



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

TRATTAMENTO

ID2

"GESTIONE MATERIALE FOTOGRAFICO E AUDIOVISIVO"

**"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 _____

ID2 "GESTIONE MATERIALE FOTOGRAFICO E AUDIOVISIVO"

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.

GESTIONE MATERIALE FOTOGRAFICO E AUDIOVISIVO

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 (LEGATE AD EVENTI IN ESSERE ALL'INTERNO DELL'ORGANIZZAZIONE), FOTOGRAFO RESPONSABILE ESTERNO, INTERESSATI (DOCENTI, ALUNNI, DIPENDENTI)

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 ricevono i dati siano essi terzi o meno) e le persone con accesso.

DATI PERSONALI ANCHE PARTICOLARI. Le riprese audiovideo e il materiale fotografico saranno visibili solo da un pubblico conosciuto, limitato e controllabile attraverso la stampa o la riproduzione su supporti da distribuire alle famiglie degli iscritti o disponibili su piattaforma CLASSROOM e Registro elettronico in area privata con accesso tramite credenziali. Internamente, tali dati possono essere gestiti dalla Direttrice, Segretaria, Coordinatrice didattica e Personale Docente.

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.

ACQUISIZIONE IMMAGINI/AUDIO/VIDEO, ARCHIVIAZIONE SU PC (LINEA GUIDA PER LA REALIZZAZIONE E L'UTILIZZO DI FOTO E VIDEO IN AMBITO SCOLASTICO) - DISTRIBUZIONE ALLE FAMIGLIE - SE NON RICONOSCIBILI SOGGETTI POSSIBILE PUBBLICAZIONE SU SITO INTERNET

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 E SEGRETERIA

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 ACQUISITO 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 FINALITA' DIDATTICHE E DI TESTIMONIANZA DI ATTIVITA' SVOLTE ALL'INTERNO DELLA SCUOLA e ad uso esclusivo dei familiari e degli alunni stessi. Le immagini verranno raccolte in occasione delle attività collettive svolte dagli iscritti e saranno visibili solo da un pubblico conosciuto, limitato e controllabile attraverso la stampa o la riproduzione su supporti da distribuire alle famiglie. Se foto di soggetti non identificabili (di spalle, volti coperti, ecc) possibile diffusione a pubblico più ampio con pubblicazione su sito internet.

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.

ILLIMITATA IN QUANTO LEGATA A FUNZIONE DI ARCHIVIO STORICO (NON ASSOCIABILI ALL'ANAGRAFICA DEL PROPRIETARIO DEL DATO)

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 accesso 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 modalità per l'esercizio 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'esercizio 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'esercizio 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

ID2 "GESTIONE MATERIALE FOTOGRAFICO E AUDIOVISIVO"

CONTROLLI ESISTENTI
<p>Crittografia <i>Descrivi qui i mezzi implementati per assicurare la confidenzialità dei dati</i></p> <p>NO</p>
<p>Anonimizzazione <i>Indicare qui i meccanismi di anonimizzazione implementati</i></p> <p>I DATI SONO ANONIMIZZATI (ELIMINATO OGNI RIFERIMENTO ANAGRAFICO CON L'INTERESSATO NELLA CONSERVAZIONE STORICA DEL DATO)</p>
<p>Partizionamento dei dati <i>Indicare qui se sono pianificati dei meccanismi di disgiunzione tra i dati comuni identificativi e le altre informazioni relative agli interessati</i></p> <p>NO</p>
<p>Controlli logici agli accessi <i>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)</i></p> <p>UTENTI ACCEDONO CON USER NAME E PASSWORD</p>
<p>Tracciabilità (logging) <i>Indicare qui se gli eventi sono registrati e quanto a lungo sono conservati</i></p> <p>ESISTONO LOG DEGLI ACCESSI SU PC ,conservati per tempo illimitato.</p>
<p>Archiviazione <i>Indicare qui se sono implementati meccanismi per monitorare l'integrità dei dati archiviati, quali sono e con quali finalità</i></p> <p>BACKUP PERIODICO AUTOMATICO SU DIPOSITIVO SEPARATO</p>
<p>Sicurezza dei documenti cartacei ARCHIVI CARTACEI ALL'INTERNO DI LOCALI AD ACCESSO RISERVATO, CHIUSI IN ARMADI DOTATI DI CHIAVE. <i>Indica qui se sono implementati meccanismi per il monitoraggio della riservatezza e dell'integrità dei documenti cartacei, quali sono e con quali finalità</i></p> <p>Ai dati contenuti nei documenti cartacei viene garantita sia la riservatezza tramite misure organizzative, le stesse misure garantiscono l'integrità dei dati</p>
<p>Minimizzare la quantità di dati personali <i>Indicare qui i mezzi implementati per ridurre la gravità del rischio limitando la quantità di dati personali impiegati</i></p> <p>I DATI PERSONALI RACCOLTI SONO QUELLI STRETTAMENTE NECESSARI PER ASSolvere AL TRATTAMENTO COME SPECIFICATO ANCHE NEL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO.</p>
<p>Vulnerabilità <i>Descrivi qui come si aggiorna il software (sistemi operativi, applicazioni, etc.) e come sono effettuati i controlli di sicurezza e patch</i></p> <p>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</p>
<p>Contromisure contro il malware <i>Descrivi qui i controlli implementati contro il codice malevolo quando accedi a reti con un livello di sicurezza inferiore</i></p> <p>Firewall SW, antivirus presente su tutte le macchine.</p>
<p>Gestione postazioni <i>Descrivi qui i controlli implementati sulle postazioni di lavoro (p.e. controllo dati di navigazione, controllo email, altro)</i></p> <p>accessi logici configurati su tutte le postazioni, dati di navigazione gestite da restrizioni del firewall.</p>
<p>Sicurezza siti Web <i>Indicare qui i controlli implementati per proteggere i siti Web</i></p> <p>sito web solo di presentazione, l'utente risulta adeguatamente informato sui dati raccolti, il sito è protetto da certificato SSL.</p>
<p>Backup <i>Indicare qui come sono gestiti i backup. Chiarisci se sono conservati in un luogo sicuro</i></p> <p>BACKUP PERIODICO AUTOMATICO SU DIPOSITIVO SEPARATO</p>
<p>Manutenzione Descrivi qui come è gestita la manutenzione fisica delle attrezzature</p> <p>ASSISTENZA TECNICA CON DITTA ESTERNA RESPONSABILE DEL TRATTAMENTO.</p>

<p>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.)</p>
<p>VEDERE NOMINE RESPONSABILI ESTERNI E AUTORIZZAZIONE PER I DESIGNATI AL TRATTAMENTO DATI - eventualmente fotografo esterno</p>
<p>Sicurezza della rete <i>Indicare qui i controlli di sicurezza della rete sulla quale il trattamento è effettuato</i></p>
<p>ANTIVIRUS - FIREWALL SW</p> <p>Controllo degli accessi fisici Indicare qui come il controllo dell'accesso fisico è effettuato nei locali che ospitano il trattamento</p>
<p>ACCESSO ALLA STRUTTURA CONTROLLATO - ACCESSO AI LOCALI IN CUI SONO TRATTATI I DATI AD ACCESSO RISERVATO CON CHIAVE</p> <p>Monitoraggio dell'attività della rete <i>Indicare qui i mezzi e i controlli implementati per rilevare incidenti che riguardano dati personali</i></p>
<p>PROCEDURA DATA BREACH - FORMAZIONE DEGLI UTENTI - SISTEMI AUTOMATICI QUALI FIREWALL E ANTIVIRUS - MONITORAGGIO PERIODICO DELL'AMMINISTRATORE DI SISTEMA.</p> <p>Sicurezza dell'hardware <i>Indicare qui i controlli operanti sulla sicurezza fisica di server e postazioni PC</i></p>
<p>ASSISTENZA TECNICA CON DITTA SPECIALIZZATA</p> <p>Evitare le fonti di rischio <i>Indicare qui se l'area delle infrastrutture può essere soggetta a disastri ambientali</i></p>
<p>CENTRO URBANO - ZONA SISMICA 2 B - Zona con pericolosità sismica media dove possono verificarsi forti terremoti.</p> <p>Protezione contro fonti di rischio non umane <i>Indicare qui le protezioni contro le fonti di rischio non umane</i></p>
<p>IMPIANTO RILEVAZIONE E SPEGNIMENTO INCENDIO</p> <p>Organizzazione <i>Indicare se i ruoli e le responsabilità per la protezione dei dati sono definite</i></p>
<p>ORGANIGRAMMA RIPORTATO NEL DOSSIER PRIVACY SEZ.5</p> <p>Politiche Descrivere qui la base documentale per impostare gli obiettivi e le regole per la protezione dei dati</p>
<p>PROCEDURE DI GESTIONE RIPORTATE NEL DOCUMENTO "DOSSIER PRIVACY" SEZ.6</p> <p>Gestione dei rischi sulla privacy <i>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</i></p>
<p>REGISTRO ATTIVITA' DI TRATTAMENTO E RELATIVA VALUTAZIONE DEI RISCHI IN REVISIONE 2 Al 26.11.21.</p> <p>Integrare la protezione della privacy nei progetti <i>Descrivere qui come la protezione della privacy è integrata nei progetti</i></p>
<p>--</p>
<p>Gestire le violazioni dei dati personali <i>Indicare qui se gli incidenti di IT sono soggetti a procedure di gestione documentate e testate</i></p>
<p>PROCEDURA DATA BREACH RIPORTATA ALL'INTERNO DEL DOCUMENTO DOSSIER PRIVACY</p> <p>Gestione del personale <i>Indicare qui quali iniziative per aumentare la consapevolezza sono effettuate nei riguardi degli impiegati</i></p>
<p>ATTIVITA' FORMATIVA EROGATA AGLI INCARICATI SIA INTERNAMENTE CHE DA PARTE DEL DPO.</p> <p>Relazioni con terze parti <i>Indicare qui, per ciascun responsabile del trattamento, denominazione/identificazione, finalità del trattamento, ambito applicativo, riferimento contratto, compliance art. 28 Gdpr</i></p>
<p>Sono state rivisitate le nomine in rif. GDPR</p> <p>Supervisione <i>Indicare qui se l'efficacia e l'adeguatezza dei controlli anche per i diritti di degli interessati (richiesta di accesso, cancellazione, limitazione, opposizione al trattamento) sono monitorate come viene monitorata e testata l'adeguatezza e l'efficacia delle misure di sicurezza/controlli</i></p>
<p>AUDIT INTERNO/DPO</p>

ID2 "GESTIONE MATERIALE FOTOGRAFICO E AUDIOVISIVO"

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'INTERESSATO POTREBBE RITENERE VIOLATA LA PROPRIA PRIVACY CON IMPATTO LIMITATO

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 - Massimo

TRASCURABILE

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

L'INTERESSATO POTREBBE RITENERE VIOLATA LA POPRIA PRIVACY CON IMPATTO LIMITATO

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 - Mssimo

LIMITATO

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

(indefinito) - Trascurabile - Limitato - Importante - Mssimo

TRASCURABILE

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

IMPATTO TRASCURABILE SUI DIRITTI E LIBERTA' DELL'INTERESSATO

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

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

(indefinito) - Trascurabile - Limitato - Importante - Massimo

TRASCURABILE

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

(indefinito) - Trascurabile - Limitato - Importante - Massimo

TRASCURABILE