

GDPR Compliance Report

example-company.com

Good Compliance



COMPLIANCE SCORE

5

ISSUES TO
ADDRESS

2

HIGH
PRIORITY

2

MEDIUM
PRIORITY

"Sitzungs-Cookies werden vor der Einwilligung gesetzt; das Recht auf Beschwerde bei einer Aufsichtsbehörde fehlt in der Datenschutzerklärung"

Executive Summary

Dies ist ein Musterbericht

Diese PDF zeigt die Struktur und den Detailgrad, den Sie nach dem Kauf eines detaillierten DSGVO-Compliance-Berichts erhalten. Die hier gezeigten Ergebnisse stammen von einer anonymisierten Beispiel-Website und stellen nicht Ihre eigene Website dar.

Die Website verfügt über solide technische Grundlagen — einwilligungsgesteuertes Tracking, HTTPS und ordnungsgemäße Formularverarbeitung — jedoch enthält die Datenschutzerklärung wesentliche Lücken, darunter fehlende Informationen zur Aufsichtsbehörde, implizierte Einwilligungssprache und unvollständige Angaben zu Betroffenenrechten.

2 High Priority

2 Medium Priority

1 Low Priority

95

PROJECTED SCORE

Fixing these 5 issues could bring your score from 72 to ~95

Address the high-priority items first — they have the greatest impact on your compliance score and carry the most regulatory risk.

What you're doing well

✓ **Cookie-Banner vorhanden**

Ein Cookie-Einwilligungsbanner wird den Besuchern angezeigt.

✓ **Sprachpräferenz-Cookie vor Einwilligung gesetzt**

Sprachpräferenz-Cookies sind technisch notwendig für die Seitenfunktionalität und erfordern keine vorherige Einwilligung.

✓ **Sitzungs-Cookie vor Einwilligung gesetzt**

Sitzungs-Cookies sind für den Grundbetrieb der Website zwingend erforderlich (z.B. Warenkorb, Login) und von der Einwilligungspflicht ausgenommen.

✓ **Einwilligungssteuerung von Drittanbieter-Trackern**

Die Website verwendet einen Einwilligungsverwaltungsansatz, der Drittanbieter-Tracker bis zur Einwilligung blockieren soll — eine gute Praxis, die regelmäßig geprüft werden sollte.

✓ **Formular mit geringer Sensitivität (GET-Methode, keine personenbezogenen Daten)**

Ein Such- oder Filterformular mit GET erfasst keine E-Mail, Telefon- oder Namensdaten — geringes Risiko, keine Einwilligungs-Checkbox erforderlich.

Aktionsplan

⚡ Start here — 3 quick wins under 15 minutes

- Recht auf Beschwerde bei einer Datenschutzbehörde ergänzen Easy (5 minutes)
- Implizierte Einwilligungsformulierungen entfernen Easy (5 minutes)
- Alle Betroffenenrechte einzeln auflühren Easy (15 minutes)

Recht auf Beschwerde bei einer Datenschutzbehörde ergänzen

HIGH

Die Datenschutzerklärung enthält keinen Hinweis auf das Recht des Nutzers, eine Beschwerde bei einer Aufsichtsbehörde einzureichen. Dies ist eine Pflichtangabe nach Art. 13 Abs. 2 lit. d DSGVO und wurde im überprüften Text nicht gefunden.

🕒 Easy (5 minutes) 📈 Medium impact 👤 Website owner 📖 Art. 13(2)(d) + Art. 77 GDPR

WHY IT MATTERS

GDPR Art. 13(2)(d) requires every Privacy Policy to inform users of their right to lodge a complaint with a data protection supervisory authority. This is a mandatory disclosure with no exceptions — even if you process very little data. Regulators take note of its absence as it suggests incomplete awareness of GDPR transparency obligations.

HOW TO FIX IT

1. Open your Privacy Policy.
2. In your 'Your Rights' section (or a separate section), add information about the right to complain to a DPA.
3. Name the relevant supervisory authority for your country.
4. Include the authority's website URL.

COPY-READY TEXT

You have the right to lodge a complaint with the data protection supervisory authority in your country. In the EU/EEA, you can find your local authority at: https://edpb.europa.eu/about-edpb/about-edpb/members_en

[If based in a specific country, also include: In [Country], the relevant authority is [Authority Name] – [website URL].]

Verhindern Sie, dass Cookies vor der Einwilligung gesetzt werden

HIGH

Der Scan hat festgestellt, dass Cookies auf dem Gerät des Besuchers gesetzt werden, bevor er mit dem Einwilligungsbanner interagiert hat. Sitzungs- und Sprachpräferenz-Cookies sind ausgenommen, aber mindestens ein nicht notwendiges Cookie wird direkt beim Seitenaufruf gesetzt.

🕒 Advanced (1–2 hours)

📊 High impact

👤 Developer

🇪🇺 Art. 6(1)(a) GDPR · ePrivacy Directive Art. 5(3)

WHY IT MATTERS

GDPR Art. 6 and the ePrivacy Directive require that non-essential cookies are only placed after the user has given freely given, specific, informed and unambiguous consent. Cookies firing before the consent choice is made means personal data is being processed without a lawful basis — even if a banner exists.

HOW TO FIX IT

1. Open your CMP settings and ensure all non-essential cookie categories default to DENIED.
2. Check that each non-essential script is wrapped or blocked by the CMP — not just listed.
3. Look for any hardcoded `<script>` tags in your site template that load analytics or marketing tools directly; these bypass CMPs.
4. Move those scripts into your CMP's script manager so they are controlled by the consent state.
5. Test: open Incognito → open DevTools → Application → Cookies. Only strictly necessary cookies (session, CSRF, language) should appear before you accept.

TECHNICAL IMPLEMENTATION

WordPress

1. In your CMP plugin (Complianz, CookieYes, Borlabs), go to Settings → Cookie Scan.
2. Ensure your analytics plugin (e.g. Site Kit, MonsterInsights) is listed and set to a non-necessary category.
3. In Complianz: go to Integrations and check that Google Analytics / other tools show 'Managed' status.

Shopify

1. Go to Online Store → Themes → Edit Code → theme.liquid.
2. Remove any analytics scripts hardcoded in the `<head>`. Instead, add them via your CMP's script injection.
3. If using Google & YouTube Sales Channel, enable Google Consent Mode in the app settings.

Implizierte Einwilligungsformulierungen entfernen

MEDIUM

Die Erklärung enthält Formulierungen, die nahelegen, dass die bloße Nutzung der Website als Einwilligung gilt. Diese Form der implizierten Einwilligung ist nach Erwägungsgrund 32 der DSGVO ungültig.

 Easy (5 minutes)  Medium impact  Website owner

 Art. 7 GDPR · Recital 32 · EDPB Guidelines 05/2020

WHY IT MATTERS

Phrases such as 'by using this website you agree to our Privacy Policy' or 'continued use of this site constitutes consent' are explicitly prohibited as a valid consent mechanism under GDPR (Recital 32, Art. 7). The EDPB guidelines state that consent must be a clear affirmative action — passive behaviour (browsing a website) does not qualify. Using this language creates a false sense of legal cover while providing none.

HOW TO FIX IT

1. Open your Privacy Policy and search for any variation of 'by using this site you agree' or 'continued use constitutes consent'.
2. Remove this language entirely.
3. Replace with a truthful statement of your lawful bases — e.g. 'We process data as described in this policy on the basis of consent (for cookies and marketing), contract (for purchases), and legitimate interest (for site security).'
4. Ensure consent for cookies is obtained via your banner, not via website usage.

COPY-READY TEXT

We process your personal data in accordance with this Privacy Policy. Depending on the purpose, we rely on the following legal bases: your consent (Art. 6(1)(a) GDPR) for cookies and marketing communications; performance of a contract (Art. 6(1)(b) GDPR) for order processing; and our legitimate interests (Art. 6(1)(f) GDPR) for security and fraud prevention.

Alle Betroffenenrechte einzeln auflisten

MEDIUM

Die Datenschutzerklärung erwähnt Betroffenenrechte nur allgemein. Eine vollständige Auflistung der DSGVO-Rechte (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Einschränkung, Widerspruch) fehlt oder ist unvollständig.

🕒 Easy (15 minutes)

📈 High impact

👤 Website owner

📖 Art. 13(2)(b) + Art. 15–21 GDPR

WHY IT MATTERS

GDPR Art. 13(2)(b) requires you to inform users of all their data subject rights: access (Art. 15), rectification (Art. 16), erasure (Art. 17), restriction (Art. 18), portability (Art. 20), and objection (Art. 21). These rights must be actively communicated — it is not sufficient to have a vague 'contact us' note. Failure to disclose rights is one of the most commonly cited gaps in DPA audits.

HOW TO FIX IT

1. Open your Privacy Policy.
2. Add (or expand) a section titled 'Your Rights' or 'Your Data Protection Rights'.
3. List each right individually with a brief plain-language explanation.
4. Provide a clear way for users to exercise their rights (email address or form).
5. State the response timeframe (GDPR requires a response within 30 days).

COPY-READY TEXT

You have the following rights regarding your personal data:

- Right to access: You can request a copy of the personal data we hold about you.
- Right to rectification: You can ask us to correct inaccurate or incomplete data.
- Right to erasure ('right to be forgotten'): You can request deletion of your data in certain circumstances.
- Right to restrict processing: You can ask us to limit how we use your data.
- Right to data portability: You can request your data in a machine-readable format.
- Right to object: You can object to processing based on legitimate interest or for direct marketing.

To exercise any of these rights, please contact us at: [your@email.com]. We will respond within 30 days.

Datenschutzfreundliches Analyse-Tool in Betracht ziehen

LOW

Ein Analyse-Skript eines Drittanbieters zur Verhaltensanalyse wurde erkannt. Der Wechsel zu einem cookiefreien Tool wie Plausible oder selbst gehostetem Matomo würde die Einwilligungspflicht für Analyse-Cookies vollständig entfallen lassen.

 Medium (30 minutes)  Low impact  Developer  Art. 5(1)(c) GDPR (data minimisation principle)

WHY IT MATTERS

Traditional analytics tools (Google Analytics, Adobe Analytics) collect detailed personal data and transfer it to servers outside the EU, requiring consent and complex data processing agreements. Privacy-friendly alternatives (Plausible, Fathom, Matomo self-hosted) collect only aggregated, anonymous data — eliminating the need for an analytics consent prompt entirely, simplifying your compliance posture, and reducing data exposure.

HOW TO FIX IT

1. Evaluate privacy-friendly alternatives: Plausible (cloud, no cookies, no personal data), Fathom (cloud, GDPR-compliant by design), Matomo (self-hostable, full control).
2. Sign up for the chosen tool and add its tracking snippet to your site.
3. Remove the existing analytics tool's script tag from your site.
4. Update your Privacy Policy to reflect the new analytics approach.
5. If switching to Plausible or Fathom: remove the analytics category from your consent banner entirely — no personal data means no consent required.

COPY-READY TEXT

This website uses Plausible Analytics, a privacy-friendly analytics tool that collects no personal data and uses no cookies. No consent is required for this analytics. [Privacy Policy of Plausible Analytics: plausible.io/privacy]

TECHNICAL IMPLEMENTATION

Plausible Analytics

1. Sign up at plausible.io and add your domain.
2. Add the snippet to your site: `<script defer data-domain="yourdomain.com" src="https://plausible.io/js/script.js"></script>`
3. Remove your existing Google Analytics or other analytics script.
4. No cookie banner needed for Plausible — it is cookieless by design.

Matomo (self-hosted)

1. Download Matomo from matomo.org and install on your own server.
2. In Matomo → Administration → Privacy → enable 'Anonymise IP'.
3. Enable 'Do Not Track support' and 'Users can opt-out from tracking'.
4. Add the tracking code to your site. With full anonymisation, consent may not be required.

MUSTERBERICHT

Detailed Findings

Cookie & Einwilligung

3 passed

1 failed

1 info

- ✓ **Cookie-Banner vorhanden**
Ein Cookie-Einwilligungsbanner wird den Besuchern angezeigt.
- ✓ **Sprachpräferenz-Cookie vor Einwilligung gesetzt**
Sprachpräferenz-Cookies sind technisch notwendig für die Seitenfunktionalität und erfordern keine vorherige Einwilligung.
- ✓ **Sitzungs-Cookie vor Einwilligung gesetzt**
Sitzungs-Cookies sind für den Grundbetrieb der Website zwingend erforderlich (z.B. Warenkorb, Login) und von der Einwilligungspflicht ausgenommen.
- ✗ **Tracking- oder funktionale Cookies vor Einwilligung geladen**
Trotz Banner erkannte der Scan, dass Cookies gesetzt werden, bevor der Nutzer mit dem Einwilligungsmechanismus interagiert hat — dies verstößt gegen die DSGVO-Anforderung zur vorherigen, freiwilligen Einwilligung.
- ! **Einwilligungsmechanismus vorhanden und sperrt Tracker**
Tracker werden durch das Einwilligungstool grundsätzlich blockiert, aber das vorzeitige Cookie-Setzen untergräbt die Wirksamkeit dieser Sperre.

Tracking & Analyse

1 passed

1 failed

2 info

- ! **Drittanbieter-Tracking-Pixel erkannt**
Ein Drittanbieter-Tracking-Pixel ist vorhanden; es scheint einwilligungsgesteuert zu sein, der Einwilligungsmechanismus muss jedoch verifiziert werden.
- ! **Verhaltensanalytik-Skript geladen**
Ein Analyseskript ist auf der Seite geladen; es sollte erst nach Nutzereinwilligung aktiviert werden, da es Verhaltensdaten erfasst.
- ✗ **Datenschutzfreundliche Analyse verwendet**
Kein datenschutzfreundliches Analyse-Tool (wie Plausible oder selbst gehostetes Matomo) wird verwendet; die aktiven Analysedienste erfordern Einwilligung und tragen ein höheres DSGVO-Risiko.
- ✓ **Einwilligungssteuerung von Drittanbieter-Trackern**
Die Website verwendet einen Einwilligungsverwaltungsansatz, der Drittanbieter-Tracker bis zur Einwilligung blockieren soll — eine gute Praxis, die regelmäßig geprüft werden sollte.

Datenerfassung

3 passed

- ✓ **Formular mit geringer Sensitivität (GET-Methode, keine personenbezogenen Daten)**
Ein Such- oder Filterformular mit GET erfasst keine E-Mail, Telefon- oder Namensdaten — geringes Risiko, keine Einwilligungs-Checkbox erforderlich.
- ✓ **Formular mit hoher Sensitivität (POST-Methode, erfasst Name und E-Mail)**
Das Kontakt- oder Newsletter-Formular verwendet POST (korrekt für sensible Daten) und erfasst Name und E-Mail-Adresse.
- ✓ **Einwilligungs-Checkbox bei sensitivem Formular**
Das sensitive Formular enthält eine Einwilligungs-Checkbox — gute Praxis zur Unterstützung einer gültigen Rechtsgrundlage für die Verarbeitung.

Datenschutzutzerklärung

5 passed

2 failed

3 info

- ✓ **Datenschutzutzerklärung vorhanden und zugänglich**
Eine öffentlich zugängliche Datenschutzerklärung ist auf der Website verfügbar.
- ✓ **Identität des Verantwortlichen und Kontaktdaten angegeben**
Die Erklärung benennt den Verantwortlichen und stellt Kontaktinformationen bereit.
- ✓ **Verarbeitungszwecke und Rechtsgrundlagen angegeben (Art. 6 DSGVO)**
Die Erklärung erläutert die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, einschließlich Einwilligung und Vertragserfüllung.
- ✓ **Empfänger der Daten benannt**
Die Erklärung nennt Zahlungs-, Hosting-, Analyse- und operative Dienstleister, die an der Datenverarbeitung beteiligt sind.
- ✓ **Aufbewahrungsfristen angegeben**
Konkrete Aufbewahrungsfristen sind für mehrere Kategorien personenbezogener Daten definiert.
- ! **Betroffenenrechte abgedeckt (Art. 15-21 DSGVO)**
Einige DSGVO-Rechte werden erwähnt, aber Auskunft, Datenübertragbarkeit, Berichtigung und Löschung sind nicht klar einzeln aufgeführt.
- ! **Recht auf Widerruf der Einwilligung erwähnt**
Die Erklärung verweist auf den Widerruf der Einwilligung, macht aber nicht klar, dass Nutzer diese jederzeit widerrufen können.
- ✗ **Recht auf Beschwerde bei einer Aufsichtsbehörde**
Die Erklärung erwähnt nicht das Recht des Nutzers, eine Beschwerde bei einer Datenschutz-Aufsichtsbehörde einzureichen.
- ✗ **Implizierte Einwilligungssprache**
Die Erklärung impliziert, dass die weitere Nutzung der Website einer Zustimmung gleichkommt — dies ist keine gültige DSGVO-Einwilligung.
- ! **Internationale Datentransfers und Schutzmaßnahmen offengelegt**
Internationale Datentransfers können stattfinden, die Erklärung erläutert die verwendeten Schutzmaßnahmen jedoch nicht klar.

Technische Sicherheit

2 passed

✓ HTTPS aktiviert

Die gesamte Website wird über HTTPS bereitgestellt, wodurch Daten während der Übertragung verschlüsselt sind.

✓ Sensitives Formular verwendet POST-Methode

Das Formular, das personenbezogene Daten erfasst, verwendet POST, sodass die Daten nicht in URLs oder Server-Logs erscheinen.

MUSTERBERICHT