



Adeguare un sito WordPress al GDPR

IN POCHI SEMPLICI PASSAGGI

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

A proposito di me

- Consulente informatico forense
- Sviluppatore software e socio di Touchlabs SRLs
- Consigliere LUG di Vicenza
- Autore di alcuni strumenti open source, inclusi **RecuperaBit** per la ricostruzione di NTFS e **Carbon14** per datare le pagine web (entrambi si trovano in CAINE)



Agenda

PUNTO DI PARTENZA

Introduzione a WordPress e al GDPR

DATI DI NAVIGAZIONE

Ciò che non dobbiamo spiattellare in giro

CONTENUTI UTENTE E SICUREZZA

Come gestirli correttamente

Punto di partenza

INTRODUZIONE A WORDPRESS E AL GDPR

Cos'è WordPress?

È probabilmente il più famoso “gestore di contenuti” (CMS) disponibile sul web ed è un software libero. Tra i siti web che fanno uso di CMS, WordPress copre una quota del 65%.

Risulta molto personalizzabile con temi e plugin.

La sua configurazione di base va ritoccata leggermente, in modo da rispettare correttamente il GDPR.

Parleremo di WordPress installato su di uno spazio hosting, non del servizio offerto da WordPress.com.



GDPR

Il GDPR è la norma europea di riferimento per la protezione dei dati e la privacy, adottata nel 2016 ed entrata pienamente in vigore il **25 maggio 2018**.

Anche se alcuni la vedono come una “scocciatura”, in realtà è un importantissimo strumento che ci tutela tutti quanti. Escludendo le aziende che operano nel settore del marketing, gli adempimenti per i siti web sono più piccoli di quanto sembra.

Attenzione! Con sentenza del 16 luglio 2020, la CGUE ha dichiarato che **il Privacy Shield è incompatibile con il GDPR**, pertanto i trasferimenti di dati con gli USA non sono più giustificabili in modo così “automatico”.

Concetti chiave

- **Dati personali** → Quelli che permettono di identificare direttamente o indirettamente una persona fisica (nome e cognome, indirizzo email, indirizzo IP, ecc...)
- **Titolare del trattamento** → Chi li tratta (gestore del sito, ecc...)
- **Base giuridica** → La ragione che legittima il trattamento, che va scelta dopo attenta valutazione tra:
 - **Consenso** → Deve essere dato in modo libero, informato, specifico, inequivocabile
 - **Legittimo interesse del titolare** → Non richiede consenso ma vi è obbligo di informativa
 - *(Altre quattro basi giuridiche che non vedremo)*



Informativa sulla privacy

È il documento con il quale il titolare informa l'interessato riguardo le finalità e le modalità con cui vengono trattati i dati.

Vanno inclusi alcuni dettagli salienti, tra cui:

- Identità e contatti del titolare del trattamento
- Dati trattati e tempo di conservazione
- Finalità e base giuridica del trattamento
- Destinatari o presenza di trasferimento verso paesi terzi

L'informativa non va fatta firmare o “accettare”!

Banner per i cookie

Anche per l'utilizzo dei cookie **deve** essere rilasciata una informativa. Dobbiamo però distinguere tra:

- **Cookie tecnici** → Funzionalmente necessari a far funzionare il sito web in modo corretto
- **Cookie di profilazione** → Si usano per la pubblicità o l'analisi del comportamento dei visitatori (potrebbero addirittura essere installati da terze parti)

I cookie analitici di prima parte sono assimilabili a cookie tecnici, **perciò non va chiesto il consenso e non serve un banner!**

[HTTPS://WWW.GARANTEPRIVACY.IT/TEMI/COOKIE](https://www.garanteprivacy.it/temi/cookie)



Partiamo dalla base

Prima di vedere dei piccoli accorgimenti per configurare correttamente WordPress, dobbiamo avere come minimo:

- **HTTPS configurato correttamente** (con certificato SSL/TLS)
- **Un servizio di hosting in UE oppure in Svizzera** e gestito da un'azienda con giurisdizione nelle medesime aree geografiche

Esistono anche altri paesi considerati adeguati dall'UE.



Dati di navigazione

CIÒ CHE NON DOBBIAMO SPIATTELLARE IN GIRO

Scansione con Detective Monk

L'EDPS (European Data Protection Supervisor) ha creato il software *Website Evidence Collector* e OVH ha sviluppato una variante "batch" che permette di **scansionare tutte le pagine di un sito web** per verificare i trasferimenti di dati.

Detective Monk è un *wrapper* che abbiamo sviluppato per poter usare *website-evidence-collector-batch* in una macchina virtuale Vagrant, **senza installare manualmente nulla**.

[HTTPS://GITHUB.COM/TOUCHLABS-SRLS/DETECTIVE-MONK/](https://github.com/TouchLabs-SRLS/detective-monk/)



INDICAZIONE DELLE SITEMAP

```
workers: 4
dnt: false
firstPartyUri: 'https://lugvi.it'
urls:
  - 'https://lugvi.it'
sitemaps:
  - url: 'https://lugvi.it/wp-sitemap-posts-post-1.xml'
  - url: 'https://lugvi.it/wp-sitemap-posts-page-1.xml'
  - url: 'https://lugvi.it/wp-sitemap-taxonomies-category-1.xml'
  #- url: 'https://lugvi.it/wp-sitemap-taxonomies-post_tag-1.xml'
  - url: 'https://lugvi.it/wp-sitemap-users-1.xml'
```

<https://lugvi.it/sitemap.xml>

INTESTAZIONE DEL PRIMO REPORT

Website Evidence Collection

<https://lugvi.it>



Evidence Collection Organisation

Target Web Service	https://lugvi.it
Automated Evidence Collection Start Time	2/7/2023, 7:00:27 PM
Automated Evidence Collection End Time	2/7/2023, 7:11:46 PM
Software Version	2.0.0
Software Host	monk

Automated Evidence Collection

The automated evidence collection is carried out using the tool [website evidence collector](#) (also on [Github](#)) in version 2.0.0 on the platform Linux in version 5.4.0-89-generic. The tool employs the browser Chromium in version HeadlessChrome/93.0.4577.0 for browsing the website.

During the browsing, the tool gathers evidence and runs a number of checks. It takes screenshots from the browser to identify potential cookie banners. It tests the use of HTTPS/SSL to check whether the website enforces a HTTPS connection. Then, the evidence collection tool scans the first web page for links to common social media and collaboration platforms for statistics on the overall use of potentially privacy-intrusive third-party web services.

The analysis of the recorded traffic between the browser and both the target web service as well as involved third-party web services, and the browser's persistent storage follows in a [subsequent section](#).

Webpage Visit

On 2/7/2023, 7:00:27 PM, the evidence collection tool navigated the browser to <https://lugvi.it>. The final location after potential redirects was <https://lugvi.it/>. The evidence collection tool took two screenshots to cover the top of the webpage and the bottom.

HOST DI TERZE PARTI

First-Party Hosts

1. [lugvi.it](#)

Requests have been made to 1 distinct first-party hosts.

Third-Party Hosts

1. [fonts.googleapis.com](#)
2. [fonts.gstatic.com](#)
3. [googleads.g.doubleclick.net](#)
4. [lytimg.com](#)
5. [jnn-pa.googleapis.com](#)
6. [s.w.org](#)
7. [secure.gravatar.com](#)
8. [spagnolostefano.altervista.org](#)
9. [static.doubleclick.net](#)
10. [tile.openstreetmap.org](#)
11. [vicenza2.linux.it](#)
12. [www.google.com](#)
13. [www.gstatic.com](#)
14. [www.openstreetmap.org](#)
15. [www.youtube.com](#)
16. [yt3.ggpht.com](#)

Requests have been made to 16 distinct third-party hosts.

First-Party Web Beacon Hosts

No first-party web beacons were found.

Third-Party Web Beacon Hosts

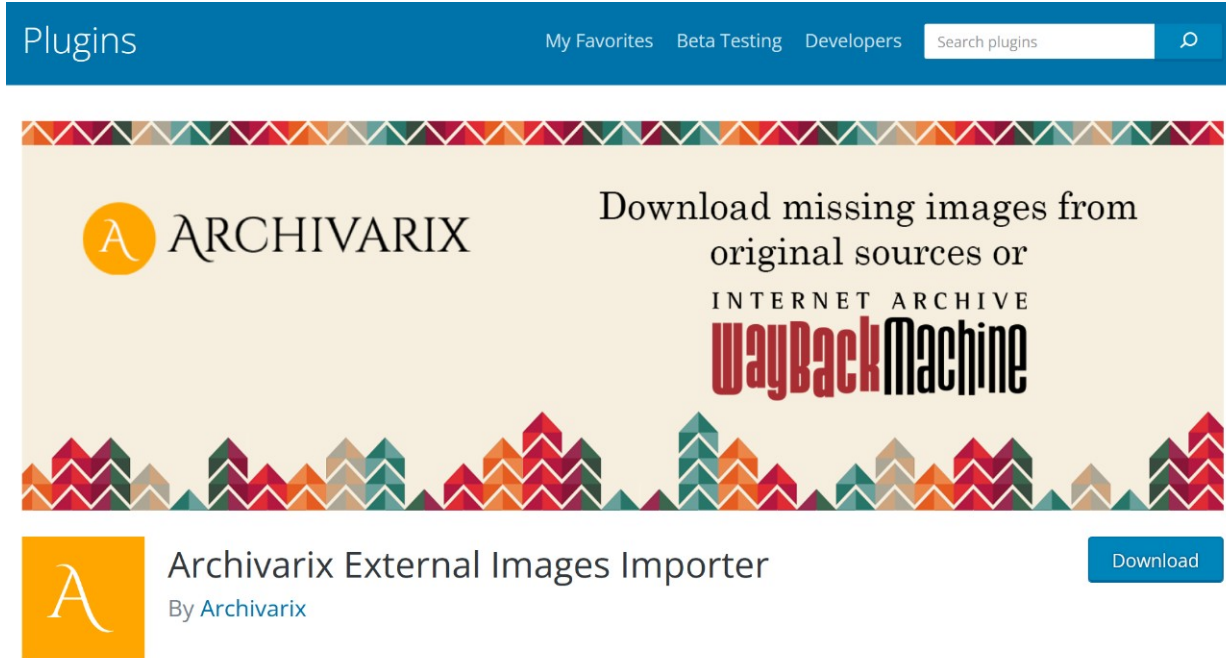
1. [www.youtube.com](#)

Potential third-party web beacons were sent to 1 distinct hosts. Corresponding HTTP requests for first- and third-parties are listed in the [Annex](#).

Web Forms with non-encrypted Transmission

No web forms submitting data without SSL encryption were detected.

IMMAGINI ESTERNE



The screenshot shows the WordPress Plugins interface. At the top is a blue header with the word 'Plugins' on the left, and links for 'My Favorites', 'Beta Testing', and 'Developers' on the right. A search bar labeled 'Search plugins' is also present. Below the header is a large promotional banner for 'Archivarix' and 'WayBack Machine'. The banner features the Archivarix logo (a yellow circle with a white 'A') and the text 'ARCHIVARIX' in a serif font. To the right, it says 'Download missing images from original sources or' followed by 'INTERNET ARCHIVE' and the 'WayBack Machine' logo in a stylized red and black font. The banner is decorated with a colorful geometric pattern of triangles at the top and bottom. Below the banner, the plugin 'Archivarix External Images Importer' is listed. It has a yellow square icon with a white 'A' and the text 'By Archivarix'. A blue 'Download' button is located to the right of the plugin name.

Plugins

My Favorites Beta Testing Developers Search plugins

ARCHIVARIX

Download missing images from original sources or

INTERNET ARCHIVE

WayBack Machine

Archivarix External Images Importer

By Archivarix

Download

Le immagini esterne possono tracciare i nostri visitatori e potrebbero sparire improvvisamente.

Usiamo **Archivarix External Images Importer** per sistamarle in modo automatico.

<https://wordpress.org/plugins/archivarix-external-images-importer/>

Emoji

Tutte le emoji dei siti WordPress vengono visualizzate come immagini fornite dal dominio **s.wp.org**, che usa un server collocato negli Stati Uniti.

Installiamo **Compressed Emoji** per fornire automaticamente le immagini dal nostro server.

[HTTPS://WORDPRESS.ORG/PLUGINS/COMPRESSED-EMOJI/](https://wordpress.org/plugins/compressed-emoji/)



Avatar

WordPress usa il servizio esterno Gravatar per mostrare le icone dei partecipanti (autori del blog e utenti che commentano).

Installiamo **Leira Letter Avatar** per generare avatar semplici e colorati a ogni utente.

Possiamo includere anche **Simple Local Avatars** se vogliamo inserire un'immagine specifica per gli autori.

[HTTPS://WORDPRESS.ORG/PLUGINS/LEIRA-LETTER-AVATAR/](https://wordpress.org/plugins/leira-letter-avatar/)

CARATTERI GOOGLE



Google Fonts

Moltissimi temi usano i caratteri di Google, ma normalmente sono caricati direttamente da server esterni.

Usiamo **Self-Hosted Google Fonts** per sistemare tutto in automatico.

<https://wordpress.org/plugins/selfhost-google-fonts/>

Pulsanti di condivisione

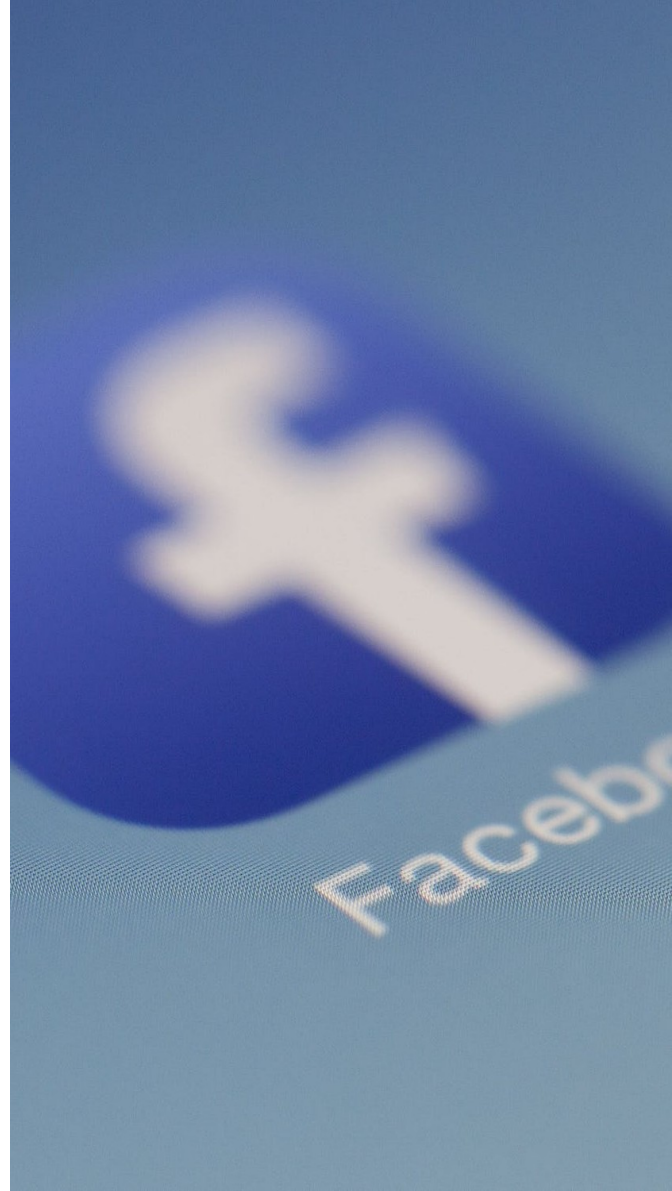
Gli script che generano i pulsanti di condivisione ufficiali dei principali social network possono tracciare le visite di ciascun utente del sito, anche se non iscritto.

Inoltre pesano decine di kilobyte, rallentando la pagina.

Installiamo **Scriptless Social Sharing** per avere pulsanti di condivisione leggerissimi e senza tracciamento.

Questo migliora *gradevolmente* il tempo di caricamento e le performance del nostro sito web!

[HTTPS://WORDPRESS.ORG/PLUGINS/SCRIPTLESS-SOCIAL-SHARING/](https://wordpress.org/plugins/scriptless-social-sharing/)

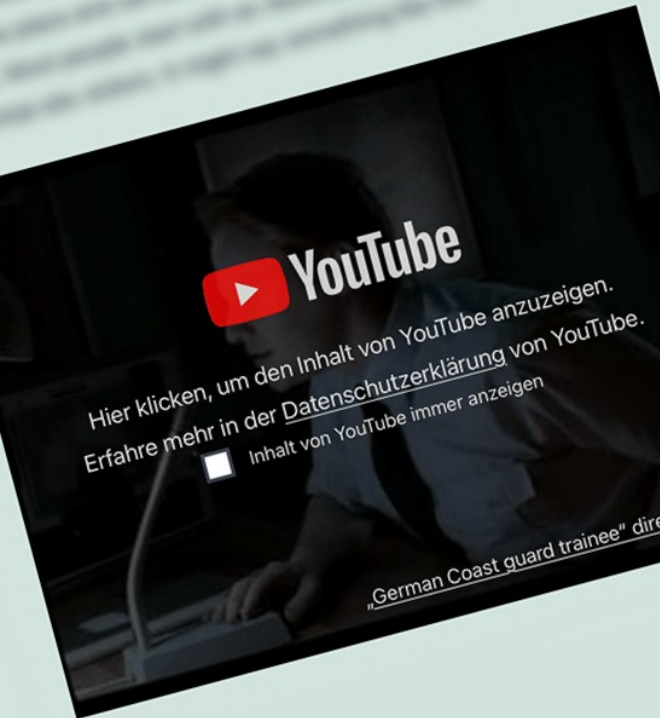


Embed di video

Anche i video (YouTube, Vimeo, eccetera) richiamano i server del gestore del servizio, inoltre rallentano il caricamento della pagina.

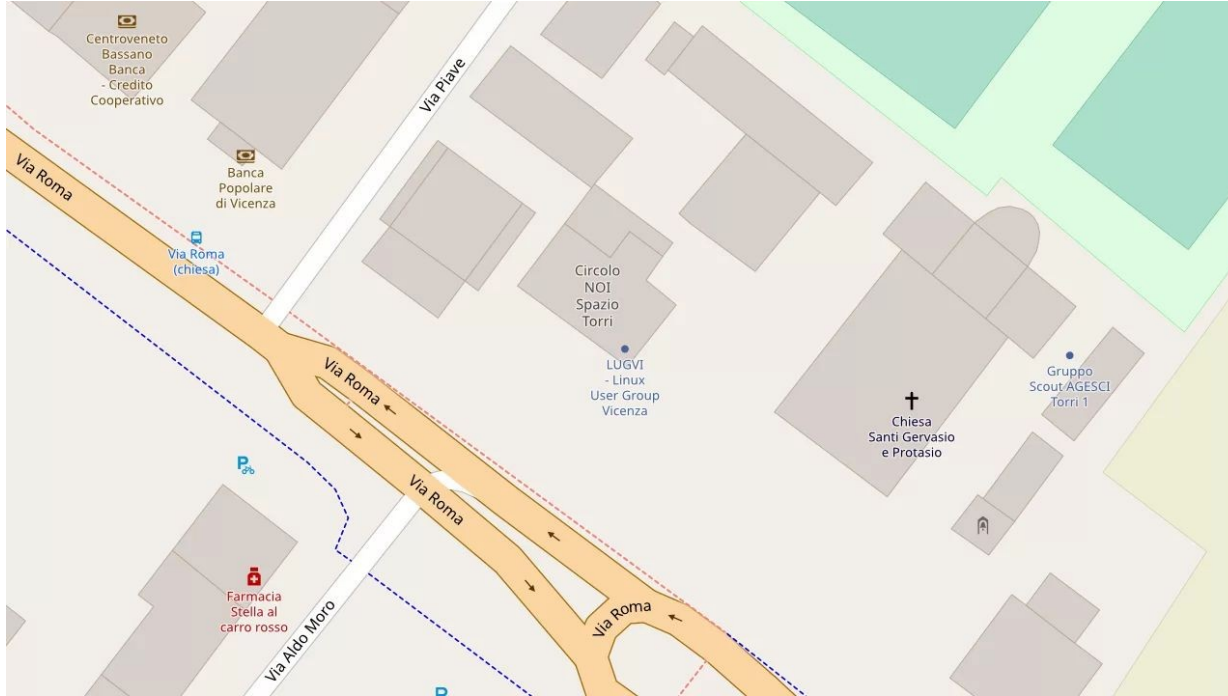
Installiamo **Embed Privacy** per inserire automaticamente un segnaposto: il contenuto si caricherà solo con il consenso esplicito dell'utente (basta un click).

Questo migliora **notevolmente** il tempo di caricamento e le performance del nostro sito web!



[HTTPS://WORDPRESS.ORG/PLUGINS/EMBED-PRIVACY/](https://wordpress.org/plugins/embed-privacy/)

MAPPE



Vale quanto detto per gli embed dei video.

Molto spesso le mappe “interattive” sono comunque piccole e scomode da usare.

Possiamo usare **un’immagine statica e un link** a un sito come Google Maps oppure OpenStreetMap.

Statistiche

Sostanzialmente **non è possibile** usare Google Analytics in modo legale in Italia (e in molti altri paesi europei).

Possiamo usare **Matomo** sia come plugin di WordPress che come applicativo web autonomo.

Impostiamo l'anonimizzazione degli IP, indichiamo il tempo massimo di conservazione e valutiamo se disattivare i cookie.



[HTTPS://WORDPRESS.ORG/PLUGINS/MATOMO/](https://wordpress.org/plugins/matomo/)

DOVE SIAMO ARRIVATI

Eventually, the evidence collection tool logged all identified web forms that potentially transmit web form data using an unencrypted connection.

First-Party Hosts

1. lugvi.it

Requests have been made to 1 distinct first-party hosts.

Third-Party Hosts

Requests have been made to 0 distinct third-party hosts.

First-Party Web Beacon Hosts

No first-party web beacons were found.

Third-Party Web Beacon Hosts

No third-party web beacons were found.

Web Forms with non-encrypted Transmission

No web forms submitting data without SSL encryption were detected.

Persistent Data Analysis

The evidence collection tool analysed persistent cookies after the browsing session. Web pages can also use the persistent HTML5 *local storage*. [The subsequent section](#) lists its content after the browsing.

Cookies linked to First-Party Hosts

No 0 first-party cookies were found.

Cookies linked to Third-Party Hosts

No 0 third-party cookies were found.

Local Storage

The local storage was found to be empty.

Annex

Previsioni e Metodi

Contenuti utente e sicurezza

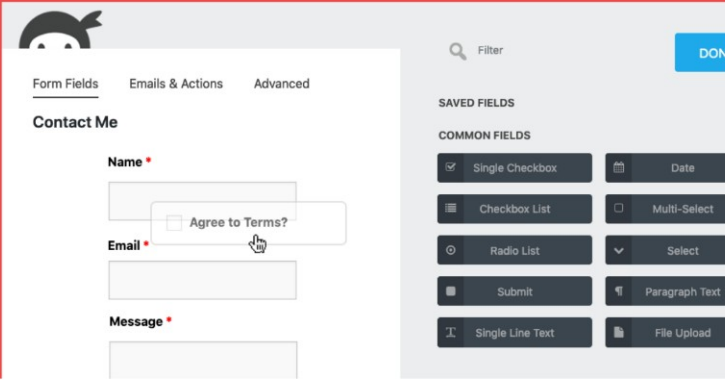

COME GESTIRLI CORRETTAMENTE


MODULI DI CONTATTO

Plugins

My Favorites Beta Testing Developers

Search plugins





Ninja Forms Contact Form – The Drag and Drop Form Builder for WordPress

By [Saturday Drive](#)

Download

Sarà sufficiente verificare che non usino servizi di terze parti (come Google Forms o Jotform) per raccogliere le richieste.

Possiamo usare plugin come **Ninja Forms** per comporre i moduli e impostare un limite di conservazione.

<https://wordpress.org/plugins/ninja-forms/>

Indirizzi IP nei commenti

Possiamo anonimizzare gli indirizzi IP nei commenti già esistenti effettuando una query:

```
UPDATE wp_comments SET comment_author_IP =  
CONCAT(SUBSTRING_INDEX(comment_author_IP, '.',3), '.0')
```

Oppure possiamo usare il plugin **Comments Advanced**, se sono pochi.

L'esempio non gestisce correttamente gli indirizzi IPv6.

SNIPPET PER I COMMENTI FUTURI

```
<?php

// Anonymize IP addresses using the new wp_privacy_anonymize_ip function,
// available in WordPress 4.9.6

if ( function_exists( 'wp_privacy_anonymize_ip' ) ) {
    add_filter( 'pre_comment_user_ip', function( $ip ) {
        return wp_privacy_anonymize_ip( $ip );
    });
}
```

<https://gist.github.com/soderlind/8e2b759e66f8cb178665745c61d72c5d>



Servizi di sicurezza e antispam

Alcuni plugin con funzionalità di sicurezza usano servizi esterni per verificare gli indirizzi email oppure gli IP.

Conviene controllare bene e rimuovere quelli che effettuano trattamenti su cui non abbiamo alcun controllo.

Per lo spam scegliamo **Antispam Bee** invece di Akismet.

[HTTPS://WORDPRESS.ORG/PLUGINS/ANTISPAM-BEE/](https://wordpress.org/plugins/antispam-bee/)


Jetpack

È un plugin piuttosto diffuso e composto da molteplici moduli. Alcuni sono totalmente innocui, altri usano (e trasmettono) i dati di navigazione degli utenti.

Vanno disattivati tutti i moduli che non si usano e vagliati quelli che invece si intende tenere:

[https://\[...\]/wp-admin/admin.php?page=jetpack_modules](https://[...]/wp-admin/admin.php?page=jetpack_modules)





*Affermare che non si è interessati al diritto alla privacy
perché non si ha nulla da nascondere
è come dire che non si è interessati alla libertà di parola
perché non si ha nulla da dire.*

EDWARD SNOWDEN

CONTATTI

Web

andrealazzarotto.com

GitHub

[Lazza](#)

Twitter

[@thelazza](#)

Mastodon

[@lazza@mastodon.social](#)

