ARTICOLO DI ELEARNINGNEWS

Year 2 - number 26 Wednesday 23 maggio 2018

eLearning e GDPR

Quali sono le implicazioni del GDPR sull'eLearning?

Il "Regolamento generale sulla protezione dei dati" dell'Unione Europea (GDPR) sarà pienamente operativo dal 25 maggio 2018 in tutti gli stati dell'Unione Europea. Il nuovo regolamento punta ad aumentare la trasparenza e la responsabilità delle società che trattano dati personali, a promuovere una "cultura della privacy" su Internet e a proteggere gli utenti.

Quali sono le principali linee guida del GDPR e quali sono le sue implicazioni generali e quelle specifiche legate all'eLearning?

A chi è rivolto?

Qualsiasi società (con sede nell'UE o extra UE) che offra servizi ai cittadini dell'UE o che tenga traccia del comportamento dei cittadini dell'UE (attraverso profili online, cookie e altri mezzi simili) è tenuta a rispettare il GDPR.

Perché?

Un'azienda non conforme può essere soggetta a multe fino al 4% del suo fatturato annuale.

Terminologia GDPR

- **Elaborazione**: tutto ciò che un'azienda può fare con i dati personali (raccolta, organizzazione, conservazione, adattamento, trasmissione, condivisione...).
- **Titolare del trattamento**: società che raccolgono, archiviano o gestiscono dati di persone per uno scopo particolare (e determinano il modo in cui avviene la raccolta).
- **Responsabile dei dati**: una società che memorizza o elabora i dati dell'utente per conto di altre società (responsabili del trattamento dei dati). I Data Controller sono società che hanno lo scopo principale di raccogliere dati, e i Data Processor sono aziende che offrono il trattamento dei dati, la memorizzazione, ecc. Il Responsabile del trattamento dei dati non può utilizzare i dati per scopi diversi da quelli per cui il Titolare del trattamento li ha raccolti.
- **Soggetto dei dati**: una persona fisica - come uno studente o un docente.
- **Dati personali**: qualsiasi informazione relativa a un soggetto come nome, email ...
- **Consenso**: una chiara indicazione da parte di un interessato che è d'accordo con la raccolta e il trattamento dei propri dati personali.

Cosa fare per essere conformi al GDPR?

Se la tua azienda utilizza un LMS per la formazione, la conformità al GDPR è una responsabilità condivisa tra la tua azienda (il "controllore") e il tuo fornitore LMS (il "processore").
In qualità di controller, devi definire gli obiettivi dell'elaborazione, controllare i dati dei discenti, degli amministratori e dei docenti che verranno elaborati.

Innanzitutto, non dovresti raccogliere più dati di quelli necessari per i tuoi scopi o utilizzare i dati per scopi diversi da quelli per cui sono stati raccolti.

Tieni traccia dei dati (fonti, sistemi in cui sono memorizzati, flussi di dati e diritti di accesso) assicurandoti che la privacy sia sempre rispettata.
Definire adeguate politiche di protezione e conservazione dei dati e predisporre controlli può essere molto utile allo scopo.
Inoltre, assicurati di mantenere database aggiornati e predisponi mezzi per la correzione.

Limita gli accessi ai dati personali raccolti dalla tua azienda ai dipendenti che hanno effettiva necessità di averli a disposizione per svolgere la propria attività.

Nel caso più specifico dell'eLearning, è necessario esaminare attentamente il programma di conformità GDPR, l'Informativa sulla privacy e le Condizioni d'uso del LMS utilizzato e firmare un DPA (**Data Processing Addendum**) conforme al GDPR con il provider LMS.
Il DPA deve specificare in modo chiaro le istruzioni che il servizio LMS dovrebbe seguire e obbliga entrambe le parti a rispettare gli obblighi legali relativi al GDPR.

Cosa deve fare il fornitore di servizi LMS per essere conforme a GDPR?

Il fornitore di servizi LMS deve dotare i clienti dei mezzi per soddisfare i diritti di riservatezza delle persone interessate tramite le funzionalità LMS.
I diritti a cui ci si riferisce sono:

- il diritto di essere informato (di avere i propri dati),
- il diritto di accesso,
- il diritto alla rettifica dei dati,
- il diritto all'oblio,
- il diritto a presentare un reclamo,
- i diritti a limitare o interrompere l'elaborazione dati,
- il diritto a ottenere i dati in un formato strutturato (es. download CSV),
- il diritto a rifiutare l'uso dei dati a scopo di marketing.

Per quanto riguarda quest'ultimo punto, è importante individuare lo staff referente della protezione dei dati (o un responsabile della protezione dei dati) che può essere facilmente raggiunto dai clienti, ad es. attraverso un indirizzo email pubblicato sul sito Web.
Inoltre, il fornitore deve dare sufficienti informazioni riguardo la sua Politica sulla privacy, Termini di servizio e DPA. Questo significa documentare l'ambito, la natura, i tipi di dati, la politica di conservazione, l'elenco dei sub-processori utilizzati (ad esempio per l'hosting Cloud o l'elaborazione dei pagamenti), le istruzioni del controllore e i trasferimenti internazionali in modo che gli utenti LMS possano prendere decisioni consapevoli sull'utilizzo del servizio .

Allo stesso modo, è importante:

- offrire agli utenti la possibilità di porre domande, presentare reclami o esercitare i diritti sanciti dal GDPR;
- esaminare tutti i sub-processori e assicurane la loro conformità con il GDPR;
- fornire giustificazioni legale per le operazioni di elaborazione e trasferimento dei dati. Un servizio che invia i dati dell'utente dall'UE agli Stati Uniti, ad esempio, dovrebbe avere quanto meno alcune Regole aziendali vincolanti legalmente approvate che disciplinano il trasferimento e la gestione di tali dati;
- supportare l'accesso ai dati personali a seconda dei ruoli;
- rispettare le certificazioni GDPR e i codici di condotta approvati.

Riguardo al **codice di condotta** è importante:

- dare chiare direttive sulle condizioni di riservatezza al personale che accede ai dati;
- collaborare con i responsabili del trattamento e le autorità di vigilanza;
- in caso di violazione dei dati, disporre di una politica e un piano da attuare per dare comunicazione alle autorità di vigilanza e agli interessati interessati entro 72 ore;
- supportare l'esportazione dei dati LMS in altri formati e la possibilità di trasferire i dati a un altro fornitore;
- revisionare, aggiornare e testare periodicamente l'efficacia delle politiche, delle procedure e dei controlli.

E' responsabilità dell'utente, in qualità di responsabile del trattamento, verificare che quanto sopra sia effettivamente supportato dal servizio LMS.

GDPR ed elaborazione dei dati

Perché ad una società sia permesso **archiviare e trattare dati personali**, dovrebbe sussistere almeno una delle seguenti condizioni, come specificato nel GDPR (articolo 6):

- l'interessato ha dato il consenso al trattamento per scopi specifici
- l'elaborazione è necessaria per l'esecuzione di un contratto che l'interessato ha sottoscritto
- il trattamento è necessario per il rispetto di un obbligo legale
- il trattamento è necessario per proteggere gli interessi dell'interessato
- l'elaborazione è necessaria per l'esecuzione di un compito svolto nell'interesse pubblico
- il trattamento è necessario per gli interessi legittimi perseguiti dal responsabile del trattamento, eccetto laddove tali interessi vadano oltre gli interessi o i diritti e le libertà fondamentali dell'interessato

GDPR ed eLearning

Ecco due peculiarità dell'eLearning in riferimento al GDPR che dovresti conoscere:

1. Limiti nazionali all'elaborazione dei dati dei dipendenti

Il GDPR consente alla legislazione nazionale di imporre norme specifiche sul trattamento dei dati personali dei dipendenti nel contesto lavorativo.
Se la tua azienda ha uffici e dipendenti in tutta l'UE, dovresti conoscere le legislazioni nazionali specifiche dei paesi in cui la tua azienda è presente.

2. Problemi di consenso

Lo squilibrio di potere tra datore di lavoro e dipendente può rendere insufficiente il semplice consenso come base legittima per l'elaborazione dei dati personali dei dipendenti: aggiungere un percorso formativo come termine contrattuale per i tuoi dipendenti servirà come giustificazione più solida per la gestione dei dati per l'eLearning.

Leggi l'articolo completo...