

Informazioni sul PIA

PIA

Istituto Comprensivo di Ostellato

Nome autore

Dott.ssa Antonietta Allegretta

Data di creazione

17/05/2018

Nome DPO

Da definire

Parere DPO

Da raccogliere

Contesto

Panoramica

Quale è il trattamento in considerazione?

L'Istituto tratta dati personali di alunni, dipendenti e fornitori, tra i quali, assimilabili alla connotazione di "dati sensibili", vengono indicati quelli relativi alla presenza di certificazione della situazione di handicap relativa ad alcuni alunni; alla casuale presentazione di documentazioni prodotte da dipendenti o utenti, recanti notizie sullo stato di salute dei soggetti interessati; alle condizioni economiche delle famiglie degli alunni; ai dati giudiziari dei fornitori.

Le finalità sono:

- Garanzia del servizio scolastico offerto all'utenza del Comune
- Gestione del personale interno con contratto a tempo determinato e indeterminato
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori

Quali sono le responsabilità legate al trattamento?

Il Titolare del trattamento dei dati è responsabile delle decisioni che assume in ordine alle modalità, alle finalità e all'esercizio della vigilanza in relazione al trattamento dei dati

Il Responsabile del Trattamento dei dati è individuato nella figura del Direttore dei Servizi Generali ed Amministrativi ed ha compiti specifici nelle seguenti aree:

- coordinamento delle procedure operative messe in atto dagli Incaricati relativamente al trattamento dei dati
- organizzazione delle procedure di archiviazione
- organizzazione delle procedure di protezione informatica dei dati trattati elettronicamente

DOCENTI Incaricati del trattamento dati personali degli Alunni

I docenti sono incaricati del trattamento dati alunni e hanno responsabilità precise nelle seguenti aree:

- organizzazione delle attività educative didattiche relativamente a scelte delle famiglie
- assenze degli alunni e relativa certificazione

- documentazione relativa ad alunni portatori di handicap
- comunicazioni riservate con la famiglia

Le unità della Segreteria sono incaricate del trattamento dati riguardanti gli alunni e hanno responsabilità precise nelle seguenti aree:

- Atti connessi all'iscrizione
- Atti gestione corrente
- Attività extrascolastiche o integrative
- Dati neutri
- Atti rari o straordinari

Le unità della Segreteria sono incaricate del trattamento dati riguardanti il personale docente e ATA dell'Istituto e hanno responsabilità precise nelle seguenti aree:

- Atti connessi alla gestione del fascicolo personale
- Atti connessi alla gestione di assenze, permessi, congedi, aspettative e simili
- Atti connessi alla carriera
- Gestione graduatorie e nomine
- Atti connessi ai rapporti sindacali
- Atti connessi ai rapporti economici, previdenziali, fiscali

Le unità della Segreteria sono incaricate del trattamento dati riguardanti la gestione finanziaria contabile dell'Istituto e hanno responsabilità precise nelle seguenti aree:

- Atti connessi alla stipula dei contratti per le collaborazioni professionali attivate nell'ambito del POF
- Atti connessi alla gestione del bilancio
- Atti connessi all'approvvigionamento di beni e servizi

Le unità della Segreteria sono incaricate del trattamento dati riguardanti la gestione della comunicazione istituzionale e hanno responsabilità precise nelle seguenti aree:

- Atti connessi alla gestione istituzionale
- Atti connessi alla gestione del Protocollo, della posta ordinaria e della posta elettronica

COLLABORATORI SCOLASTICI

I Collaboratori scolastici e il personale ausiliario sono incaricati del trattamento dati alunni e hanno responsabilità precise nelle seguenti aree:

- Atti connessi ad attività di collaborazione con la segreteria nelle operazioni di fotocopiatura
- Atti connessi al trasporto, spostamento di registri e documenti contenenti dati riguardanti gli alunni
- Stato di salute degli alunni nei casi particolari in cui si richiede un loro intervento o assistenza (es. alunni H o che hanno alcune problematiche tipo diabete o che necessitano di farmaci salvavita).

ORGANI COLLEGIALI

I membri degli organi collegiali in funzione della loro carica elettiva possono venire a contatto con informazioni e decisioni riguardanti terzi, pertanto devono essere destinatari di incarico di

trattamento dati e hanno responsabilità precise in tutte le delibere relative alle materie trattate dagli Organi Collegiali di appartenenza.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

L'istituzione Scolastica, con riferimento ai destinatari o famigliari dei destinatari dell'offerta formativa, ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo coinvolti in rapporti negoziali con l'istituzione scolastica, o aspiranti ad assumere tale ruolo, dichiara di trattare i dati di seguito elencati:

- a. dati identificativi univocamente riconducibili ad un soggetto fisico identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio stato di famiglia, codice fiscale;
- b. dati identificativi univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la partita IVA e il codice Fiscale;
- c. dati sensibili o particolari;
- d. dati giudiziari;
- e. dati inerenti il livello d'istruzione e culturale nonché dati relativi all'esito di scrutini ed esami, piani di studio personalizzati, piani di studio individualizzati;
- f. dati inerenti le condizioni economiche;
- g. dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, presso autorità giurisdizionali italiane o estere
- h. dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei famigliari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;
- i. dati provenienti da pubblici registri, elenchi, graduatorie o documenti conoscibili da chiunque;
- j. dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi, o di opere ovvero proposte ed offerte inerenti le medesime negoziazioni;
- k. dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionali a fini formativi;
- l. dati contabili e fiscali;
- m. dati inerenti la titolarità dei diritti;
- n. dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali;

Com'è il ciclo di vita del trattamento dei dati?

Dati personali in ingresso

1) Ogni documento cartaceo in ingresso ricevuto tramite posta o ricevuto in busta chiusa consegnata a mano viene di norma consegnato chiuso al Dirigente Scolastico, che lo apre, lo esamina e – nei casi di documenti con dati particolarmente riservati o sensibili – lo protocolla personalmente nel Registro di Protocollo Riservato e lo custodisce nel cassetto della sua scrivania, chiuso a chiave, ad accesso esclusivo, dentro il proprio ufficio normalmente chiuso a chiave quando non presenziato dal Dirigente stesso. Naturalmente per trattare la pratica relativa il Dirigente può portare il documento a conoscenza di un incaricato, raccomandandogli la massima riservatezza nella gestione del documento stesso e di nuovi documenti prodotti per sviluppare la pratica stessa.

2) I documenti cartacei consegnati aperti agli Uffici vengono comunque consegnati al Dirigente Scolastico, che opera a quel punto la stessa funzione di filtro evidenziata nel punto 1. Fanno eccezione i documenti con dati neutri (ad esempio: ricevute di tasse scolastiche o domande di certificazione di routine), che vengono trattati direttamente dalla Segreteria.

3) I documenti ricevuti tramite posta elettronica sono accessibili attraverso il software di Segreteria Digitale Nuvola di Madisoft, stampati in una sola copia e consegnati subito al Dirigente Scolastico, che ne decide l'iter. E' assai raro che contengano dati personali di qualche sensibilità.

4) I documenti cartacei ricevuti tramite fax pervengono sull'apparecchio sito nella stanza della Segreteria Didattica, presenziata da Incaricati, e subito consegnati di norma al Dirigente Scolastico al fine di evitare che dipendenti non incaricati o estranei ne possano in qualunque modo prendere visione (E' comunque rarissimo che tramite telefax pervengano documenti contenenti dati di qualche sensibilità.)

Documenti nella fase di sviluppo della pratica

5) La fase principale di sviluppo avviene di norma su documento informatico. I documenti contenenti dati sensibili vengono trattati in ambiente ad accesso selezionato dagli incaricati e archiviati in ambiente di Segreteria Digitale (Nuvola - Madisoft).

Documenti in uscita

6) I documenti cartacei e informatici in uscita sono mandati all'Incaricato che esegue la protocollazione informatica (Nuvola), a meno che il Dirigente Scolastico non decida che, per la natura del loro contenuto, debbano essere sottoposti a Protocollazione Riservata, che viene eseguita dal Dirigente stesso. In quest'ultimo caso, il Dirigente si occupa di fare anche una fotocopia e di archiviare il documento nella apposita cartella contenente il Protocollo riservato

7) I documenti, dopo la protocollazione, vengono di regola fotocopiati o stampati (per la copia che resta all'Istituto), se non già eseguiti in doppia copia. Se ne occupa un Incaricato (che può essere un Collaboratore Scolastico) e imbustati da un Incaricato (di norma un Assistente Amministrativo). Particolare attenzione è posta nella fase di eventuale fotocopiatura dei documenti contenenti dati di qualche sensibilità che viene eseguita sempre da un Incaricato responsabile anche di vigilare sia che non ci siano estranei nelle vicinanze in grado di vedere il documento sia che lo stesso non venga mai lasciato incustodito.

7) I documenti da spedire via fax vengono spediti da un incaricato.

8) I documenti da spedire via posta elettronica vengono spediti da un Incaricato con l'ambiente di segreteria Digitale Nuvola di Madisoft

9) Infine la copia rimasta alla Scuola viene archiviata nel fascicolo personale dell'interessato, se riguarda una persona, oppure in uno dei fascicoli intitolati ai vari argomenti, secondo una classificazione sistematica che fa riferimento alle sigle di protocollo.

Quali sono le risorse di supporto ai dati?

La Segreteria dell'Istituto Comprensivo dispone di un server con sistema operativo Microsoft Windows 2012R2 Foundation per poter autenticare i pc client e archiviare buona parte della documentazione gestita in ambiente di Segreteria Digitale; dispone di pc client con sistema operativo Microsoft Windows 10 Professional e Microsoft Windows 7 Professional per la gestione delle pratiche di segreteria; dei software gestionali in cloud Nuvola di Madisoft e di Mediasoft Web di Mediasoft per la gestione di alunni, personale, classi e pratiche; del software gestionale SISSI in rete (non più in uso), installato localmente sul server, utilizzato quasi esclusivamente per l'accesso all'archivio storico delle pratiche.

L'Istituto possiede anche un sito web accessibile da internet, ove sono pubblicate notizie riguardanti la didattica, foto di alunni, docenti e genitori per le quali sono state acquisite le liberatorie. I nominativi e gli elenchi pubblicati sono stati preventivamente "ripuliti" dei dati personali.

Il controllo degli accessi alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autenticazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati tramite riconoscimento di una credenziale logica costituita da un nome utente identificativo associato ad una password.

Principi Fondamentali

Proporzionalità, necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono specifiche, esplicite e legittime per garantire il servizio scolastico offerto all'utenza del Comune di Ferrara e gestire i rapporti con dipendenti e collaboratori in virtù del proprio specifico contratto che ne regola il rapporto di lavoro

Quali sono le basi legali che rendono il trattamento legittimo?

Il trattamento è legittimato dall'iscrizione dell'alunno ai corsi dell'Istituto Scolastico effettuata dal genitore o tutore legale

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

I dati raccolti sono esclusivamente quelli necessari per la corretta gestione dell'iter scolastico dell'alunno e del rapporto di lavoro esistente con dipendenti e collaboratori

I dati sono accurati e mantenuti aggiornati?

I dati raccolti sono desunti dai documenti di identità dei soggetti e incrociati con le principali banche dati di altri enti

Quale è la durata della conservazione dei dati?

I dati raccolti sono conservati per un periodo di tempo illimitato, dovendo costituire un archivio storico accessibile anche alle altre istituzioni in caso di necessità.

Controlli per proteggere i diritti personali dei soggetti interessati

I soggetti interessati come sono informati del trattamento?

I soggetti interessati al trattamento sono informati con apposita informativa, sottoscritta all'atto dell'iscrizione o raccolta all'instaurarsi del rapporto di lavoro con dipendenti, collaboratori e fornitori.

Come si ottiene il consenso dei soggetti interessati?

Il consenso dei soggetti si ottiene attraverso un contatto diretto, telefonico o email

I soggetti interessati come esercitano i loro diritti di accesso alla portabilità dei dati?

I soggetti interessati possono esercitare i loro diritti di accesso alla portabilità dei dati attraverso il contatto con gli uffici di segreteria.

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

I soggetti interessati esercitano i propri diritti alla rettifica e alla cancellazione dei propri dati attraverso il contatto con gli uffici di segreteria.

I soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

I soggetti interessati possono esercitare il proprio diritto di restrizione e obiezione attraverso il contatto con gli uffici di segreteria.

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Dal punto di vista della normativa europea, chiunque, all'interno di una organizzazione, effettui operazioni di trattamento è «persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare».

Il GDPR non fa alcun riferimento alla necessità di «nominare» formalmente queste persone, tra le quali sono compresi anche gli incaricati (secondo la definizione del Codice Privacy).

In merito alle operazioni di trattamento dei dati personali, tutto quello che avviene dentro un'impresa si colloca nell'ambito del rapporto di lavoro instaurato tra il Titolare e i propri dipendenti e/o collaboratori e fa riferimento alle mansioni assegnate a questi ultimi. Sono ovviamente esclusi fatti di rilevanza penale, per i quali la responsabilità è individuale.

Il Direttore dei Servizi Generali di un istituto scolastico è ovviamente responsabile del trattamento dei dati personali effettuato all'interno della direzione organizzativa affidatagli; si tratta di un compito insito nel ruolo svolto e non di un dovere discendente da una nomina scritta.

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

Non avvengono trattamenti al di fuori dell'Unione Europea

Rischi

Controlli esistenti o pianificati

Crittografia

Il database del gestionale in cloud Nuvola di Madisoft utilizzato in segreteria è opportunamente criptato e quotidianamente verificato dal fornitore stesso

Controllo degli accessi

I profili degli utenti sono gestiti dal server di dominio e attribuiti a ciascun dipendente della Segreteria, al Dirigente e ai collaboratori del Dirigente

Tracciabilità

Gli eventi di accesso sono registrati dal server fino a saturazione dell'archivio ma comunque per non meno di 1 mese

Vulnerabilità

I sistemi operativi client si aggiornano quotidianamente; il sistema operativo del server, per compatibilità con il gestionale SISSI in rete, si aggiorna in modo presidiato una volta al mese; il sistema antivirus aggiorna le definizioni dei virus in tempo reale.

Lotta contro il malware

Client e server della Segreteria sono protetti dai malware dal software antivirus Eset NOD32

Gestione postazioni

Le postazioni client della Segreteria e della Presidenza subiscono periodici controlli di integrità hardware e software.

Sicurezza dei siti web

Il CMS Joomla con cui è implementato il sito web istituzionale è aggiornato costantemente e con esso si aggiornano anche gli innumerevoli controlli di terze parti.

Backup

I backup del gestionale Nuvola in cloud sono gestiti automaticamente dal fornitore Madisoft; i backup del server sono riversati su unità USB connessa al server; a breve si provvederà ad implementare un "disaster recovery" con l'aggiunta di un NAS da installare in un locale separato.

Manutenzione

La manutenzione delle postazioni PC e del server avviene periodicamente attraverso l'operato di un tecnico esterno.

Sicurezza della rete

Firewall hardware e software proteggono gli accessi dall'esterno alla rete e ne limitano i servizi per garantire la sicurezza agli alunni; la crittografia del segnale wi-fi impedisce l'accesso a persone non autorizzate ai sistemi informatici.

Controllo degli accessi fisici

I locali della Segreteria, dove si effettua materialmente il trattamento, dispongono di porte con chiusura a chiave

Monitoraggio dell'attività della rete

Attraverso il portale web di amministrazione del controller wi-fi viene costantemente monitorata l'attività di rete e l'eventuale presenza di accessi indesiderati.

Sicurezza dell'hardware

Le postazioni PC e il server della Segreteria, sede del trattamento dei dati, sono periodicamente sottoposti a check-up hardware per prevenire malfunzionamenti bloccanti. Il lavoro è svolto da una azienda esterna.

Evitare le fonti di rischio

Difficilmente l'edificio scolastico può essere soggetto a danni ambientali.

Organizzazione

I ruoli e le responsabilità per la protezione dei dati sono in corso di definizione.

Integrare la protezione della privacy nei progetti

Ogni progetto scolastico viene attuato tenendo conto della protezione dei dati personali.

Gestione del personale

Saranno organizzati corsi per istruire opportunamente il personale sulla normativa per la protezione dei dati personali.

Accesso illegittimo ai dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?

Perdita o alterazione, anche irreversibile, dei dati; perdita o alterazione, anche irreversibile, dei programmi; impossibilità temporanea di accesso ai dati; impossibilità temporanea di utilizzo dei programmi

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accessi non autorizzati agli uffici, Intrusione da remoto nel sistema informatico

Quali sono le fonti di rischio?

Ladri, Malintenzionati, Hacker, Vandali

Quali dei controlli identificati contribuiscono a gestire il rischio?

Crittografia, Lotta contro il malware, Backup, Controllo degli accessi fisici, Monitoraggio dell'attività della rete, Vulnerabilità, Gestione del personale

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?

Limitata, I controlli e le misure di sicurezza limitano le probabilità che si verifichi il problema.

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?

Limitata, I controlli e le misure di sicurezza limitano le probabilità che si verifichi il problema.

Modifiche indesiderate dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?

Perdita o alterazione, anche irreversibile, dei dati, manomissione dei programmi, impossibilità temporanea di accesso ai dati, impossibilità temporanea di accesso ai programmi

Quali sono le principali minacce che possono portare al rischio?

Errori umani nella gestione dei sistemi informativi, Sabotaggio dei sistemi informatici

Quali sono le fonti di rischio?

Personale non adeguatamente preparato, Hacker

Quali dei controlli identificati contribuiscono a gestire il rischio?

Vulnerabilità, Controllo degli accessi, Backup, Controllo degli accessi fisici, Gestione del personale

Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

Limitata, Misure di sicurezza minime adottate

Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

Limitata, Misure di sicurezza minime adottate

Scomparsa di dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?

Impossibilità temporanea di accesso ai dati, impossibilità temporanea di accesso ai programmi

Quali sono le minacce che potrebbero portare al rischio?

Furto, Atto vandalico

Quali sono le fonti di rischio?

Ladri, Hacker, Vandalò

Quali dei controlli identificati contribuisce a gestire il rischio?

Controllo degli accessi, Vulnerabilità, Backup, Sicurezza della rete, Monitoraggio dell'attività della rete, Organizzazione

Come stimeresti la gravità del rischio, specialmente riguardo il potenziale impatto e i controlli pianificati?

Limitata, Misure di sicurezza minime adottate

Come stimeresti la probabilità del rischio, specialmente rispetto le minacce, fonti di rischio e i controlli pianificati?

Limitata, Misure di sicurezza minime adottate

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Controlli esistenti o pianificati

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.