UNIVERSITÀ
DI PAVIA

Linee guida in materia di sicurezza e privacy dei siti web di Ateneo

Versione 1.0 – 29/04/2019

UNIVERSITÀ
DI PAVIA

Sommario

UNIVERSITÀ
DI PAVIA

Premessa

Le presenti linee guida hanno lo scopo a fornire agli amministratori dei siti web di Ateneo realizzati mediante piattaforme di Content Management System (CMS) alcune indicazioni di base utili a garantire tanto la loro sicurezza quanto la loro conformità alle vigenti disposizioni in materia di trattamento di dati personali.
Le norme generali apposte in questo documento vanno applicate adeguandole allo specifico contesto nell'ottica dell'accountability.

Aggiornamento, sicurezza e conformità del CMS

Al fine di incrementare il livello di sicurezza della piattaforma CMS adottata, occorre utilizzare un protocollo di trasmissione dati sicuro di tipo https:// ed aggiornare la piattaforma CMS alla sua ultima versione attivando, se possibile, la funzionalità di aggiornamento automatico. In mancanza dell'automatismo, verificare con frequenza le disponibilità di nuovi rilasci anche attraverso le notifiche che appaiono nel pannello di amministrazione ed eseguire manualmente l'attività. In entrambi i casi prima di procedere è opportuno:

- risalire alla versione della piattaforma CMS su cui il sito internet è basato;
- verificare la disponibilità di una copia di backup del sito web;
- verificare che l'aggiornamento della piattaforma CMS sia compatibile con le estensioni (plugin / moduli) già installate;
- mettere il sito offline prima di effettuare le attività di aggiornamento e sicurezza.

Al solo fine di effettuare il passaggio ad un protocollo di trasmissione dati sicuro di tipo https://:

- se il sito web è ospitato su server di Ateneo, verificare, col supporto del Servizio Gestione Infrastrutturre Tecnologiche, che sul web server in uso sia già installato un certificato SSL, altrimenti inviare al Servizio richiesta di acquisizione, seguire le indicazioni fornite e quindi procedere all'attivazione del protocollo https:// secondo le istruzioni dello specifico CMS
- se il sito web è ospitato su server non di proprietà dell'Ateneo, contattare il provider di servizi e seguire le istruzioni impartite.

Il sito internet non deve in ogni caso effettuare chiamate di tipo http:// a pagine web, file javascript, immagini o fogli di stile, onde evitare la generazione di errori di certificato.

In genere le ultime versioni delle piattaforme CMS introducono nuovi strumenti utili a garantire l'attuazione dei principi sanciti nel Regolamento UE 2016/679 in materia di protezione di dati personali (GDPR).
Per ulteriori dettagli in merito, si consiglia di visitare le sezioni dei siti internet ufficiali dei CMS che trattano dell'argomento "GDPR".

Sicurezza e conformità di plugin e temi

Al fine di migliorare la sicurezza del sito web, in presenza di plugin e temi, dopo aver verificato la disponibilità di una copia di backup del sito occorre:

- aggiornare i plugin alle loro ultime versioni servendosi dell'apposita funzionalità di back-end di "aggiornamento automatico" o, in alternativa, verificare periodicamente la disponibilità di nuove release ed eseguire manualmente l'attività;
- rimuovere i plugin non utilizzati ed eventuali plugin "premium" hackerati per renderli utilizzabili senza aver acquistato apposita licenza;

- installare esclusivamente plugin compatibili con la versione del CMS, citati nel sito web ufficiale del CMS e che siano aggiornati di frequente.

Per quanto riguarda i temi, occorre altresì:

- aggiornare i temi utilizzati quando si rendono disponibili nuove release e disinstallare quelli non usati (eccezion fatta per quelli di default). È opportuno prediligere temi che garantiscano supporto tecnico, siano aggiornati di frequente e non siano temi "premium" hackerati per renderli utilizzabili senza aver acquistato apposita licenza.

E' possibile che alcuni plugin installati sul sito web non siano sicuri e neppure conformi di default alle nuove disposizioni normative in materia di trattamento dei dati personali ai sensi del Regolamento UE 2016/679 (GDPR). Si raccomanda, pertanto, di:

- consultare le privacy policy reperibili sui siti internet delle aziende produttrici di plugin o api di dubbia provenienza per accertarsi che il trattamento dei dati personali eventualmente raccolti venga effettuato nel rispetto della tutela degli utenti;
- verificare che i dati personali trattati attraverso determinate tecnologie (es. plugin o api) non vengano trasferiti all'interno di un Paese che non abbia sottoscritto accordi con l'UE (es. il c.d. Privacy Shield) o che non sia stato giudicato conforme in tal senso.

Nel caso in cui i punti precedentemente indicati non venissero rispettati, si raccomanda di disinstallare o sostituire il plugin o il servizio con equivalenti prodotti che dichiarino esplicitamente il rispetto dei principi definiti del Regolamento UE 2016/679 (GDPR).

Sicurezza e confidenzialità delle informazioni contenute nei database

Qualora il sito web utilizzi un database, al fine di incrementarne la sicurezza, è opportuno implementare misure di conformità alle Linee guida per lo sviluppo del software sicuro definite dall'Agid a cui si rimanda (cfr. https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro).
Al fine di certificare, in particolare, la corretta implementazione delle procedure di validazione degli input e di sicurezza menzionate in questo documento, è raccomandato l'utilizzo di appositi strumenti di stress test prima dell'avvio in esercizio dell'applicazione.
Al fine di limitare il rischio di perdita accidentale di dati personali e/o particolari immagazzinati in database non sufficientemente protetti, si suggerisce di disinstallare quelle estensioni per CMS (plugin, moduli) che consentano di salvare al loro interno informazioni e, più in generale, di ridurre allo stretto necessario l'upload sul sito di files (immagini, documenti) che potrebbero contenere dati inerenti a persone fisiche.
E' utile effettuare verifiche di Vulnerability Assessment del sito web periodicamente al fine di rilevare eventuali situazioni che rappresentano potenziali problemi di sicurezza.

Backup del sito

L'Area Tecnica Informatica e Sicurezza effettua con regolarità copie di sicurezza dei siti web ospitati sui server di Ateneo, ma non può garantire l'esistenza, l'accuratezza, la regolarità, la disponibilità dei propri servizi di backup.
Pertanto, gli amministratori di un sito web sono responsabili della realizzazione delle copie di sicurezza. A tal proposito, si rammenta che queste ultime dovranno includere:

- file del CMS
  - Installazione del core del CMS
  - Plugin del CMS

- Temi di CMS
- Immagini e file
- JavaScript e script PHP e altri file di codice
- File aggiuntivi e pagine Web statiche

- Database

Conformità dei Web form

I web form ospitati sui siti web di Ateneo devono essere conformi alle prescrizioni di cui al Regolamento UE 2016/679 in materia di protezione di dati personali. In base ai principi di necessità e pertinenza il titolare deve trattare i soli dati necessari che abbiano una stretta correlazione con la finalità che si intende perseguire (Regolamento UE 2016/679, articolo 5). Occorre quindi limitare la richiesta di dati a quelle informazioni indispensabili che siano funzionali alla finalità perseguita (minimizzazione dei dati), nel caso di un servizio di newsletter, ad esempio, è molto probabile che l'unico dato indispensabile per il raggiungimento della finalità di invio sia l'indirizzo e-mail del destinatario.
Occorre sempre fornire l'informativa secondo quanto indicato nell'art. 13 del GDPR indicando le finalità della raccolta (es. si richiede la e-mail per poter fornire, successivamente, risposta alla richiesta), esplicitando anche le modalità con cui i dati verranno trattati.
L'implementazione di web form deve sempre prevedere la presenza di una checkbox, da spuntare obbligatoriamente, attraverso cui l'utente dichiari di aver preso visione dell'informativa (da linkare) e di averne compreso la finalità, deve inoltre comprendere un sistema che consenta di "registrare" l'azione positiva che l'utente compie:

"Dichiaro di aver letto e compreso l'informativa (link)…."

Tale campo non dovrà in nessun caso essere presentato all'utente già spuntato.
All'utente deve essere garantito il diritto di opt-out tramite un apposito link riportato in ogni comunicazione, qualora decidesse di terminare del tutto il servizio o non voler più ricevere newsletter.
Al fine di evitare abusi in materia di utilizzo non autorizzato di indirizzi email da parte di utenti malintenzionati che compilino web form servendosi di email non proprie, si raccomanda di implementare un meccanismo di "double-opt-in" che preveda la possibilità, per un potenziale mittente, di confermare l'intenzione di entrare in contatto con l'Ateneo solo dopo aver cliccato sul link ricevuto in un primo messaggio di posta elettronica.
Per ulteriori informazioni sulla creazione di web form sicuri consultare le Linee guida AGID in materia di sviluppo sicuro di software.

Rimozione dei metadati dai file caricati sul sito

I files caricati sul sito web potrebbero contenere informazioni personali sull'autore del documento. Tali informazioni non sono necessarie. Si suggerisce pertanto di rimuovere dai files ogni specifico riferimento al suo autore.

Creazione di utenze

Nella creazione di apposite utenze del sito web si raccomanda in particolare di:

- eliminare le utenze di amministrazione il cui nome di login sia facilmente individuabile e/o inserito di default (es. "admin") e crearne di nuove;

- limitare i tentativi di accesso che un singolo indirizzo IP può effettuare tramite un plugin. In alternativa, valutare l'oscuramento dell'url da utilizzare per effettuare il login all'atto della creazione di utenze, assumere come regola quella del "privilegio minimo" quando si assegnano i ruoli;
- valutare la possibilità di implementare un meccanismo di autenticazione a due fattori. Qualora non fosse possibile, utilizzare password robuste (almeno 8 caratteri, formate da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente), univoche per ciascun account, forzarne la sostituzione al primo accesso e successivamente con una certa frequenza (es. 6 mesi);
- disabilitare la registrazione dell'utente se non necessaria dalla dashboard;
- eliminare le utenze non più attive per scongiurare il rischio di accessi al sito non più autorizzati o effettuati con finalità malevole.

Aggiornamento della Privacy policy del sito al nuovo Regolamento UE 2016/679

La Privacy policy del sito, in base alle disposizioni normative in materia di trattamento dei dati personali (GDPR) deve:

- essere comprensibile e facilmente raggiungibile visitando qualunque pagina del sito web. A tal proposito, si suggerisce di inserire un link ad essa nel footer;
- essere aggiornata alle disposizioni normative di cui al GDPR;
- essere linkata dai web form utilizzati per la raccolta di dati personali (web form di contatto, newsletter, commenti).
- essere sempre presente, anche quando si utilizzano solo cookies tecnici.

Al seguente link è disponibile la privacy policy del sito web di Ateneo: http://privacy.unipv.it/

Limitare le attività di profilazione di utenti dovute all'implementazione sul sito di alcuni servizi.

L'attivazione di alcuni servizi sul sito web (es.Google Analytics) o tramite esso erogati (es. video incorporati da Vimeo) comporta lo svolgimento, da parte dei gestori delle piattaforme erogatrici dei servizi "collegati" al sito, di attività di profilazione di utenti connessi al portale web. E' pertanto necessario provvedere alla loro limitazione.

Cookie tecnici, cookie analitici convertiti in tecnici e cookie non tecnici usati senza effettuare profilazione.

Nel caso in cui il sito web faccia uso di soli cookie tecnici, di cookie analitici convertiti in tecnici o di cookie non tecnici usati senza effettuare profilazione, è sufficiente indicare un riferimento ad essi nella privacy policy generale del sito e/o in un'informativa sui cookie estesa.
Se la fruizione del sito internet da parte dei suoi visitatori comporta l'installazione sui loro client dei cookie elencati in precedenza:

- non è obbligatorio comunicare tramite apposito banner (o pop up) all'utente del sito l'utilizzo di cookie;
- non è necessario richiedere agli utenti il consenso all'installazione dei cookie appartenenti alle categorie in esame (blocco preventivo dei cookie).

Permane, tuttavia, l'obbligo di indicare all'interno del sito web un riferimento alle caratteristiche dei cookie di cui esso fa uso.

UNIVERSITÀ
DI PAVIA

Convertire in cookie tecnici i cookie analitici di Google Analytics

Nel caso in cui venga utilizzato il servizio di analisi del traffico dei dati fornito da "Google Analytics", è necessario effettuare la conversione dei corrispondenti cookie analitici in cookie tecnici al fine di evitare l'immagazzinamento da parte di Google di informazioni non necessarie e consentire all'Ateneo, in questo modo, di garantire il rispetto delle vigenti disposizioni in materia di privacy e cookie.

Per ulteriori informazioni consultare il sito del Garante.

https://www.garanteprivacy.it/cookie
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3585077
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1826713

Ulteriori indicazioni

Le pagine del sito, i servizi web e i documenti su di esso pubblicati devono avere essere conformi a leggi, decreti e regolamenti vigenti. In particolare, dovranno rispettare:

- le raccomandazioni GARR Acceptable Use Policy (AUP) circa le modalità di utilizzo della rete della Ricerca;
- le norme relative alla protezione del Diritto d'Autore (ivi inclusa legge 22/5/93 n. 159, D.L. 22 marzo 2004, n. 72, e sua legge di conversione 21 maggio 2004, n. 128;
- le norme sulla Tutela legale del software (D.lgs. 518/92 e successive modificazioni);
- le norme del Codice Penale in tema di criminalità informatica;
- il D. lgs 196/2003 e ss.mm.ii e il Regolamento UE 2016/679 in materia di protezione dati personali;
- le norme sull'accessibilità applicabili a chiunque usufruisca di contributi pubblici o agevolazioni per l'erogazione dei propri servizi tramite sistemi informativi o internet (Legge n. 4/2004, D.P.R. n. 75/2005, D.M. 8 luglio 2005, D.L. n. 179/2012, Decreto 20 marzo 2013);
- le disposizioni Agid in materia di design dei siti web della Pubblica Amministrazione: https://www.agid.gov.it/it/argomenti/linee-guida-design-pa.

Informazioni di maggior dettaglio in materia di sicurezza delle piattaforme CMS possono essere reperite visitando i corrispondenti siti web ufficiali, oltre che consultando i bollettini di sicurezza emanati periodicamente dai loro curatori.
Si consiglia, altresì, di visitare il sito web dell'Open Web Application Security Project (OWASP) per reperire informazioni utili alla creazione di applicazioni internet sicure: https://www.owasp.org e di consultare le Linee guida per lo sviluppo del software sicuro Agid: www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software- sicuro.
Informazioni di maggior dettaglio in materia di conformità al c.d. GDPR delle piattaforme CMS oggetto della presente trattazione possono essere reperite visitando le pagine web create sui portali internet ad esse corrispondenti.
Ulteriori approfondimenti in merito alle ultime disposizioni in materia di trattamento dei dati personali sono pubblicate sul sito del Garante della Privacy all'indirizzo https://www.garanteprivacy.it/regolamentoue.

Le presenti linee guida saranno soggette a periodici aggiornamenti.