**Valutazione d'Impatto sulla Protezione dei Dati (DPIA)**
**per il Trattamento dei Dati Personali tramite il Registro Elettronico**

---

**1. Premessa**

Il presente documento costituisce la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) per il trattamento dei dati personali realizzato tramite il Registro Elettronico dell'Istituto Liceo Statale "Salvatore Pizzi".
La DPIA è redatta in conformità al Regolamento Europeo (GDPR, artt. 35 e ss.) e alle indicazioni ministeriali (Registro Ufficiale n. 0002773.04-04-2025) ed ha l'obiettivo di:

- Analizzare i rischi connessi al trattamento dei dati personali.
- Definire le misure tecniche e organizzative necessarie per garantire la sicurezza, la riservatezza e la conformità del sistema.

**2. Descrizione del Trattamento**

**2.1 Finalità**

- Gestione Didattica: Registrazione e gestione di assenze, voti, annotazioni e comunicazioni istituzionali.
- Adempimento Normativo: Rispetto degli obblighi derivanti dall'art. 7, comma 31, del D.L. n. 95/2012 e dalle direttive ministeriali.

**2.2 Categorie di Dati Trattati**

- Studenti e Genitori: Dati anagrafici (nome, cognome, data di nascita), dati scolastici (voti, assenze, annotazioni) e dati di contatto.
- Personale Scolastico: Dati identificativi e relativi al percorso professionale.

**2.3 Modalità di Trattamento**

- Il trattamento è prevalentemente informatizzato tramite il Registro Elettronico, accessibile esclusivamente tramite sistemi di autenticazione (SPID, CIE, eIDAS, ETC) e protetto da misure di sicurezza avanzate.
- Il sistema adotta misure tecniche (crittografia dei dati in transito e a riposo, backup regolari, firewall) e organizzative (accessi riservati, formazione del personale).

**2.4 Ambito di Applicazione**

- Il trattamento interessa l'intera struttura dell'Istituto Liceo Statale "Salvatore Pizzi" di Capua (CE) e si integra con altri sistemi informativi, quali il Sistema Informativo dell'Istruzione (SIDI) e altre piattaforme correlate.

**3. Analisi dei Rischi**

**3.1 Rischio di Accesso Non Autorizzato**

- Probabilità: Bassa
- Impatto: Alto
- Descrizione: Possibilità che soggetti non autorizzati accedano ai dati attraverso vulnerabilità del sistema o credenziali compromesse.

**3.2 Rischio di Perdita o Divulgazione Accidentale dei Dati**

- Probabilità: Bassa
- Impatto: Alto
- Descrizione: Rischio derivante da errori umani, malfunzionamenti tecnici o incidenti che potrebbero causare la perdita o la divulgazione accidentale dei dati personali.

**3.3 Rischio di Attacchi Informatici (Malware, Phishing, Hacking)**

- Probabilità: Media
- Impatto: Alto
- Descrizione: Possibilità di attacchi esterni che compromettano l'integrità, la riservatezza e la disponibilità dei dati gestiti.

**4. Misure di Mitigazione e Sicurezza**

**4.1 Controllo degli Accessi e Autenticazione**

- Implementazione obbligatoria di identità digitali (SPID, CIE, eIDAS,ETC) e autenticazione a due fattori per garantire l'accesso esclusivo agli utenti autorizzati.

**4.2 Protezione Tecnica dei Dati**

- Crittografia dei dati in transito e a riposo.
- Backup periodici e procedure di disaster recovery per garantire il ripristino dei dati in caso di incidenti.
- Utilizzo di firewall, sistemi di monitoraggio attivo e software antivirus aggiornati.

**4.3 Formazione e Controlli Interni**

- Programma di formazione periodica per il personale sull'uso sicuro del sistema e le migliori pratiche in materia di sicurezza informatica.
- Audit interni regolari per verificare l'efficacia delle misure di sicurezza e l'aderenza alle procedure.

**4.4 Procedure di Gestione delle Violazioni**

- Definizione di un protocollo interno per la gestione tempestiva delle violazioni (data breach), con comunicazione immediata al Titolare del Trattamento e al DPO, in conformità agli articoli 33 e 34 del GDPR.

**5. Conclusioni e Piano d'Azione**

- Sintesi dei Rischi: I principali rischi (accesso non autorizzato, perdita/divulgazione accidentale, attacchi informatici) sono stati identificati e valutati, con un impatto potenzialmente elevato.
- Misure Adottate: Le misure di sicurezza implementate sono ritenute efficaci per mitigare i rischi, pur richiedendo un monitoraggio costante.
- Esito della valutazione: Il rischio residuo è stato valutato come basso/medio, in quanto mitigato da misure tecniche e organizzative efficaci. Il trattamento può quindi essere effettuato nel rispetto del GDPR.

Il Titolare del Trattamento, in collaborazione con il DPO, si impegna a garantire il costante aggiornamento delle procedure e a intervenire tempestivamente in caso di emergenze o violazioni.

**IL DIRIGENTE SCOLASTICO**
**Titolare del trattamento dati**
**Prof.ssa Carmela Mascolo**
**Documento firmato digitalmente ai sensi del c.d. Codice dell'Amministrazione Digitale e normativa connessa**

Firmato dal Dirigente Scolastico
Prof.ssa Carmela Mascolo
21/10/2025 10:06:54