Valutazione d'impatto sulla protezione dei dati
(art.35 GDPR 2016/679)

TRATTAMENTO

ID1

"ISCRIZIONE ALUNNI"

"Istituto delle Suore Benedettine della Provvidenza
Benedetta Cambiagio Scuola paritaria dell'Infanzia e Primaria
Sede Legale: Via San Giuliano, 10 – 16100 GENOVA
Sede operativa: Via della Moletta, 10 - 00154 Roma
T .+ 39 06.57069101 – F. +39 06. 57069719"

ALLEGATO DPIA Emesso in Rev. 0 16.12.2021

Firma Legale Rappresentante _____

ID1 "ISCRIZIONE ALUNNI"

TRATTAMENTO
Quale trattamento dei dati personali viene effettuato (per ogni trattamento/ripetere il questionario)? *Presenta un breve sunto del trattamento (consigliabile indicare un ID di ciascun trattamento, per ID. 1, ID.2): nome, scopo, finalità, contesto di uso, etc.* **ISCRIZIONE ALUNNI**
Quali sono le responsabilità legate al trattamento? *Descrivi le responsabilità degli stakeholder: il titolare del trattamento, gli eventuali responsabili esterni o co-titolare (che condividono le prerogative in ordine alle finalità)* **TITOLARE (EROGAZIONE DEL SERVIZIO), SEGRETERIA, MINORI ISCRITTI ALLE SCUOLE**
Ci sono standard applicabili al trattamento? *Elenca gli standard rilevanti applicabili al trattamento, specialmente i codici di condotta e le certificazioni di protezione dati.* **NON CI SONO**
Quali sono i dati trattati? *Elenca i dati raccolti e trattati. Definisci per ognuno la durata dell'archiviazione, i destinatari (soggetti che ricevutono i dati siano essi terzi o meno) e le persone con accesso.* **DATI PERSONALI ANCHE PARTICOLARI.**
Com'è il ciclo di vita del trattamento dei dati? *Presenta e descrivi come funziona il processo (dalla raccolta alla distruzione, i passaggi del trattamento, archiviazione, etc.), usando per esempio un diagramma di flusso dei dati (come allegato) e una dettagliata descrizione del processi effettuati.* **RACCOLTA DATI, INFORMATIVA E CONSENSO DEI RESPONSABILI GENITORIALI-CONSERVAZIONE DELLE INFORMAZIONI RACCOLTE**
Quali sono le risorse di supporto ai dati? *Elenca le risorse che ospitano i dati (sistemi operativi, applicazioni aziendali, database management systems, pacchetti office, protocolli, configurazioni etc.)* **PC DIREZIONE/SEGRETERIA per caricamento su SCUOLA ONLINE+ ARCHIVI CARTACEI PRESSO UFFICIO DIREZIONE**
Gli scopi del trattamento sono specifici, espliciti e legittimi? *Spiegare perché le finalità del trattamento sono specifiche, esplicite e legittime.* **VALUTATE LE BASI GIURIDICHE DI CIASCUN TRATTAMENTO.**
Quali sono le basi legali che rendono il trattamento legittimo? *Presentare le basi del trattamento (ad esempio consenso, esecuzione di un contratto, obbligo legale, interessi vitali etc.)* **TRA LE BASI DEL TRATTAMENTO PER IL TRATTAMENTO C'E' IL CONSENSO CHE VIENE ACCQUISITO DIRETTAMENTE PRESSO INTERESSATI**

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

Spiegare perchè ogni dato raccolto è necessario per le finalità del trattamento.

NECESSARIO PER POTER EROGARE IL SERVIZIO SCOLASTICO

I dati sono accurati e mantenuti aggiornati?

Descrivere quali sono i passaggi intrapresi per assicurare la qualità dei dati.

VEDERE DOCUMENTAZIONE IN ESSERE.

Quale è la durata della conservazione dei dati?

Spiegare perchè la durata della conservazione è giustificata in termini di requisiti legali e/o necessità i trattamento.

IN BASE ALLE LINEE GUIDA DEGLI ARCHIVI SCOLASTICI

I soggetti interessati come sono informati del trattamento?

Descrivere quali informazioni sono fornite ai soggetti interessati e quali mezzi vengono impiegati.

AGLI INTERESSATI COINVOLTI VIENE DATA IDONEA INFORMATIVA.

Come si ottiene il consenso dei soggetti interessati?

Descrivere i controlli intesi ad assicurare che il consenso dell'utente sia ottenuto.

Viene sottoscritto il consenso direttamente dall'interessato (in quanto minore, da entrambi i genitori)

I soggetti interessati, come esercitano i loro diritti di acceso alla portabilità dei dati (se applicabile)?

Descrivere i controlli intesi a permettere ai soggetti interessati di accedere, ricevere e trasmettere i loro dati in forma strutturata

Nell'informativa si specificano i contatti e le modalitià per l'esercizione dei diritti dell'interessato

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

Descrivere i controlli intesi ad abilitare i soggetti interessati a rettificare e la cancellazione dei loro dati.

Nell'informativa si specificano i contatti e le modalità per l'esercizione dei diritti dell'interessato, un volta ricevuta la richiesta viene elaborata nei termini di legge

I soggetti interessati come esercitano il loro diritto di limitazione e di opposizione?

Descrivere i controlli intesi ad abilitare i soggetti interessati a limitare e opporsi al trattamento dei loro dati.

Nell'informativa si specificano i contatti e le modalità per l'esercizione dei diritti dell'interessato, un volta ricevuta la richiesta viene elaborata nei termini di legge

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

Per ogni responsabile del trattamento, descrivere le sue responsabilità, durata, finalità, scopo, istruzioni documentate, previa autorizzazione) e fornire i contratti, codici di condotta e certificazioni determinanti le missioni e gli obblighi.

sì viene sottoscritto un contratto ex art. 28 del Gdpr con ciascun fornitore

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

Per ogni nazione fuori dall'Unione Europea dove i dati sono archiviati e processati, indicare e descrivere se sono riconosciuti come offerenti di un livello adeguato di protezione dei dati o descrivere la fornitura di servizi concernenti il trasferimento

non si effettuano trasferimenti dei dati fuori dell'UE

ID1 "ISCRIZIONE ALUNNI"

CONTROLLI ESISTENTI
Crittografia *Descrivi qui i mezzi implementati per assicurare la confidenzialità dei dati* **NO**
Anonimizzazione Indicare qui i meccanismi di anonimizzazione implementati **NO**
Partizionamento dei dati *Indicare qui se sono pianificati dei meccanismi di disgunzione tra i dati comuni identificativi e le altre informazioni relative agli interessati* **NO**
Controlli logici agli accessi *Indicare qui come i profili degli utenti sono definiti e attribuiti (specificare i requisiti delle parole chiave: lunghezza, caratteri obbligatori, validità, numero di tentativi falliti prima del blocco)* **UTENTI ACCEDONO CON USER NAME E PASSWORD**
Tracciabilità (logging) *Indicare qui se gli eventi sono registrati e quanto a lungo sono conservati* **ESISTONO LOG DEGLI ACCESSI SU PC conservati per tempo illimitato.**
Archiviazione *Indicare qui se sono implementati meccanismi per monitorare l'integrità dei dati archiviati, quali sono e con quali finalità* **BACKUP PERIODICO AUTOMATICO SU DIPOSITIVO SEPARATO**
Sicurezza dei documenti cartacei ARCHIVI CARTACEI ALL'INTERNO DI LOCALI AD ACCESSO RISERVATO, CHIUSI IN ARMADI DOTATI DI CHIAVE. *Indica qui se sono implementati meccanismi per il monitoraggio della riservatezza e dell'integrità dei documenti cartacei, quali sono e con quali finalità* **Ai dati contenuti nei documenti cartacei viene garantita sia la riservatezza tramite misure organizzative, le stesse misure garantiscono l'integrità dei dati**
Minimizzare la quantità di dati personali *Indicare qui i mezzi implementati per ridurre la gravità del rischio limitando la quantità di dai personali impiegati* **I DATI PERSONALI RACCOLTI SONO QUELLI STRETTAMENTE NECESSARI PER ASSOLVERE AL TRATTAMENTO COME SPECIFICATO ANCHE NEL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO.**
Vulnerabilità *Descrivi qui come si aggiorna il software (sistemi operativi, applicazioni, etc.) e come sono effettuati i controlli di sicurezza e patch* **MONITORAGGIO PERIODICO DEI SISTEMI E ASSISTENZA TECNICA, SU CONDIZIONE, DA PARTE Di APPOSITA AZIENDA . CONFIGURATI SUI DIVERSI SISTEMI (S.O., ANTIVIRUS) QUANDO POSSIBILE L'AGGIORNAMENTO AUTOMATICO**
Contromisure contro il malware *Descrivi qui i controlli implementati contro il codice malevolo quando accedi a reti con un livello di sicurezza inferiore* **Firewall SW, antivirus presente su tutte le macchine.**
Gestione postazioni *Descrivi qui i controlli implementati sulle postazioni di lavoro (p.e. controllo dati di navigazione, controllo email, altro)* **accessi logici configurati su tutte le postazioni, dati di navigazione gestite da restrizioni del firewall.**
Sicurezza siti Web *Indicare qui i controlli implementati per proteggere i siti Web* **sito web solo di presentazione, l'utente risulta adeguatamente informato sui dati raccolti, il sito è protetto da certificato SSL.**
Backup *Indicare qui come sono gestiti i backup. Chiarisci se sono conservati in un luogo sicuro* **BACKUP PERIODICO AUTOMATICO SU DIPOSITIVO SEPARATO**
Manutenzione Descrivi qui come è gestita la manutenzione fisica delle attrezzature **ASSISTENA TECNICA CON DITTA ESTERNA RESPONSABILE DEL TRATTAMENTO.**

Nomine e contratti relativi al trattamento

Descrivere qui le misure specifiche per gli autorizzati al trattamento e i responsabili del trattamento (hosting, società di manutenzione, amministratore, gestori di servizi specialistici, etc.)

AUTORIZZAZIONE PER I DESIGNATI AL TRATTAMENTO DATI - No esterni

Sicurezza della rete

Indicare qui i controlli di sicurezza della rete sulla quale il trattamento è effettuato

ANTIVIRUS - FIREWALL SW

Controllo degi accessi fisici

Indicare qui come il controllo dell'accesso fisico è effettuato nei locali che ospitano il trattamento

ACCESSO ALLA STRUTTURA CONTROLLATO - ACCESSO AI LOCALI IN CUI SONO TRATTATI I DATI AD ACCESSO RISERVATO CON CHIAVE

Monitoraggio dell'attività della rete

Indicare qui i mezzi e i cointrolli implementati per rilevare incidenti che riguardano dati personali

PROCEDURA DATA BREACH - FORMAZIONE DEGLI UTENTI - SISTEMI AUTOMATICI QUALI FIREWALL E ANTIVIRUS - MONITORAGGIO PERIODICO DELL'AMMINISTRATORE DI SISTEMA.

Sicurezza dell'hardware

Indicare qui i controlli operanti sulla sicurezza fisica di server e postazioni PC

ASSISTENZA TECNICA CON DITTA SPECIALIZZATA

Evitare le fonti di rischio

Indicare qui se l'area delle infrastrutture può essere soggetta a disastri ambientali

CENTRO URBANO - ZONA SISMICA 2 B - Zona con pericolosità sismica media dove possono verificarsi forti terremoti.

Protezione contro fonti di rischio non umane

Indicare qui le protezioni contro le fonti i rischio non umane

IMPIANTO RILEVAZIONE E SPEGNIMENTO INCENDIO

Organizzazione

Indicare se i ruoli e le responsabilità per la protezione dei dati sono definite

ORGANIGRAMMA RIPORTATO NEL DOSSIER PRIVACY SEZ.5

Politiche

Descrivere qui la base documentale per impostare gli obiettivi e le regole per la protezione dei dati

PROCEDURE DI GESTIONE RIPORTATE NEL DOCUMENTO "DOSSIER PRIVACY" SEZ.6

Gestione dei rischi sulla privacy

Indicare se è stata effettuato una mappatura dei trattamenti dell'organizzazione ed è stato effettuato una valutazione dei rischi inerenti tutti i trattamenti della stessa

REGISTRO ATTIVITA' DI TRATTAMENTO E RELATIVA VALUTAZIONE DEI RISCHI IN REVISIONE 2 Al 26.11.21.

Integrare la protezione della privacy nei progetti

Descrivere qui come la protezione della privacy è integrata nei progetti

--

Gestire le violazioni dei dati personali

Indicare qui se gli incidenti di IT sono soggetti a procedure di gestione documentate e testate

PROCEDURA DATA BREACH RIPORTATA ALL'INTERNO DEL DOCUMENTO DOSSIER PRIVACY

Gestione del personale

Indicare qui quali iniziative per aumentare la consapevolezza sono effettuate nei riguardi degli impiegati

ATTIVITA' FORMATIVA EROGATA AGLI INCARICATI SIA INTERNAMENTE CHE DA PARTE DEL DPO.

Relazioni con terze parti

Indicare qui, per ciascun responsabile del trattamento, denominazione/indentificazione, finalità del trattamanto, ambito applicativo, riferimento contratto, compliance art. 28 Gdpr

Sono state rivisionate le nomine in rif. GDPR

Supervisione

Indicare qui se l'efficacia e l'adeguatezza dei controlli anche per i diritti di degli interessati (richiesta di accesso, cancellazione, limitazione, opposizione al tramento) sono monitorate come viene monitorata e testata l'adeguatezza e l'efficacia delle misure di sicurezza/controlli

AUDIT INTERNO/DPO

Controlli Esistenti

ID1 "ISCRIZIONE ALUNNI"

ACCESSO ILLEGITTIMO AI DATI

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

Inserire possibili rischi sui diritti e libertà fondamentali degli interessati, in termini di riservatezza

L'IMPATTO PUO' ESSERE CONSIDERATO TRASCURABILE IN QUANTO LE INFORMAZIONI RELATIVE ALLE ISCRIZIONI SONO LEGALMENTE REGOLAMENTATE

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Inserire le minacce per la riservatezza

Perdita di riservatezza del dato

Quali sono le fonti di rischio?

Inserire le fonti di rischio in termini di riservatezza

ACCESSO NON AUTORIZZATO SIA FISICO CHE LOGICO - ERRORI DEGLI UTENTI AUTORIZZATI - GUASTI TECNICI O ERRATA CONFIGURAZIONE SISTEMI.

Quali dei controlli identificati contribuiscono a gestire il rischio?

Clicca qui per selezionare i controlli che gestiscono il rischio.

Attribuzione delle credenziali di autenticazioni e sul piano fisico accesso riservato e protetto, MONITORAGGIO E MANUTENZIONE DEI SISTEMI

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

(indefinito) - Trascurabile - Limitato - Importante - Massimo

Giustificare qui la gravità stimata del rischio.

TRASCURABILE

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

(indefinito) - Trascurabile - Limitato - Importante - Msssimo

TRASCURABILE

ID1 "ISCRIZIONE ALUNNI"

MODIFICHE INDESIDERATE AI DATI

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

L'INTERESSATO POTREBBE RITENERE VIOLATA LA PROPRIA RIVACY ANCHE SE CON IMPATTO LIMITATO PROPRIO IN VIRTU' DEL FATTO CHE ESSENDO INFORMAZIONI LEGALMENTE REGOLAMNTATE, LA LORO MODIFICA POTREBBE CREARE IMBARAZZO ALL'INTERESSATO

modifica del dato o perdita di integrità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

ERRORI DEGLI INCARICATI

Quali sono le fonti di rischio?

ERRORI DEGLI INCARICATI

Quali dei controlli identificati contribuiscono a gestire il rischio?

FORMAZIONE DEGLI INCARICATI - ACCESSI CONTROLLATI AI SISTEMI - CIFRATURA E BK

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

(indefinito) - Trascurabile - Limitato - Importante - Msssimo

LIMITATO

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

(indefinito) - Trascurabile - Limitato - Importante - Msssimo

TRASCURABILE

ID1 "ISCRIZIONE ALUNNI"

PERDITA DISPONIBILITA' DEI DATI

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

Quali sono le principali minacce che potrebbero concretizzare il rischio?
FURTO/PERDITA DI DOCUMENTI - FURTO DEL PC/BK -EVENTI CALAMITOSI - FURTO DI CREDENZIALI

Quali sono le fonti di rischio?
ACCESSI NON AUTORIZZATI SIA FISICI CHE LOGICI - IMPRUDENZA/INCOMPETENZA DEGLI OPERATORI - EVENTI CALAMITOSI

Quali dei controlli identificati contribuiscono a gestire il rischio?
FORMAZIONE DEGLI OPERATORI AUTORIZZATI - ACCESSI FISICI E LOGICI CONTROLLATI - DISLOCAZIONE DELLE APPARECCHIATURE E DEGLI ARCHIVI - SITEMI DI RILEVAZIONE E SPEGNI MENTO INCIENDIO

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?
(indefinito) - Trascurabile - Limitato - Importante - Massimo
IMPORTANTE

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?
(indefinito) - Trascurabile - Limitato - Importante - Massimo
TRASCURABILE