

PARERE DPO

In seguito alla somministrazione del questionario ai fini dell'emissione del parere per la valutazione dei rischi, nonché al sopralluogo tecnico fisico presso l'Istituto, viene redatto il seguente parere alla valutazione DPIA che si rilascia per gli usi consentiti dalla legge.

Preliminarmente si deve rilevare come l'Istituto cine-tv R. Rossellini di Roma, 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. Nel particolare del trattamento del dato tramite sistema di video sorveglianza, le finalità sottese riguardano la tutela del patrimonio aziendale, nonché la tutela e la prevenzione di reati all'interno dello stabile scolastico.

Viene, quindi, dato seguito a quanto previsto dall'art. 35 del GDPR, secondo il quale viene svolta una valutazione preventiva (Data Protection Impact Assessment – DPIA) sui trattamenti eseguiti e l'impatto di essi sulla libertà ed i diritti delle persone fisiche, specificamente nell'ambito dell'utilizzazione dei sistemi di videosorveglianza. Il presente documento rappresenta gli esiti della DPIA svolta nell'ambito dei sistemi di videosorveglianza utilizzati dal Istituto Cine-TV R. Rossellini finalizzati al raggiungimento di obiettivi relativi a prevenzione di reati ed illeciti nonché di tutela del patrimonio aziendale.

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 Scolastico Cine-Tv Roberto Rossellini risulta aver ottemperato all'adeguamento alla normativa prevista nel GDPR 679/2016, in linea anche con la normativa di settore relativa alla tutela della sicurezza sul luogo di lavoro per i dipendenti avendo richiesto ed ottenuto già a maggio del 2014 provvedimento di autorizzazione all'installazione di sistema di video sorveglianza dal Ministero del Lavoro e delle Politiche Sociali (che per opportunità sono allegati al seguente parere all. 1 e 2).

La conservazione del dato, in linea con la normativa di settore non può superare le 24 ore, decorse le quali, i dati vengono sovrascritti e cancellati in automatico. Solo in ragione di: a) eventuali ulteriori periodi legati a festività o chiusura dello studio, b) di specifiche richieste investigative della competente autorità giudiziaria il trattamento del dato può essere prolungato.

Nello specifico del parere richiesto, le risultanze ottenute in merito alla valutazione sulla gestione del rischio sono suddivise per le macro aree costituenti la gestione del rischio (relativamente all'accesso illegittimo ai dati, modifiche indesiderate ai dati e perdita dei dati) che devono essere intese sia in termini di gravità del rischio che 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.

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	Importante	Trascurabile	Trascurabile
Probabilità del rischio	Limitata	Limitata	Trascurabile

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

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

Roma, lì 20.10.2021

Il DPO

Dott.ssa Francesca Costabile
