

Praxis-Website prüfen

13 Punkte, die eine Praxis-Website erfüllen muss



Alle Links zum Anklicken

Der wichtigste Unterschied: EINGEBETTET heißt, der fremde Dienst wird beim Aufruf Ihrer Seite geladen — er sieht die IP-Adresse Ihrer Besucher und erfährt, dass jemand IHRE Praxis aufgerufen hat. Bei einer Facharztpraxis ist das ein Gesundheitsdatum nach Art. 9 DSGVO. NUR VERLINKT heißt: es passiert erst beim Klick etwas.

DIE 13 PRÜFPUNKTE

Prüfpunkt	Worum es geht	Was zu tun ist
HTTPS/SSL aktiv	Verschlüsselte Verbindung Pflicht	Ein SSL-Zertifikat einrichten — bei Let's Encrypt kostenlos, jeder Hostet bietet es an. Ohne HTTPS gehen auch Kontaktformulare unverschlüsselt über die Leitung.
Impressum vorhanden	§ 5 DDG – Anbieterkennzeichnung	Ein Impressum nach § 5 DDG anlegen und von jeder Seite aus verlinken — mit Name, Anschrift, Kontakt, Berufsbezeichnung, zuständiger Kammer und Aufsichtsbehörde. Kostenloser Generator: custodio-compliance.de/impressum-generator
Datenschutzerklärung verlinkt	Art. 13 DSGVO Pflichtinformation	Eine Datenschutzerklärung nach Art. 13 DSGVO anlegen und von jeder Seite aus verlinken. Kostenloser Generator: custodio-compliance.de/datenschutzerklaerung-generator
Cookie-Hinweis vorhanden	Eingebettete Dienste laden ohne Einwilligung (§ 25 TDDDG)	Eine Einwilligungsabfrage einrichten, die die Dienste erst NACH dem Klick lädt. Ein Banner, der nur informiert, während im Hintergrund schon geladen wird, erfüllt § 25 TDDDG nicht.
Keine fremden Cookies vor der Einwilligung	§ 25 Abs. 1 TDDDG: die Einwilligung muss VOR dem Speichern im Endgerät vorliegen	Beim Aufruf lag nichts im Gerät, wofür eine Einwilligung nötig gewesen wäre. Genau das verlangt § 25 Abs. 1 TDDDG — dabei bleiben.
Keine externen Google Fonts	IP-Weiterleitung = einwilligungspflichtig	Die Schriften herunterladen und vom eigenen Server ausliefern (lokales Hosting). Dann geht keine IP-Adresse mehr an Google, und es braucht auch keine Einwilligung dafür.
Kein unkonsentes Tracking	Tracking ohne Einwilligung ist unzulässig	Das Tracking erst NACH einer aktiven Einwilligung nachladen (Zwei-Klick-Lösung). Ein Banner, der schon beim Aufruf lädt, erfüllt § 25 TDDDG nicht.
Kein Facebook-Tracking	Meta-Pixel erfordert eine Einwilligung	Den Pixel erst nach Einwilligung laden — und prüfen, ob er auf einer Praxis-Website überhaupt gebraucht wird. Meta erfährt sonst, wer Ihre Praxis aufruft.
Kein YouTube ohne Einwilligung	YouTube-Einbettung überträgt Daten an Google	Auf youtube-nocookie.com umstellen und das Video erst nach einem Klick laden (Vorschaubild statt Einbettung).
Kein Google Maps ohne Einwilligung	Google Maps überträgt Daten an Google	Die Karte erst nach Einwilligung laden, oder ein statisches Bild des Anfahrtswegs einbinden. Für eine Praxisanfahrt reicht das meist.
Kein Google reCAPTCHA ohne Einwilligung	reCAPTCHA überträgt Daten an Google	Auf ein Verfahren ohne Drittanbieter umstellen — etwa eine Rechenaufgabe oder ein verstecktes Feld (Honeypot). Für ein Praxis-Kontaktformular genügt das.
Kontaktformular DSGVO-Hinweis	Hinweispflicht bei Dateneingabe	Beim Formular auf die Datenschutzerklärung verweisen und sagen, wofür die Daten verwendet werden (Art. 13 DSGVO).
Termin-/Videodienst nur mit Einwilligung	Eingebetteter Praxis-Dienst lädt vor der Einwilligung	Termin- und Videodienste erst nach der Einwilligung nachladen und für jeden einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO schließen.

Kostenlos selbst prüfen: custodio-compliance.de/website-check — ohne Anmeldung, ohne E-Mail-Adresse. Wir speichern weder die Adresse noch das Ergebnis. Die Prüfung öffnet Ihre Startseite in einem echten Browser und sieht auch, was erst per JavaScript nachgeladen wird.

Praxis-Website prüfen

13 Punkte, die eine Praxis-Website erfüllen muss



Alle Links zum Anklicken

PRAXIS-DIENSTE, DIE DER CHECK KENNT

Diese Dienste kommen fast nur auf Praxis-Websites vor. Wird einer davon gefunden, braucht es in aller Regel einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO und einen Eintrag in der Datenschutzerklärung — und wenn er eingebettet ist, zusätzlich eine Einwilligung nach § 25 TDDDG.

Art	Dienste	Anzahl
Anamnese	Idana, Nelly, Simpleprax (anamnese.app)	3
Bewertungsportal	Arzt-Auskunft (Stiftung Gesundheit), DocFinder, DocInsider, Klinikbewertungen, Medführer, ProvenExpert, sanego, topmedis, ÄRZTE.DE	9
Praxiskommunikation	medflex, medondo	2
Rezept und Apotheke	IhreApotheken, apotheken.de, gesund.de	3
Terminbuchung	116117 Patientenservice, Acuity Scheduling, CLICKDOC (CGM), Calendly, Doctena, Doctolib, Doodle, Dr. Flex, Setmore, Shore, SimplyBook.me, TIMIFY, Termin2go, Terminland, appointmed, arzt-direkt, arzttermine.de, cituro, dubidoc, eTermin, eTerminservice (116117), jameda, medatixx Online-Terminservice, samedi, tomedo Terminbuchung	25
Videosprechstunde	Arztkonsultation, CGM VideoSprechstunde (eVi), Jitsi Meet, Kry, Microsoft Teams, Patientus, RED connect, TeleClinic, ZAVA, Zoom, doxy.me, sprechstunde.online	12

ALLGEMEINE DIENSTE, DIE DER CHECK KENNT

Diese kommen auf jeder Art von Website vor. Auf einer Praxis-Website wiegen sie schwerer: wer die Seite einer Facharztpraxis aufruft, gibt damit einen Hinweis auf seine Gesundheit — ein Datum nach Art. 9 DSGVO.

Gruppe	Dienste	Anzahl
Reichweitenmessung	Amplitude, Chartbeat, Countly, Fathom Analytics, Google Analytics, Google Tag Manager, Heap, Mapp Intelligence, Matomo Cloud, Mixpanel, Piwik PRO, Plausible, PostHog, Segment, StatCounter, Woopra, Yandex Metrika, etracker	18 (7 hoch)
Chat und Beratungsfenster	Crisp, Drift (Salesloft), Freshchat, HubSpot, Intercom, LiveChat, Olark, Smartsupp, Userlike, WhatsApp-Kontakt, Zendesk, tawk.to	12 (9 hoch)
Newsletter	ActiveCampaign, Brevo, CleverReach, GetResponse, Inxmail, KlickTipp, Mailchimp, Mailchimp (Anmeldeformular), MailerLite, Mailjet, rapidmail	11 (3 hoch)
Werbung und Erfolgsmessung	Facebook Pixel, Google DoubleClick, LinkedIn Insight Tag, Microsoft Advertising (UET), Pinterest Tag, TikTok Pixel, X (Twitter) Pixel	7 (7 hoch)
Schriften	Adobe Fonts, BootstrapCDN, Bunny Fonts, Font Awesome, Google Fonts, Monotype Fonts, MyFonts	7
Video und Ton	Dailymotion, JW Player, SoundCloud, Vimeo, Wistia, YouTube, YouTube (No-Cookie-Variante)	7 (1 hoch)
Aufzeichnung des Besucherverhaltens	Crazy Egg, Hotjar, Lucky Orange, Microsoft Clarity, Mouseflow, Smartlook	6 (6 hoch)
Programmbibliotheken aus fremdem Netz	Amazon CloudFront, Cloudflare, Google Hosted Libraries, jQuery CDN, jsDelivr, unpkg	6
Stellenanzeigen und Bewerbung	Indeed, JOIN, Personio, Recrutee, StepStone, softgarden	6 (4 hoch)
Soziale Netze als Einbettung	Instagram, LinkedIn, Pinterest, X (Twitter), XING	5 (3 hoch)
Karten	Google Maps, HERE Maps, Mapbox, OpenStreetMap	4 (1 hoch)
Formulare und Umfragen	Formspree, JotForm, SurveyMonkey, Typeform	4 (4 hoch)

Praxis-Website prüfen

13 Punkte, die eine Praxis-Website erfüllen muss



Alle Links zum Anklicken

WordPress und seine Zulieferer	Akismet, Gravatar, Jetpack / WordPress.com, WordPress.org (Emoji)	4
Baukästen	Jimdo, Squarespace, Webflow, Wix	4
Bewertungen und Siegel als Einbettung	Elfsight, Trusted Shops, Trustpilot, eKomi	4 (1 hoch)
Schutz vor automatisierten Zugriffen	Cloudflare Turnstile, Friendly Captcha, hCaptcha	3
Bezahlen	Klarna, PayPal, Stripe	3
Barrierefreiheits-Einblendungen	Eye-Able, UserWay, accessiBe	3 (2 hoch)
Übersetzung und Teilen-Schaltflächen	AddToAny, Google Übersetzer, ShareThis	3 (2 hoch)

EINWILLIGUNGSBANNER, DIE DER CHECK AM NAMEN ERKENNT

Für Ihr Banner brauchen Sie einen Auftragsverarbeitungsvertrag und einen Eintrag in der Datenschutzerklärung. Beides geht nur mit dem Namen des Anbieters — deshalb nennt der Bericht ihn. Läuft das Banner auf Ihrem eigenen Server, entfällt der Vertrag.

Anbieter	Sitz	Bauart
Borlabs Cookie	Deutschland	auf Ihrem Server
Complianz	Niederlande	auf Ihrem Server
Klaro	Deutschland	auf Ihrem Server
Real Cookie Banner	Deutschland	auf Ihrem Server
CCM19	Deutschland	lädt extern
Civic Cookie Control	Großbritannien	lädt extern
CookieFirst	Niederlande	lädt extern
CookieScript	Litauen	lädt extern
CookieYes	Indien / USA	lädt extern
Cookiebot (Usercentrics)	Dänemark / Deutschland	lädt extern
Didomi	Frankreich	lädt extern
OneTrust	USA	lädt extern
Osano	USA	lädt extern
Secure Privacy	USA	lädt extern
Termly	USA	lädt extern
Usercentrics	Deutschland	lädt extern
consentmanager	Deutschland	lädt extern
iubenda	Italien	lädt extern

Die Liste ist nicht abschließend. Sie wächst mit jedem Fund — der Terminplaner eines Praxissoftware-Herstellers kam erst dazu, nachdem er auf einer echten Praxis-Website übersehen worden war.