decareto

Monitoring Report

Website: careers.vodafone.com/de/
Zeitpunkt des Scans: 03.07.2023 17:52

Risikobewertung

D	3	15	✓
Risiko-Score	Externe Dienste gefunden	Cookies gefunden	Datenschutzerklärung gefunden

Die Website läuft auf der Infrastruktur von **Google Cloud Platform** (USA). Der Standort des Cloud-Servers ist USA.
Es besteht das Risiko, dass Ihre Website nicht rechtssicher betrieben wird, da wegen der Standorte von Infrastruktur-Betreiber und Cloud-Server personenbezogene Daten in einen unsicheren Drittstaat übertragen werden.

Sie setzen auf Ihrer Website die Consent Management Software **OneTrust CMP** ein, um vom Benutzer eine Einwilligung zum Setzen von Cookies zu einzuholen.

Wir konnten keine nicht notwendigen Cookies identifizieren, die ohne Einwilligung des Benutzers gesetzt werden.
Achtung: Wir untersuchen nicht, ob das Einholen der Einwilligung DSGVO-konform erfolgt!

Wir konnten keine nicht notwendigen Dienste identifizieren, die ohne Einwilligung des Benutzers geladen werden.
Achtung: Wir untersuchen nicht, ob das Einholen der Einwilligung DSGVO-konform erfolgt!

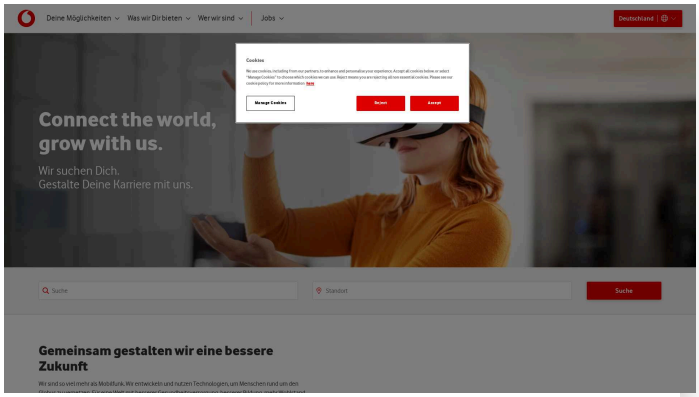
Sie setzen **Google Fonts** ohne Einwilligung des Benutzers ein. Dies hat das Landgericht München mit Urteil vom 20.01.2022 als schadenersatzpflichtig bewertet. [1]

Ihre Website lädt mindestens 2 Externe Dienste, die per IP-Adresse und Cookies personenbezogene Daten aus dem Rechtsraum der EU in Drittstaaten ausleiten, ohne dass eine Einwilligung des Benutzers vorliegt.

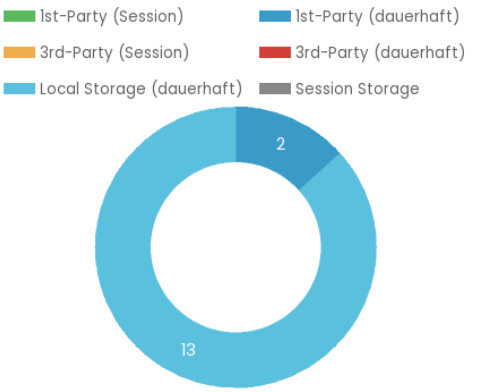
Sie binden **3 Externe Dienste** in Ihre Website ein, zu denen wir in der Datenschutzerklärung keinen Hinweis finden konnten. Damit verstoßen Sie gegen Ihre Informationspflicht nach Art. 13 der DSGVO.

Bitte beachten Sie, dass trotz aller Sorgfalt bei der Untersuchung nicht ausgeschlossen werden kann, dass die Website Datenschutzschwachstellen aufweist, die in diesem Report nicht aufgezeigt werden. Wir können keine Haftung für die Vollständigkeit dieses Reports übernehmen.

Ansicht Startseite

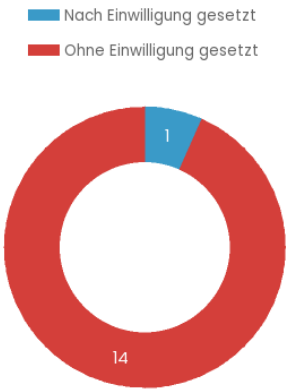


Cookies und Web-Speicher



Cookie-Typ

Verwendung



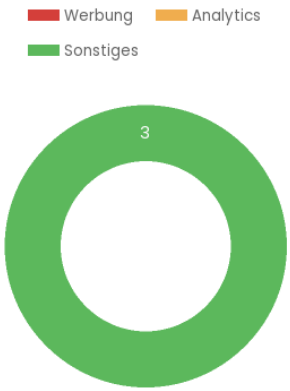
Einwilligung zum Setzen

Cookies und Web-Speicher Übersicht

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
elementor	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
OptanonAlertBoxClosed	1st-Party (dauerhaft)	365	vodafone.com	OneTrust CMP	Ja (USA)	Consent Management	
OptanonConsent	1st-Party (dauerhaft)	365	vodafone.com	OneTrust CMP	Ja (USA)	Consent Management	
t3D	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tADe	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tADu	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tAE	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tC	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tMQ	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tnsApp	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tPL	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tTDe	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein

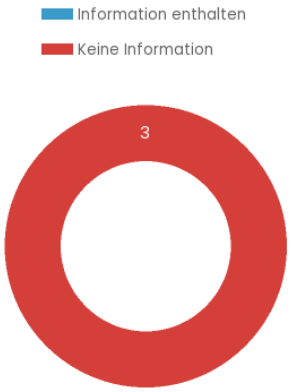
Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
tTDu	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tTE	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein
tTf	Local Storage (dauerhaft)	unbegrenzt		Wordpress		Hosting	Nein

Externe Dienste



Verwendung

Einwilligung zum Laden



Information in Datenschutzerklärung

Externe Dienste Übersicht

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
Google Fonts [1] Auf der Startseite gefunden	fonts.googleapis.com	Google	Ja (USA)	Funktional	Nein	Nein
OneTrust CMP Auf der Startseite gefunden	cookielaw.org	OneTrust	Ja (USA)	Consent Management		Nein
Polyfill Auf der Startseite gefunden	polyfill.io	Polyfill.io		Funktional	Nein	Nein

TLS/SSL-Verschlüsselung und Sicherheit des Webservers

- Das Zertifikat enthält korrekte und vollständige Informationen [2]
- Das Zertifikat ist zeitlich gültig bis 17.11.2023
- Das Zertifikat wird akzeptiert auf allen gängigen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) [3]
- Der Server ist geschützt gegen die verbreitetsten TLS/SSL-Angriffe [4]
- Der Webserver akzeptiert keine veralteten und unsicheren TLS/SSL-Protokolle. [5]
- Die aktuellen Protokolle TLS 1.2 bzw. TLS 1.3 werden akzeptiert [6]

Erläuterungen und Handlungsempfehlungen

[1] Der Betreiber der Website sollte die Google-Schriftdaten auf dem Webserver installieren, so dass keine Verbindung mehr zum Google-Server aufgebaut werden muss.

[2] Wir untersuchen das TLS/SSL-Zertifikat darauf, ob der Server-Name im Zertifikat mit dem tatsächlichen Servernamen

übereinstimmt, und ob das Zertifikat von einer vertrauenswürdigen Quelle stammt. Wenn eins von beiden nicht gegeben ist, zeigt ein Web-Browser normalerweise an, dass die Verbindung nicht sicher ist, weil in diesen Fällen sog. "Man-in-the-middle-Angriffe" möglich sind. Außerdem prüfen wir, ob die "Intermediate-Zertifikate" auf dem Server enthalten sind, die die Vertrauenswürdigkeit des Ausstellers nachweisen. Wenn diese fehlen, dann zeigen ältere Web-Browser möglicherweise Fehler an. Die Prüfungen zeigten keine Probleme.

[3] Die Zertifizierungsstelle, über die das Zertifikat des Webservers erworben wurden, muss von den großen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) als vertrauenswürdig eingestuft und in deren "Trust Store" aufgenommen worden sein. Wenn das nicht der Fall ist, dann stufen die Geräte dieser Plattformen das Zertifikat als nicht gültig ein. Im Fall dieses Webservers wird das Zertifikat von allen Plattformen als vertrauenswürdig eingestuft.

[4] Wir untersuchen den Server auf die Schwachstellen "Heartbleed", "CRIME" und "Downgrade". Alle drei stehen in Zusammenhang mit veralteter Systemsoftware oder dem Akzeptieren veralteter Verschlüsselungsprotokolle. Wir konnten bei dem Server diese Schwachstellen nicht feststellen.

[5] Veraltete TLS/SSL-Protokolle bieten keine sichere Verschlüsselung mehr, so dass Daten für Angreifer sichtbar sein können. Insbesondere die sehr alten Protokolle SSL 2.0 und SSL 3.0 sollten auf keinen Fall mehr eingesetzt werden, aber auch TLS 1.0 und TLS 1.1 sind nicht mehr sicher genug. Der Webserver ist korrekt konfiguriert und akzeptiert diese Protokolle nicht.

[6] Der Webserver sollte für ausreichende Sicherheit die neuen TLS/SSL-Protokolle TLS 1.3 und ggfs. TLS 1.2 unterstützen. Der Webserver ist korrekt konfiguriert und unterstützt diese.