

# **Die DSGVO in der WordPress-Praxis**

Marc Nilius

WordCamp Köln, 20. Oktober 2018



# Über mich

- Diplom-Informatiker, selbständig
- WordPress-Wartung und WordPress-Sicherheit
- @marcnilius oder @wpsicherheit
- <https://www.wp-wartung24.de>
- Organizer diverser Meetups und WordCamps





# **Schnelle DSGVO-Basics**



# DSGVO-Basics

- **In Kraft seit Ende Mai 2018**
- **Schutz personenbezogener Daten**
- **Speichern und Verarbeiten der personenbezogenen Daten generell nur nach vorheriger Einwilligung**
- **Das Übel**
  - Auch IP-Adressen sind personenbezogene Daten
  - Bei jedem Aufruf eines fremden Servers wird eine IP-Adresse technisch bedingt übertragen
- **We have to deal with it...**



# **Social Media Sharing / Embedding**



# Social Media Sharing / Embedding

- Einfache Links zu Social-Media-Angeboten sind kein Problem
- Problematisch sind nur die Share-Buttons der Anbieter selbst
- Lösungen wie insbesondere Shariff Wrapper sind unproblematisch
- Shariff: Achtung bei Erwähnung in Datenschutzerklärungen!
  - Falsche Angaben durch Datenschutzgeneratoren





# Social Media Sharing / Embedding

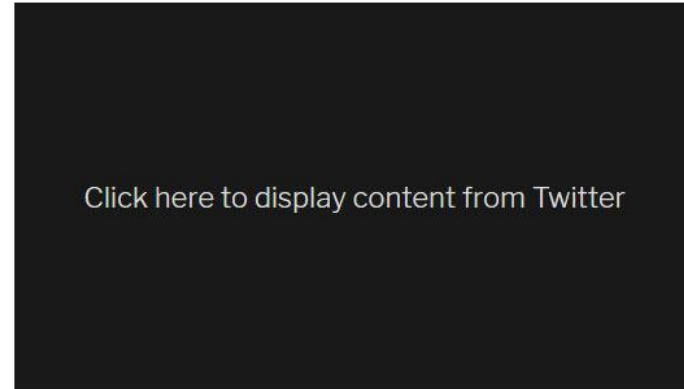
- Das Einbetten von SocialMedia-Content ist nicht erlaubt
  - Erst Einwilligung des Besuchers notwendig
- Neues Plugin „Embed Privacy“

Hier kommt ein Text mit einer Beispiel-Embed von Twitter:



Und weiter im Text...

Hier kommt ein Text mit einer Beispiel-Embed von Twitter:



Und weiter im Text...

**Google Analytics, Matomo & Co.**





# Google Analytics, Matomo & Co.

- IP-Anonymisierung! Vertrag mit Google!
- Einbindung des Google-Codes prüfen (Theme, Child-Theme, Plugin, ...)
- Opt-Out in der Datenschutzerklärung notwendig
  - Standard-Opt-Out-Link mittels JavaScript-Attribut
  - Der Opt-Out-Link wird durch den WP-Editor zerstört
  - Lösung via Shortcode notwendig
    - Plugins zB „Google Analytics Opt-Out“
  - Matomo/Piwik mit Opt-Out-Iframe
- Cookie-Banner hierfür nicht zwingend notwendig!

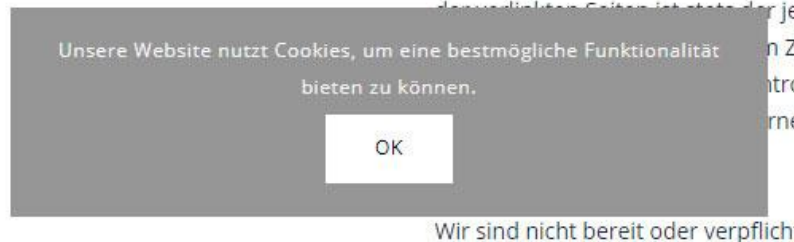


# **Cookie-Banner**



# Cookie-Banner

- Die allermeisten Cookie-Banner sind vollkommen nutzlos und nicht notwendig!
  - Banner mit reiner Info sind nutzlos
  - Nur Banner mit Opt-Out haben eine Berechtigung
  - ePrivacy-Richtlinie ggf. in 2019
  - Verdeckt der Banner den Link zum Impressum, ist dies abmahnfähig
- Für Analytics, Matomo etc. reicht Opt-Out in der DSE





# Videos



# Videos

- Wie SocialMedia-Inhalte: dürfen nur nach Einwilligung eingebunden werden
- Lösungen
  - WP Youtube Lyte, Embed Videos and Respect Privacy
  - Embed Privacy
  - Borlabs Cookies
  - Avada-Theme mit Consent-Settings
- Auch Vorschaubilder dürfen nicht direkt von Youtube geladen werden
- Lokales Speichern der Vorschaubilder kann Urheberrechtsverstoß sein



# Videos

- WP Youtube Lyte:

Also act on normal YouTube links and iframes? ☒ Ja (Standard) ☐ Nein danke.

Cache thumbnails locally? ☒ Yes. ☐ No (default).  
Having the thumbnails cached locally can improve performance and will enhance visitor privacy as by default no requests will be sent to YouTube unless the video is played.

Text to be added under every LYTE video. 

Mit Abspielen des Videos stimmen Sie einer Übertragung von Daten an Youtube zu. Bitte beachten Sie die [Datenschutzerklärung](/datenschutz)

  
If you want to add e.g. a privacy disclaimer under every LYTE embedded video, you can do so here. Some HTML is allowed. Simply leave empty not to show anything.

Den Zwischenspeicher von WP YouTube Lyte leeren ☐



# Videos

**IMPORTANT NOTE:** The options in this section will help to easier comply with data privacy regulations, like the European GDPR. When the "Privacy Consent" option is used, Avada will create a cookie with the name "**privacy\_embeds**" on user clients browsing your site to manage and store user consent to load the different third party embeds and tracking scripts. You may want to add information about this cookie to your privacy page.

## Google Fonts Mode

When set to "Local", the Google fonts set in Theme Options will be downloaded to your server. Set to "CDN" to use the Google CDN.

Local ☒ CDN ☐

## Privacy Consent

Turn on to prevent embeds and scripts from loading until user consent is given.

An ☒ Aus ☐

## Privacy Consent Cookie Expiration

Controls how long the consent cookie should be stored for. In days.

30



## Privacy Consent Types

Select the types of embeds which you would like to require consent.

☒ YouTube ☒ Vimeo ☒ SoundCloud ☒ Facebook ☒ Flickr  
☒ Twitter ☒ Google Maps

**Google Maps / Open Street Map**



# Google Maps / Open Street Map

- Auch hier: Einbindung nur nach Einwilligung
- Maps-Plugins mit GDPR-Funktionen:
  - WP Google Maps
  - MapPress
  - Borlabs Cookies
- Theme
  - Avada mit integrierter Zustimmungsfunktion
- Achtung: Google Maps lädt Google Fonts nach
  - => deswegen müssen bei Maps-Nutzung auch Google Fonts in der Datenschutzerklärung erwähnt werden
- Prinzipiell gilt dies alles ebenso auch für Open Street Map
  - OSM-Nutzung nach Brexit könnte problematisch sein





# **Google Fonts**



# Google Fonts

- Auch hier: Einbindung nur nach Einwilligung
- Häufiges Argument „berechtigtes Interesse“ ist falsch
  - Nur mit Opt-Out-Möglichkeit
  - Berechtigtes Interesse wird meist verneint, da lokale Implementierung möglich ist
- Häufig Anpassung über Child-Theme empfohlen
- Viele Themes und Plugins verwenden nicht WP-konformen Weg der Einbindung
  - Anpassung schwierig bis unmöglich



# Google Fonts

- Plugin „Self-hosted Google Fonts“

Important Info About Self-Hosted Fonts

Once Processing is enabled, the plugin will scan for Google Fonts on your site and download them to your server. Your visitors will then get these fonts from your server. These fonts are downloaded from [fonts.gstatic.com](https://fonts.gstatic.com) and have [opensource licenses](#) (SIL v1.1 or compatible).

Enable Processing	<input type="button" value="Yes, Enable"/>	<small>Once this is enabled, fonts will be served from your server.</small>
Disable for Admins	<input type="checkbox"/>	<small>Disable processing for logged in admin users or any user with capability "manage_options". (Useful if using a pagebuilder that conflicts)</small>
Process Enqueues	<input checked="" type="checkbox"/>	<small>Process properly enqueued Google Fonts. This should be enough for most themes and plugins.</small>
Process CSS Files	<input checked="" type="checkbox"/>	<small>Scan all local CSS files in HTML. Use if processing enqueue is not enough for your themes and plugins. Has slight performance impact - best used with cache plugins.</small>
Process Inline CSS	<input checked="" type="checkbox"/>	<small>Scan all inline CSS. Has slight performance impact - best used with cache plugins.</small>
Protocol Relative URLs	<input checked="" type="checkbox"/>	<small>Use protocol-relative URLs for generated CSS files. This can fix issues with a partial SSL move such as CloudFlare where the backend is actually on HTTP.</small>

- Themes:
  - Avada hat auch „self-hosted“-Funktion
  - Enfold: Upload von Custom Fonts



# Google Fonts

- Achtung: Enfold und Self-Hosted Google Fonts mögen sich nicht

```
<!-- google webfont font replacement -->

<script type='text/javascript'>
if(!document.cookie.match(/aviaPrivacyGoogleWebfontsDisabled/)){
  (function() {
    var f = document.createElement('link');

    f.type = 'text/css';
    f.rel = 'stylesheet';
    f.href = '//fonts.googleapis.com/css?family=Open+Sans:400,600';
    f.id = 'avia-google-webfont';

    document.getElementsByTagName('head')[0].appendChild(f);
  })();
}
</script>
```

# **Formulare und Kommentare**



# Formulare und Kommentare

- Formular sollte Hinweis haben auf die Verarbeitung der eingegebenen Daten
- Gilt auch für das Kommentar-Formular
  - Möglich mittels Filter „comment\_form\_defaults“
  - Abhängig vom Theme nicht immer möglich

Schreibe einen Kommentar

Deine E-Mail-Adresse wird nicht veröffentlicht. Erforderliche Felder sind mit \* markiert.

**Kommentar**

Mit Absenden des Formulars stimmen Sie der Speicherung und Verarbeitung Ihrer darin eingegebenen personenbezogenen Daten zu. Weitere Informationen dazu finden Sie in unserer Datenschutzerklärung.

**Name \***

**E-Mail \***

**Website**

**Kommentar abschicken**



# Formulare und Kommentare

- Kommentare
  - IP-Adressen der Einträge löschen, ggf. zeitversetzt
  - Zeitversetztes Löschen wegen rechtlichen Problemen (Beweise) ggf. erlaubt
  - Beispiel-Plugins:
    - Remove IP (löscht sofort)
    - Remove Comments IP (löscht nach 2 Monaten)





# **Gravatar und Emojis**



# Gravatar und Emojis

- Gravatar ist in WP standardmässig aktiv
- Sendet Benutzer- und Kommentatordaten an externen Server in den USA
- In den Einstellungen deaktivieren
- Bei Bedarf Plugin „Avatar Privacy“ nutzen für Nutzer-Zustimmung  
=> Gravatar in DSE erwähnen

Name \*

E-Mail \*

Website

☐ Display a Gravatar image next to my comments.

**Kommentar abschicken**



# Gravatar und Emojis

- Emojis: Fallback-Grafiken für alte Browser werden von amerikanischem Server geladen
- Neuere Browser haben Emoji-UTF8-Support und nutzen diese Grafiken erst gar nicht
- Per Plugin oder Snippet deaktivieren
  - Plugin: „Disable Emojis“



**Plugins: Jetpack, Sicherheitsplugins, ...**





# Plugins: Jetpack, Sicherheitsplugins, ...

- Jetpack enthält einige problematische Funktionen
  - Brute-Force-Login-Schutz
  - Besucherstatistiken
  - Social Counts
- Sicherheitsplugins
  - Brute-Force-Login-Schutz in Wordfence, iThemes Security
  - Protokollierung der IPs in Security-Logs (Firewalls, ....)
- Interner Like-Counter
  - Protokollierung der IP-Adressen gegen betrügerisches Liken



# **SSL-Verschlüsselung**



# SSL-Verschlüsselung

- DSGVO fordert Maßnahmen zur Sicherung der personenbezogenen Daten auf dem aktuellen Stand der Technik (siehe auch IT-Sicherheitsgesetz)
- Dazu gehört unumstritten die SSL-Verschlüsselung der Website
  - Kostenlose Let's-Encrypt-Zertifikate
- Aber: auch Transportverschlüsselung des Mailversands!
  - Plugins: WP Mail SMTP, Easy WP SMTP, ...



# **Datenschutzerklärung**





# Datenschutzerklärung

- Website-Betreiber wollen keinen Anwalt beauftragen
- Verwendung von Datenschutzgeneratoren
- Fragen der Haftung für Dienstleister
  - Aufgrund der technischen Fragen wird der Generator durch den Dienstleister bedient
  - Wer haftet bei fehlerhafter Bedienung?
  - Wer kontrolliert Änderungen der Rechtslage / Aktualisierungen der Generatoren?



# **Vertrag zur Auftragsverarbeitung**



# Vertrag zur Auftragsverarbeitung

- Notwendig mit
  - Dem Hoster
  - Dem WordPress-Dienstleister (bei laufender Betreuung)
  - Ggf. weiteren Dienstleistern (SEO-Agentur, ...)
  - Tracking-Dienstleistern: Google Analytics, ...
  - Jedem Anbieter, dessen Inhalte als Embeds eingefügt werden (sofern dies ohne explizite Einwilligung des Besuchers geschehen soll)
- Für den Abschluss dieser Verträge ist der Website-Betreiber verantwortlich
  - Und nicht der Dienstleister...



# Vielen Dank!

Zeit für Fragen und Diskussion!

Vortragsfolien auch unter  
<https://www.marcnilius.de>

Marc Nilius  
@marcnilius / @wpsicherheit  
<https://www.wp-wartung24.de>

