



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

**TRATTAMENTO  
ID6  
"PROGETTI PEI"**

**"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 18 Giugno 2019

Firma Legale Rappresentante \_\_\_\_\_

## ID6 "PROGETTAZIONE PEI"

TRATTAMENTO
Quale trattamento dei dati personali viene effettuato (per ogni trattamento/ripetere il questionario)? <i>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.</i>
<b>PROGETTI PEI</b>
Quali sono le responsabilità legate al trattamento? <i>Descrivi le responsabilità degli stakeholder: il titolare del trattamento, gli eventuali responsabili esterni o co-titolare (che condividono le prerogative in ordine alle finalità)</i>
<b>TITOLARE (EROGAZIONE DEL SERVIZIO), DOCENTI, ALUNNI</b>
Ci sono standard applicabili al trattamento? <i>Elenca gli standard rilevanti applicabili al trattamento, specialmente i codici di condotta e le certificazioni di protezione dati.</i>
<b>NON CI SONO</b>
Quali sono i dati trattati? <i>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.</i>
<b>DATI PERSONALI ANCHE PARTICOLARI.</b>
Com'è il ciclo di vita del trattamento dei dati? <i>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.</i>
<b>GENITORE RICHIEDE ATTIVAZIONE PROGETTO PEI, I DOCENTI COINVOLTI PROMUOVONO UN PIANO EDUCATIVO INDIVIDUALE, LA DURATA DEL TRATTAMENTO E' LEGATA ALLA DURATA DEL PIANO, DELLA FREQUENZA DELL'ALUNNO E DELLA DURATA AMMINISTRATIVA DELLA DOCUMENTAZIONE SCOLASTICA.</b>
Quali sono le risorse di supporto ai dati? <i>Elenca le risorse che ospitano i dati (sistemi operativi, applicazioni aziendali, database management systems, pacchetti office, protocolli, configurazioni etc.)</i>
<b>PC DIREZIONE E SEGRETERIA+ ARCHIVI CARTACEI PRESSO SEGRETERIA</b>
Gli scopi del trattamento sono specifici, espliciti e legittimi? <i>Spiegare perché le finalità del trattamento sono specifiche, esplicite e legittime.</i>
<b>VALUTATE LE BASI GIURIDICHE DI CIASCUN TRATTAMENTO.</b>
Quali sono le basi legali che rendono il trattamento legittimo? <i>Presentare le basi del trattamento (ad esempio consenso, esecuzione di un contratto, obbligo legale, interessi vitali etc.)</i>
<b>TRA LE BASI DEL TRATTAMENTO PER IL TRATTAMENTO C'E' IL CONSENSO CHE VIENE ACQUISITO DIRETTAMENTE PRESSO INTERESSATI</b>

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 EROGARE IL RELATIVO SERVIZIO.**

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 di 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 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.*

**si 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**

## ID6 "PROGETTAZIONE PEI"

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

<p>Nomine e contratti relativi al trattamento</p> <p>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><b>AUTORIZZAZIONE PER I DESIGNATI AL TRATTAMENTO DATI - No esterni</b></p> <p>Sicurezza della rete</p> <p><i>Indicare qui i controlli di sicurezza della rete sulla quale il trattamento è effettuato</i></p>
<p><b>ANTIVIRUS - FIREWALL SW</b></p> <p>Controllo degli accessi fisici</p> <p>Indicare qui come il controllo dell'accesso fisico è effettuato nei locali che ospitano il trattamento</p>
<p><b>ACCESSO ALLA STRUTTURA CONTROLLATO - ACCESSO AI LOCALI IN CUI SONO TRATTATI I DATI AD ACCESSO RISERVATO CON CHIAVE</b></p> <p>Monitoraggio dell'attività della rete</p> <p><i>Indicare qui i mezzi e i controlli implementati per rilevare incidenti che riguardano dati personali</i></p>
<p><b>PROCEDURA DATA BREACH - FORMAZIONE DEGLI UTENTI - SISTEMI AUTOMATICI QUALI FIREWALL E ANTIVIRUS - MONITORAGGIO PERIODICO DELL'AMMINISTRATORE DI SISTEMA.</b></p> <p>Sicurezza dell'hardware</p> <p><i>Indicare qui i controlli operanti sulla sicurezza fisica di server e postazioni PC</i></p>
<p><b>ASSISTENZA TECNICA CON DITTA SPECIALIZZATA</b></p> <p>Evitare le fonti di rischio</p> <p><i>Indicare qui se l'area delle infrastrutture può essere soggetta a disastri ambientali</i></p>
<p><b>CENTRO URBANO - ZONA SISMICA 2 B - Zona con pericolosità sismica media dove possono verificarsi forti terremoti.</b></p> <p>Protezione contro fonti di rischio non umane</p> <p><i>Indicare qui le protezioni contro le fonti a rischio non umane</i></p>
<p><b>IMPIANTO RILEVAZIONE E SPEGNIMENTO INCENDIO</b></p> <p>Organizzazione</p> <p><i>Indicare se i ruoli e le responsabilità per la protezione dei dati sono definite</i></p>
<p><b>ORGANIGRAMMA RIPORTATO NEL DOSSIER PRIVACY SEZ.5</b></p> <p>Politiche</p> <p>Descrivere qui la base documentale per impostare gli obiettivi e le regole per la protezione dei dati</p>
<p><b>PROCEDURE DI GESTIONE RIPORTATE NEL DOCUMENTO "DOSSIER PRIVACY" SEZ.6</b></p> <p>Gestione dei rischi sulla privacy</p> <p><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><b>REGISTRO ATTIVITA' DI TRATTAMENTO E RELATIVA VALUTAZIONE DEI RISCHI IN REVISIONE 2 Al 26.11.21.</b></p> <p>Integrare la protezione della privacy nei progetti</p> <p><i>Descrivere qui come la protezione della privacy è integrata nei progetti</i></p>
<p>--</p> <p>Gestire le violazioni dei dati personali</p> <p><i>Indicare qui se gli incidenti di IT sono soggetti a procedure di gestione documentate e testate</i></p>
<p><b>PROCEDURA DATA BREACH RIPORTATA ALL'INTERNO DEL DOCUMENTO DOSSIER PRIVACY</b></p> <p>Gestione del personale</p> <p><i>Indicare qui quali iniziative per aumentare la consapevolezza sono effettuate nei riguardi degli impiegati</i></p>
<p><b>ATTIVITA' FORMATIVA EROGATA AGLI INCARICATI SIA INTERNAMENTE CHE DA PARTE DEL DPO.</b></p> <p>Relazioni con terze parti</p> <p><i>Indicare qui, per ciascun responsabile del trattamento, denominazione/identificazione, finalità del trattamento, ambito applicativo, riferimento contratto, compliance art. 28 Gdpr</i></p>
<p><b>Sono state rivisitate le nomine in rif. GDPR</b></p> <p>Supervisione</p> <p><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><b>AUDIT INTERNO/DPO</b></p>

## ID6 "PROGETTAZIONE PEI"

### 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 CONSEGUENZE NON TRASCURABILI.**

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.

**IMPORTANTE**

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

**(indefinito) - Trascurabile - Limitato - Importante - Massimo**

**TRASCURABILE**

## ID6 "PROGETTAZIONE PEI"

### MODIFICHE INDESIDERATE AI DATI

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

**L'INTERESSATO POTREBBE RITENERE VIOLATA LA POPRIA PRIVACY CN CONSEGUENZE NON TRASCURABILI.**

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**

**IMPORTANTE**

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

**(indefinito) - Trascurabile - Limitato - Importante - Mssimo**

**TRASCURABILE**

## ID6 "PROGETTAZIONE PEI"

### PERDITA DISPONIBILITA' DEI DATI

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

**LA PERDITA DEL DATO POTREBBE AVERE IMPATTI NON TRASCURABILI SULLA CARRIERA SCOLASTICA 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  
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**