dipendente

4. Rischi e Correttivi

Metodologia di valutazione del rischio

Il campo di applicazione di questa valutazione è limitato ai rischi che potrebbero comportare danni fisici, materiali o immateriali alla persona interessata (soggetto portatore di interessi), comprese eventuali discriminazioni, danni alla reputazione, perdita di riservatezza dei dati protetti dal segreto professionale, o qualsiasi altro significativo svantaggio economico o sociale. Eventuali altri rischi cui l'organizzazione può esporsi, ma che non incidono sulla privacy, sono oltre lo scopo della presente DPIA.

Nella analisi, tutti i rischi sono anche associati a una probabilità:

- ☐ **4: Quasi certo.** Probabilità estremamente alta. Il verificarsi dello scenario costituisce un evento quasi certo.
- ☐ **3: Probabile.** Alta possibilità che lo scenario descritto possa verificarsi.
- ☐ **2: Possibile.** Possibilità media che lo scenario descritto possa verificarsi.
- ☐ **1: Improbabile.** Possibilità bassa che lo scenario possa verificarsi.
- ☐ **0: Quasi impossibile.** Possibilità quasi nulla che lo scenario possa verificarsi.

I rischi sono anche associati a una gravità.

- ☐ **4: Critico.** Danno significativo e reale a un gran numero di interessati (soggetti dei dati), ad esempio una violazione dei dati su larga scala.
- ☐ **3: Grave.** Danno significativo e reale a uno o ad un numero limitato di interessati o danno di entità minore a un gran numero di interessati.
- ☐ **2: Moderato.** Danno di entità limitata a uno o ad un numero limitato di interessati o invece danno di entità minima a un gran numero di interessati.
- ☐ **1: Minimo.** Problema minore o procedurale che non comporta danni significativi.
- ☐ **0: Quasi nullo.** Non vi è praticamente alcun danno reale (*e.g. furto/perdita di dati anonimizzati o pseudonimizzati*).

Minacce ai dati personali

A seguire vengono indicate le possibili minacce alla privacy, dal punto di vista dell'interessato:

- 1. Divulgazione di dati personali.** Le informazioni fornite al titolare del trattamento sono confidenziali e potrebbero arrecare un danno all'interessato se circolassero impropriamente.
- 2. Integrità dei dati personali.** L'interessato potrebbe subire un danno qualora i suoi dati personali - sebbene utilizzati legittimamente - risultassero non corretti, o venissero corrotti durante il trasporto/elaborazione/archiviazione, oppure risultassero confusi erroneamente con i dati di un'altra persona.
- 3. Perdita di dati personali.** L'interessato ha la legittima aspettativa che i propri dati vengano custoditi in maniera sicura e possano essere recuperati durante l'intero periodo di conservazione.
- 4. Mancanza di capacità di esercitare i diritti previsti dalla legge sulla protezione dei dati.** L'interessato ha la legittima aspettativa di poter esercitare i diritti garantiti dal Regolamento UE 679/2016 e potrebbe subire un danno dalla mancata capacità del Titolare del trattamento di adempiere ai suoi doveri.

Le sezioni seguenti trattano i rischi relativi a queste minacce, considerando separatamente:

- Minacce alla riservatezza o all'integrità dei dati personali (punti 1 e 2 dell'elenco);
- Minacce alla perdita o alla disponibilità di dati personali (punto 3 dell'elenco);
- Minacce alla facoltà di esercitare i propri diritti secondo GDPR (punto 4 dell'elenco).

Rischi connessi alla violazione della riservatezza o dell'integrità dei dati

La tabella seguente mostra i rischi relativi alla perdita o alla cancellazione dei dati personali.

Ar	ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
T	1	Intercettazione di dati in transito nel software gestionale esterno durante la trasmissione, l'utilizzo o la visualizzazione.	1	1	Correttivi in atto: - Il software gestionale cloud-based, accessibile via browser web, solo con credenziali - la connessione con il sito web avviene con il protocollo HTTPS, quindi sicuro e crittografato Correttivi suggeriti: Correttivi possibili:
T	2	Accesso fisico ai dati in trattamento memorizzati nei server.	0	1	Correttivi in atto: - Il server e le workstation dei dipendenti sono in locali ad accesso ristretto. - l'accesso alle informazioni memorizzate nel server è permesso solo personale qualificato e di fiducia Correttivi suggeriti: - proteggere l'accesso fisico con sistemi anti intrusione Correttivi possibili:
T	3	La vulnerabilità del software, la mancata patch o il malware nel sistema consentono l'accesso di un utente malintenzionato e causano una violazione dei dati.	2	2	Correttivi in atto: - Antivirus omogeneo installato sulle workstation dei dipendenti. - Aggiornamenti del S.O. e dei browser per l'accesso a internet Correttivi suggeriti: Correttivi possibili:

T	4	La password dell'amministratore o degli incaricati per l'accesso al software gestionale esterno viene indovinata, trovata o ottenuta consentendo l'accesso ai dati nel sistema o nei sistemi organizzativi.	1	2	Correttivi in atto: - Password policy in atto per la definizione delle credenziali dei dipendenti aziendali. - Accessi al gestionale distinti per ogni dipendente. Correttivi suggeriti: Correttivi possibili:
T	5	Le informazioni vengono recuperate in modo illecito dall'accesso non autorizzato ai sistemi dell'Istituzione Scolastica da locazioni remote.	1	2	Correttivi in atto: - Firewall attivi sulle workstation Correttivi suggeriti: - Installazione di un firewall aziendale perimetrale, a protezione della rete interna Correttivi possibili:

Rischi connessi alla perdita di dati personali

La tabella seguente mostra i rischi relativi alla perdita o alla cancellazione dei dati personali. Si noti che alcuni dei rischi valutati nella precedente tabella potrebbero anche comportare la cancellazione/perdita dei dati, e pertanto figurare anche nella presente Sezione

Ar	ID	Natura del rischio	Probabilità	Gravità	- Correttivi e adeguamenti possibili
T	6	Il fallimento del backup che implica una perdita permanente di dati	0	1	Correttivi in atto: - Il backup dei database del software gestionale esterno gestito dalla società Axios - Archivio documenti interno i Backup avvengono con periodicità giornaliera e settimanale su HD Esterni e NAS Correttivi suggeriti: Correttivi possibili: - Archivio documenti interno Possibilità di eseguire una copia mensile su cloud
T	7	La vulnerabilità del software, le mancata patch o il malware possono causare la perdita di dati di dati (Ex. ransomware)	2	2	Correttivi in atto: - Antivirus omogeneo installato sulle workstation dei dipendenti. - Aggiornamenti del S.O. e dei browser per l'accesso a internet Correttivi suggeriti: Correttivi possibili:

T	8	Interruzione durante il trattamento (ad esempio guasto dell'attrezzatura, guasto della connettività, allarme antincendio)	0	0	Correttivi in atto: - Vengono eseguiti controlli regolari, ed aggiornati annualmente, sullo stato di sicurezza fisica dell'edificio e della struttura annessa. Correttivi suggeriti: - Correttivi possibili:
---	---	---	---	---	--

Rischi connessi all'esercizio dei diritti conferiti dal GDPR

La tabella seguente mostra i rischi relativi alla mancata facoltà di esercitare i propri diritti.

Ar	ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
T	9	Rischio che i dati vengano elaborati da un incaricato (al trattamento dei dati personali) che non soddisfa i requisiti di protezione dei dati	0	1	Correttivi in atto: - Gli incaricati che hanno accesso ai dati personali sono definiti chiaramente nell'organigramma aziendale. - L'accesso all'archivio cartaceo è ristretto e limitato ai soli aventi diritto. - Esistono account distinti, per ciascun dipendente, per l'accesso al gestionale. Correttivi suggeriti: Correttivi possibili:
T	10	I dati personali vengono conservati più a lungo del necessario	2	1	Correttivi in atto: - E' facile tracciare i dati immagazzinati nel software gestionale a fine di cancellazione. Correttivi suggeriti: - Definire un tempo di vita massimo per tutti i dati ed un processo interno per cancellare quei dati che hanno oltrepassato il tempo di vita massimo Correttivi possibili:
T	11	Difficoltà e non immediatezza nel rilevare ed identificare una fuoriuscita dei dati archiviati nelle Basi di Dati del software gestionale esterno, può condurre alla non possibilità di ottemperare all'obbligo di notifica al Garante.	2	2	Correttivi in atto: Correttivi suggeriti: - Richiedere l'attivazione della feature che abilita il controllo e la notifica degli accessi al software gestionale. Correttivi possibili: - Backup dei log degli accessi al server e delle operazioni utente.

Misure relative alla sicurezza e controlli esistenti o pianificati

Ar	ID	Misura di sicurezza	Tipologia	SI	NO
T	1	Crittografia			X
T	2	Anonimizzazione			X
T	3	Partizionamento dei dati		X	
T	4	Controllo degli accessi	Archivi di Dati personali in locali ad accesso ristretto ai soli aventi diritto.	X	
T	5	Tracciabilità			X
T	6	Archiviazione		X	
T	7	Sicurezza dei documenti cartacei	Archivio documentale cartaceo ad accesso ristretto.	X	
L T	8	Minimizzazione dei dati			X
T	9	Vulnerabilità			X
T	10	Prevenzione malware	Postazioni PC con antivirus installati	X	
T	11	Gestione postazioni		X	
T	12	Sicurezza dei siti web		X	
T	13	Backup	Pianificato: backup regolari su supporti esterni dei dati presenti nel server interno Pianificato: backup del software gestionale.	X	
T	14	Manutenzione	La Scuola ha un contratto per la manutenzione dei propri sistemi (hardware e software) con professionista esterno	X	
L	15	Contratti di trattamento	I responsabili sia interni che esterni hanno adeguato i prodotti al GDPR. Stipulare nomine agli incaricati	X	
T	16	Sicurezza della rete		X	
L T	17	Controllo degli accessi fisici	Locali ad accesso ristretto	X	
T	18	Monitoraggio dell'attività della rete		X	
T	19	Sicurezza dell'hardware			X
L	20	Prevenzione dalle fonti di rischio	Controlli regolari ed aggiornati annualmente sullo stato di sicurezza fisica dell'edificio e delle strutture annesse. Sistemi antintrusione e videosorveglianza per proteggere gli accessi alla struttura.	X	
L	21	Protezione contro le fonti di rischio	Controlli regolari ed aggiornati annualmente sullo stato di sicurezza fisica dell'edificio e delle strutture annesse.	X	
L	22	Organizzazione		X	
L T	23	Politiche		X	
L T	24	Gestione dei rischi sulla privacy		X	
T	25	Privacy by Design		X	
L T	26	Gestire le violazioni della privacy		X	
L	27	Gestione del personale		X	
L	28	Relazioni con terze parti		X	
L	29	Supervisione		X	
T	30	Pseudonimizzazione			X

5. Informazioni di supporto

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- "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";
 - "dimostrare la conformità al regolamento". Nel valutare l'impatto di un trattamento va tenuto conto (articolo 35, paragrafo 8) del rispetto di un codice di condotta (articolo 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata.

Codici di condotta

CCNL Scuola – Codice di comportamento dei dipendenti pubblici

Certificazioni

L'istituzione scolastica non è in possesso di certificazioni aziendali di tipo ISO, certificazioni di qualità o procedurali, certificazioni tecniche, che riducono la responsabilità diretta del titolare del trattamento.

Richieste degli interessati

L'articolo 35, paragrafo 9, del GDPR stabilisce che, se del caso, il Titolare del trattamento deve chiedere il parere degli interessati o dei loro rappresentanti in merito al trattamento previsto. Il parere non è stato richiesto poiché non necessario.

Consultazione con il responsabile della protezione dei dati (DPO)/Indicazione dei remedies

Ai fini di una corretta ed adeguata *compliance* si consigliano le seguenti attività:

- Definizione di tempi di vita massima dei dati raccolti;
- Attivare procedure di controllo a cadenza (almeno) annuale dei rimedi messi in atto;
- Previsione di un vademecum (codice di condotta) da sottoporre al personale incaricato al momento del conferimento dell'incarico e della sottoscrizione del consenso. Il codice deve contenere una sanzione per la violazione degli obblighi di correttezza nel trattamento dei dati personali;
- Redigere i contratti di nomina dei responsabili esterni;
- Redigere le lettere d'incarico per il personale interno;
- Assicurarsi che il personale sia adeguatamente formato sulla sicurezza informatica;
- Implementare politiche di backup efficaci e investire in misure di protezione migliorate.

Valutazione finale

Il Titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché delle diverse probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche, mette in atto

misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento. Dette misure saranno riesaminate e aggiornate qualora necessario.

Nelle precedenti sezioni di questa DPIA:

- è stato presentato il processo di trattamento dei dati personali e fornita una panoramica funzionale;
- è stata descritta la mappatura dei dati personali identificati ed è stato evidenziato il loro percorso nel contesto dell'Istituzione Scolastica;
- sono stati identificati i trattamenti, i loro scopi e gli interessi legittimi nel condurre tale elaborazione;
- sono stati analizzati e mappati i rischi per la privacy dell'interessato e le contromisure in atto per la mitigazione di tali rischi;
- sono state identificate le criticità e le mancanze che sono causa di rischio e proposti rimedi atti alla mitigazione del rischio.

Nella Sezione successiva si andrà a valutare se permane un rischio residuo elevato e se risulti pertanto necessaria una consultazione con l'autorità di controllo.

Rischio residuale

Il Gruppo dell'articolo 29 (WP29) per la tutela dei dati, nelle Linee Guida sulla DPIA, fornisce una definizione di rischio residuo elevato inaccettabile: *“casi in cui le persone gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota)”*.

Nei trattamenti di questa Istituzione Scolastica, non si rilevano condizioni di rischio residuo elevato. Questa Istituzione Scolastica gestisce il suo programma di valutazione in modo professionale e attenua i rischi in larga misura.

Un rischio marginale di violazione dati potrebbe derivare nel caso di attacchi informatici portato con successo (virus) o in caso di furto di macchinari e/o dispositivi.

Non sembra che il rischio residuo esista in quest'area.

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi elevati residui.

..... Settembre 2025

Il Titolare del Trattamento