alla luce delle linee guida del WP Art. 29 del 4.10.2017 e del Decreto Legislativo N.101 del 10 Agosto 2018 (Modifica del Codice Privacy D. Lgs. n. 101/2018)

Composizione:

Parte 1 - Normativa di riferimento e chiarimenti in merito al presente documento

Parte 2 - Valutazione d'Impatto per il trattamento dati del **personale docente e ATA**

Parte 3 - Valutazione d'Impatto per il trattamento dati relativo alla **gestione delle iscrizioni**

Parte 4 - Valutazione d'Impatto per il trattamento dati relativo alla **carriera scolastica degli alunni**

I.C. PIERSANTI MATTARELLA EX VIA CORTINA
VIA SEBASTIANO SATTA 84 – 00159 Roma
rmic8em008@istruzione.it
rmic8em008@pec.istruzione.it

Data Creazione: Maggio 2020

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (ART.35 GDPR 2016/679)

PARTE 1

Premessa

La disciplina sulla DPIA contenuta nel GDPR viene ad essere integrata con quanto specificato dal WP art. 29 nelle linee guida pubblicate in data 4.10.2017.
In particolare, con il WP art. 29 vengono definiti i criteri in base ai quali decidere se fare ricorso o meno a una DPIA, quali sono le metodologie utilizzabili dai titolari per condurre una DPIA e quali sono gli elementi necessari per la redazione della DPIA.

1. Soggetto obbligato

Il GDPR impone al solo titolare del trattamento di effettuare la DPIA, qualora ne ricorrano i presupposti (cfr. art. 35). In particolare nello svolgimento di una DPIA il titolare potrà essere coadiuvato dal DPO e dal responsabile.
Quando un trattamento è svolto in contitolarità, nella DPIA devono essere specificati gli obblighi che incombono su ciascun titolare con riferimento alla responsabilità delle singole misure finalizzate alla gestione dei rischi.

2. Casi in cui è necessario effettuare una DPIA

La DPIA è obbligatoria solo qualora un trattamento "possa presentare un rischio elevato" per i diritti e le libertà delle persone fisiche.
Il riferimento ai "diritti e alle libertà" va inteso in relazione al diritto alla privacy e anche ad 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.

2.a) Casi previsti dal GDPR

L'art. 35, paragrafo 3, GDPR cita espressamente tre casi in cui sussiste un rischio elevato ed è quindi necessaria l'effettuazione di una DPIA, ossia:

a) valutazione sistematica e globale, basata su un trattamento automatizzato, degli aspetti personali relativi a persone fisiche (compresa la profilazione), e sulla quale si fondano decisioni che hanno effetti giuridici o incidono significativamente su tali soggetti;
b) trattamento su larga scala di dati sensibili o giudiziari;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tale elenco non è esaustivo. la DPIA deve essere anche condotta per valutare l'impatto di un nuovo dispositivo tecnologico in termini di protezione dei dati (cfr. WP art. 29). Il GDPR assegna alle autorità di controllo (per l'Italia, al Garante) il compito di redigere e rendere pubblico un elenco delle tipologie di trattamento da assoggettare e da non assoggettare a DPIA (cfr. art. 35, paragrafi 4 e 5).

2.b) I 9 criteri enunciati dal WP art. 29

Secondo il WP art. 29 i seguenti **9 criteri** devono essere presi in esame sia dalle autorità di controllo per redigere l'elenco delle tipologie di trattamento da assoggettare a DPIA ex art. 35, par. 4, GDPR, sia dai titolari per comprendere quando siano tenuti a svolgere una DPIA:

1. trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "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" (considerando 71 e 91). Ad es.: società che crea profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito internet;

2. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura. Ad es.: trattamento che possa comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione;

3. monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico";

4. dati sensibili o dati di natura estremamente personale: si tratta dei dati sensibili di cui all'art. 9 e dei dati giudiziari di cui all'art. 10;

5. trattamenti di dati su larga scala: il GDPR si occupa del termine "larga scala" nel considerando 91. Il Gruppo art. 29 raccomanda di tenere conto dei seguenti fattori al fine di stabile se un trattamento sia svolto su larga scala: **a)** numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; **b)** volume dei dati e/ o ambito delle diverse tipologie di dati oggetto di trattamento; **c)** durata, o persistenza, dell'attività di trattamento; **d)** ambito geografico dell'attività di trattamento;

6. combinazione o raffronto di insieme di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/ o da titolari distinti;

7. dati relativi a interessati vulnerabili (cons. 75), compresi i minori, i dipendenti, i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti e ogni interessato rispetto al quale possa identificarsi una situazione di disequilibrio con il rispettivo titolare del trattamento;

8. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9. trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (art. 22 e cons. 91). Ad es.: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno ad un finanziamento.

Quando ricorrono **almeno due dei criteri sopra indicati**, il titolare dovrà condurre una DPIA.
Tuttavia, in alcuni casi si dovrà procedere a una DPIA anche di fronte ad un trattamento che soddisfi **solo uno dei criteri** di cui sopra.
È, inoltre, possibile che vi sia perfetta coincidenza tra le ipotesi legislative e i criteri enucleati dal WP art. 29 (ad es. la profilazione sistematica che impatta significativamente sull'interessato non è solo un caso legislativamente previsto di DPIA obbligatoria ex art. 35, par. 3, lett. a) GDPR, ma anche la combinazione dei criteri n° 1, 2 e 3 stabiliti dal WP art. 29).
Si potrebbe verificare anche il caso, ma il WP art. 29 non chiarisce quando tale ipotesi potrebbe verificarsi in concreto, in cui il titolare esclude che debba svolgersi una DPIA perché, pur in presenza dei criteri summenzionati, il trattamento **non** presenta un rischio elevato. In questo caso, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando il parere del DPO. Possiamo immaginare che si tratti della situazione in cui vengano adottate dal titolare misure di sicurezza tali da scongiurare la possibilità di rischio (elevato) per i diritti e le libertà degli interessati (ad es. mediante la pseudonimizzazione e la cifratura dei dati che vengono profilati).

Titolo VI - Istruzione

Capo I Profili generali

Art. 96 (Trattamento di dati relativi a studenti)

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché' le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'Istituto Scolastico e di rilascio di diplomi e certificati.

Titolo VII

Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici Capo I - Profili generali

Art. 97 (Ambito applicativo)

Il presente titolo disciplina il trattamento dei dati personali effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'articolo 89 del regolamento.

Art. 98 - Finalità di rilevante interesse pubblico (abrogato)

Art. 99 (Durata del trattamento)

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.
2. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del Regolamento.

Art. 100 - Dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli di cui agli articoli 9 e 1 O del Regolamento.
2. Resta fermo il diritto dell'interessato di rettifica, cancellazione, limitazione e opposizione ai sensi degli articoli 16, 17, 18 e 21 del Regolamento.
3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della Legge 7 agosto 1990, n. 241.
4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.
5. 4-bis. I diritti di cui al comma 2 si esercitano con le modalità previste dalle regole deontologiche.

Capo II - Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica

Art. 101 - Modalità di trattamento

1. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 5 del regolamento.
2. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.
3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

Art. 102 - Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica

1. Il Garante promuove, ai sensi dell'articolo 2-quater, la sottoscrizione di regole deontologiche per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.

2. Le regole deontologiche di cui al comma 1 individuano garanzie adeguate per i diritti e le libertà dell'interessato in particolare:

a) le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del presente codice e del Regolamento applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica;
b) le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati;
c) le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 103 - Consultazione di documenti conservati in archivi

1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati dichiarati di interesse storico particolarmente importante è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 e dalle relative regole deontologiche.

TITOLO VIII - Trattamenti nell'ambito del rapporto di lavoro

Capo I - Profili generali

Art. 111 (Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro)

1. Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

Art. 111-bis (Informazioni in caso di ricezione di curriculum)

1. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

Art. 112 - Finalità di rilevante interesse pubblico (abrogato)

Capo II - Trattamento di dati riguardanti i prestatori di lavoro

Art. 113 Raccolta di dati e pertinenza

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n.300 nonché dall'articolo 1 O del decreto legislativo 1 O settembre 2003, n. 276.

Capo III - Controllo a distanza, lavoro agile e telelavoro

Art. 114 (Garanzie in materia di controllo a distanza)

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300.

Art. 115 (Telelavoro, lavoro agile e lavoro domestico)

1. Nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale. 2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

Capo IV - Istituti di patronato e di assistenza sociale

Art. 116 Conoscibilità di dati su mandato dell'interessato

1. Per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato dall'interessato medesimo.
2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee- guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

Titolo IX - Altri trattamenti in ambito pubblico o di interesse pubblico

Capo I - (Assicurazioni)

Art. 117 - Affidabilità e puntualità nei pagamenti(abrogato)

Art. 118 - Informazioni commerciali (abrogato)

Art. 119 - Dati relativi al comportamento debitorio (abrogato)

Art. 120 - Sinistri

1. L'Istituto Scolastico per la vigilanza sulle assicurazioni definisce con proprio provvedimento le procedure e le modalità di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalità di accesso alle informazioni raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.

2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.

3. Per quanto non previsto dal presente articolo si applicano le disposizioni dall'articolo 135 del codice delle assicurazioni private di cui al decreto legislativo 7 settembre 2005, n. 209.

Titolo X - Comunicazioni elettroniche

Capo I - Servizi di comunicazione elettronica

Art. 121 (Servizi interessati e definizioni)

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, comprese quelle che supportano i dispositivi di raccolta dei dati e di identificazione.

   1-bis. Ai fini dell'applicazione delle disposizioni del presente titolo si intende per:

   a) «comunicazione elettronica», ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

   b) «chiamata», la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

   c) «reti di comunicazione elettronica», i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella

misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) «rete pubblica di comunicazioni», una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

e) «servizio di comunicazione elettronica», i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera e), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) «contraente», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) «utente», qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) «dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) «dati relativi all'ubicazione», ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

j) «servizio a valore aggiunto», il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

k) email, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Trattamenti

Alla luce della richiamata normativa, si è deciso di svolgere la DPIA inerente a tre trattamenti principali svolti dall’Istituto Scolastico:

A - Gestione iscrizioni;

B - Gestione della carriera scolastica degli alunni;

C - Gestone del personale docente e ATA contrattualizzazione

Termini di Valutazione:

- ☐ Non accettabile
- ☐ Da rivedere
- ☐ Accettabile

Vista la liceità del trattamento come conseguimento di un obbligo derivato dalla Legge, non si richiede il parere da parte degli interessati ma si effettua l'informazione necessaria tramite i regolamenti interni e la presa visione delle informative privacy.

PARTE 2: Informazioni sulla DPIA Relativa al trattamento dei dati del personale

DPIA

Relativa al trattamento dei dati del personale

Descrizione del trattamento:

Il trattamento ha per oggetto la gestione del rapporto di lavoro del personale dipendente instaurato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'Istituto Scolastico ovvero in aziende o istituzioni collegate o vigilate, compresi tutti i procedimenti concorsuali o le altre procedure di selezione previste, così come per i corsi di formazione. I dati sono oggetto di trattamento presso le diverse aree funzionali e strutture relativamente alla prestazione del servizio, orario, assenze per malattia o altro e in generale ricezione, registrazione, trasmissione, conservazione, corrispondenza, archiviazione delle delibere degli Organi. Sono comprese nel trattamento tutte le elaborazioni a fini statistici e per le attività di controllo della gestione. Dati afferenti a particolari categorie, quali quelli relativi alle convinzioni religiose filosofiche, sulla vita sessuale o di altro genere possono eventualmente essere compresi tra quelli trattati in caso di accesso a diversi servizi erogati dalla P.A., come quelli sanitari relativi ai familiari dei Dipendenti ai fini della concessione di benefici nei casi previsti dalla Legge. Tutti i dati pervengono all'Amministrazione su iniziativa dei Dipendenti e/o a richiesta, e vengono trattati per l'applicazione dei diversi istituti contrattuali disciplinati dalla Legge (gestione giuridica, economica, previdenziale, pensionistica, attività di aggiornamento e formazione). È possibile, infine, l'esecuzione di interrogazioni e incroci con altre banche dati a cui l'Amministrazione ha accesso, per raffronti con Amministrazioni e Gestori di pubblici servizi, finalizzate all'accertamento d'ufficio di uno stato, qualità o fatto ovvero al controllo a campione o massivo delle dichiarazioni sostitutive rese ai sensi dell'art.43 del D.P.R. n.445/2000

Finalità associate al trattamento Gestione del Personale

Gestione delle presenze del Personale; gestione ferie e malattie; gestione permessi; gestioni di attività scolastiche esterne all'Istituto Scolastico es. gite etc.; adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali; adempimenti in materia di assicurazione contro gli infortuni; adempimenti previdenziali; adempimenti fiscali; trattamento giuridico ed economico del Personale.

Soggetti interessati dal trattamento

Personale docente e ATA

Titolari del trattamento

I.C. PIERSANTI MATTARELLA

Norme di riferimento

D. Lgs. n. 165/2001; D. Lgs. n. 101/2018; GDPR 679/2016

Dati, processi e asset di supporto

Descrizione dei dati trattati

Dati anagrafici; dati contabili, fiscali e finanziari; dati inerenti il rapporto di lavoro; dati inerenti situazioni giudiziarie civili, amministrative, tributarie, stato di salute, adesione ad associazioni od organizzazioni a carattere politico o sindacale, casellario giudiziario.

Durata di archiviazione dei dati

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: il trattamento dei dati avrà una durata non superiore a quella necessaria agli scopi per i quali i dati sono stati raccolti, come riportato nelle singole finalità; e comunque non oltre la normativa vigente.
Tuttavia, qualora l'Interessato ritenga, per qualsiasi motivo, esaurito lo scopo del trattamento, potrà esercitare i propri diritti inviando una richiesta ai recapiti sopra indicati.

Categorie di destinatari dei dati

Consulenti e liberi Professionisti in forma singola o associata, Enti previdenziali ed assistenziali, Organizzazioni sindacali, Centri di formazione professionale, altre Amministrazioni pubbliche, portali amministrazioni pubbliche

Soggetti autorizzati al trattamento

Soggetti autorizzati al trattamento, personale amministrativo incaricato alla didattica

Termini di conservazione in relazione ai principali trattamenti effettuati dall'Istituto Scolastico

Finalità amministrative, contabili e fiscali: fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di accertamento e repressione dei reati: 12/24/72 mesi, come previsto dalle specifiche disposizioni normative. Finalità di conservazione previste da obblighi di Legge (ad esempio, la prescrizione legale dei diritti): fino a 10 anni dopo la cessazione della fornitura del servizio. Sono oggetto di trattamento solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

Asset di supporto

Archivio cartaceo, rete interna informatica, postazioni di lavoro in Amministrazione, informazioni su Albo Pretorio

Valutazione

Accettabile

Rispondenza ai principi fondamentali

Proporzionalità e necessità

Le finalità del trattamento sono esplicite e legittime?

È consentito il trattamento dei soli dati personali indispensabili per svolgere le attività istituzionali, previa verifica della loro pertinenza e completezza, ferma restando l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati.
Qualora l'Istituto Scolastico, nell'espletamento della propria attività istituzionale, venga a conoscenza, mediante comunicazione da parte dell'Interessato o, comunque, non a richiesta dell'Istituzione, di dati personali non indispensabili allo svolgimento dei fini istituzionali sopra citati, tali dati non potranno essere utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di Legge, dell'atto o del documento che li contiene seguendo i principi di liceità del trattamento. Le operazioni di interconnessione, raffronto e comunicazione individuate nel presente Regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati, per il perseguimento delle rilevanti finalità di interesse pubblico specificate e nel rispetto delle disposizioni rilevanti in materia di protezione dei dati personali, nonché degli altri limiti stabiliti dalla Legge e dai regolamenti. Le predette operazioni, se effettuate utilizzando banche di dati di diversi Titolari del trattamento, sono ammesse esclusivamente previa verifica della loro stretta indispensabilità nei singoli casi e nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono.

Valutazione

Accettabile

Quali sono i principi di liceità che rendono il trattamento legittimo?

Seguendo le indicazioni del Decreto Legislativo n. 165 del 30 marzo 2001 e successive modifiche ed integrazioni, gli interventi legislativi degli anni più recenti sono scaturiti dalla necessità di risolvere alcune anomalie verificatesi nella gestione delle risorse umane e strumentali che hanno generato inefficienze e costi crescenti nelle Pubbliche Amministrazioni. Le politiche di riduzione del costo del lavoro pubblico, perseguite dalle diverse Leggi finanziarie attraverso la riduzione del Personale in servizio e delle dotazioni organiche, nonché il blocco delle procedure di reclutamento, pur con limitate deroghe, debbono essere lette in stretta correlazione con i principi generali che regolano l'organizzazione ed il funzionamento delle Amministrazioni. Infatti, con l'imposizione di vincoli di spesa, il Legislatore ha di fatto inteso sanare situazioni spesso derivanti dall'utilizzo improprio delle diverse tipologie contrattuali chiedendo, quindi, alle Amministrazioni comportamenti più corretti ed efficienti nella gestione delle risorse umane. Da ultimo, l'entrata in vigore del Decreto Legge 1 O gennaio 2004, n. 4 e della relativa Legge di conversione, 9 marzo 2006, n. 80, che si aggiunge alle diverse Disposizioni in tema di organizzazione e funzionamento della Pubblica Amministrazione, comporta la necessità di fornire puntuali indicazioni sul corretto utilizzo di tutti gli strumenti gestionali che l'Ordinamento ha individuato e sulla responsabilità che grava sul Personale dirigenziale. Al riguardo, appare utile ricordare che per rendere effettiva l'attuazione dei principi di cui all'articolo 97 della Costituzione, l'articolo 1, comma 1, del Decreto Legislativo 30 marzo 2001, n. 165 ha stabilito che l'organizzazione ed i rapporti di lavoro e di impiego alle dipendenze delle Amministrazioni pubbliche devono essere finalizzati ad accrescere l'efficienza delle Amministrazioni stesse, razionalizzare il costo del lavoro pubblico, realizzare la migliore utilizzazione delle risorse umane, in particolare curando la formazione e lo sviluppo professionale dei Dipendenti.

Valutazione

Accettabile

I dati raccolti sono adeguati e indispensabili per finalità per cui sono trattati?

Il trattamento ha per oggetto la gestione del Personale dipendente, intesa come la gestione del rapporto di lavoro avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'Ente ovvero in aziende o istituzioni collegate o vigilate, compresi tutti i procedimenti concorsuali o le altre procedure di selezione previste così come per i corsi di formazione. I dati sono oggetto di trattamento presso le diverse aree funzionali e strutture relativamente alla prestazione del servizio, orario, assenze per malattia o altro e in generale ricezione, registrazione, trasmissione, conservazione, corrispondenza, archiviazione delle Delibere degli Organi. Sono compresi nel trattamento tutte le elaborazioni a fini statistici e per le attività di controllo della gestione. Dati afferenti a particolari categorie, quali quelli relativi alle convinzioni religiose filosofiche, sulla vita sessuale o di altro genere possono eventualmente essere compresi tra quelli trattati in caso di particolari progetti previsti dal POF o in caso di accesso a diversi servizi erogati dalla P.A., come quelli sanitari relativi ai Familiari dei Dipendenti ai fini della concessione di benefici nei casi previsti dalla Legge. Tutti i dati pervengono all'Amministrazione su iniziativa dei Dipendenti e/o a richiesta e vengono trattati per l'applicazione dei diversi istituti contrattuali disciplinati dalla Legge (gestione giuridica, economica, previdenziale, pensionistica, attività di aggiornamento e formazione). È possibile, infine, l'esecuzione di interrogazioni e incroci con altre banche dati a cui l'Amministrazione ha accesso, per raffronti con Amministrazioni e Gestori di pubblici servizi, finalizzate all'accertamento d'ufficio di uno stato, qualità o fatto ovvero al controllo a campione o massivo delle dichiarazioni sostitutive rese ai sensi dell'art.43 del D.P.R. n. 445/2000

Valutazione

Accettabile

I dati sono accurati e mantenuti aggiornati?

Il trattamento sarà svolto da Incaricati in forma manuale e/o automatizzata nel rispetto degli artt. 30, 32 e 35 del R.E. 2016/679 con la supervisione del Responsabile della Protezione dei Dati e verrà comunicata, se necessario, all'Interessato ogni modifica dei dati in possesso

Valutazione

Accettabile

Qual è la durata della conservazione dei dati?

Termini di conservazione in relazione ai principali trattamenti effettuati dall'Istituto Scolastico. Finalità amministrative, contabili e fiscali: fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di accertamento e repressione dei reati: 12/24/72 mesi, come previsto dalle specifiche disposizioni normative. Finalità di conservazione previste da obblighi di Legge (ad esempio la prescrizione legale dei diritti): fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di profilazione e altri trattamenti automatizzati: fino a un massimo di 18 mesi. Finalità tecniche di Assurance (come quelle per il miglioramento dei servizi): fino a un massimo di 24 mesi.

Valutazione

Accettabile

Misure di protezione dei diritti degli interessati

I soggetti interessati come sono informati del trattamento?

Gli Interessati vengono informati al primo contatto con le strutture dell'istituto Scolastico nonché con la reperibilità delle informative sul sito web istituzionale nella sezione dedicata alla privacy

Valutazione

Accettabile

Come si ottiene il consenso dei soggetti interessati?

Il consenso, quando necessario, per le attività inerenti all'art. 9 del GDPR, viene raccolto in forma cartacea

Valutazione

Accettabile

I soggetti interessati come esercitano i loro diritti di accesso e alla portabilità dei dati? Come possono rettificarli o cancellarli? Come possono limitarne il trattamento?

Ogni Interessato ha i seguenti diritti relativi alla protezione dei dati: • richiedere l'accesso ai propri dati personali (comunemente noto come "diritto di accesso"). Ciò consente di ricevere una copia dei dati personali che deteniamo sull'Interessato e di controllarne la corretta elaborazione; • richiedere la correzione dei propri dati personali. Ciò consente di correggere eventuali dati incompleti o inaccurati che conserviamo, sebbene potremmo aver bisogno di verificare l'esattezza dei nuovi dati forniti; • richiedere la cancellazione dei propri dati personali. Ciò consente di chiederci di eliminare o rimuovere i dati personali laddove non ci fossero validi motivi per continuare a elaborarli. Ciò consente, inoltre, di richiedere la cancellazione dei propri dati personali quando: si è esercitato con successo il "diritto all'oblio"; potremmo aver elaborato le informazioni illegalmente o laddove ci venisse richiesto di cancellare i propri dati personali per conformarci con la Legge locale. Tuttavia, potremmo non essere sempre in grado di soddisfare la richiesta di cancellazione per specifici motivi legali che verrebbero notificati al momento della richiesta; • opporsi al trattamento dei propri dati personali nel caso di interesse legittimo o nel caso di situazioni particolari che potrebbero avere un impatto verso i propri diritti e le libertà fondamentali. È possibile opporsi anche all'utilizzo dei propri dati ai fini di marketing diretto, ove previsto; • richiedere la limitazione del trattamento dei propri dati personali. Ciò consente di chiederci di sospendere il trattamento dei dati personali nei seguenti scenari: (a) se si richiede una verifica per la precisione dei dati; (b) laddove vi sia esplicita richiesta di conservazione dei dati, anche se non più necessari per la nostra operatività, in quanto potrebbe esserci il bisogno di stabilire, difendere o esercitare i propri diritti legali; (c) si contesta il nostro utilizzo dei dati, ma vi è la preventiva necessità di verifica per l'esistenza di motivi legittimi obbligatori per usarli; • richiedere il trasferimento dei dati personali. Forniremo i dati personali in un formato strutturato, comunemente utilizzato e leggibile da un dispositivo elettronico comune (computer). Tale diritto si applica solo alle informazioni automatizzate per le quali è stato fornito preventivamente il consenso, oppure laddove siano state utilizzate le informazioni acquisite per l'esecuzione di un Accordo comune; • revocare il consenso in qualsiasi momento laddove avessimo la necessita del consenso per processare i dati personali. Tuttavia, ciò non pregiudica la liceità di qualsiasi trattamento effettuato prima di revocare il consenso. Se si ritira il consenso, potremmo non essere in grado di fornire determinati prodotti o servizi. Sarà nostra premura informare circa tali evenienze in caso di ritiro del consenso. Per esercitare uno o più dei diritti sopra indicati, è possibile contattare l'Istituto Scolastico utilizzando le modalità indicate sul sito istituzionale dell'Istituto Scolastico alla voce "Contatti" oppure all'indirizzo di posta elettronica ordinaria o Pec.
Nel caso di insoddisfazione della risposta a qualsiasi richiesta o reclamo o nel caso si ravvisi un uso non corretto dei propri dati, è possibile presentare reclamo diretto all'Autorità Garante per la Protezione dei Dati Personali. Tuttavia, l'Istituto Scolastico tiene in alta considerazione la riservatezza di chiunque venga a

contatto con l'Istituto Scolastico; pertanto, vi sarà sempre la totale e piena disponibilità ad esaminare e risolvere qualsiasi necessità fin dall'inizio.

Valutazione

Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e formalizzati in un contratto?

Come previsto dall' Art. 5 del GDPR Il Titolare del trattamento nomina in forma scritta gli Incaricati al trattamento dei dati, scelti tra il Personale amministrativo in base ai rispettivi ambiti d'impiego, autorizzandoli al trattamento dei dati personali contenuti in atti e documenti riguardanti archivi di tipo cartaceo o effettuati con strumenti automatizzati e/o contenuti nelle eventuali banche dati elettroniche automatizzate, nonché il Responsabile della Protezione Dati (RPD / DPO - Data Protection Officer).La scelta e la nomina dell'RPD / DPO viene effettuata rispettando i parametri indicati nel capo IV Sezione 3 (artt. 37, 38, 39) Il Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (semplicemente definito anche RGPD), in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile della Protezione dei dati personali (artt. 37-39). Il predetto Regolamento prevede l'obbligo per il Titolare o per il Responsabile del trattamento di designare l'RPD «quando il trattamento è effettuato da una Autorità pubblica o da un Organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali» (art.37, paragrafo 1, lett. a). Le predette disposizioni prevedono che l'RPD deve essere individuato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39» (art. 37, paragrafo 5) e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal Titolare del trattamento o dal Responsabile del trattamento». La carica di Incaricati al trattamento dei dati relativamente ai sistemi informatici può essere affidata a più Persone anche in ragione della diversa ubicazione delle varie sedi dell'Istituto Scolastico.

Valutazione

Accettabile

I dati sono adeguatamente protetti nel caso di trasferimento ad altri Soggetti pubblici o al di fuori dell'Unione Europea?

Art. 12 del Regolamento Privacy - Richieste di trattamento, comunicazione o diffusione di dati personali La comunicazione e la diffusione dei dati personali da parte dell'Istituto Scolastico ad un altro Soggetto pubblico è consentito ed avviene nell'ambito dei rapporti che essi hanno ai fini dello svolgimento delle rispettive attività istituzionali. Non divulgheremo le informazioni personali che deteniamo, eccetto dove previsto direttamente dalla Legge o nelle seguenti condizioni:(i) alle sedi secondarie dell'Istituto Scolastico ;(ii) a Soggetti terzi che ci forniscono servizi e che agiscono come Responsabili del trattamento dei dati;(iii) a Consulenti professionali tra cui Istituto Scolastico bancario che gestisce il servizio di cassa, al gestore del conto corrente per i contributi, ai Revisori dei conti, ecc.;(iv) all'Agenzia delle Entrate, alle Autorità di regolamentazione e ad altre Autorità che possono richiedere dati in determinate circostanze. La comunicazione e la diffusione dei dati personali a Terzi sono ammesse solo se previste da disposizioni di Legge o equiparate, con le formalità dalle stesse indicate. Eventuali richieste all'Istituto Scolastico finalizzate ad ottenere il trattamento, la comunicazione o la diffusione di dati personali devono essere presentate sotto forma scritta ed essere adeguatamente motivate. Nella domanda dovranno essere indicati o debbono essere desumibili:- il nome, la denominazione o la ragione sociale del Richiedente;- i dati cui la domanda si

riferisce, gli scopi per cui gli stessi sono richiesti e le modalità del loro utilizzo;- l'eventuale ambito di comunicazione e diffusione dei dati richiesti;- la dichiarazione che il richiedente s'impegna ad utilizzare i dati ricevuti esclusivamente per le finalità e nell'ambito delle modalità per cui sono stati richiesti;- copia di un documento di riconoscimento (ove previsto).11 Responsabile del trattamento, dopo aver verificato che la diffusione dei dati personali o la comunicazione dei medesimi ai Richiedenti, ovvero il loro eventuale trattamento da parte di questi ultimi siano ammissibili, provvede a trasmettere i dati a chi ne ha fatto richiesta, nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta. La comunicazione e la diffusione dei dati personali sono comunque permesse quando:- siano necessarie per fini di ricerca scientifica o di statistica e si tratti di dati anonimi e/o aggregati;- siano necessarie per il soddisfacimento di richieste di accesso ai documenti amministrativi;- siano effettuate nei confronti della Stampa, in riferimento a notizie di pubblico dominio;- i dati siano inseriti in annuari, o pubblicazioni simili, fatta eccezione per i dati strettamente personali e non riguardanti l'ambito dell'Istituto Scolastico ;- i dati relativi agli Studenti siano comunicati a Enti al fine di favorirne l'inserimento nel mondo del lavoro o perché gli stessi possano essere invitati a incontri, manifestazioni o riunioni riguardanti tematiche connesse alla loro attività di studio.

Valutazione

Accettabile

Rischi

Misure esistenti o pianificate

Protezione dei documenti cartacei

Documenti conservati in segreteria in armadi chiusi con sistema di allarme per l'edificio,
locale archivio chiuso a chiave e con accesso riservato al personale addetto per l'archivio storico

Valutazione

Accettabile

Sicurezza fisica

Controllo visivo delle aree contenenti documenti cartacei con l'ausilio del Personale in attività. Sistema di allarme.

Valutazione

Accettabile

Backup dei dati

Backup giornaliero in SERVER con cifratura e codifica di accesso al contenuto.

Gestione delle postazioni di lavoro

Tutte le postazioni di lavoro contengono applicativi non modificabili dall'Utente finale, eccezione fatta nei casi di autorizzazione tramite password amministratore dal Responsabile e dall'Amministratore dei sistemi.

Valutazione

Accettabile

Protezione dei canali informativi

L'accesso fraudolento alla rete viene bloccato tramite il firewall inserito direttamente all'ingresso del dato informatico dal provider della connessione dati, e tale misura software e hardware non può essere modificata da nessun operatore interno.

Valutazione

Accettabile

Gestione del personale

Il Personale viene ciclicamente formato sulle novità normative inerenti alla propria funzione all'interno dell'Istituto Scolastico.

Valutazione

Accettabile

Controllo dell'accesso logico

Il cambio password viene effettuato automaticamente dal sistema ogni tre mesi.
l'Amministratore di rete consegna il registro password in busta chiusa sigillata al Direttore amministrativo.
Le password sono univoche, alfanumeriche con caratteri speciali e maiuscole.

Valutazione

Accettabile

Manutenzione

In essere un contratto di manutenzione software, hardware e gestione reti.

Valutazione

Accettabile

Sicurezza delle attrezzature

Le apparecchiature in dotazione all'istituto Scolastico relative alla gestione amministrativa si trovano in stanze chiuse a chiave apribili solo in caso di svolgimento della funzione quando è presente l'incaricato all'utilizzo di tale punto di lavoro.

Valutazione

Accettabile

Protezione contro le fonti di rischio non antropico

L'edificio è protetto dalle fonti antropiche, come da normativa vigente, con l'impianto di scarico delle potenze a terra nonché da batterie UPS per la protezione dei dati in caso di assenza di energia elettrica.

Valutazione

Accettabile

Lotta contro il malware

Oltre al firewall ogni postazione di lavoro contiene un software anti malware installato e monitorato mensilmente per mitigare furti di identità e uso improprio ed illecito del dato contenuto

Valutazione

Accettabile

Rischio di accesso illegittimo ai dati

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

Diffusione non autorizzata dei dati personali comuni e particolari

Quali sono le principali vulnerabilità che possono condurre al rischio?

Abilitazione di servizi non necessari; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; storage non protetto; linee di comunicazione non protette; errata attribuzione dei diritti di accesso; utilizzo di software su dati non aggiornati; date non corrette

Quali sono le minacce?

Accessi esterni non autorizzati; mancata manutenzione del sistema informativo; furto di apparecchiature o documenti; malfunzionamento hardware; malfunzionamento software; intercettazione dati; azione di virus informativi o di codici malefici; spamming o tecniche di sabotaggio; uso improprio del software; errato uso del software; corruzione dei dati; trattamento illecito dei dati; manomissione del software; furto o copiatura software; uso non autorizzato di apparecchiature; ingressi non autorizzati a locali/aree ad accesso ristretto; sabotaggio

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; sicurezza fisica; backup dei dati; gestione delle postazioni di lavoro; protezione dei canali informativi; gestione del personale; controllo dell'accesso logico; gestione dei rischi in materia di privacy; lotta contro il malware

Stima della gravità del rischio

Basso - le funzioni attuate minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

Stima della probabilità del rischio

Mai verificatosi ma possibile

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure attuate ogni giorno nella gestione del dato personale affidato

Valutazione

Accettabile

Rischio di modifica non desiderata dei dati

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

Trattamento errato del dato personale

Quali sono le principali vulnerabilità che possono condurre al rischio?

Abilitazione di servizi non necessari; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; storage non protetto; linee di comunicazione non protette; errata attribuzione dei diritti di accesso; utilizzo di software su dati non aggiornati; date non corrette

Quali sono minacce?

Malfunzionamento software; distruzione di apparecchiature o di supporti; furto di apparecchiature o documenti; accessi esterni non autorizzati; trattamento illecito dei dati; malfunzionamento software; distruzione di apparecchiature o di supporti; furto di apparecchiature o documenti; accessi esterni non autorizzati; trattamento illecito dei dati; uso non autorizzato di apparecchiature; Ingressi non autorizzati a locali/aree ad accesso ristretto; Alterazione dolosa o colposa dei dati; Comunicazione illegale dei dati e dei documenti

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; sicurezza fisica; backup dei dati; gestione delle postazioni di lavoro; protezione dei canali informativi; gestione del personale; controllo dell'accesso logico; gestione dei rischi in materia di privacy; lotta contro il malware

Stima della gravità del rischio

Medio - le funzioni attuate minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

Stima della probabilità del rischio

Mai verificatosi ma possibile.

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate, il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse

Valutazione

Accettabile

Rischio di perdita dei dati

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

Perdita temporanea dei dati e diffusione non condivisa dall'Interessato

Quali sono le principali vulnerabilità che possono condurre al rischio?

Storage non protetto; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; insufficiente test del software; utilizzo di software su dati non aggiornati; parametri di settaggio non corretti; connessioni non protette a reti pubbliche; assenza di Personale; mancanza di consapevolezza della sicurezza; mancata sorveglianza delle aree protette; assenza piani di emergenza; mancanza di schemi di sostituzione periodici; mancanza procedure di accesso con credenziali; insufficiente formazione del Personale; mancato controllo fotocopiatura; impianto non certificato; linee di comunicazione non protette; gestione inadeguata della rete (bilanciamento di routing); sensibilità all'umidità, allo sporco, alla polvere; mancanza di schemi di sostituzione periodici; mancanza di software antivirus; insufficiente formazione del Personale; insufficiente test del software

Quali sono minacce?

Furto di apparecchiature o documenti; malfunzionamento hardware; malfunzionamento software; corruzione dei dati; errato uso del software; uso non autorizzato di apparecchiature; mancata disponibilità di Personale; accesso archivi dati sensibili o giudiziari; accesso archivi dati comuni; sabotaggio; guasto di apparecchiature; accessi esterni non autorizzati; uso non autorizzato dei dati; comunicazione illegale dei dati e dei documenti; cortocircuito; intercettazione dati; blocco/saturazione del sistema informativo; polvere, corrosione o gelo; distruzione di apparecchiature o di supporti; azione di virus informativi o di codici malefici; spamming o tecniche di sabotaggio; uso improprio del software

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; backup dei dati; gestione delle postazioni di lavoro; gestione del Personale; controllo dell'accesso logico; manutenzione; sicurezza delle attrezzature; protezione dei canali informativi; protezione contro le fonti di rischio non antropico; lotta contro il malware; sicurezza fisica

Stima della gravità del rischio

Basso - le funzioni attuate minimizzano al massimo il rischio di perdita dei dati

Stima della probabilità del rischio

Mai verificatosi ma possibile

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure attuate ogni giorno nella gestione del dato personale affidato. Nel caso di cancellazioni errate il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse

Valutazione

Accettabile

PARTE 3: Informazioni sulla DPIA Relativa al trattamento gestione delle iscrizioni

DPIA

Relativa al trattamento dati relativo alla gestione delle iscrizioni

Descrizione del trattamento:

I dati sensibili e giudiziari sotto elencati e inerenti il rapporto tra Istituto Scolastico e Studenti, raccolti sia presso gli Interessati che presso Terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti dell'Ente, sia su base cartacea che su base informatica. Principali tipologie di dati oggetto di privacy: dati relativi agli Studenti e/o a Familiari diversamente abili o ad elementi reddituali ai fini di un eventuale controllo sulle autocertificazioni relativi a eventuali esoneri e/o fruizione di eventuali agevolazioni previste dalla Legge, nonché dati relativi alla gestione dei contributi straordinari per iniziative degli Studenti; dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio; dati sensibili e giudiziari che rilevano nell'ambito di procedimenti disciplinari a carico degli Studenti; dati relativi alla condizione di disabile per attività di interpretariato, tutorato, trasporto e servizi analoghi per tutti gli Studenti portatori di handicap. È, di seguito, descritto sinteticamente il flusso informativo dei dati. I dati sensibili e giudiziari sopra descritti inerenti all'attività didattica e alla gestione delle iscrizioni e delle carriere degli Studenti, raccolti sia presso gli Interessati che presso i Terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti, sia su base cartacea che su base informatica. Principali fonti normative R.D. 1592/1933 e successive modificazioni e integrazioni. (Testo unico delle leggi sull'istruzione superiore); R.D. 1269/1938 e successive modificazioni e integrazioni (Approvazione del regolamento sugli Studenti); D.P.R. 382/1980 (Riordinamento della Docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica); L. 398/1989 (Norme in materia di borse di studio universitarie); L. 341 /1990 (Riforma degli Ordinamenti didattici universitari); L.390/1991 (Norme sul diritto agli studi universitari); L. 104/1992 (Legge-quadro per l'assistenza, l'integrazione sociale ed i diritti delle Persone handicappate); D.M. 224/1999 (Norme in materia di Dottorato di ricerca); D. Lgs. n. 445/2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa); L. 148/2002 (Ratifica ed esecuzione della Convenzione di Lisbona dell'11 aprile 1997); D.M. 270/2004 (Modifiche al Regolamento recante norme concernenti l'autonomia didattica degli Atenei, approvato con decreto MURST 3 novembre 1999, n. 509); D.P.R. 334/2004 (Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello Straniero); D.M. n. 142 del 25/3/1998 e L. 24 giugno 1997, n. 196 (Normativa relativa agli stages); DPCM 9 aprile 2001; L. 14 febbraio 2003, n. 30 (c.d. Legge Biagi, di riforma del mercato del lavoro); Contratto Istituzionale Erasmus+ vigente; Statuto dell'Istituto Scolastico; Regolamento per l'Amministrazione, la Finanza e la Contabilità dell'Istituto Scolastico; Regolamento sugli Studenti ed altri Regolamenti d'Istituto Scolastico vigenti; Leggi regionali vigenti in materia di diritto allo studio universitario.

Finalità associate al trattamento Gestione delle iscrizioni

Accettazione delle domande di iscrizione e elaborazione delle eventuali domande in lista di attesa in relazione alla disponibilità di posti e dei criteri di precedenza, deliberati dal Consiglio di Istituto, in caso di richieste eccedenti, perfezionamento dell'iscrizione per la successiva gestione amministrativa e didattica dell'alunno.

Soggetti interessati dal trattamento

Studenti

Titolari del trattamento

I.C. PIERSANTI MATTARELLA

Norme di riferimento

GDPR 2016/679; Decreto 10 agosto 2018 n.101

Descrizione dei dati trattati

Dati Comuni: Dati anagrafici alunni, fratelli frequentanti, e dei genitori o di chi esercita la responsabilità genitoriale, stato civile (genitori)

Dati personali particolari: Dati sanitari: stato di salute, necessità assistenza sanitaria, situazione vaccinale (fino ai 16 anni), deficit cognitivi (disabilità, DSA), bisogni educativi speciali. convinzioni religiose, origine raziale/etnica, sesso di appartenenza, situazioni di disagio sociale riferito alla famiglia di origine (affidi a servizi sociali), situazioni giuridiche (genitori separati, affidi ecc.)

Dati relativi a condanne penali: Nessuno

Durata di archiviazione dei dati

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: il trattamento dei dati avrà una durata non superiore a quella necessaria agli scopi per i quali i dati sono stati raccolti, come riportato nelle singole finalità; tuttavia, qualora l'Interessato ritenga, per qualsiasi motivo, esaurito lo scopo del trattamento, potrà esercitare i propri diritti inviando una richiesta ai recapiti dell'Istituto Scolastico.

Categorie di destinatari dei dati

Enti locali (Progetti vari di collaborazione), Organi istituzionali (Progetto Erasmus+), Enti previdenziali ed assistenziali (Inps e Inail), Istituti, scuole e università (Comparto AFAM ed altri Istituti Scolastic), Imprese di assicurazione (per ottemperare ad obblighi normativi), Associazioni e Fondazioni (Entità collegate al mondo dell'Istituto Scolastico)

Soggetti autorizzati al trattamento

Soggetti autorizzati al trattamento, personale amministrativo incaricato alla didattica

Termini di conservazione in relazione ai principali trattamenti effettuati dall'Istituto Scolastico

È di seguito descritto sinteticamente il flusso informativo dei dati e la loro conservazione temporale. I dati sensibili e giudiziari inerenti all'attività didattica e la gestione delle iscrizioni e delle carriere degli Studenti, raccolti sia presso gli Interessati che presso i Terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti, sia su base cartacea che su base informatica. In relazione alle diverse finalità e agli scopi per i quali sono stati raccolti, i dati saranno conservati per il tempo previsto dalla normativa di riferimento ovvero per quello strettamente necessario al perseguimento delle finalità. In particolare: I dati conferiti per l'espletamento del servizio didattico saranno archiviati e mantenuti in coerenza con il consenso acquisito per un periodo massimo di 10 anni. Tale periodo è valutato sulla base del termine massimo di durata di un percorso universitario riferito a un singolo interessato. L'anagrafica degli studenti e i dati di carriera, per obblighi di legge, sono conservati dall'Istituto Scolastico illimitatamente nel tempo. I dati inerenti graduatorie o verbali, per obblighi di legge, sono conservati illimitatamente nel tempo.

Asset di supporto

Rete Interna Informatica, Informazioni Albo Pretorio - Gestione informatica e cartacea delle carriere dei studenti secondo normativa vigente e informazione sul sito web istituzionale

Valutazione

Accettabile

Rispondenza ai principi fondamentali

Proporzionalità e necessità

Le finalità del trattamento sono esplicite e legittime?

Finalità di rilevante interesse pubblico perseguite secondo l'Art. 23 del GDPR 679/2016 nonché dalle Norme vigenti sul diritto allo studio

Valutazione

Accettabile

Quali sono i principi di liceità che rendono il trattamento legittimo?

Principi di liceità di rilevante interesse pubblico perseguite secondo l'Art. 23 del GDPR 679/2016 e secondo le Normative vigenti per il proseguimento della missione della struttura

Valutazione

Accettabile

I dati raccolti sono adeguati e indispensabili per finalità per cui sono trattati?

Relativamente agli Studenti, con l'iscrizione, per tutto il periodo dell'iscrizione ed anche successivamente.

Il trattamento di tali dati è essenziale per poter regolarmente adempiere ai compiti affidati all'Istituto Scolastico e per l'erogazione dei servizi, didattici ed ausiliari. Tali dati, tuttavia, hanno un grande valore perché attengono alla persona degli Studenti e disegnano la propria identità personale. Per questi motivi, ed in conformità a quanto disposto dalle normative di riferimento che disciplinano il trattamento dei dati personali da parte di Soggetti pubblici, l'Istituto Scolastico ha predisposto il presente Regolamento, disponibile anche sul sito internet dell'Istituto Scolastico che regola le modalità del trattamento dei dati. In virtù di tale Regolamento, e più in generale del RGPD2016/679, l'Istituto Scolastico desidera portare a conoscenza che:- i dati vengono raccolti e trattati al fine di consentire l'erogazione dei servizi didattici e di adempiere alle funzioni istituzionali dell'Istituto Scolastico;- il trattamento dei dati avverrà, di norma, in forma elettronica, anche se alcune fasi,(segnatamente, quella della raccolta) potranno avvenire su supporti cartacei;- il conferimento dei dati richiesti nella modulistica è, in linea generale, obbligatorio, in quanto il mancato conferimento non consente agli Uffici di adempiere alle loro funzioni. Vi possono essere, tuttavia, dei casi (che verranno esplicitati nella modulistica) nei quali il conferimento è solo facoltativo;- i dati conferiti all'Istituto Scolastico potranno essere comunicati, anche senza un ulteriore specifico consenso degli Interessati, agli Enti pubblici, nazionali, regionali e locali con i quali l'Istituto Scolastico ha rapporti di scambio di informazioni al fine di adempiere ai propri compiti istituzionali;- analogamente al punto precedente, anche senza un ulteriore specifico consenso degli Interessati. infine, anche senza un ulteriore specifico consenso degli Interessati, i dati personali anagrafici, di residenza e quelli relativi al curriculum studiorum (ivi compresi il voto finale, i voti riportati nel corso degli studi ecc.) potranno essere comunicati ad Enti pubblici a fini statistici oppure ad Enti privati per finalità istituzionali; restano escluse le informazioni non rispondenti alle predette finalità

Valutazione

Accettabile

I dati sono accurati e mantenuti aggiornati?

Il trattamento sarà svolto da Incaricati in forma manuale e/o automatizzata nel rispetto degli artt. 30, 32 e 35 del R.E. 2016/679 con la supervisione del Responsabile della Protezione dei Dati e verrà comunicata, se necessario, all'interessato ogni modifica dei dati in possesso.

Valutazione

Accettabile

Qual è la durata della conservazione dei dati?

Termini di conservazione in relazione ai principali trattamenti effettuati dall'Istituto Scolastico. Finalità amministrative, contabili e fiscali: fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di accertamento e repressione dei reati: 12/24/72 mesi, come previsto dalle specifiche disposizioni normative. Finalità di conservazione previste da obblighi di Legge (ad esempio, la prescrizione legale dei diritti): fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di profilazione e altri trattamenti automatizzati: fino a un massimo di 18 mesi. Finalità tecniche di Assurance (come quelle per il miglioramento dei servizi): fino a un massimo di 24 mesi.

Valutazione

Accettabile

Misure di protezione dei diritti degli interessati

I soggetti interessati come sono informati del trattamento?

Gli Interessati vengono informati al primo contatto con le strutture dell'istituto Scolastico nonché con la reperibilità delle informative sul sito web istituzionale nella sezione dedicata alla privacy

Valutazione

Accettabile

Come si ottiene il consenso dei soggetti interessati?

Il consenso, per le attività inerenti all'art. 9 del GDPR, viene raccolto in forma cartacea

Valutazione

Accettabile

I soggetti interessati come esercitano i loro diritti di accesso e alla portabilità dei dati? Come possono rettificarli o cancellarli? Come possono limitarne il trattamento?

Ogni Interessato ha i seguenti diritti relativi alla protezione dei dati: • richiedere l'accesso ai propri dati personali (comunemente noto come "diritto di accesso"). Ciò consente di ricevere una copia dei dati personali che deteniamo sull'Interessato e di controllarne la corretta elaborazione; • richiedere la correzione dei propri dati personali. Ciò consente di correggere eventuali dati incompleti o inaccurati che conserviamo, sebbene potremmo aver bisogno di verificare l'esattezza dei nuovi dati forniti; • richiedere la cancellazione dei propri dati personali. Ciò consente di chiederci di eliminare o rimuovere i dati personali laddove non ci fossero validi motivi per continuare a elaborarli. Ciò consente, inoltre, di richiedere la cancellazione dei propri dati personali quando: si è esercitato con successo il "diritto all'oblio"; potremmo aver elaborato le informazioni illegalmente o laddove ci venisse richiesto di cancellare i propri dati personali

per conformarci con la Legge locale. Tuttavia, potremmo non essere sempre in grado di soddisfare la richiesta di cancellazione per specifici motivi legali che verrebbero notificati al momento della richiesta; • opporsi al trattamento dei propri dati personali nel caso di interesse legittimo o nel caso di situazioni particolari che potrebbero avere un impatto verso i propri diritti e le libertà fondamentali. È possibile opporsi anche all'utilizzo dei propri dati ai fini di marketing diretto, ove previsto; • richiedere la limitazione del trattamento dei propri dati personali. Ciò consente di chiederci di sospendere il trattamento dei dati personali nei seguenti scenari: (a) se si richiede una verifica per la precisione dei dati; (b) laddove vi sia esplicita richiesta di conservazione dei dati, anche se non più necessari per la nostra operatività, in quanto potrebbe esserci il bisogno di stabilire, difendere o esercitare i propri diritti legali; (c) si contesta il nostro utilizzo dei dati, ma vi è la preventiva necessità di verifica per l'esistenza di motivi legittimi obbligatori per usarli; • richiedere il trasferimento dei dati personali. Forniremo i dati personali in un formato strutturato, comunemente utilizzato e leggibile da un dispositivo elettronico comune (computer). Tale diritto si applica solo alle informazioni automatizzate per le quali è stato fornito preventivamente il consenso, oppure laddove siano state utilizzate le informazioni acquisite per l'esecuzione di un Accordo comune; • revocare il consenso in qualsiasi momento laddove avessimo la necessita del consenso per processare i dati personali. Tuttavia, ciò non pregiudica la liceità di qualsiasi trattamento effettuato prima di revocare il consenso. Se si ritira il consenso, potremmo non essere in grado di fornire determinati prodotti o servizi. Sarà nostra premura informare circa tali evenienze in caso di ritiro del consenso. Per esercitare uno o più dei diritti sopra indicati, è possibile contattare l'Istituto Scolastico. utilizzando le modalità indicate sul sito istituzionale alla voce "Contatti" oppure al seguente indirizzo di posta elettronica ordinaria o Pec. Nel caso di insoddisfazione della risposta a qualsiasi richiesta o reclamo o nel caso si ravvisi un uso non corretto dei propri dati, è possibile presentare reclamo diretto all'Autorità Garante per la Protezione dei Dati Personali. Tuttavia, l'Istituto Scolastico tiene in alta considerazione la riservatezza di chiunque venga a contatto con l'Istituto Scolastico; pertanto, vi sarà sempre la totale e piena disponibilità ad esaminare e risolvere qualsiasi necessità fin dall'inizio.

Valutazione

Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e formalizzati in un contratto?

Art. 5 del Regolamento Privacy- Responsabile Protezione Dati e Incaricati al trattamento dei dati Il Titolare del trattamento, sentito il parere del Responsabile del Trattamento dei Dati e del Direttore amministrativo (se tali figure non coincidono), nomina in forma scritta gli Incaricati al trattamento dei dati, scelti tra il Personale amministrativo in base ai rispettivi ambiti d'impiego, autorizzandoli al trattamento dei dati personali contenuti in atti e documenti riguardanti archivi di tipo cartaceo o effettuati con strumenti automatizzati e/o contenuti nelle eventuali banche dati elettroniche automatizzate, nonché il Responsabile della Protezione Dati (RPD / DPO - Data Protection Officer).La scelta e la nomina dell'RPD / DPO viene effettuata rispettando i parametri indicati nel capo IV Sezione 3 (artt. 37, 38, 39) Il Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (semplicemente definito anche RGPD), in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile della Protezione dei dati personali (artt. 37-39). Il predetto Regolamento prevede l'obbligo per il Titolare o per il Responsabile del trattamento di designare l'RPD «quando il trattamento è effettuato da una Autorità pubblica o da un Organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali» (art.37, paragrafo 1, lett.a). Le predette disposizioni prevedono che l'RPD deve essere individuato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39» (art. 37, paragrafo 5) e «il livello necessario di conoscenza specialistica dovrebbe essere

determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal Titolare del trattamento o dal Responsabile del trattamento". La carica di Incaricati al trattamento dei dati relativamente ai sistemi informatici può essere affidata a più Persone anche in ragione della diversa ubicazione delle varie sedi dell'Istituto Scolastico.

Valutazione

Accettabile

I dati sono adeguatamente protetti nel caso di trasferimento ad altri Soggetti pubblici o al di fuori dell'Unione Europea?

Art.12 del Regolamento Privacy - Richieste di trattamento, comunicazione o diffusione di dati personali La comunicazione e la diffusione dei dati personali da parte dell'Istituto Scolastico ad un altro Soggetto pubblico è consentito ed avviene nell'ambito dei rapporti che essi hanno ai fini dello svolgimento delle rispettive attività istituzionali. Non divulgheremo le informazioni personali che deteniamo, eccetto dove previsto direttamente dalla Legge o nelle seguenti condizioni: (i) alle sedi dell'Istituto Scolastico; (ii) a Soggetti terzi che ci forniscono servizi e che agiscono come Responsabili del trattamento dei dati; (iii) a Consulenti professionali tra cui Istituto Scolastico bancario che gestisce il servizio di cassa, ai Revisori dei conti, ecc.; (iv) all'Agenzia delle Entrate, ad altre Autorità che possono richiedere dati in determinate circostanze. La comunicazione e la diffusione dei dati personali a Terzi sono ammesse solo se previste da disposizioni di Legge o equiparate, con le formalità dalle stesse indicate. Eventuali richieste all'Istituto Scolastico finalizzate ad ottenere il trattamento, la comunicazione o la diffusione di dati personali devono essere presentate sotto forma scritta ed essere adeguatamente motivate. Nella domanda dovranno essere indicati o debbono essere desumibili: - il nome, la denominazione o la ragione sociale del Richiedente; - i dati cui la domanda si riferisce, gli scopi per cui gli stessi sono richiesti e le modalità del loro utilizzo; - l'eventuale ambito di comunicazione e diffusione dei dati richiesti; - la dichiarazione che il richiedente s'impegna ad utilizzare i dati ricevuti esclusivamente per le finalità e nell'ambito delle modalità per cui sono stati richiesti; - copia di un documento di riconoscimento (ove previsto). Il Responsabile del trattamento, dopo aver verificato che la diffusione dei dati personali o la comunicazione dei medesimi ai Richiedenti, ovvero il loro eventuale trattamento da parte di questi ultimi siano ammissibili, provvede a trasmettere i dati a chi ne ha fatto richiesta, nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.

Valutazione

Accettabile

Rischi

Misure esistenti o pianificate

Protezione dei documenti cartacei

Documenti conservati in armadi chiusi a chiave

Valutazione

Accettabile

Sicurezza fisica

Controllo visivo delle aree contenenti documenti cartacei con l'ausilio del Personale in attività

Valutazione

Accettabile

Backup dei dati

Su server.

Valutazione

Ciclo di backup settimanale su supporti fisici magnetici con cifratura e codifica di accesso al contenuto.

Gestione delle postazioni di lavoro

Le postazioni di lavoro vengono configurate tenendo conto del regolamento interno privacy e gestione delle apparecchiature informatiche

Valutazione

Accettabile

Protezione dei canali informativi

L'accesso fraudolento alla rete viene bloccato tramite il firewall inserito direttamente all'ingresso del dato informatico dal provider della connessione dati, e tale misura software e hardware non può essere modificata da nessun operatore interno.

Valutazione

Accettabile

Gestione del personale

Il Personale viene ciclicamente formato sulle novità normative inerenti alla propria funzione all'interno dell'Istituto Scolastico.

Valutazione

Accettabile

Controllo dell'accesso logico

Il cambio password viene effettuato automaticamente dal sistema ogni tre mesi.

l'Amministratore di rete consegna il registro password in busta chiusa sigillata al Direttore amministrativo.
Le password sono univoche, alfanumeriche con caratteri speciali e maiuscole.

Valutazione

Accettabile

Protezione contro le fonti di rischio non antropico

L'edificio è protetto dalle fonti antropiche, come da normativa vigente, con l'impianto di scarico delle potenze a terra. Il Server è dotato di batterie UPS per la protezione dei dati in caso di assenza di energia elettrica.

Valutazione

Accettabile

Lotta contro il malware

Oltre al firewall ogni postazione di lavoro contiene un software anti malware installato e monitorato mensilmente per mitigare furti di identità e uso improprio ed illecito del dato contenuto

Valutazione

Accettabile

Rischio di accesso illegittimo ai dati

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

Diffusione non autorizzata dei dati personali comuni e particolari

Quali sono le principali vulnerabilità che possono condurre al rischio?

Abilitazione di servizi non necessari; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; storage non protetto; linee di comunicazione non protette; errata attribuzione dei diritti di accesso; utilizzo di software su dati non aggiornati; date non corrette

Quali sono le minacce?

Accessi esterni non autorizzati; mancata manutenzione del sistema informativo; furto di apparecchiature o documenti; malfunzionamento hardware; malfunzionamento software; intercettazione dati; azione di virus informativi o di codici malefici; spamming o tecniche di sabotaggio; uso improprio del software; errato uso del software; corruzione dei dati; trattamento illecito dei dati; manomissione del software; furto o copiatura software; uso non autorizzato di apparecchiature; ingressi non autorizzati a locali/aree ad accesso ristretto; sabotaggio

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; sicurezza fisica; backup dei dati; gestione delle postazioni di lavoro; protezione dei canali informativi; gestione del personale; controllo dell'accesso logico; gestione dei rischi in materia di privacy; lotta contro il malware

Stima della gravità del rischio

Medio - e funzioni attuate minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

Stima della probabilità del rischio

Mai verificatosi ma possibile.

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate, il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse

Valutazione

Accettabile

Rischio di modifica non desiderata dei dati

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

Trattamento errato del dato personale

Quali sono le principali vulnerabilità che possono condurre al rischio?

Mancate o incomplete specifiche fornite agli sviluppatori; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; mancato controllo delle copie; insufficiente test del software; errata attribuzione dei diritti di accesso

Quali sono minacce?

Malfunzionamento software; distruzione di apparecchiature o di supporti; furto di apparecchiature o documenti; accessi esterni non autorizzati; trattamento illecito dei dati; malfunzionamento software; distruzione di apparecchiature o di supporti; furto di apparecchiature o documenti; accessi esterni non autorizzati; trattamento illecito dei dati; uso non autorizzato di apparecchiature; Ingressi non autorizzati a locali/aree ad accesso ristretto; Alterazione dolosa o colposa dati automatizzati; Comunicazione illegale dei dati e dei documenti

Quali tra le misure identificate contribuiscono a gestire il rischio?

Backup dei dati; gestione delle postazioni di lavoro (workstation); sicurezza fisica; protezione dei documenti cartacei; protezione dei canali informativi; gestione del personale; controllo dell'accesso logico; gestione dei rischi in materia di privacy; lotta contro il malware

Stima della gravità del rischio

Basso - le funzioni attuate minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

Stima della probabilità del rischio Mai verificatosi ma possibile

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro e delle procedure nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse

Valutazione

Accettabile

Rischio di perdita dei dati

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

Perdita temporanea dei dati e diffusione non condivisa dall'Interessato

Quali sono le principali vulnerabilità che possono condurre al rischio?

Storage non protetto; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; sensibilità all'umidità, allo sporco, alla polvere; sensibilità alle variazioni di tensione; errato smaltimento materiale; mancato controllo delle copie; linee di comunicazione non protette; utilizzo di software su dati non aggiornati; utilizzo di software su dati non aggiornati; parametri di settaggio non corretti; assenza di Personale; mancanza di consapevolezza della sicurezza; mancata sorveglianza delle aree protette; mancanza procedure di accesso con credenziali; insufficiente formazione del Personale; mancato controllo fotocopiatura; impianto elettrico non certificato; gestione inadeguata della rete (bilanciamento di routing); mancanza di software antivirus; insufficiente formazione del Personale.

Quali sono minacce?

Mancata manutenzione del sistema informativo; furto di apparecchiature o documenti; malfunzionamento hardware; malfunzionamento software; intercettazione dati; corruzione dei dati; errato uso del software; uso non autorizzato di apparecchiature; blocco/saturazione del sistema informativo; mancata conservazione o restituzione di documenti; mancata disponibilità di Personale; errore nello svolgimento di mansioni; accesso archivi dati sensibili o giudiziari; accesso archivi dati comuni; sabotaggio; guasto di apparecchiature; accessi esterni non autorizzati; comunicazione illegale dei dati e dei documenti; polvere, corrosione o gelo; distruzione di apparecchiature o di supporti; azione di virus informativi o di codici malefici; spamming o tecniche di sabotaggio; uso improprio del software

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; backup dei dati; gestione delle postazioni di lavoro; gestione del Personale; controllo dell'accesso logico; manutenzione; sicurezza delle attrezzature; protezione dei canali informativi; protezione contro le fonti di rischio non antropico; lotta contro il malware; sicurezza fisica

Stima della probabilità del rischio

Basso - le funzioni ed i processi attuati minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse.

PARTE 4: Informazioni sulla DPIA Relativa al trattamento della carriera scolastica degli alunni

DPIA

Relativa al trattamento dati relativo alla gestione della carriera scolastica degli alunni

Descrizione del trattamento:

I dati sensibili e giudiziari sotto elencati e inerenti il rapporto tra Istituto Scolastico e Studenti, raccolti sia presso gli Interessati che presso Terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti dell'Ente, sia su base cartacea che su base informatica. Principali tipologie di dati oggetto di privacy: dati relativi agli Studenti e/o a Familiari diversamente abili o ad elementi reddituali ai fini di un eventuale controllo sulle autocertificazioni relativi a eventuali esoneri e/o fruizione di eventuali agevolazioni previste dalla Legge, nonché dati relativi alla gestione dei contributi straordinari per iniziative degli Studenti; dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio; dati sensibili e giudiziari che rilevano nell'ambito di procedimenti disciplinari a carico degli Studenti; dati relativi alla condizione di disabile per attività di interpretariato, tutorato, trasporto e servizi analoghi per tutti gli Studenti portatori di handicap. È, di seguito, descritto sinteticamente il flusso informativo dei dati. I dati sensibili e giudiziari sopra descritti inerenti all'attività didattica e alla gestione delle iscrizioni e delle carriere degli Studenti, raccolti sia presso gli Interessati che presso i Terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti, sia su base cartacea che su base informatica. Principali fonti normative R.D. 1592/1933 e successive modificazioni e integrazioni. (Testo unico delle leggi sull'istruzione superiore); R.D. 1269/1938 e successive modificazioni e integrazioni (Approvazione del regolamento sugli Studenti); D.P.R. 382/1980 (Riordinamento della Docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica); L. 398/1989 (Norme in materia di borse di studio universitarie); L. 341 /1990 (Riforma degli Ordinamenti didattici universitari); L.390/1991 (Norme sul diritto agli studi universitari); L. 104/1992 (Legge-quadro per l'assistenza, l'integrazione sociale ed i diritti delle Persone handicappate); D.M. 224/1999 (Norme in materia di Dottorato di ricerca); D. Lgs. n. 445/2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa); L. 148/2002 (Ratifica ed esecuzione della Convenzione di Lisbona dell'11 aprile 1997); D.M. 270/2004 (Modifiche al Regolamento recante norme concernenti l'autonomia didattica degli Atenei, approvato con decreto MURST 3 novembre 1999, n. 509); D.P.R. 334/2004 (Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello Straniero); D.M. n. 142 del 25/3/1998 e L. 24 giugno 1997, n. 196 (Normativa relativa agli stages); DPCM 9 aprile 2001; L. 14 febbraio 2003, n. 30 (c.d. Legge Biagi, di riforma del mercato del lavoro); Contratto Istituzionale Erasmus+ vigente; Statuto dell'Istituto Scolastico; Regolamento per l'Amministrazione, la Finanza e la Contabilità dell'Istituto Scolastico; Regolamento sugli Studenti ed altri Regolamenti d'Istituto Scolastico vigenti; Leggi regionali vigenti in materia di diritto allo studio universitario.

Finalità associate al trattamento Gestione delle iscrizioni

Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi aggiuntivi e adempimento degli obblighi previsti dal D.M. 692/2017 - Anagrafe nazionale degli studenti

Soggetti interessati dal trattamento

Studenti

Titolari del trattamento

Norme di riferimento

GDPR 2016/679; Decreto 10 agosto 2018 n.101

Descrizione dei dati trattati

Dati Comuni: Dati aggiuntivi di alunni e genitori, dati di valutazione della carriera scolastica

Dati personali particolari: Le convinzioni religiose filosofiche e di altro genere; disagi personali di alunni e genitori, Lo stato di salute nel corso della carriera scolastica e per finalità nell'ambito di viaggi d'istruzione,

Dati relativi a condanne penali: Situazioni giudiziarie riferite ai genitori: conosciute solo se comunicate dai diretti interessati o da terzi (figure giuridiche) come tribunale, forze dell'ordine, figure giuridiche a vario titolo:
-Condizione di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)
- Sottoposizione a misure detentive carcerarie
- Status di testimoni di giustizia

Durata di archiviazione dei dati

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: il trattamento dei dati avrà una durata non superiore a quella necessaria agli scopi per i quali i dati sono stati raccolti, come riportato nelle singole finalità; tuttavia, qualora l'Interessato ritenga, per qualsiasi motivo, esaurito lo scopo del trattamento, potrà esercitare i propri diritti inviando una richiesta ai recapiti dell'Istituto Scolastico.

Categorie di destinatari dei dati

Pubblica Amministrazione; INVALSI, Soggetti privati (persone fisiche o giuridiche), agenzie di viaggi, Enti locali (Regione, Comune, Municipio, ASL) ecc.

Soggetti autorizzati al trattamento

Soggetti autorizzati al trattamento, personale amministrativo incaricato alla didattica

Termini di conservazione in relazione ai principali trattamenti effettuati dall'Istituto Scolastico

È di seguito descritto sinteticamente il flusso informativo dei dati e la loro conservazione temporale. I dati sensibili e giudiziari inerenti all'attività didattica e la gestione delle iscrizioni e delle carriere degli Studenti, raccolti sia presso gli Interessati che presso i Terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti, sia su base cartacea che su base informatica. In relazione alle diverse finalità e agli scopi per i quali sono stati raccolti, i dati saranno conservati per il tempo previsto dalla normativa di riferimento ovvero per quello strettamente necessario al perseguimento delle finalità. In particolare: I dati conferiti per l'espletamento del servizio didattico saranno archiviati e mantenuti in coerenza con il consenso acquisito per un periodo massimo di 10 anni. Tale periodo è valutato sulla base del termine massimo di durata di un percorso universitario riferito a un singolo interessato. L'anagrafica degli studenti e i dati di carriera, per obblighi di legge, sono conservati dall'Istituto Scolastico illimitatamente nel tempo. I dati inerenti graduatorie o verbali, per obblighi di legge, sono conservati illimitatamente nel tempo.

Asset di supporto

Rete Interna Informatica, Informazioni Albo Pretorio - Gestione informatica e cartacea delle carriere dei studenti secondo normativa vigente e informazione sul sito web istituzionale

Valutazione

Accettabile

RISPONDENZA AI PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Le finalità del trattamento sono esplicite e legittime?

Finalità di rilevante interesse pubblico perseguite secondo l'Art. 23 del GDPR 679/2016 nonché dalle Norme vigenti sul diritto allo studio

Valutazione

Accettabile

Quali sono i principi di liceità che rendono il trattamento legittimo?

Principi di liceità di rilevante interesse pubblico perseguite secondo l'Art. 23 del GDPR 679/2016 e secondo le Normative vigenti per il proseguimento della missione della struttura

Valutazione

Accettabile

I dati raccolti sono adeguati e indispensabili per finalità per cui sono trattati?

Il trattamento di tali dati è essenziale per poter regolarmente adempiere ai compiti affidati all'Istituto Scolastico e per l'erogazione dei servizi, didattici ed ausiliari. Tali dati, tuttavia, hanno un grande valore perché attengono alla persona degli Studenti e disegnano la propria identità personale. Per questi motivi, ed in conformità a quanto disposto dalle normative di riferimento che disciplinano il trattamento dei dati personali da parte di Soggetti pubblici, l'Istituto Scolastico ha predisposto il presente Regolamento, disponibile anche sul sito internet dell'Istituto Scolastico che regola le modalità del trattamento dei dati. In virtù di tale Regolamento, e più in generale del RGPD2016/679, l'Istituto Scolastico desidera portare a conoscenza che:- i dati vengono raccolti e trattati al fine di consentire l'erogazione dei servizi didattici e di adempiere alle funzioni istituzionali dell'Istituto Scolastico;- il trattamento dei dati avverrà, di norma, in forma elettronica, anche se alcune fasi,(segnatamente, quella della raccolta) potranno avvenire su supporti cartacei;- il conferimento dei dati richiesti nella modulistica è, in linea generale, obbligatorio, in quanto il mancato conferimento non consente agli Uffici di adempiere alle loro funzioni. Vi possono essere, tuttavia, dei casi (che verranno esplicitati nella modulistica) nei quali il conferimento è solo facoltativo;- i dati conferiti all'Istituto Scolastico potranno essere comunicati, anche senza un ulteriore specifico consenso degli Interessati, agli Enti pubblici, nazionali, regionali e locali con i quali l'Istituto Scolastico ha rapporti di scambio di informazioni al fine di adempiere ai propri compiti istituzionali;- analogamente al punto precedente, anche senza un ulteriore specifico consenso degli Interessati. infine, anche senza un ulteriore specifico consenso degli Interessati, i dati personali anagrafici, di residenza e quelli relativi al *curriculum studiorum* (ivi compresi il voto finale, i voti riportati nel corso degli studi ecc.) potranno essere comunicati ad Enti pubblici a fini statistici oppure ad Enti privati per finalità istituzionali; restano escluse le informazioni non rispondenti alle predette finalità

Valutazione

Accettabile

I dati sono accurati e mantenuti aggiornati?

Il trattamento sarà svolto da Incaricati in forma manuale e/o automatizzata nel rispetto degli artt. 30, 32 e 35 del R.E. 2016/679 con la supervisione del Responsabile della Protezione dei Dati e verrà comunicata, se necessario, all'interessato ogni modifica dei dati in possesso.

Valutazione

Accettabile

Qual è la durata della conservazione dei dati?

Termini di conservazione in relazione ai principali trattamenti effettuati dall'Istituto Scolastico. Finalità amministrative, contabili e fiscali: fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di accertamento e repressione dei reati: 12/24/72 mesi, come previsto dalle specifiche disposizioni normative. Finalità di conservazione previste da obblighi di Legge (ad esempio, la prescrizione legale dei diritti): fino a 10 anni dopo la cessazione della fornitura dei servizi. Finalità di profilazione e altri trattamenti automatizzati: fino a un massimo di 18 mesi. Finalità tecniche di assurance (come quelle per il miglioramento dei servizi): fino a un massimo di 24 mesi.

Valutazione

Accettabile

Misure di protezione dei diritti degli interessati

I soggetti interessati come sono informati del trattamento?

Gli Interessati vengono informati al primo contatto con le strutture dell'I.C. PIERSANTI MATTARELLA nonché con la reperibilità delle informative sul sito web istituzionale nella sezione dedicata alla privacy.

Valutazione

Accettabile

Come si ottiene il consenso dei soggetti interessati?

Il consenso, per le attività inerenti all'art. 9 del GDPR, viene raccolto in forma cartacea

Valutazione

Accettabile

I soggetti interessati come esercitano i loro diritti di accesso e alla portabilità dei dati? Come possono rettificarli o cancellarli? Come possono limitarne il trattamento?

Ogni Interessato ha i seguenti diritti relativi alla protezione dei dati: • richiedere l'accesso ai propri dati personali (comunemente noto come "diritto di accesso"). Ciò consente di ricevere una copia dei dati personali che deteniamo sull'Interessato e di controllarne la corretta elaborazione; • richiedere la correzione dei propri dati personali. Ciò consente di correggere eventuali dati incompleti o inaccurati che conserviamo, sebbene potremmo aver bisogno di verificare l'esattezza dei nuovi dati forniti; • richiedere la cancellazione dei propri dati personali. Ciò consente di chiederci di eliminare o rimuovere i dati personali laddove non ci fossero validi motivi per continuare a elaborarli. Ciò consente, inoltre, di richiedere la cancellazione dei propri dati personali quando: si è esercitato con successo il "diritto all'oblio"; potremmo aver elaborato le informazioni illegalmente o laddove ci venisse richiesto di cancellare i propri dati personali

per conformarci con la Legge locale. Tuttavia, potremmo non essere sempre in grado di soddisfare la richiesta di cancellazione per specifici motivi legali che verrebbero notificati al momento della richiesta; • opporsi al trattamento dei propri dati personali nel caso di interesse legittimo o nel caso di situazioni particolari che potrebbero avere un impatto verso i propri diritti e le libertà fondamentali. È possibile opporsi anche all'utilizzo dei propri dati ai fini di marketing diretto, ove previsto; • richiedere la limitazione del trattamento dei propri dati personali. Ciò consente di chiederci di sospendere il trattamento dei dati personali nei seguenti scenari: (a) se si richiede una verifica per la precisione dei dati; (b) laddove vi sia esplicita richiesta di conservazione dei dati, anche se non più necessari per la nostra operatività, in quanto potrebbe esserci il bisogno di stabilire, difendere o esercitare i propri diritti legali; (c) si contesta il nostro utilizzo dei dati, ma vi è la preventiva necessità di verifica per l'esistenza di motivi legittimi obbligatori per usarli; • richiedere il trasferimento dei dati personali. Forniremo i dati personali in un formato strutturato, comunemente utilizzato e leggibile da un dispositivo elettronico comune (computer). Tale diritto si applica solo alle informazioni automatizzate per le quali è stato fornito preventivamente il consenso, oppure laddove siano state utilizzate le informazioni acquisite per l'esecuzione di un Accordo comune; • revocare il consenso in qualsiasi momento laddove avessimo la necessita del consenso per processare i dati personali. Tuttavia, ciò non pregiudica la liceità di qualsiasi trattamento effettuato prima di revocare il consenso. Se si ritira il consenso, potremmo non essere in grado di fornire determinati prodotti o servizi. Sarà nostra premura informare circa tali evenienze in caso di ritiro del consenso. Per esercitare uno o più dei diritti sopra indicati, è possibile contattare l'Istituto Scolastico. utilizzando le modalità indicate sul sito istituzionale alla voce "Contatti" oppure al seguente indirizzo di posta elettronica ordinaria o Pec. Nel caso di insoddisfazione della risposta a qualsiasi richiesta o reclamo o nel caso si ravvisi un uso non corretto dei propri dati, è possibile presentare reclamo diretto all'Autorità Garante per la Protezione dei Dati Personali. Tuttavia, l'Istituto Scolastico tiene in alta considerazione la riservatezza di chiunque venga a contatto con l'Istituto Scolastico; pertanto, vi sarà sempre la totale e piena disponibilità ad esaminare e risolvere qualsiasi necessità fin dall'inizio.

Valutazione

Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e formalizzati in un contratto?

Art. 5 del Regolamento Privacy- Responsabile Protezione Dati e Incaricati al trattamento dei dati Il Titolare del trattamento, sentito il parere del Responsabile del Trattamento dei Dati e del Direttore amministrativo (se tali figure non coincidono), nomina in forma scritta gli Incaricati al trattamento dei dati, scelti tra il Personale amministrativo in base ai rispettivi ambiti d'impiego, autorizzandoli al trattamento dei dati personali contenuti in atti e documenti riguardanti archivi di tipo cartaceo o effettuati con strumenti automatizzati e/o contenuti nelle eventuali banche dati elettroniche automatizzate, nonché il Responsabile della Protezione Dati (RPD / DPO - Data Protection Officer).La scelta e la nomina dell'RPD / DPO viene effettuata rispettando i parametri indicati nel capo IV Sezione 3 (artt. 37, 38, 39) Il Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (semplicemente definito anche RGPD), in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile della Protezione dei dati personali (artt. 37-39). Il predetto Regolamento prevede l'obbligo per il Titolare o per il Responsabile del trattamento di designare l'RPD «quando il trattamento è effettuato da una Autorità pubblica o da un Organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali» (art.37, paragrafo 1, lett.a). Le predette disposizioni prevedono che l'RPD deve essere individuato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39» (art. 37, paragrafo 5) e «il livello necessario di conoscenza specialistica dovrebbe essere

determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal Titolare del trattamento o dal Responsabile del trattamento". La carica di Incaricati al trattamento dei dati relativamente ai sistemi informatici può essere affidata a più Persone anche in ragione della diversa ubicazione delle varie sedi dell'Istituto Scolastico.

Valutazione

Accettabile

I dati sono adeguatamente protetti nel caso di trasferimento ad altri Soggetti pubblici o al di fuori dell'Unione Europea?

Art.12 del Regolamento Privacy - Richieste di trattamento, comunicazione o diffusione di dati personali La comunicazione e la diffusione dei dati personali da parte dell'Istituto Scolastico ad un altro Soggetto pubblico è consentito ed avviene nell'ambito dei rapporti che essi hanno ai fini dello svolgimento delle rispettive attività istituzionali. Non divulgheremo le informazioni personali che deteniamo, eccetto dove previsto direttamente dalla Legge o nelle seguenti condizioni: (i) alle sedi dell'Istituto Scolastico; (ii) a Soggetti terzi che ci forniscono servizi e che agiscono come Responsabili del trattamento dei dati; (iii) a Consulenti professionali tra cui Istituto Scolastico bancario che gestisce il servizio di cassa, ai Revisori dei conti, ecc.; (iv) all'Agenzia delle Entrate, ad altre Autorità che possono richiedere dati in determinate circostanze. La comunicazione e la diffusione dei dati personali a Terzi sono ammesse solo se previste da disposizioni di Legge o equiparate, con le formalità dalle stesse indicate. Eventuali richieste all'Istituto Scolastico finalizzate ad ottenere il trattamento, la comunicazione o la diffusione di dati personali devono essere presentate sotto forma scritta ed essere adeguatamente motivate. Nella domanda dovranno essere indicati o debbono essere desumibili: - il nome, la denominazione o la ragione sociale del Richiedente; - i dati cui la domanda si riferisce, gli scopi per cui gli stessi sono richiesti e le modalità del loro utilizzo; - l'eventuale ambito di comunicazione e diffusione dei dati richiesti; - la dichiarazione che il richiedente s'impegna ad utilizzare i dati ricevuti esclusivamente per le finalità e nell'ambito delle modalità per cui sono stati richiesti; - copia di un documento di riconoscimento (ove previsto). Il Responsabile del trattamento, dopo aver verificato che la diffusione dei dati personali o la comunicazione dei medesimi ai Richiedenti, ovvero il loro eventuale trattamento da parte di questi ultimi siano ammissibili, provvede a trasmettere i dati a chi ne ha fatto richiesta, nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.

Valutazione

Accettabile

Rischi

Misure esistenti o pianificate

Protezione dei documenti cartacei

Documenti conservati in armadi chiusi a chiave

Valutazione

Accettabile

Sicurezza fisica

Controllo visivo delle aree contenenti documenti cartacei con l'ausilio del Personale in attività

Valutazione

Accettabile

Backup dei dati

Ciclo di backup settimanale su supporti fisici magnetici con cifratura e codifica di accesso al contenuto.

Valutazione

Accettabile

Gestione delle postazioni di lavoro

Le postazioni di lavoro vengono configurate tenendo conto del regolamento interno privacy e gestione delle apparecchiature informatiche

Valutazione

Accettabile

Protezione dei canali informativi

L'accesso fraudolento alla rete viene bloccato tramite il firewall inserito direttamente all'ingresso del dato informatico dal provider della connessione dati, e tale misura software e hardware non può essere modificata da nessun operatore interno.

Valutazione

Accettabile

Gestione del personale

Il Personale viene ciclicamente formato sulle novità normative inerenti alla propria funzione all'interno dell'Istituto Scolastico.

Valutazione

Accettabile

Controllo dell'accesso logico

Il cambio password viene effettuato automaticamente dal sistema ogni tre mesi.

l'Amministratore di rete consegna il registro password in busta chiusa sigillata al Direttore amministrativo.
Le password sono univoche, alfanumeriche con caratteri speciali e maiuscole.

Valutazione

Accettabile

Protezione contro le fonti di rischio non antropico

L'edificio è protetto dalle fonti antropiche, come da normativa vigente, con l'impianto di scarico delle potenze a terra nonché da batterie UPS per la protezione dei dati in caso di assenza di energia elettrica.

Valutazione

Accettabile

Lotta contro il malware

Oltre al firewall ogni postazione di lavoro contiene un software anti malware installato e monitorato mensilmente per mitigare furti di identità e uso improprio ed illecito del dato contenuto

Valutazione

Accettabile

Rischio di accesso illegittimo ai dati

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

Diffusione non autorizzata dei dati personali comuni e particolari

Quali sono le principali vulnerabilità che possono condurre al rischio?

Abilitazione di servizi non necessari; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; storage non protetto; linee di comunicazione non protette; errata attribuzione dei diritti di accesso; utilizzo di software su dati non aggiornati; date non corrette

Quali sono le minacce?

Accessi esterni non autorizzati; mancata manutenzione del sistema informativo; furto di apparecchiature o documenti; malfunzionamento hardware; malfunzionamento software; intercettazione dati; azione di virus informativi o di codici malefici; spamming o tecniche di sabotaggio; uso improprio del software; errato uso del software; corruzione dei dati; trattamento illecito dei dati; manomissione del software; furto o copiatura software; uso non autorizzato di apparecchiature; ingressi non autorizzati a locali/aree ad accesso ristretto; sabotaggio

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; sicurezza fisica; backup dei dati; gestione delle postazioni di lavoro; protezione dei canali informativi; gestione del personale; controllo dell'accesso logico; gestione dei rischi in materia di privacy; lotta contro il malware

Stima della gravità del rischio

Medio - e funzioni attuate minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

Stima della probabilità del rischio

Mai verificatosi ma possibile.

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate, il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse

Valutazione

Accettabile

Rischio di modifica non desiderata dei dati

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

Trattamento errato del dato personale

Quali sono le principali vulnerabilità che possono condurre al rischio?

Mancate o incomplete specifiche fornite agli sviluppatori; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; mancato controllo delle copie; insufficiente test del software; errata attribuzione dei diritti di accesso

Quali sono minacce?

Malfunzionamento software; distruzione di apparecchiature o di supporti; furto di apparecchiature o documenti; accessi esterni non autorizzati; trattamento illecito dei dati; malfunzionamento software; distruzione di apparecchiature o di supporti; furto di apparecchiature o documenti; accessi esterni non autorizzati; trattamento illecito dei dati; uso non autorizzato di apparecchiature; Ingressi non autorizzati a locali/aree ad accesso ristretto; Alterazione dolosa o colposa dati automatizzati; Comunicazione illegale dei dati e dei documenti

Quali tra le misure identificate contribuiscono a gestire il rischio?

Backup dei dati; gestione delle postazioni di lavoro (workstation); sicurezza fisica; protezione dei documenti cartacei; protezione dei canali informativi; gestione del personale; controllo dell'accesso logico; gestione dei rischi in materia di privacy; lotta contro il malware

Stima della gravità del rischio

Basso - le funzioni attuate minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

Stima della probabilità del rischio Mai verificatosi ma possibile

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro e delle procedure nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse

Valutazione

Accettabile

Rischio di perdita dei dati

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

Perdita temporanea dei dati e diffusione non condivisa dall'Interessato

Quali sono le principali vulnerabilità che possono condurre al rischio?

Storage non protetto; manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione; sensibilità all'umidità, allo sporco, alla polvere; sensibilità alle variazioni di tensione; errato smaltimento materiale; mancato controllo delle copie; linee di comunicazione non protette; utilizzo di software su dati non aggiornati; utilizzo di software su dati non aggiornati; parametri di settaggio non corretti; assenza di Personale; mancanza di consapevolezza della sicurezza; mancata sorveglianza delle aree protette; mancanza procedure di accesso con credenziali; insufficiente formazione del Personale; mancato controllo fotocopiatura; impianto elettrico non certificato; gestione inadeguata della rete (bilanciamento di routing); mancanza di software antivirus; insufficiente formazione del Personale.

Quali sono minacce?

Mancata manutenzione del sistema informativo; furto di apparecchiature o documenti; malfunzionamento hardware; malfunzionamento software; intercettazione dati; corruzione dei dati; errato uso del software; uso non autorizzato di apparecchiature; blocco/saturazione del sistema informativo; mancata conservazione o restituzione di documenti; mancata disponibilità di Personale; errore nello svolgimento di mansioni; accesso archivi dati sensibili o giudiziari; accesso archivi dati comuni; sabotaggio; guasto di apparecchiature; accessi esterni non autorizzati; comunicazione illegale dei dati e dei documenti; polvere, corrosione o gelo; distruzione di apparecchiature o di supporti; azione di virus informativi o di codici malefici; spamming o tecniche di sabotaggio; uso improprio del software

Quali tra le misure identificate contribuiscono a gestire il rischio?

Protezione dei documenti cartacei; backup dei dati; gestione delle postazioni di lavoro; gestione del Personale; controllo dell'accesso logico; manutenzione; sicurezza delle attrezzature; protezione dei canali informativi; protezione contro le fonti di rischio non antropico; lotta contro il malware; sicurezza fisica

Stima della probabilità del rischio

Basso - le funzioni ed i processi attuati minimizzano al massimo il rischio di perdita e modifica indesiderata dei dati

La probabilità stimata viene fuori dallo storico della gestione dei punti di lavoro nonché dalle misure ferree che vengono attuate ogni giorno nella gestione del dato personale affidato. Nel caso di modifiche errate il sistema prevede un confronto con il dato già memorizzato sui sistemi in uso e indica le incongruenze emerse