

PARERE DPO

Il presente parere si rilascia in seguito a:

- somministrazione del questionario ai fini dell'emissione del parere per la valutazione dei rischi;
- al sopralluogo tecnico fisico presso l'Istituto ed al controllo tecnico sul sito dell'Istituto ed agli adeguamenti tecnici sopravvenuti in seguito del 02.05.2024;
- Formazione su tematiche specifiche della privacy tenutasi in data 13.12.2023 alla quale ha partecipato tutto il personale;
- valutazione DPIA che si rilascia per gli usi consentiti dalla legge.

Preliminarmente si deve rilevare come l'Istituto Comprensivo Silvio Canevari di Viterbo, in qualità di pubblica amministrazione, effettua in via generale il trattamento del dato per dare esecuzione ad un compito di interesse pubblico o per l'esercizio di pubblici poteri, come meglio specificato nel capitolo dedicato all'analisi del contesto – Panoramica del trattamento – (pagina 2).

Viene, quindi, dato seguito a quanto previsto dal considerando 50 del GDPR, secondo cui gli Stati membri possono stabilire per il trattamento dei dati finalità ulteriori e considerare tale trattamento compatibile e lecito.

Le finalità statistiche, l'archiviazione nel pubblico interesse, nonché gestione amministrativa dei dipendenti determinano un trattamento ulteriore legittimo da parte dell'Istituto che può prevedere per alcuni dati personali tempi di conservazione superiori rispetto ai tempi di conservazione previsti in via generale.

In particolare, la normativa di riferimento, oltre che al GDPR 267/2016, D.Lgs 101/2018, si rinviene in: R.D. n. 653/1925, D.Lgs. n. 297/1994, D.P.R. n. 275/1999; Decreto Interministeriale 1 febbraio 2001, n. 44 e le norme in materia di contabilità generale dello Stato; Legge n. 104/1992, Legge n. 53/2003, D.Lgs. n. 165/2001, Dlgs 196/2003 e Regolamento Europeo 2016/679, D.M 305/2006; Dlgs 76/05; Dlgs 77/05; Dlgs 226/05; Dlgs 82/2005, D.Lgs. n. 151/2001, i Contratti Collettivi di Lavoro Nazionali ed Integrativi stipulati ai sensi delle norme vigenti; D.P.C.M. 23 febbraio 2006 n. 185 fatto salvo quanto disposto dal Dlgs 66/2017; D.P.R. 20 marzo 2009, n.89; Legge 170 dell'8.10.2010; D.M. n. 5669 12 luglio 2011; DPR 28 marzo 2013 n.80, Dlgs 33/2013, DL 12 settembre 2013, n.104, convertito, con modificazioni, dalla Legge 8 novembre 2013, n. 128, Legge 13 luglio 2015 n. 107, Dlgs 50/2016 e relativi decreti applicativi e tutta la normativa richiamata e collegata alle citate disposizioni e s.m. e i.

In via generale si rileva come dall'analisi del contesto, della necessità e proporzionalità del trattamento rispetto ai principi fondamentali e della valutazione sulla gestione dei rischi, l'Istituto Comprensivo Silvio Canevari di Viterbo risulta aver ottemperato all'adeguamento alla normativa prevista nel GDPR 679/2016, in linea anche con la normativa di settore relativa agli adeguamenti minimi previsti dall'AgID per quanto concerne la protezione informatica dei sistemi gestionali, nonché sito istituzionale della scuola che si affida ad Argoweb.

Inoltre, si rileva come a distanza di anni l'Istituto abbia costantemente apportato miglioramenti sull'apparato informatico al fine di effettuare un corretto trattamento del dato, ma – allo stesso tempo – anche una maggiore sicurezza informatica che diminuisca il pericolo di accesso illegittimo ai dati nonché ha effettuato scelte sui fornitori in linea con la normativa AgID preferendo soggetti accreditati presso ACN.

Per quanto concerne il trattamento del dato effettuato per la formazione a distanza (DAD) si fa presente come tale ulteriore trattamento sia tutt'oggi possibile solo nei casi di comprovata necessità medica degli studenti al fine di adempiere il diritto costituzionalmente garantito alla studio.

Si fa presente, infine, come appare opportuno provvedere ad una nuova valutazione DPIA a distanza di nove mesi dall'emissione della presente, al fine di valutare eventuali nuovi trattamenti da effettuarsi separatamente al presente parere.

Nello specifico del parere richiesto, le risultanze ottenute sono suddivise nelle tre macro aree di cui è composta la valutazione sulla gestione del rischio e consistenti in: 1) accesso illegittimo ai dati, 2) modifiche indesiderate ai dati e 3) perdita dei dati.

La tabella di seguito riportata viene, quindi, intesa sia in termini di:

- gravità del rischio consistente nella gravità dell'accesso abusivo, modifiche indesiderate ai dati e perdita dei dati sui diritti degli interessati qualora l'evento data breach si realizzasse;
- probabilità del rischio che l'evento data breach possa avverarsi in relazione alle misure poste in essere o ai miglioramenti che si intendono porre in essere da parte dell'Istituto Comprensivo in termini di accesso illegittimo ai dati, modifiche indesiderate ai dati e perdita dei dati.

Di seguito si riporta tabella sinottica divisa per tre aree e gestione del rischio (gravità e probabilità).

	Accesso illegittimo ai dati	Modifiche indesiderate ai dati	Perdita dei dati
Gravità del rischio	Massima	Limitata	Trascurabile
Probabilità del rischio	Trascurabile	Trascurabile	Trascurabile

TABELLA SINOTTICA

Gravità del rischio	4	Massima	Individui possono avere conseguenze significative, o addirittura irreversibili
	3	Importante	Gli individui possono avere conseguenze significative, che dovrebbero essere in grado di superare anche se con difficoltà
	2	Limitata	Gli interessati possono incontrare significativi disagi, che saranno in grado di superare nonostante alcune difficoltà
	1	Trascurabile	Gli interessati non incontrano inconvenienti significativi

TABELLA SINOTTICA

Probabilità del rischio	4	Massima	Sembra estremamente prevedibile che le fonti di rischio identificate si materializzino in una minaccia sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto
	3	Importante	Sembra possibile che le fonti di rischio identificate si materializzino in una minaccia sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto
	2	Limitata	Sembra difficile che le fonti di rischio identificate si materializzino in una minaccia sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto
	1	Trascurabile	Non sembra possibile che le fonti di rischio identificate si materializzino in una minaccia sfruttando possibili vulnerabilità esistenti nei dispositivi di supporto

Di seguito vengono indicati dei correttivi che potrebbero essere ulteriormente apportati per migliorare la gestione dei rischi e, pertanto, viene riportata una tabella sinottica nella quale sono

indicati gli ambiti, la pagina di riferimento, la situazione al momento del rilievo e le implementazioni ulteriori per migliorare la gestione del rischio.

Ambito	Pagina	Situazione al momento del rilievo	Implementazioni
Ciclo di vita del trattamento del dato	3	Conservazione di alcuni dati che non vengono cancellati	In linea con la normativa pubblicitaria, si consiglia di prevedere, almeno per alcuni dati, la cancellazione decorsi i termini legali come previsto dall'allegato A Direzione Generale per gli archivi. Valevole tanto per la conservazione dei dati relativi agli studenti ed il personale quanto per il dovere di trasparenza mediante pubblicazione sul sito dell'Istituto Scolastico nella sezione "Amministrazione Trasparente".
Controllo accessi fisici	9	L'accesso agli archivi fisici, dopo un controllo in entrata, non viene fatto un ulteriore controllo	Per garantire gli accessi fisici più sicuri, si consiglia di installare sulle porte la scritta "Vietato l'accesso al personale non autorizzato" ed in un secondo momento sostituire le porte con accesso mediante badge.
Perdita di dati	11	Manutenzione backup	Aggiornare quotidianamente il backup per evitare che i dati conservati nel NAS non vengano rimossi.
Relazione tecnica informatica	-	Sistema operativo client di segreteria.	Tutte le postazioni hanno installato Windows 10. Sarebbe opportuno installare una versione Professional su PDL Dirigente.

Roma, lì 28.05.2024

Il DPO

Dott.ssa Francesca Costabile
