Privacy Check

For WordPress Sites

Website owner:	MUSTERMANN
Website URL:	https://www.example.com
Contact:	E-Mail oder Slack Adresse
Audit date:	2022-10-05

Disclaimer: This document was not created or reviewed by a lawyer, and is no legal advice. The following details are designed to help you minimize the risks for legal steps taken against you, as a website owner. However, the recommended measures are no guarantee against warnings.

🧐 1. Audit

This audit lists all services and technologies that are relevant for GDPR/CCPA laws.

A) Technology

• WordPress version?	✅ 6.0.2
• PHP version?	⚠️ n/a
• SSL certificate?	✅ Yes
• WP Theme and version?	✅ Divi 4.18.0
• Are plugins outdated?	⚠️ n/a

Für kompletten Technik-Review brauche ich den Bericht von wp-admin > Werkzeuge > Webseiten-Zustand; erster Eindruck ist aber sehr gut.

B) Third-Party Cookies

Cookies and localStorage entries that are generated by external scripts.

Cookies found

- ⚠️ Google Analytics
- ⚠️ Google Tag Manager

⚠️ Keine Zustimmung für Google Analytics

C) External Services

Google Fonts

Loading fonts from Google's servers requires a consent *before* loading them.

⚠️ Es werden Google Fonts geladen

ReCaptcha

User must consent before ReCaptcha is loaded. Reason: ReCaptcha loads the "Roboto" font from Google's servers.

✅ Kein ReCaptcha

CDNs

Talk to the owner and make sure they have a data processing agreement. Also check the servers geographical locations.

✅ Kein CDN

Iframes, Videos, Maps

Using an iframe to show external content on a website is identical to redirecting the visitor to that website. Therefore, consent must be collected before embedding any third-party element via an iframe.

Most video platforms, such as YouTube, load the video inside an

iframe. Therefore, consent must be collected before displaying such a video.

✅ Keine Iframes, Videos, oder Maps

Social Share

Social share buttons must be loaded after consent.

Note, that only **share buttons** are affected. Simple links to a social media platform, like a LinkedIn page, do not require any change.

✅ Keine “Teilen” Buttons

D) Data collection

Review section “5 Notes” *for critical details.*

Contact Forms

- Do contact form ask for *non-essential* personal data?

✅ Keine Kontaktformulare

Comments

- Login required before comment?
- Personal data (like email) required?
- Are comment cookies set?
- Is the user's IP address tracked?

✅ Keine Kommentarfunktion

Other Forms

- Is *non-essential* personal data collected?

✅ Keine sonstigen Formulare

User Registration

- Can users register an account on the website? If yes, additional data control options need to be present

> ✅ Keine Account-Erstellung nötig

Web shop

- Can visitors complete a checkout with payment on the website? If yes, additional data control options need to be present.
- B2C shops also require “Terms Of Services”

> ⚠️ Ja, WooCommerce vorhanden
> ⚠️ Die AGB für den Shop fehlen

Data Control

- Can visitors request and erase their data?

> ⚠️ WooCommerce Kunden haben keine Datenkontrolle

🤝 2. Consent

Details about the Cookie Consent banner.

There are two levels of consent that is possible:

1. A **consent banner** is required for GDPR-relevant actions that happen automatically on page-load, for example requesting a Google font, adding a Facebook pixel or other analytics tag.
2. Before transferring non-essential personal data, a consent must be collected. A typical case is asking for the user's name in a newsletter subscription form (to send newsletters, you only need an email address, the name is non-essential for this).

Side note: A consent banner is a gray area, as most consent tools do not fully cover all GDPR requirements. Still, they solve most issues and help to prove that the website owner takes privacy seriously.

The best option is, to remove external requests and cookies.

⚠️ Fehlende Zustimmung: Google Analytics

ℹ️ 3. Information

A) Privacy Policy

- Check, if the privacy policy covers all aspects.
- The privacy policy must be available from any other page with a single click. That link must be visible to every visitor - when the link is hidden behind the consent banner or in a sub-menu (esp on mobile), it can risk a warning.

⚠️ Info zu Zahlungsanbietern fehlt

⚠️ Keine Möglichkeit der Datenauskunft

B) Imprint (DE/AT/CH)

- The imprint must be present when the website owner is a resident of Germany, Austria or Switzerland.
- When a VAT-Number or trade register entry exists, it must be included here.

✅ Impressum ist vollständig und richtig verlinkt

C) Other pages

- Terms of Service are required for all B2C shops.

⚠️ Keine AGB für den WooCommerce Shop vorhanden

👉 4. Recommendations

Allgemein

- ☐ Google Fonts lokal einbetten
- ☐ Datenschutzerklärung aktualisieren – v.a. Google Fonts*, Google Analytics*, Datenauskunft, PayPal

Google Analytics

- ☐ Option 1: DSGVO-konforme Lösung verwenden
  - GTM Code entfernen
  - Neues Tracking Plugin einrichten
  - Datenschutzerklärung: Google Analytics entfernen
- ☐ Option 2: GA erst nach Zustimmung laden
  - Cookie Banner einbauen
  - GTM Code anpassen (erst nach Zustimmung laden)
  - Datenschutzerklärung: Zustimmungs-Details

WooCommerce

- ☐ Datenschutzerklärung erweitern
  - Formular für Datenauskunft/-löschung anbieten
  - Details zu Zahlungsanbietern ergänzen (PayPal)
- ☐ AGB erstellen