Spett.le

c.a.

via mail

oggetto: verifica dei sistemi di sicurezza informatica ai sensi dell’art. 32, art. 35 comma 1

Gentilissimi,

dopo il primo anno di avvio del sistema di protezione del dato personale che rientra nella definizione del regolamento europeo 679/2016, viene la necessità di stabilire un punto fermo nelle attività svolte in modo da poter certificare la compliance al regolamento di ciascuna scuola.

In questo senso occorre iniziare un percorso di verifica dello status delle attività ed un eventuale pronto intervento in caso di ritardi.

A tal fine ricordiamo che le seguenti attività dovrebbero esser state svolte:

1. nomina del DPO
2. informativa generale sull’utilizzo del dato personale legato alle attività scolastiche (ns. modello 5) ai sensi dell’art.12, 13, 14
3. nomine dei responsabili del trattamento interni ed esterni (nostri modelli serie 7) ai sensi dell’art. 28
4. conseguente definizione dell’organigramma
5. delibera di consiglio di istituto per il regolamento privacy (nostro modello 34) ai sensi degli art. 5, 12, 24
6. compilazione del registro dei trattamenti (nostro modello 9.4) ai sensi dell’art. 30
7. verifica dello stato delle misure minime di sicurezza (nostro fac simile modello di documento per le misure minime) ai sensi dell’art. 32 e 35
8. predisposizione pagina privacy nella home del sito .edu.it (nostro modello 30)
9. utilizzo dei modelli di informativa particolare (ad esempio il nostro modello 17 per l’informativa in calce alle mail)
10. formazione base agli addetti ed ai docenti

Con queste attività svolte sono state messe le basi per la gestione del regolamento.

Nel caso in cui questi punti non siano stati correttamente sviluppati ricordiamo che è disponibile per supportare le scuole alla loro realizzazione il numero di segreteria 351.8886018.

Altro elemento importante è la DPIA, ovvero la valutazione di impatto sulla situazione della scuola.

La valutazione di impatto del trattamento (D.P.I.A., cioè Data Protection Impact Assessment) è un onere posto direttamente a carico del titolare del trattamento (art. 35 GDPR), col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali.

Con questo strumento il titolare del trattamento verifica lo stato del pericolo dei trattamenti e con cui effettua l'analisi dei rischi derivanti dai trattamenti posti in essere.

Il titolare, quindi, deve sviluppare una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati.

Il responsabile del trattamento deve assistere il titolare fornendogli ogni informazione necessaria.

Fuor di dubbio che prima di ragionare sulla DPIA è necessario aver sviluppato la fase precedente.

Preme sottolineare che il nuovo regolamento generale ha un approccio basato sulla valutazione del rischio (risk based), piuttosto che sulla mera protezione dell'utente.

La DPIA non è obbligatoria ma richiesta nei seguenti casi:

1) se il trattamento può comportare discriminazioni, furto o usurpazione d’identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione , o qualsiasi altro danno economico o sociale significativo;

2) se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l’esercizio del controllo sui dati personali che li riguardano;

3) se sono trattati dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

4) in caso di valutazione di aspetti personali, in particolare mediante l’analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

5) se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;

6) se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

In merito alle istituzioni scolastiche rientrano in pieno i commi 3 e 5.

Per poter quindi verificare la corretta impostazione della DPIA sono necessari:

1. dichiarazioni di tutti i gestori di dati della scuola di conformità alle leggi ed al gdpr
2. relazione dell’amministratore di sistema sulla perfetta tenuta dell’ambiente informatico scolastico

questi due documenti devono essere inviati alla seguente mail direzione@cceditore.it al fine di permettere al DPO di valutare la necessaria profondità della DPIA.

Qualora il DPO dovesse valutare di concerto con il titolare la necessità di condurre approfondita analisi del rischio sarà necessario ulteriore incontro presso la scuola.

A breve sarà anche messo a disposizione un questionario on line da compilare da parte del referente privacy della scuola per verificare lo stato dell’arte degli adempimenti.

Il referente privacy della scuola sarà coinvolto ogni mese a partire dal gennaio 2020 per una verifica puntuale dello stato dell’arte (il coinvolgimento sarà tramite chiamata o videochiamata).

A far tempo dal giorno 11 la password per l’accesso al sito controllerprivacy.it sarà modificata da Dpo2018. a **Gdpr2019Y6792016**

Con l’occasione segnaliamo che sono stati messi a disposizione di tutti gli istituti scolastici i quaderni della privacy che illustrano più approfonditamente gli aspetti salienti del nuovo regolamento.