PRIVACY E MOODLE: GESTIRE UTENTI, CONTENUTI E CONSERVAZIONE IN AMBIENTI E-LEARNING BASATI SU MOODLE

Marco Meli

Edw International Srl
meli@edw.it

-- WORKSHOP --

***ARGOMENTO**: Implementazioni e soluzioni tecniche*

Abstract

Moodle come LMS completo e innovativo rende possibile, tra le altre cose, la realizzazione di contenuti formativi, che possono essere fruiti, modificati anche in modo dinamico e personalizzato, strutturati in repository e interscambiati con altri.

Diviene evidente che non è possibile gestire questi processi senza focalizzarsi e confrontarsi con la crescente attenzione ai diritti individuali.

Anche la comunità Moodle ha percepito questa esigenza: sia utilizzando gli strumenti già presenti, che sviluppando un'architettura in grado di gestirli.

In questo lavoro si cerca di sottolineare alcuni temi affrontando, sia tecnicamente che da un punto di vista dei principi, la gestione dei dati personali in una installazione Moodle.

Keywords – Moodle, Privacy, GDPR, Portfolio riflessivo, autovalutazione

1 INTRODUZIONE

Moodle come LMS completo e innovativo rende possibile, tra le altre cose, la realizzazione di contenuti formativi, che possono essere fruiti, modificati anche in modo dinamico e personalizzato, strutturati in repository e interscambiati con altri. L'ambiente mette a disposizione strumenti che rendono possibile condividere la progettazione e la distribuzione di contenuti in modalità collaborativa e con una costante modalità costruttivista.

Diviene evidente che non è possibile gestire questi processi senza focalizzarsi e confrontarsi con la crescente attenzione ai diritti individuali.

Anche la comunità Moodle ha percepito questa esigenza: sia utilizzando gli strumenti già presenti, che sviluppando una architettura in grado di gestirli. Non è stato ostacolo nemmeno la diversità di tipologie di utenti, né la diversità dei contenuti, tantomeno gli ambienti coinvolti e le istituzioni, o l'ambiente multinazionale, tutti attori con proprie politiche di privacy e una storia di regole e provvedimenti al riguardo.

2 FONDAMENTI DI PRIVACY E PRINCIPI NORMATIVI

La diffusione di Moodle in tutto il mondo mostra come sia uno degli strumenti più utilizzati nell'ambito dell'e-learning.

La figura 1 ci fornisce una idea dimensionale del fenomeno Moodle, e della sua pervasività a livello mondiale.

In un ambiente formativo esteso come Moodle le esigenze di controllo e sicurezza delle informazioni trattate divengono sempre più rilevanti. Internet è diventato sempre più ricco di comportamenti invasivi,

per scopi personali e commerciali, alcuni decisamente fraudolenti: prevenire i pericoli e garantire i diritti degli utenti, e' diventato irrinunciabile e fondamentale.

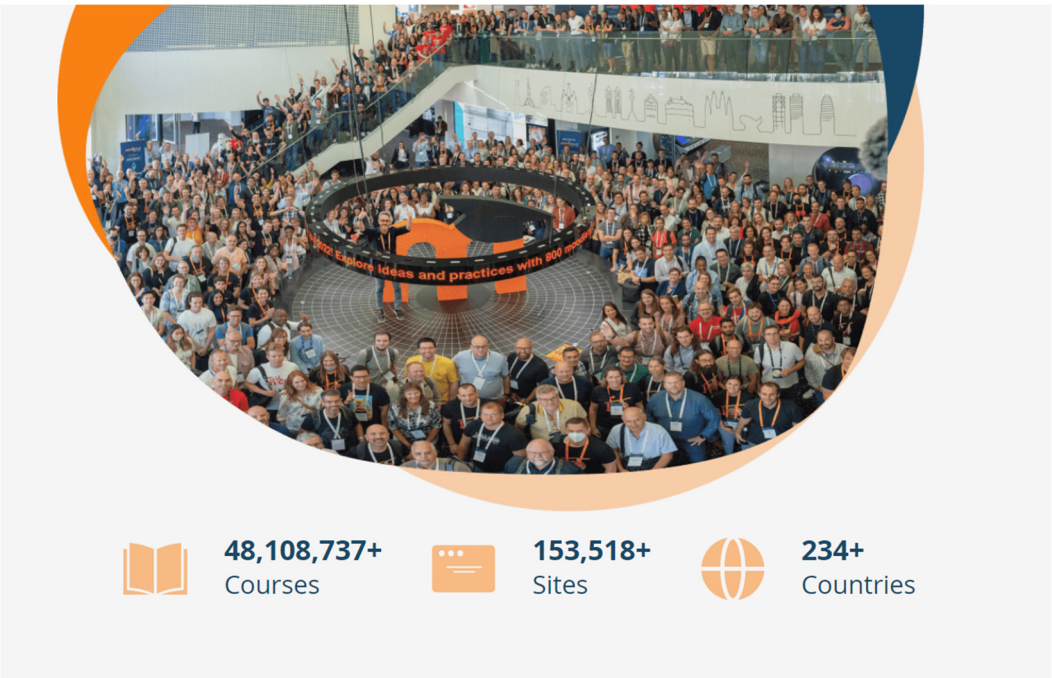

Fig. 1: I numeri di Moodle nel mondo (Da Moodle.org)

Dal 2016, il mondo, europeo prima e globale poi, è stato percorso dall'entrata in vigore di provvedimenti normativi di ampio livello, il cui primo e più rilevante è stato il Regolamento 679 (Global Data Processing Regulation), che ha influenzato il disegno di tutti i framework successivi in tutto il mondo.

Molte delle regolamentazioni tra i vari paesi, pur nella loro diversità, sono state ispirate dal GDPR. Questo fattore rende ragionevole un approccio simile alla rilevazione dei rischi potenziali tra normative diverse, permettendo di implementare soluzioni di compliance che possano coprire in genere entrambe le normative, richiedendo azioni specifiche solo in alcuni casi.

Di seguito, è inserita una analisi comparativa permetterà di verificare come si confrontano i concetti principali e le applicazioni alle differenti platee di utilizzatori, tra il GDPR, valido in Europa, e il CCPA, l'equivalente normativa in vigore in California (e la più avanzata negli Stati Uniti).

Fianco a fianco, in Tabella 1 il confronto tra le due normative.

California Consumer Privacy Act (CCPA)	**General Data Protection Regulation (GDPR)**
Legge sulla privacy dei consumatori della California (CCPA)	Regolamento generale sulla protezione dei dati (GDPR)
Informazioni personali (CCPA)	**Dati personali (GDPR)**
Il CCPA definisce i diritti dei consumatori che sono residenti in California.	Ai sensi del GDPR, i dati personali si riferiscono a qualsiasi informazione che identifica direttamente o indirettamente qualcuno.

Le informazioni personali come qualsiasi informazione che identifichi, descriva, si riferisca o possa essere ragionevolmente collegata a un consumatore o a una famiglia. NB1: Si noti che il CCPA esenta alcune categorie specifiche dal suo campo di applicazione, come alcune informazioni mediche. NB2: Sebbene le normative utilizzino termini diversi con definizioni leggermente diverse, "dati personali", "informazioni personali" e "informazioni di identificazione personale (PII)" sono spesso usati in modo intercambiabile.	Alcuni esempi di "informazioni personali" e "dati personali" includono nome completo, indirizzi e-mail, numeri di documenti ufficiali (ad esempio, passaporto, patente di guida e previdenza sociale) e identificatori online. NB: Si noti che il CCPA esenta alcune categorie specifiche dal suo campo di applicazione, come alcune informazioni mediche. NB: Sebbene le normative utilizzino termini diversi con definizioni leggermente diverse, "dati personali", "informazioni personali" e "informazioni di identificazione personale (PII)" sono spesso usati in modo intercambiabile.
Soggetti Interessati Il CCPA protegge i consumatori, ovvero le persone fisiche residenti in California.	**Soggetti Interessati** Il GDPR si concentra sugli interessati, ovvero qualsiasi persona identificabile residente nell'UE che possa essere identificata direttamente o indirettamente.
A chi si applicano le leggi? Il CCPA regola le aziende, ovvero le organizzazioni a scopo di lucro che operano in California, raccolgono informazioni personali dai consumatori con sede in California e determinano come e perché verranno elaborate. Devono inoltre valere una o più delle seguenti condizioni: Hanno un fatturato lordo annuo di 25 milioni di dollari o più (23 M€). Acquista, riceve, vende o condivide le informazioni personali di almeno 50.000 consumatori, famiglie o dispositivi Ricava almeno il 50% delle entrate annuali dalla vendita delle informazioni personali dei consumatori. Il CCPA stabilisce anche i requisiti per i **fornitori di servizi**, ovvero le organizzazioni che elaborano informazioni personali per conto di un'azienda.	**A chi si applicano le leggi?** Il GDPR si rivolge ai titolari del trattamento dei dati, ovvero le organizzazioni che decidono come e perché trattare i dati personali appartenenti ai residenti dell'UE. Inoltre, il GDPR regola i responsabili del trattamento, ovvero le organizzazioni che elaborano i dati personali per conto dei titolari del trattamento. Il GDPR si applica quando il titolare del trattamento o il suo responsabile del trattamento è stabilito nell'UE, o quando non UE tratta dati di interessati stabilti nella UE.
Portata del provvedimento: **Globale**	**Portata del provvedimento:** **Globale**

Tabella 1: confronto CCPA e GDPR

2.1 A chi si applicano le leggi?

Entrambe le normative sono nate per proteggere le persone in un mondo di crescente interconnettività globale, in cui i trasferimenti internazionali di dati personali sono più frequenti ed elaborati e i progressi nella tecnologia hanno portato a scandali sull'uso improprio dei dati e sofisticati attacchi informatici.

Sebbene le normative utilizzino termini diversi con definizioni leggermente diverse, "dati personali", "informazioni personali" e "informazioni di identificazione personale (PII)" sono spesso usati in modo intercambiabile.

Il CCPA e il GDPR si applicano alle singole organizzazioni in modi diversi e, sebbene ci siano alcune sfumature nell'ambito di applicazione che distinguono entrambi i gruppi di legislazione, condividono obiettivi simili. Osservando come si completano a vicenda, è possibile creare politiche scalabili per la privacy e la sicurezza dei dati conformi a entrambe le leggi.

Le due normative si sovrappongono per quanto riguarda alcuni diritti; quindi, se si è già conforme al GDPR, si è sulla buona strada per soddisfare i requisiti CCPA. Conoscere le somiglianze può anche aiutare a prepararsi per la conformità alle normative future in tutte le aree geografiche che probabilmente rispecchieranno quelle esistenti. Questo approccio è in genere replicabile con altre legislazioni in altri paesi (es: GDPR UK, Privacy in Svizzera).

È quindi probabile che l'attenzione e le cure che verranno implementate nel sito Moodle da voi gestito risulteranno valide o facilmente modificabili per altre legislazioni.

2.2 Come valutare la conformità della propria installazione Moodle ad una legislazione come il GDPR?

È necessario comprendere gli elementi chiave della Normativa, comprendere come coinvolgono i dati e le azioni che vengono o possono venire compiute in Moodle ed assicurarsi che i dati conservati siano catalogati ed operati con azioni compatibili con la normativa. Si tratta di un lavoro puntuale per ogni sito, che va mantenuto aggiornato nel tempo. Per fortuna, la piattaforma Moodle a partire dalla versione 3.5 rende questo compito molto più agevole.

Iniziamo quindi vedendo cosa è la privacy secondo il GDPR.

2.3 Fondamenti di Privacy nel GDPR Reg 679/2016: principi e normative.

La definizione di Privacy in Italia si è evoluta nel tempo. Ad esempio, nella legge originale della Privacy in Italia D. Lgs 196/2003, in vigore dal 2003, recita:

> *(Art. 2 D.Lgs 196/03) Finalità: "Il presente testo unico, di seguito donominato "Codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".*

Come si deduce da questi primi articoli, alla base del significato del provvedimento, la ratio di una **Norma sulla Protezione dei dati è un Diritto di Libertà**. Essa riguarda il trattare i dati personali solo se necessario, nella misura minore possibile, prevedendo ogni sistema di sicurezza utile alla tutela del dato trattato, nel rispetto delle libertà delle persone.

Nel GDPR, il testo recita:

> *(Art. 1 Reg. 679/2016) Oggetto e Finalità:*
>
> *1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.*
>
> *2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.*

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

2.4 Ma cosa sono per il GDPR i Dati personali?

Secondo la legge, con «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (ad esempio nome e cognome, data di nascita, dati biometrici, impronte digitali, DNA...)

La definizione è abbastanza ampia e si appoggia non solo su dati statici ma anche su dati dinamici, facilmente deducibili dalla realtà. Ad esempio, la posizione nello spazio o nel tempo di un soggetto lo rende identificabile.

Per definire i dati personali, si deve tenere conto di tutti i mezzi a disposizione del "titolare del trattamento" per determinare se una persona è identificabile. I dati personali sono tutti i dati anonimi che possono essere controllati per identificare una persona specifica (ad esempio impronte digitali, DNA o informazioni come "il figlio del medico che vive in Via Roma 11 a Cusago non ha buoni risultati a scuola").

Le tecnologie dell'informazione e della comunicazione generano una quantità crescente di dati sempre più precisi su di noi (pagamento con carta di credito, chiamate effettuate da un telefono cellulare che consentono di identificare con una precisione di 393,2 m il luogo in cui si trova il chiamante, una connessione Internet).

Come ormai è stato mostrato pubblicamente, i dati personali, tra l'altro, possiedono un grande valore commerciale. Di conseguenza sono sempre più ricercati: i file vengono acquistati e venduti, i gruppi commerciali possono essere tentati di identificare e raggruppare in un file i "buoni clienti" di ciascuna delle loro filiali o i "cattivi clienti". I dati vengono via via raccolti, immagazzinati anche per lungo tempo, incrociati con altri dati, per poter profilare in maniera esauriente un consumatore/elettore, e grazie a tali profili proporgli scelte ritenute di maggior interesse per lui, condizionandone il comportamento.

Le "tracce informatiche" lasciate dagli utenti sono sempre più facili da sfruttare, grazie ai miglioramenti del software (ad esempio la tecnologia dei motori di ricerca Internet o il software di "ricerca" dei dati).

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, il suo stato legale, ecc…

Particolarmente importanti sono:

- i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale; i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Una particolare attenzione è messa sulla pratica della profilazione: i dati personali possono essere dati che non sono associati al nome di una persona ma possono essere facilmente utilizzati per identificarla e per conoscerne le abitudini e i gusti. (Ad esempio “il titolare del numero di linea 02 53 73 22 00 chiama spesso in Senegal”, oppure “il proprietario del veicolo DB363AT è abbonato a questa o quella rivista” oppure “il beneficiario dell’assicurazione sociale 1600530189196 vede il medico più di una volta al mese”.).

2.5 Come si devono usare i dati? Il Trattamento.

Alla base di ogni operazione sui dati esiste una azione sugli stessi, detta trattamento.

Usiamo direttamente le definizioni dello standard per descriverli. Le principali definizioni sono disponibili in Appendice A.

- «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzioni;
- questa definizione, che proviene dall’art. 4 del GDPR, descrive l’insieme delle operazioni che nel tempo si possono eseguire sui dati. Alcune di queste operazioni non si possono eseguire sempre, ma si ritiene che sia necessario conservare (Limitazioni). Un esempio di possibile limitazione all’accesso è la pseudo-anonimizzazione. Altra operazione da mantenere sono controllo è la profilazione, che analizza i dati personali in forma aggregata per valutare aspetti personali. Le definizioni GDPR di questi trattamenti sono disponibili in Appendice A.;
- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- «pseudo-anonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

2.6 Chi tratta i dati? Le persone coinvolte.

Attori: interessati, titolari del trattamento, responsabili del trattamento

- **Interessato** è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è *l’interessato* (articolo 4, paragrafo 1, punto 1) del Regolamento UE 2016/679);
- **Titolare** è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (vd articolo 4, paragrafo 1, punto 7 del Regolamento UE 2016/679);
- **Responsabile** è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (vd articolo 4, paragrafo 1, punto 8 del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. "sub-responsabile" (articolo 28, paragrafo 2 del Regolamento UE 2016/679).

2.7 Accountability - Responsabilizzazione

Come correttamente ricorda il Garante, il Regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability in inglese) di titolari e responsabili. La "responsabilizzazione" prevede l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt. 23-25, in particolare, e l'intero Capo IV). Spetta ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

A. Risk analysis

Il primo criterio è sintetizzato dall'espressione inglese "data protection by default and by design" (art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo nel quale il trattamento viene svolto e dei rischi per i diritti e le libertà degli interessati.

B. Privacy by design, privacy by default

Tutte queste attività devono avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo Reg 679/2016 -art. 25, par. 1) e richiedono, pertanto, un'analisi preventiva e un impegno da parte dei titolari che devono realizzarsi in una serie di attività specifiche e dimostrabili.

C. Valutazione di impatto (DPIA)

Fondamentali fra tali attività sono quelle connesse al rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati. Tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito della valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) o consultare il Garante per ottenere indicazioni su come gestire il rischio residuale. L'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare.

2.8 In che modo si trattano i dati? I principi dei trattamenti dei dati personali .

La definizione di un trattamento richiede un insieme di attenzioni che ne definiscono le caratteristiche. I principi diventano la sensibilità con i quali si deduce che il trattamento implicato sia accettabile. L'art 5 del GDPR li elenca tali principi e noi qui li citiamo brevemente. La validità per un certo trattamento è un fondamentale elemento per valutare che un trattamento sia accettabile.

A. Lecito, corretto e trasparenti nei confronti dell'interessato

B. Le finalità del trattamento dati

- Raccolti per finalità determinate, esplicite e legittime.
- Limitate.

I dati raccolti, in seguito devono essere trattati in modo che ci sia compatibilità con le finalità, ad esempio: il trattamento per archiviazione nel pubblico interesse, per ricerca scientifica o storica non è considerato incompatibile con tali finalità

C. La limitazione delle finalità

- Adeguati, pertinenti e limitati per le finalità per le quali sono trattati.
- Esatti e, se necessario, aggiornati.
- Conservati per il tempo necessario al trattamento e se archiviati mantenuti in mediante misure tecniche e organizzative adeguate.

3 MOODLE CI AIUTA, SE LO USIAMO CON ATTENZIONE

3.1 Considerazioni in ambito Moodle

La descrizione precedente è stata redatta per mostrare i punti che sono da tenere in considerazione per verificare che un trattamento sia conforme alle normative sulla privacy. Ma come si realizzano praticamente in un sistema come Moodle?

Le prestazioni inserite nei rilasci hanno portato le versioni più recenti (ad es. le versioni a partire dalla 3.5 LTS e successive) a permettere la realizzazione di sistemi conformi alle Regolamentazioni, .

Di seguito, gli strumenti e policy disponibili in Moodle sono:

- Strumenti per configurare la Privacy in Moodle.
- Data privacy: gestione dei dati utente in Moodle (ruoli, permessi e accesso ai dati).
- Alla base dell'architettura privacy di Moodle ci sono alcuni obiettivi da raggiungere nella configurazione del sistema:
    - la possibilità di definire data privacy e policies rispetto ad ogni classe di utilizzatore del sistema; ciò permette anche la creazione di figure il cui compito sia di eseguire azioni relative alla privacy anche per terzi, senza per forza che siano amministratori;
    - la possibilità di definire schermate di consenso ad hoc e di ottenere il consenso dell'utente addirittura prima che entri nel sito; tali consensi verranno categorizzati, archiviati e mantenuti per uno specifico periodo, potenzialmente diverso per ciascuno di loro;
    - la possibilità di poter centralizzare le decisioni ed i comportamenti relativi ad azioni che implicano potenziali rischi alla privacy degli interessati (es:: accesso ai datti dei minori, permesso di esportazione dei dati, ecc);
    - il completo controllo su tutti gli interessati e sui loro dati, grazie anche ad un data registry che permette di definire i tipi di dati coinvolti e la durata del loro periodo di conservazione;
    - la possibilità di definire i ruoli e le gestioni dei permessi basati su di essi. Ad esempio, si possono gestire con facilità le situazioni relative ai minori e su chi puo' permettere, accedere, esportare o cancellare i dati a loro collegati;
    - una architettura della privacy che si estende a tutto il sistema, plugin compresi.

Per ottemperare a questi obiettivi architetturali, Moodle HQ ha progettato ed eseguito un processo di raggiungimento alla compliance, mantenuto anche adesso. Il processo è riassumibile nelle seguenti azioni/fasi/raccomandazioni:

- se si desidera sviluppare dei plugin Moodle per il GDPR:
    - si può fare riferimento alla documentazione specifica GDPR per sviluppatori di plugin nei documenti di sviluppo e mantenere i contatti con i propri pari nei forum dedicati alla discussione sulla conformità al Regolamento generale sulla protezione dei dati (GDPR) dell'UE;
- nel caso di Moodle e GDPR utilizzato da insegnanti e studenti
    - Se un insegnante o uno studente desidera saperne di più sui tuoi diritti ai sensi del GDPR e su come le funzionalità di Moodle possono aiutarlo a proteggere la privacy dei tuoi dati, si consiglia di rivolgersi ad esperti. È opportuno avere disponibili persone con competenze specifiche. Gli amministratori di sistema insieme a queste persone dedicate potranno aiutare nei problemi, fornendo informazioni specifiche per lo specifico ambiente.

Moodle HQ rimarca il ruolo che le organizzazioni devono giocare nella gestione dei loro siti dal punto di vista dellaprivacy. Vanno incoraggiate l'implementazione di misure di sicurezza per la loro installazione di Moodle. Ecco alcuni consigli:

- scrivere più documenti di policy (inclusa la policy del sito per gli ospiti) in modo che possano essere completamente trasparenti con i loro studenti, educatori e chiunque visiti il loro sito su come raccolgono, usano o divulgano i loro dati;
- proteggere i minori digitali con controlli sull'età del consenso e gestire l'accesso per i minori che necessitano del consenso dei genitori per accedere al loro sistema di gestione dell'apprendimento;
- gestire tutte le richieste di dati da parte degli studenti e tenere traccia dei periodi di conservazione in un luogo centralizzato;
- consentire agli utenti di richiedere facilmente l'accesso o scaricare i propri dati, di vedere le policy che hanno accettato e di nominare un responsabile della privacy per gestire centralmente le richieste di accesso/cancellazione dei dati da parte di tali utenti.

3.2 Attivare la formazione

La formazione si estende a tutti i player del mondo Moodle, sviluppatori compresi. Esistono policy e consigli, oltre che esempi, per scrivere plugin attenti alle problematiche privacy, agli studenti ed ai docenti, ed ovviamente agli amministratori di sistema. DI seguito, ad esempio, una situazione di prova relativa al ruolo di responsabile della privacy, dalle versioni di demo di Moodle

Il ruolo di responsabile della privacy è un ruolo personalizzato appositamente per consentire a un membro non amministratore dello staff di visualizzare le richieste di dati (come l'esportazione o l'eliminazione dei dati) e di rispondere alle domande. Il nostro responsabile della privacy è anche in grado di accettare le policy per conto dei nostri studenti più giovani.

- *Richieste di dati: guarda chi ha chiesto che i propri dati vengano esportati o eliminati.*
- *Registro dati: controlla i tipi di dati e i relativi periodi di conservazione.*
- *Registro privacy dei plugin: assicurati che i plugin del sito siano conformi al GDPR e guarda quali dati utilizzano.*
- *Gestisci le policy: visualizza le policy sul sito e guarda chi le ha accettate e chi no.*
- *Accordi utente: accetta manualmente le policy per conto degli studenti. (Particolarmente importante poiché alcuni dei nostri studenti sono al di sotto dell'età digitale del consenso.)*

4 CONSIGLI PRATICI

Un responsabile di Installazione Moodle deve mantenere sotto controllo la postura privacy. Può essere utile strutturare questa attività utilizzando un questionario, come successivamente descritto (in Appendice B è presente anche una checklist relativa).

4.1 Questionario su sito Moodle, contenuti e ruoli nella privacy aziendale

A. Stabilire il ruolo del sistema Moodle che si vuole proteggere all'interno dell'organizzazione

- Di che processi aziendali il sito Moodle fa parte?
- Che scopo ha?
- Chi sono i soggetti coinvolti ed in quale ruolo?
- Chi sono gli interessati?
- Ci si rivolge a minori?

- Esistono particolari vincoli di durata dei dati?
- Come è organizzata la gestione della sicurezza e della privacy della Istituzione di cui si fa parte?

B. Pianificare l'installazione e utilizzare gli strumenti che Moodle fornisce per la gestione dei dati personali

Moodle al suo interno è dotato di architettura e strumenti che permettono di attuare ogni policy di sicurezza, tracciamento, durata e esportazione dei dati che potranno essere utili per trattamenti GDPR, inclusi l'attenzione ai diritti dei minori. Il sistema permette anche di creare ruoli per gli opportuni controllori che il profilo privacy richiesto dalla organizzazione ospite ritiene necessario.

C. Valutare gli elementi principali del processo per la messa in conformità di un sito.

La risposta a queste domande guida nelle scelte di configurazione.

- **Che tipo di dati personali possono esserci in un sito Moodle?**
    - Sono tutte le informazioni che possono essere associate a una persona fisica. Ogni account utente e tutte le attività associate a tale account utente sono classificate come informazioni personali. Ogni presenza in una chat e' una informazione personale. Ciò si estende anche alle informazioni associate come i file di log del server Web.
- **Chi è l'interessato, ovvero il proprietario dei dati personali che sono presenti nel sito?**
    - Qualsiasi individuo o organizzazione che archivia o elabora informazioni personali su una persona identificabile di uno stato membro dell'UE (indipendentemente dal fatto che l'elaborazione o l'archiviazione delle informazioni avvenga o meno nell'UE). Si applica anche se l'individuo o l'organizzazione stessa si trova in uno stato membro dell'UE.
- **Quali specifiche funzionalità utilizza per raggiungere la conformità al GDPR?**
    - Le funzionalità coprono le seguenti aree:
        - **onboarding di nuovi utenti**, tra cui; controllo di età e posizione per identificare i minori, controllo delle versioni delle policy sulla privacy e monitoraggio dei consensi degli utenti;
        - **gestione delle richieste di accesso ai dati e delle richieste di cancellazione e mantenimento di un registro dei dati**.

D. Definire chiaramente i trattamenti e le persone coinvolte nei vari ruoli

Svolgere questo compito crea una chiara matrice di associazione tra le persone ed i dati che trattano o forniscono.

E. Considerare il vostro sito come una parte del sistema dell'organizzazione, e verificare come interagite in tutti i processi della stessa, incluso scelta dei fornitori, politica di backup, disaster recovery, amministratori di sistema.

F. Schedulare ed eseguire compliance reviews regolari (almeno 1 all'anno).

G. Utilizzare il materiale e gli strumenti che Moodle fornisce per gestire e mantenere aggiornati glii archive.

H. Coordinarsi con la gestione privacy dell'organizzazione: la privacy e' una problematica a livello aziendale, più' esteso di quello che un singolo sito può gestire.

5 CONCLUSIONI

La implementazione di una politica privacy, anche se complessa, è non solo necessaria, ma anche un valore aggiunto per un sito. L'autore spera di aver fornito una spiegazione, per quanto incompleta,

sufficientemente esauriente. La problematica è complessa e, per poterla padroneggiare, è sicuramente utile poter sperimentare, confrontandosi con altri e con esperti.

6 APPENDICE A

Definizioni dal GDPR (Art. 4)

A. Articolo 4 Definizioni

Ai fini del presente regolamento s'intende per:

1. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3. «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4. «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5. «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6. «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7. «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8. «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9. «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10. «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11. «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12. «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
13. «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
14. «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
15. «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
16. «stabilimento principale»:
    a. per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    b. con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
17. «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
18. «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
19. «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20. «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
21. «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22. «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
    b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
    c. un reclamo è stato proposto a tale autorità di controllo;
23. «trattamento transfrontaliero»:
    a. trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
    b. trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
24. «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25. «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
26. «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

7 APPENDICE B

Checklist su Gdpr e adempimenti nel sito per amministratori Moodle.

A. Checklist generale

- ✓ **Il sito Moodle è ospitato in uno stato membro dell'UE o è possibile che un utente del sito Moodle sia un individuo di uno stato membro dell'UE?**
  - Se hai risposto no a questa domanda, non sei interessato da questa normativa. Tuttavia, i vantaggi della protezione dei dati offerti dalla normativa sono universalmente applicabili e potresti prendere in considerazione di conformarti volontariamente a questa legislazione a vantaggio degli utenti del tuo sito.
- ✓ **Richiedi agli utenti del tuo sito di accettare un documento di informativa sul sito o sulla privacy prima di utilizzare il tuo sito (sia in Moodle che in qualcosa di esterno a Moodle, come un modulo cartaceo)?**
  - Se hai risposto no a questa domanda, devi iniziare a farlo. Gli utenti devono essere consapevoli dei propri diritti e dei processi con cui possono esercitarli.
  - Se hai risposto sì a questa domanda, devi rivedere la tua politica per assicurarti che copra tutti i requisiti delle nuove normative (vedi "Politica del sito" di seguito). Se modifichi la tua politica, devi far sì che tutti gli utenti del sito accettino la nuova politica prima che possano continuare a utilizzare il sito.

- ✓ **È possibile che il tuo sito venga utilizzato da minorenni? (Sotto i 16 anni nella maggior parte degli stati membri, ma alcuni stati possono ridurre questo limite fino a 13 anni).**
    - ➢ Se hai risposto sì a questa domanda, devi assicurarti di ottenere il consenso dal loro tutore legale. Tieni presente che la raccolta e l'elaborazione di informazioni personali su minorenni possono influire sulla tua valutazione del rischio. Dovresti prestare particolare attenzione a proteggere adeguatamente queste informazioni e conservarle per il periodo più breve necessario.
- ✓ **È probabile che la raccolta o l'archiviazione di dati personali degli utenti del tuo sito comporti un rischio elevato per i loro diritti e le loro libertà?**
    - o Alcuni esempi che indicherebbero un rischio elevato sono:
        - una valutazione sistematica ed estesa di aspetti personali relativi a persone fisiche che si basa su un trattamento automatizzato, inclusa la profilazione, e su cui si basano decisioni che producono effetti giuridici sulla persona fisica o che incidono in modo analogo e significativo sulla persona fisica;
        - trattamento su larga scala di categorie speciali di dati tra cui:
            - origine razziale o etnica
            - opinioni politiche
            - convinzioni religiose o filosofiche
            - appartenenza sindacale
            - dati genetici
            - dati biometrici
            - dati relativi alla salute
            - orientamento sessuale
            - dati relativi alla vita sessuale di una persona fisica
            - condanne penali

    Questo elenco non è esaustivo e se non sei sicuro di dover considerare i dati raccolti dai tuoi utenti come "ad alto rischio", dovresti fare riferimento alla legislazione e chiedere una consulenza professionale.
    - ➢ Se la risposta è "Sì", dovresti eseguire una valutazione dell'impatto sulla protezione dei dati. Fai riferimento alla legislazione e chiedi una consulenza professionale.
- ✓ **Utilizzi alcune delle informazioni personali raccolte per scopi di marketing?**
    - ➢ Se hai risposto sì a questa domanda, devi ottenere un consenso separato da ciascun utente per utilizzare questi dati per questo scopo. Il consenso all'uso dei dati per il marketing deve essere revocabile separatamente dall'utente.
- ✓ **Utilizzi alcune delle informazioni personali raccolte per scopi di ricerca?**
    - ➢ Se hai risposto sì a questa domanda, devi ottenere un consenso specifico da ciascun utente per utilizzare i dati per questo scopo o rendere completamente anonimi i dati prima di utilizzarli per la ricerca. https://github.com/moodlehq/moodle-local_anonymise è un esempio di uno strumento progettato per rendere anonimi tutti i dati su un sito Moodle.
- ✓ **Condividi alcuni dei dati raccolti con terze parti? Ciò include siti e servizi che si integrano con Moodle come: Google Analytics, LTI, repository (Google Docs, OneDrive ecc.), sistemi di autenticazione e include anche siti e servizi utilizzati nella fornitura del tuo sito Moodle come provider di hosting.**

- Se hai risposto sì a questa domanda, sei responsabile di tutti i dati condivisi con terze parti. Devi ottenere il consenso dell'utente per condividere questi dati con ciascuna terza parte. Se l'elenco dei servizi di terze parti cambia, devi ottenere nuovamente il consenso da tutti gli utenti del sito per ogni nuovo sito/servizio di terze parti. Dovresti anche adottare misure ragionevoli per garantire che ciascuna terza parte protegga adeguatamente i dati personali degli utenti, tra cui:
    - rivedere l'informativa sulla privacy di terze parti per assicurarti che sia coerente con la tua;
    - monitorare e notificare agli utenti del tuo sito le modifiche all'informativa sulla privacy di terze parti;
    - identificare il meccanismo per l'elaborazione delle richieste di cancellazione o correzione dei dati personali con ciascuna terza parte in modo da poter seguire questa procedura quando ricevi una di queste richieste per il tuo sito;
    - identificare ed elencare il responsabile della protezione dei dati e l'informativa sulla privacy per ciascun sito di terze parti come parte della tua informativa sulla privacy.

Ad esempio, Google Analytics non ha ancora fornito chiare istruzioni aggiornate su come conformarsi al nuovo GDPR quando si utilizza il proprio servizio (Al momento Versioni inferiori alla G.A 2.1 non sono compliant. Questo esempio dimostra che è responsabilità responsabilità garantire la protezione della privacy degli utenti del tuo sito e che non è legale utilizzare servizi cloud senza considerare le implicazioni sulla privacy di ogni singolo fornitore di servizi.

✓ **Segui le best practice e le procedure per garantire la sicurezza dei dati?**

- Se hai risposto no a questa domanda, devi rivedere le tue policy e procedure per assicurarti di non mettere a rischio i dati personali degli utenti del tuo sito.
- Le "migliori pratiche" includono, ma non sono limitate a, misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio, come:
    - pseudo-anonimizzazione e crittografia dei dati personali;
    - la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza in corso dei sistemi e dei servizi di elaborazione;
    - la capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico;
    - un processo per testare, valutare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza dell'elaborazione.
    - Esempi:
        - uso appropriato della crittografia (https);
        - manutenzione di tutti i sistemi e software con aggiornamenti di sicurezza pertinenti;
        - eliminazione dei dati personali il prima possibile, una volta che non sono più necessari per lo scopo per cui sono stati raccolti.

✓ **Hai definito politiche e procedure per la divulgazione delle violazioni dei dati?**

- Se hai risposto no a questa domanda, devi definire alcune.
- Se hai delle policy e procedure esistenti, queste devono essere riviste.

Queste policy e procedure devono includere la notifica all'Autorità di vigilanza entro 72 ore dalla violazione dei dati e la notifica a tutti gli utenti interessati se sono stati negativamente coinvolti (dati personali divulgati).

- ✓ **Hai nominato un responsabile della protezione dei dati e lo hai elencato nella tua informativa sulla privacy?**
  - ➢ Se hai risposto no a questa domanda, devi nominarne uno ed elencarlo nell'informativa sulla privacy del tuo sito. Il responsabile della protezione dei dati deve essere competente nella gestione dei processi IT, della sicurezza dei dati (inclusa la gestione degli attacchi informatici) e di altri problemi critici di continuità aziendale relativi alla conservazione e all'elaborazione di dati personali e sensibili.
- ✓ **Hai un meccanismo con cui gli utenti del tuo sito possono richiedere che i loro dati personali vengano cancellati, corretti o resi disponibili all'utente richiedente sul tuo sito?**
  - ➢ Se hai risposto sì a questa domanda, assicurati che sia elencato nell'informativa sulla privacy del tuo sito.
  - ➢ Se hai risposto no a questa domanda, definiscine uno ed elencalo nell'informativa sulla privacy del tuo sito.

  Per un sito Moodle che non utilizza i plugin GDPR:

  un meccanismo adatto sarebbe un indirizzo e-mail, riservato a questo scopo e monitorato da un amministratore per il tuo sito Moodle. Una volta ricevuta una richiesta, devono essere adottate misure ragionevoli per garantire l'autenticità della richiesta e l'identità dell'utente che effettua la richiesta.
  - Le correzioni dei dati personali possono essere elaborate modificando i dati in Moodle direttamente tramite un account amministratore.
  - Le cancellazioni dei dati personali possono essere elaborate eliminando l'account utente o modificando l'account utente per rimuovere tutte le informazioni identificative e renderlo inattivo.
  - I record dei dati personali possono essere ottenuti da "Amministrazione sito -> Report -> Registri" scaricando tutti i registri per un singolo utente come file CSV. Probabilmente ci saranno dati personali aggiuntivi su un utente che vengono archiviati all'esterno di Moodle, come i registri di accesso al server web.
- ✓ **La tua organizzazione ha più di 250 dipendenti?**
  - ➢ Se hai risposto sì a questa domanda, devi tenere registri dettagliati su tutti i trattamenti di dati personali. Fai riferimento al regolamento per i dettagli sui registri che devono essere tenuti.

B. Checklist Politica del sito per Amministratori

- ✓ Una politica del sito può essere utilizzata per raccogliere il consenso ai fini della conformità al GDPR. Il documento della politica del sito deve essere esaminato attentamente per assicurarsi che copra tutte le informazioni elencate di seguito, in un linguaggio semplice e succinto.
- ✓ In Moodle 3.4.2 e versioni successive, per abilitare una politica del sito, inserisci l'URL della pagina in "URL della politica del sito" (sitepolicy) in "Impostazioni politica" nell'amministrazione del sito.
- ✓ La pagina della politica del sito deve contenere tutte le informazioni elencate di seguito. La politica del sito verrà visualizzata in un iframe come parte del processo di accesso, quindi non richiede intestazioni e piè di pagina.
- ✓ Una pratica consigliata è quella di creare una risorsa file nella home page del sito Moodle e copiare l'URL di questa risorsa da utilizzare come policy del sito. Ciò significa che la policy del sito è sempre disponibile per l'accesso da parte degli utenti e può essere facilmente aggiornata da Moodle. Si noti che questa tecnica è incompatibile con l'impostazione "Forza gli utenti ad accedere (forcelogin)" (anche in "Policy del sito" nell'amministrazione del sito), poiché la risorsa file non sarà più visibile finché l'utente non avrà effettuato l'accesso al sito.

- ✓ La policy del sito deve includere tutte le seguenti informazioni in un linguaggio semplice:
  - quali informazioni vengono raccolte;
  - lo scopo di tutte le elaborazioni da eseguire sui dati degli utenti. Il marketing deve essere elencato separatamente con un "consenso" revocabile separato;
  - identità del titolare del trattamento dei dati e informazioni di contatto;
  - elenco dei diritti;
  - periodo di conservazione dei dati;
  - meccanismo per revocare il consenso;
  - meccanismo per richiedere correzioni o cancellazioni dei dati personali;
  - meccanismo per richiedere un registro di tutti i dati personali;
  - elenco delle terze parti con cui i dati saranno condivisi (ciò include integrazioni come LTI, portfolio, plagio, repository, autenticazione ecc.) tra cui:
    - i dettagli di contatto del responsabile della protezione dei dati per ciascuno;
    - l'informativa sulla privacy per ciascuno;
  - se i dati personali saranno utilizzati per qualsiasi processo decisionale automatizzato, inclusa l'importanza e i dettagli del processo (ad esempio analisi).

Riferimenti Bibliografici

[1] Avv.Enrico Corradini., Cognome N. La Privacy a scuola con il Nuovo Regolamento Europeo. Intervento in Raise Academy, (2017), pp. 769-822.

[2] Danielle Kucera, CCPA vs. GDPR: Similarities and Differences Explained, (2021), https://www.okta.com/blog/2021/04/ccpa-vs-gdpr/

[3] https://cnil.fr

[4] Moodle.org, percorso Security, Privacy, esempio di Moodle Demo

[5] Guida all'applicazione del GDPR - Garante Privacy - https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

[6] Testo del Regolamento (Ue) 2016/679 - Arricchito con riferimenti ai Considerando e aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018 https://www.garanteprivacy.it/garante/document?ID=6264597