WEBDESIGN-AUDIT 2026 · PHASE 5 VON 6

Master-Leitfaden Phase 5: DSGVO & Rechtssicherheit

Rechtssicheres Impressum nach § 5 DDG, DSGVO-Datenschutzerklärung, Cookie-Consent nach TDDDG, Lokales Font-Hosting, AV-Verträge & modernste SSL/TLS-Chiffren nach BSI-Standards.

Herausgeber: Hauptstadt Homepage Berlin
Experte: Benjamin Machalz
Stand: 2026/2027 Edition
Dokument: Technischer Praxisleitfaden (Download-Version)

1. Executive Summary: Rechtssicherheit als unternehmerische Risikovorsorge

Die gesetzlichen Anforderungen an gewerbliche Websites im europäischen und deutschen Rechtsraum gehören zu den strengsten der Welt. Was früher als Formalie galt, ist heute ein hochgradig abmahngefährdetes Minenfeld. Datenschutzbehörden, Verbraucherschutzzentralen und spezialisierte Abmahnkanzleien nutzen automatisierte Scanner, um Webseiten binnen Sekunden auf rechtliche Schwachstellen zu durchleuchten: Veraltete Impressumsangaben, unzulässig eingebundene Drittanbieter-Schriftarten (Google Fonts Urteil des LG München), intransparente Cookie-Banner ohne echten Ablehnen-Button oder unverschlüsselte Kontaktformulare.

Im Mai 2024 trat zudem das neue **Digitale-Dienste-Gesetz (DDG)** in Kraft, welches das bisherige Telemediengesetz (TMG) ablöste. Wer im Impressum nach wie vor auf „§ 5 TMG“ verweist, riskiert formale wettbewerbsrechtliche Abmahnungen. Hinzu kommen die Vorgaben des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG, ehemals TTDSG), das für jedes Setzen von Cookies und Auslesen von Endgeräte-Informationen eine informierte, ausdrückliche Einwilligung vorschreibt.

Phase 5 des Webdesign-Audits schützt Ihr Unternehmen vor existenzbedrohenden Abmahnungen, Bußgeldern der Landesdatenschutzbeauftragten (bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes) und irreversiblen Reputationsschäden.

> **Haftungsgrundsatz für Geschäftsführer**
> Datenschutz- und Impressumsverstöße sind keine bloßen Bagatellen. Die Geschäftsführung haftet persönlich für die Einhaltung der gesetzlichen Compliance-Vorgaben im Unternehmen.

2. Die 5 Kernprüfpunkte von Phase 5 im Detail

Prüfpunkt 5.1: Vollständiges Impressum nach § 5 DDG mit 2 Klicks erreichbar

Jede geschäftsmäßige Webpräsenz in Deutschland unterliegt der gesetzlichen Anbieterkennzeichnungspflicht. Mit dem Inkrafttreten des Digitalen-Dienste-Gesetzes lautet die korrekte Rechtsgrundlage verbindlich **§ 5 DDG**.

Folgende Pflichtangaben müssen vollständig, aktuell und fehlerfrei enthalten sein:

- **Vollständiger Unternehmensname & Rechtsform:** Exakte Firmierung gemäß Handelsregister (z. B. *Hauptstadt Homepage GmbH*). Bei Einzelunternehmen der vollständige Vor- und Zuname des Inhabers.
- **Vollständige ladungsfähige Anschrift:** Straße, Hausnummer, Postleitzahl und Ort. Ein reines Postfach ist gesetzlich unzulässig!
- **Vertretungsberechtigte Personen:** Vor- und Zuname der Geschäftsführer oder Vorstände.
- **Schnelle elektronische Kontaktaufnahme:** Telefonnummer und E-Mail-Adresse. Die Angabe einer reinen Kontaktformular-Maske ohne sichtbare E-Mail-Adresse verstößt gegen § 5 Abs. 1 Nr. 2 DDG.
- **Registereintrag & Registernummer:** Handelsregister, Vereinsregister oder Partnerschaftsregister inklusive Registergericht und Registernummer (z. B. Amtsgericht Charlottenburg, HRB 123456 B).
- **Umsatzsteuer-Identifikationsnummer (USt-IdNr.):** Sofern nach § 27a UStG vergeben (nicht zu verwechseln mit der internen Steuernummer, die aus Datenschutzgründen nicht ins Impressum gehört).
- **Aufsichtsbehörde & Kammerangaben:** Bei reglementierten Berufen (z. B. Rechtsanwälte, Steuerberater, Ärzte, Immobilienmakler nach § 34c GewO, Handwerker) die zuständige Aufsichtsbehörde, Kammer, gesetzliche Berufsbezeichnung und berufsrechtliche Regelungen.

Das Impressum muss gemäß ständiger BGH-Rechtsprechung *leicht erkennbar, unmittelbar erreichbar und ständig verfügbar* sein. Dies bedeutet: Ein Klickpfad von maximal zwei Klicks (z. B. über einen fest verankerten Link in der globalen Fußzeile) von jeder einzelnen Unterseite aus.

Prüfpunkt 5.2: DSGVO-Datenschutzerklärung mit allen Tools & AV-Verträgen

Die Datenschutzerklärung nach Art. 13 und 14 DSGVO informiert die Besucher transparent und in verständlicher Sprache über Art, Umfang und Zweck der Verarbeitung personenbezogener Daten (z. B. IP-Adressen, Cookies, Formulareingaben).

Zwingende Bestandteile einer wasserdichten Datenschutzerklärung:

1. **Verantwortlicher & Datenschutzbeauftragter:** Name und Kontaktdaten des Verantwortlichen; falls gesetzlich vorgeschrieben (ab 20 Mitarbeitern mit ständiger Datenverarbeitung), Kontaktdaten des Datenschutzbeauftragten.
2. **Rechtsgrundlagen der Verarbeitung:** Jede Datenverarbeitung muss präzise auf einen Erlaubnistatbestand nach Art. 6 Abs. 1 DSGVO gestützt werden (z. B. berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO für Server-Logs; Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO für Marketing-Cookies; Vertragserfüllung nach Art. 6 Abs. 1 lit. b DSGVO für Anfragen).
3. **Lückenloses Tool-Inventar:** Sämtliche eingesetzten Technologien müssen explizit benannt und beschrieben werden (z. B. Google Analytics 4, Meta Pixel, Brevo, HubSpot, reCAPTCHA, Cloudflare, Stripe).
4. **Auftragsverarbeitungsverträge (AV-Verträge / DPA):** Mit jedem externen Dienstleister, der personenbezogene Daten verarbeitet (Hosting-Provider, E-Mail-Dienste, Analysetools), muss ein rechtsgültiger AV-Vertrag nach Art. 28 DSGVO abgeschlossen sein.
5. **Drittlandübermittlung (USA-Transfer):** Bei Anbietern mit Sitz in den USA (z. B. Google, Microsoft, Meta) muss die Zertifizierung unter dem *EU-U.S. Data Privacy Framework (DPF)* oder das Vorliegen von Standardvertragsklauseln (SCCs) dokumentiert sein.
6. **Betroffenenrechte:** Ausführliche Belehrung über das Recht auf Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung (Art. 18), Datenübertragbarkeit (Art. 20) und Widerruf erteilter Einwilligungen (Art. 7 Abs. 3).

Prüfpunkt 5.3: Cookie-Consent-Banner für Marketing- & Tracking-Skripte

Gemäß § 25 TDDDG und der Rechtsprechung des EuGH (Planet49-Urteil) sowie des BGH ist das Speichern von Informationen auf dem Endgerät des Nutzers (Cookies, Local Storage, Session Storage) sowie der Zugriff darauf grundsätzlich nur mit vorheriger, aktiver und informierter **Einwilligung (Opt-in)** zulässig.

Einzige Ausnahme: Technisch unbedingt erforderliche Cookies (z. B. Session-Cookies für den Warenkorb, CSRF-Sicherheitstoken oder das Speichern der Cookie-Entscheidung selbst).

Anforderungen an ein rechtskonformes Consent-Management-System (CMP):

- **Keine vorangekreuzten Kästchen:** Opt-in-Checkboxen für Statistik- oder Marketing-Kategorien müssen standardmäßig deaktiviert sein.
- **Gleichwertiger Ablehnen-Button:** Auf der ersten Ebene des Banners muss die Option „Alle ablehnen“ genauso prominent, barrierefrei und mit derselben visuellen Gewichtung gestaltet sein wie „Alle akzeptieren“. Sogenannte *Dark Patterns* (z. B. versteckter Ablehnen-Link in grau auf grau) sind rechtswidrig und abmahnbar!
- **Echtes Script-Blocking vor Consent:** Kein einziges Tracking-Skript (Google Tag Manager, Meta Pixel, Hotjar) darf vor dem aktiven Klick auf „Akzeptieren“ geladen werden. Ein rein informativer Banner mit dem Text „Wir nutzen Cookies...“ ohne technische Blockade ist illegal.
- **Widerrufsmöglichkeit zu jeder Zeit:** Nutzer müssen ihre Entscheidung jederzeit mit einem Klick (z. B. über ein kleines Fingerabdruck-Icon am Bildschirmrand) ändern oder widerrufen können.

Prüfpunkt 5.4: Lokales Hosting aller Schriftarten (Google Fonts) ohne US-Übertragung

Im Januar 2022 fällte das Landgericht München I ein wegweisendes Urteil (Az. 3 O 17493/20): Die dynamische Einbindung von Schriftarten über Google-Server (Google Fonts API) stellt eine unberechtigte Weitergabe der dynamischen IP-Adresse des Nutzers in die USA dar und begründet einen Schadensersatzanspruch nach Art. 82 DSGVO. In der Folge kam es bundesweit zu zehntausenden Abmahnungen.

Im Rahmen des Webdesign-Audits gilt die unumstößliche Regel:

> Alle Schriftarten (Google Fonts, Adobe Fonts, Font Awesome Icons) müssen zu 100 % lokal auf dem eigenen Webserver im modernen WOFF2-Format gehostet werden. Externe Verweise auf fonts.googleapis.com oder use.fontawesome.com im Quellcode sind strikt verboten!

Rechtskonforme lokale Einbindung via CSS @font-face

```
@font-face {
  font-family: 'Plus Jakarta Sans';
  font-style: normal;
  font-weight: 400 800;
  font-display: swap;
  src: url('/assets/fonts/plus-jakarta-sans.woff2') format('woff2');
}
```

Prüfpunkt 5.5: SSL/TLS-Verschlüsselung mit modernsten Chiffren & HSTS

Gemäß Art. 32 DSGVO und § 19 Abs. 4 DDG sind Webseitenbetreiber gesetzlich verpflichtet, dem Stand der Technik entsprechende technische und organisatorische Maßnahmen (TOM) zum Schutz personenbezogener

Daten umzusetzen. Dies gilt insbesondere für alle Übertragungswege, über die Nutzerdaten transportiert werden (Kontaktformulare, Login-Masken, Checkout).

Technische Sicherheits-Vorgaben nach den Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI TR-02102-2):

1. **Deaktivierung veralteter Protokolle:** SSL 2.0, SSL 3.0, TLS 1.0 und TLS 1.1 müssen auf Serverebene vollständig deaktiviert sein. Erlaubt sind ausschließlich **TLS 1.2** und **TLS 1.3**.
2. **Starke Chiffren-Suiten (Cipher Suites):** Ausschluss unsicherer Algorithmen (z. B. RC4, 3DES, CBC-Chiffren). Zwingender Einsatz von *Forward Secrecy (PFS)* via ECDHE.
3. **HTTP Strict Transport Security (HSTS):** Erzwingt, dass Browser die Website ausnahmslos über eine verschlüsselte HTTPS-Verbindung aufrufen und verhindert Man-in-the-Middle-Angriffe (SSL-Stripping). Header-Empfehlung: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.
4. **Sicherheits-Header implementieren:**
   - `X-Content-Type-Options: nosniff` (verhindert MIME-Type-Sniffing).
   - `X-Frame-Options: DENY` oder `SAMEORIGIN` (Schutz vor Clickjacking-Angriffen).
   - `Referrer-Policy: strict-origin-when-cross-origin` (schützt vertrauliche URL-Parameter bei ausgehenden Links).

3. Datenschutz-Dokumentationspflichten: Verzeichnis von Verarbeitungstätigkeiten (VVT)

Viele Unternehmen übersehen, dass die DSGVO neben der öffentlichen Datenschutzerklärung auf der Website auch interne Dokumentationspflichten vorschreibt. Gemäß Art. 30 DSGVO muss jedes Unternehmen ein **Verzeichnis von Verarbeitungstätigkeiten (VVT)** führen, sobald Daten nicht nur gelegentlich verarbeitet werden.

Für den Website-Betrieb müssen im VVT folgende Verarbeitungsprozesse sauber erfasst sein:

- **Server-Logfiles:** Speicherung von IP-Adresse, Browserkennung, Zugriffszeitpunkt und Referrer-URL zur Gewährleistung der Netzsicherheit und Abwehr von DDoS-Angriffen (Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO; Löschfrist: maximal 7 bis 14 Tage).
- **Kontaktformular-Anfragen:** Erfassung von Interessenten-Daten zur Angebotserstellung und Kundenkommunikation (Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO; Löschfrist: nach Ablauf handels- und steuerrechtlicher Aufbewahrungsfristen).
- **Web-Analytics & Conversion-Tracking:** Messung des Nutzerverhaltens (Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO; Löschfrist: max. 14 Monate bei GA4).
- **E-Mail-Marketing & Newsletter:** Verwaltung von Abonnenten mit Protokollierung des Double-Opt-In-Zeitstempels (Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO).

4. Datenschutz-Folgenabschätzung (DSFA) & Drittland-Datentransfers

Gemäß Art. 35 DSGVO ist eine formelle **Datenschutz-Folgenabschätzung (DSFA)** zwingend durchzuführen, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies betrifft im Webdesign insbesondere:

- **Umfangreiches Nutzer-Profiling:** Die Zusammenführung von Webseiten-Tracking, CRM-Daten und Werbe-Netzwerken zur Erstellung detaillierter Persönlichkeits- und Verhaltensprofile.
- **KI-basierte Chatbots & automatisierte Entscheidungsfindung:** Werden Anfragen von KI-Systemen (wie OpenAI ChatGPT oder Anthropic Claude) analysiert oder vorqualifiziert, müssen Risikoanalysen bezüglich Datenweitergabe, Halluzinationen und Diskriminierungsfreiheit vorliegen.
- **Datentransfers in unsichere Drittstaaten:** Durch das *EU-U.S. Data Privacy Framework (DPF)* besteht zwar seit Juli 2023 ein Angemessenheitsbeschluss der EU-Kommission für zertifizierte US-Unternehmen. Dennoch müssen Unternehmen im Rahmen eines Transfer Impact Assessments (TIA) prüfen, ob der jeweilige US-Dienstleister aktiv auf der DPF-Liste des US-Handelsministeriums geführt wird. Fehlt die Zertifizierung, müssen Standardvertragsklauseln (SCCs) vereinbart und zusätzliche technische Schutzmaßnahmen (z. B. Ende-zu-Ende-Verschlüsselung) ergriffen werden.

5. Content Security Policy (CSP): Technischer Schutz vor Cross-Site Scripting (XSS)

Eine oft vernachlässigte, aber vom BSI dringend empfohlene Sicherheitsmaßnahme ist die **Content Security Policy (CSP)**. Hierbei handelt es sich um einen HTTP-Header, der dem Browser strikt vorschreibt, aus welchen vertrauenswürdigen Quellen Skripte, Stylesheets, Bilder und Schriftarten nachgeladen werden dürfen:

> **Empfohlener Content-Security-Policy Header**
>
> ```
> Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' https://trusted-cdn.c
> ```

Durch das Verbot von `eval()` und die strikte Beschränkung auf eigene Domains (`'self'`) wird verhindert, dass böswillige Dritte über manipulierte Formularfelder oder Drittanbieter-Skripte schädlichen JavaScript-Code in den Browser Ihrer Besucher einschleusen (Cross-Site Scripting / Formjacking).

6. Abmahnfalle Kontaktformular: Was 2026 beachtet werden muss

Kontaktformulare sind ein häufiges Ziel von Abmahnanwälten. Um rechtssicher Leads zu generieren, müssen folgende Regeln beachtet werden:

- **Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO):** Nur die Daten dürfen als Pflichtfeld (*) markiert werden, die für die Bearbeitung der Anfrage zwingend erforderlich sind (in der Regel Name und E-Mail-Adresse). Telefonnummer oder Firmenname dürfen nur optional abgefragt werden, es sei denn, die Kontaktaufnahme soll explizit telefonisch erfolgen.
- **Transparenzhinweis am Formular:** Direkt unter dem Formular muss ein gut lesbarer Hinweis auf die Datenschutzerklärung platziert werden (z. B. *„Mit dem Absenden erklären Sie sich mit der Verarbeitung Ihrer Daten gemäß unserer Datenschutzerklärung einverstanden.“*).
- **Keine ungefragte Newsletter-Kopplung:** Es ist rechtswidrig, das Absenden einer Kontaktanfrage automatisch mit der Eintragung in einen E-Mail-Newsletter zu verknüpfen (Kopplungsverbot). Für Newsletter ist stets eine separate, unangekreuzte Checkbox mit anschließendem Double-Opt-In-Verfahren erforderlich.

7. Häufige Fragen zu Phase 5 (FAQ)

Gilt die Impressumspflicht nach § 5 DDG auch für reine Informationsseiten ohne Shop?

Ja! Das Digitale-Dienste-Gesetz unterscheidet nicht zwischen E-Commerce-Shops und reinen Informations-Websites. Jedes geschäftsmäßige Angebot (hierzu zählt jede Unternehmens-, Freiberufler- oder Handwerker-Website, die Leistungen darstellt oder der Kundenakquise dient) unterliegt der vollen Impressumspflicht.

Brauche ich zwingend einen Cookie-Banner, wenn ich keine Tracking-Tools nutze?

Nein. Wenn Ihre Website ausschließlich technisch notwendige Session-Cookies setzt und keine externen Tracking-Dienste (wie Google Analytics, Meta Pixel oder Werbenetzwerke) einbindet, ist nach § 25 Abs. 2 TDDDG kein Cookie-Banner erforderlich. In diesem Fall genügt ein transparenter Hinweis in der Datenschutzerklärung.

Darf ich Google Analytics mit IP-Anonymisierung ohne Einwilligung nutzen?

Nein! Die Datenschutzkonferenz (DSK) und die europäischen Aufsichtsbehörden haben unmissverständlich klargestellt, dass Google Analytics (auch in der Version GA4) Cookies und Geräte-IDs auf dem Endgerät speichert. Dies erfordert nach § 25 Abs. 1 TDDDG zwingend ein vorheriges, aktives Opt-in über einen rechtssicheren Cookie-Consent-Banner.

Was passiert bei einer berechtigten DSGVO-Abmahnung?

Wird eine formelle Abmahnung zugestellt, drohen erhebliche Abmahnkosten (Streitwerte im Wettbewerbsrecht liegen regelmäßig zwischen 10.000 € und 50.000 €) sowie die Abgabe einer strafbewehrten Unterlassungserklärung. Bei Zuwiderhandlung fallen Vertragsstrafen von mehreren tausend Euro pro Einzelfall an. Durch die Einhaltung unserer Checkliste Phase 5 schließen Sie diese Risiken systematisch aus.

6. Qualitäts-Checkliste zur Freigabe von Phase 5

Status	Prüfpunkt / Meilenstein	Verantwortlich	Kriterium
	Impressum nach § 5 DDG mit 2 Klicks erreichbar	Rechtsexperte / Projektleitung	Vollständige Firmierung, ladungsfähige Anschrift, Vertretung, Kontakt & Register.
	DSGVO-Datenschutzerklärung lückenlos aktuell	Datenschutzbeauftragter	Alle Tools deklariert; Rechtsgrundlagen benannt; AV-Verträge unterzeichnet.
	TDDDG-konformer Cookie-Consent aktiv	Frontend-Entwickler	Gleichwertiger Ablehnen-Button; echtes Script-Blocking vor Opt-in; kein Dark Pattern.
	Google Fonts & Assets 100 % lokal gehostet	Frontend-Entwickler	0 externe Verbindungen zu US-Servern im Netzwerk-Tab der Entwicklertools.
	SSL/TLS-Verschlüsselung mit modernsten Chiffren	Systemadministrator	TLS 1.2/1.3 only; HSTS-Header aktiv; Qualys SSL Labs Rating A+.

Hauptstadt Homepage · Dresselstraße 1, 14057 Berlin · Tel: 030 283 709 96 · hallo@hauptstadt-homepage.de

Dokument-ID: HH-AUDIT-P5-2026 · Alle Rechte vorbehalten.