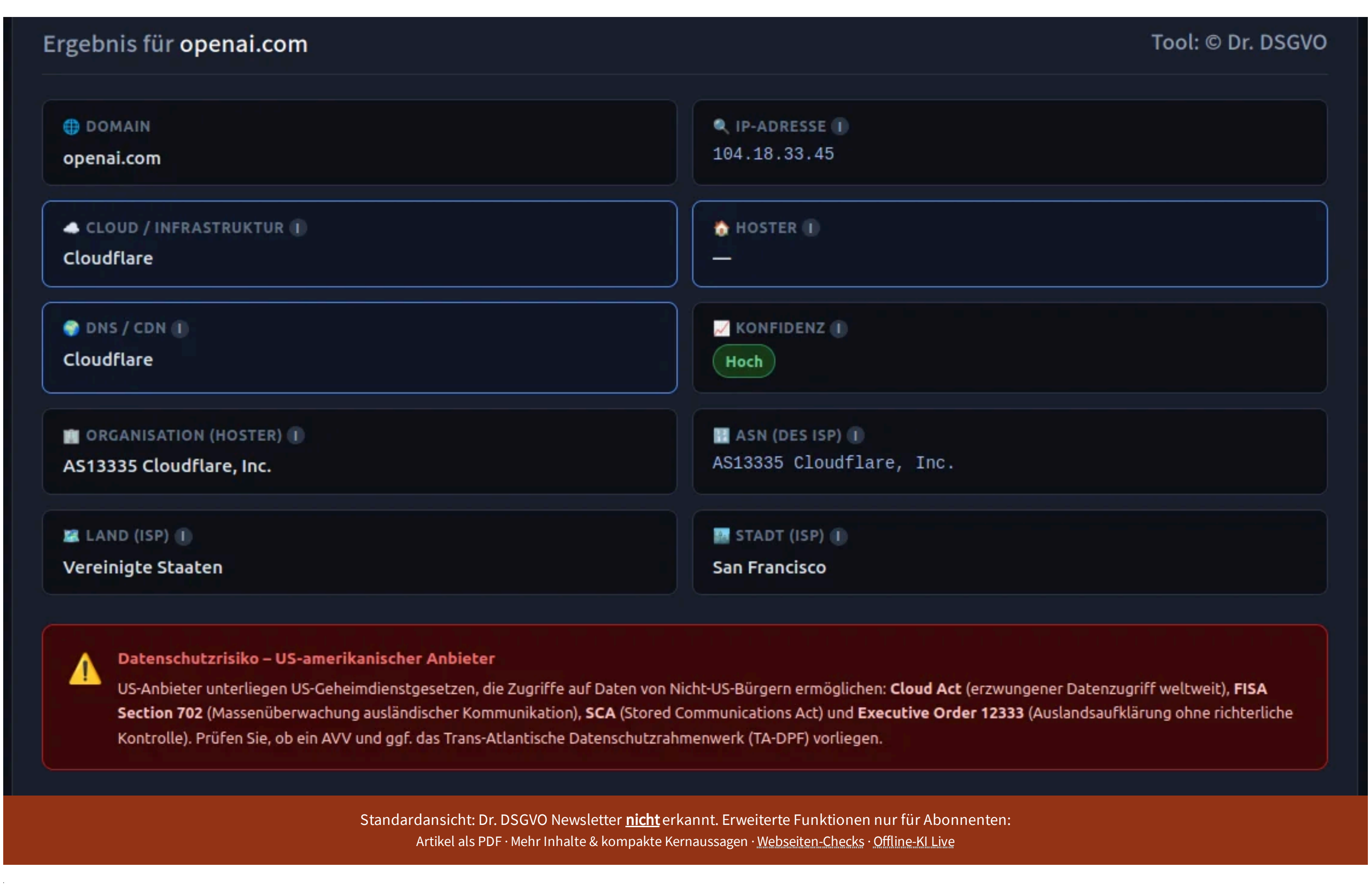
Webseiten-Analyse-Tool: Wie souverän ist Ihre Infrastruktur?

Veröffentlicht am 19. Februar 2026 von Dr. DSGVO · Zuletzt aktualisiert am 26. Februar 2026 · Lesezeit: 8 Minuten



Ergebnis für **openai.com** Tool: © Dr. DSGVO

🌐 DOMAIN
openai.com

🔍 IP-ADRESSE
`104.18.33.45`

☁ CLOUD / INFRASTRUKTUR
Cloudflare

🏠 HOSTER
—

🌍 DNS / CDN
Cloudflare

📈 KONFIDENZ
Hoch

🏢 ORGANISATION (HOSTER)
AS13335 Cloudflare, Inc.

🔢 ASN (DES ISP)
`AS13335 Cloudflare, Inc.`

🗺 LAND (ISP)
Vereinigte Staaten

🏙 STADT (ISP)
San Francisco

⚠ **Datenschutzrisiko – US-amerikanischer Anbieter**
US-Anbieter unterliegen US-Geheimdienstgesetzen, die Zugriffe auf Daten von Nicht-US-Bürgern ermöglichen: **Cloud Act** (erzwungener Datenzugriff weltweit), **FISA Section 702** (Massenüberwachung ausländischer Kommunikation), **SCA** (Stored Communications Act) und **Executive Order 12333** (Auslandsaufklärung ohne richterliche Kontrolle). Prüfen Sie, ob ein AVV und ggf. das Trans-Atlantische Datenschutzrahmenwerk (TA-DPF) vorliegen.

Kategorien: Datenschutz

Die technische Infrastruktur, die einer Webseite zugrunde liegt, lässt zahlreiche Rückschlüsse für Datenschutz und Datensicherheit sowie Abhängigkeiten von Dritten zu. Wird beispielsweise eine Webseite auf einem Server in den USA gehostet, landen alle Daten von Besuchern der Webseite dort. Mit dem Domain-Tool kann eine Webseite in Sekunden geprüft und die digitale Souveränität beurteilt werden.

Datenschutz beginnt nicht erst beim Cookie-Banner. Er beginnt dort, wo Daten tatsächlich fließen – und das ist oft tief in der technischen Infrastruktur einer Webseite verborgen. Wer hostet den Server? Wer liefert die DNS-Auflösung? Welcher Anbieter empfängt E-Mails? Und welche externen Dienste sind in die Seite eingebunden?

Zum Domain-Tool

Unser kostenfreier **Hoster-Erkenner** beantwortet all diese Fragen automatisch – und liefert damit die technische Grundlage für eine fundierte Datenschutz-Folgenabschätzung.

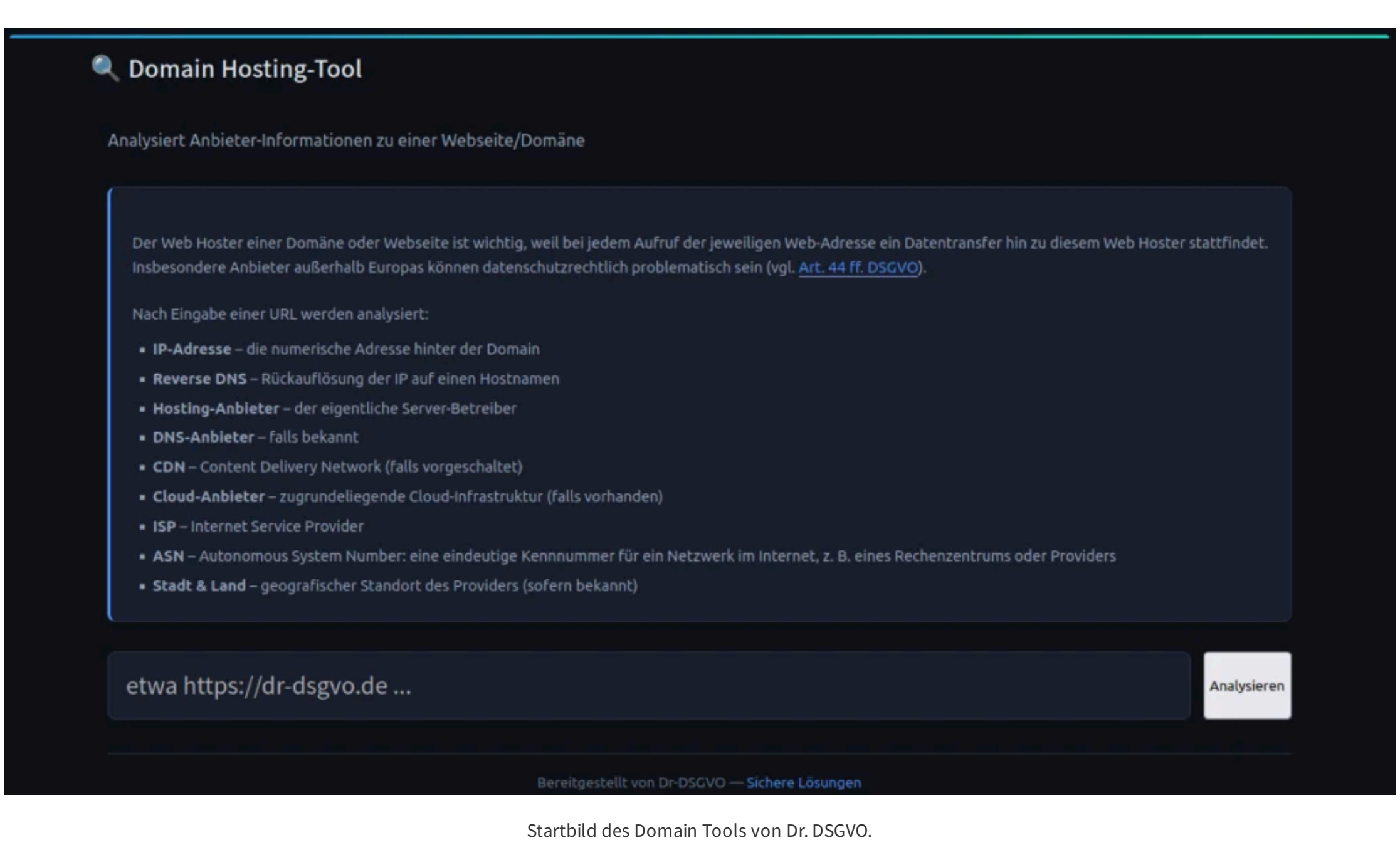
Was passiert, wenn jemand eine Webseite aufruft?

Viele Webseitenbetreiber denken: „Ich habe einen Hoster, der hostet meine Seite – fertig." Die Realität ist komplexer:

```
Besucher
   │
   ▼
[CDN / Proxy]          ← z. B. Cloudflare (USA)
   │                      → empfängt IP-Adresse, Zeitstempel, Browser-Info
   ▼
[Web Hoster]           ← z. B. Hetzner (Deutschland)
   │                      → speichert Zugriffslogs
   ▼
[Cloud-Infrastruktur]  ← z. B. AWS dahinter
   │                      → verarbeitet Daten auf US-Servern
   ▼
[Externe Dienste]      ← z. B. Google Fonts, Analytics, Social Plugins
                          → empfangen Besucherdaten ohne Einwilligung?
```

An jedem dieser Punkte fließen personenbezogene Daten. An jedem dieser Punkte stellen sich datenschutzrechtliche Fragen.

Mit dem Domain-Tool von Dr. DSGVO kann der **Datenfluss beim Aufruf einer Webseite** schnell ermittelt werden.



🔍 Domain Hosting-Tool

Analysiert Anbieter-Informationen zu einer Webseite/Domäne

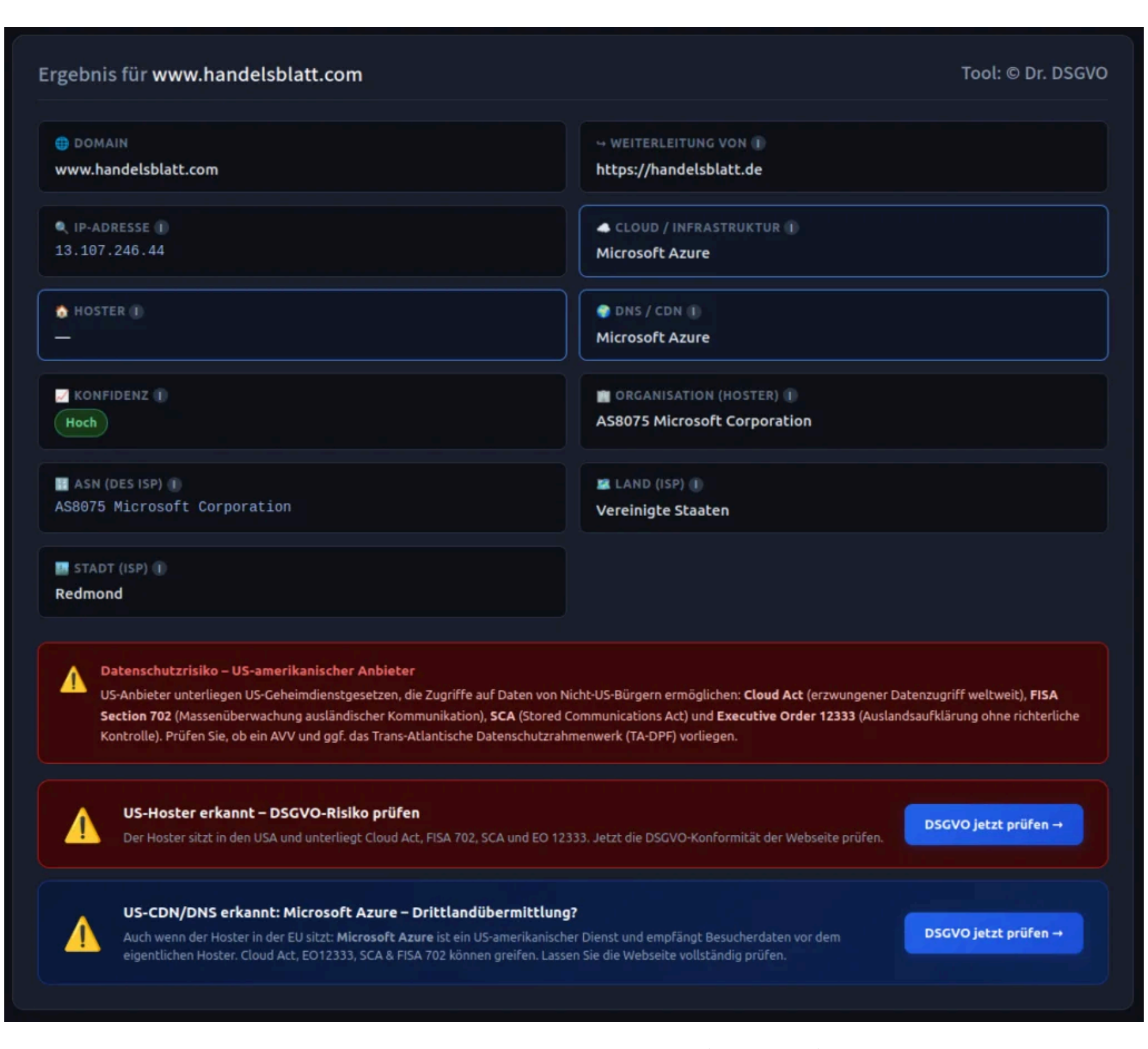
Der Web Hoster einer Domäne oder Webseite ist wichtig, weil bei jedem Aufruf der jeweiligen Web-Adresse ein Datentransfer hin zu diesem Web Hoster stattfindet. Insbesondere Anbieter außerhalb Europas können datenschutzrechtlich problematisch sein (vgl. Art. 44 ff. DSGVO).

Nach Eingabe einer URL werden analysiert:

- **IP-Adresse** – die numerische Adresse hinter der Domain
- **Reverse DNS** – Rückauflösung der IP auf einen Hostnamen
- **Hosting-Anbieter** – der eigentliche Server-Betreiber
- **DNS-Anbieter** – falls bekannt
- **CDN** – Content Delivery Network (falls vorgeschaltet)
- **Cloud-Anbieter** – zugrundeliegende Cloud-Infrastruktur (falls vorhanden)
- **ISP** – Internet Service Provider
- **ASN** – Autonomous System Number: eine eindeutige Kennnummer für ein Netzwerk im Internet, z. B. eines Rechenzentrums oder Providers
- **Stadt & Land** – geografischer Standort des Providers (sofern bekannt)

Startbild des Domain Tools von Dr. DSGVO.

Nach Eingabe einer Webseite oder Domäne und Klick auf den „Analysieren"-Button startet das Tool die Datenanalyse. Das Ergebnis steht nach 1-2 Sekunden bereit und sieht so aus:



Ergebnis für **www.handelsblatt.com** Tool: © Dr. DSGVO

🌐 DOMAIN
www.handelsblatt.com

↪ WEITERLEITUNG VON
https://handelsblatt.de

🔍 IP-ADRESSE
`13.107.246.44`

☁ CLOUD / INFRASTRUKTUR
Microsoft Azure

🏠 HOSTER
—

🌍 DNS / CDN
Microsoft Azure

📈 KONFIDENZ
Hoch

🏢 ORGANISATION (HOSTER)
AS8075 Microsoft Corporation

🔢 ASN (DES ISP)
`AS8075 Microsoft Corporation`

🗺 LAND (ISP)
Vereinigte Staaten

🏙 STADT (ISP)
Redmond

⚠ **Datenschutzrisiko – US-amerikanischer Anbieter**
US-Anbieter unterliegen US-Geheimdienstgesetzen, die Zugriffe auf Daten von Nicht-US-Bürgern ermöglichen: **Cloud Act** (erzwungener Datenzugriff weltweit), **FISA Section 702** (Massenüberwachung ausländischer Kommunikation), **SCA** (Stored Communications Act) und **Executive Order 12333** (Auslandsaufklärung ohne richterliche Kontrolle). Prüfen Sie, ob ein AVV und ggf. das Trans-Atlantische Datenschutzrahmenwerk (TA-DPF) vorliegen.

⚠ **US-Hoster erkannt – DSGVO-Risiko prüfen**
Der Hoster sitzt in den USA und unterliegt Cloud Act, FISA 702, SCA und EO 12333. Jetzt die DSGVO-Konformität der Webseite prüfen.
DSGVO jetzt prüfen →

⚠ **US-CDN/DNS erkannt: Microsoft Azure – Drittlandübermittlung?**
Auch wenn der Hoster in der EU sitzt: **Microsoft Azure** ist ein US-amerikanischer Dienst und empfängt Besucherdaten vor dem eigentlichen Hoster. Cloud Act, EO12333, SCA & FISA 702 können greifen. Lassen Sie die Webseite vollständig prüfen.
DSGVO jetzt prüfen →

Ergebnis der Analyse der Handelsblatt-Webseite (bzw. Domäne).

Wird vom Tool festgestellt, dass beim Aufruf der Webseite Daten nach außerhalb Europa bzw. dem DSGVO-Raum abfließen könnten, erscheint eine Warnung. Dabei werden verschiedene Beteiligte unterschieden, nämlich neben dem Web Hoster auch das DNS-Routing oder verwendete CDNs (Content Delivery Networks, wie Cloudflare oder Azure).

Was analysiert das Tool?

Viele glauben, wenn ein Server in Deutschland oder Europa steht, wäre alles gut. Der Serverstandort ist mehr oder weniger irrelevant! Jeder, der Zugangsdaten hat, kann von überall auf der Welt auf einen Server zugreifen, egal ob der Server in Deutschland oder auf dem Mond steht.

Deswegen unterscheidet das Tool auch Standorte, die aus IP-Adressen ermittelt werden, und rechtlichen Einheiten, deren Standort/Land der Muttergesellschaft bekannt ist.

🌐 IP-Adresse und Serverstandort

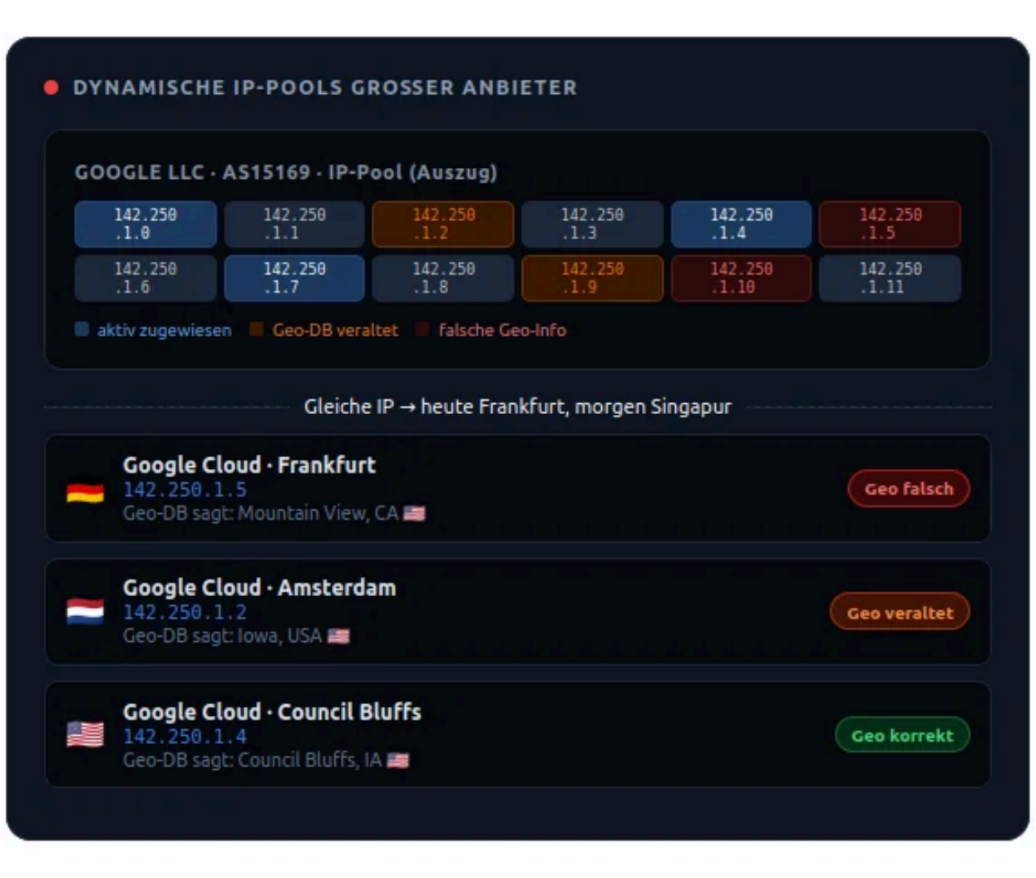
Der erste Schritt ist die Auflösung der Domain zu einer IP-Adresse. Darüber lässt sich oft schon viel erfahren: Welches Unternehmen besitzt diesen IP-Block? In welchem Land ist der Anbieter registriert?

Wichtige Einschränkung: Der geografische Standort einer IP-Adresse ist kein verlässlicher Beweis für den tatsächlichen Serverstandort – besonders bei großen Anbietern wie Google, AWS oder Cloudflare. Diese Betreiber verwalten globale IP-Pools, die dynamisch verschiedenen Servern auf verschiedenen Kontinenten zugewiesen werden können.

```
Beispiel: IP 142.250.1.5
────────────────────────────
Eigentümer:     Google LLC (AS15169)
Geo-Datenbank:  Mountain View, CA 🇺🇸
Tatsächlich:    Google Cloud · Frankfurt 🇩🇪
────────────────────────────
→ Geo-Information ist falsch!
```

Für eine belastbare Aussage zum Verarbeitungsort sollte eine **vertragliche Bestätigung** des Anbieters vorhanden sein.

Oft kann aus einer IP-Adresse der Serverstandort nicht ermittelt werden, wie die folgende Abbildung veranschaulicht.



🇩🇪 **Google Cloud · Frankfurt**
`142.250.1.5`
Geo-DB sagt: Mountain View, CA 🇺🇸
Geo falsch

🇳🇱 **Google Cloud · Amsterdam**
`142.250.1.2`
Geo-DB sagt: Iowa, USA 🇺🇸
Geo veraltet

🇺🇸 **Google Cloud · Council Bluffs**
`142.250.1.4`
Geo-DB sagt: Council Bluffs, IA 🇺🇸
Geo korrekt

Große Anbieter nutzen häufig Pools von Netzwerkadressen.

Vor allem große Anbieter sind von dieser Tatsache betroffen.

WARUM GROSSE ANBIETER BESONDERS PROBLEMATISCH SIND

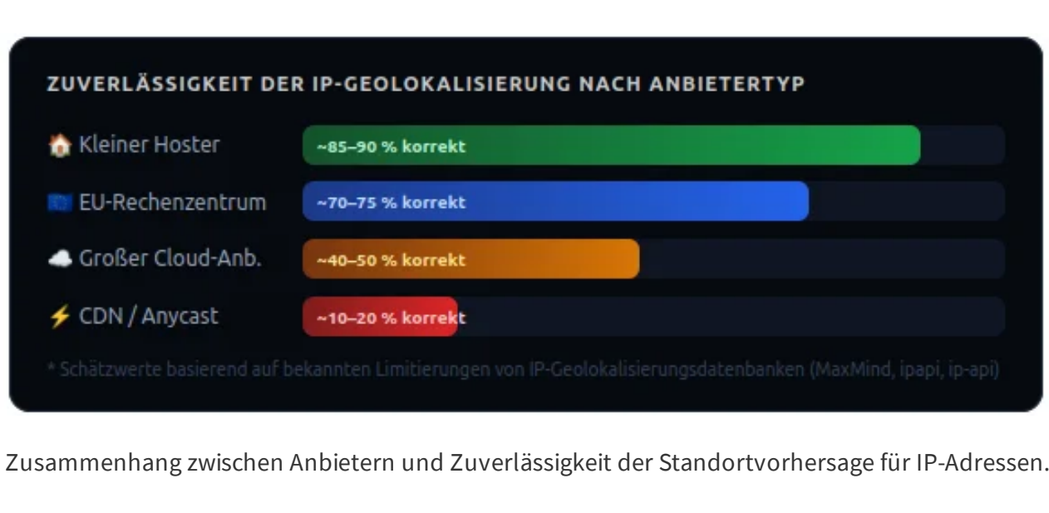
Google LLC / Google Cloud
Betreibt über **200 Rechenzentren** weltweit. Ein IP-Block (z. B. `142.250.0.0/15`) ist Google global zugewiesen – welcher Server tatsächlich antwortet, hängt von internem Load Balancing ab und kann sich **jederzeit ändern**.

Cloudflare
Nutzt **Anycast-Routing**: Dieselbe IP-Adresse ist gleichzeitig an hunderten Standorten aktiv. Die Geo-Datenbank zeigt den **Registrierungsort des IP-Blocks** (San Francisco) – nicht den Server, der tatsächlich antwortet.

Amazon Web Services (AWS)
Veröffentlicht IP-Ranges je Region – aber Kunden können IPs **zwischen Regionen migrieren**. Elastic IPs können binnen Minuten einem Server in einer anderen Region zugewiesen werden, ohne dass Geo-Datenbanken aktualisiert werden.

Große Anbieter betreiben weltweit zahlreich Rechenzentren und wechseln Netzwerkadressen häufig aus.

Als Faustformel kann man sagen, dass die Ermittlung des Standorts aus der Netzwerkadresse heraus umso zuverlässiger ist, je kleiner der Anbieter ist und je eher er der DSGVO unterliegt.



Zusammenhang zwischen Anbietern und Zuverlässigkeit der Standortvorhersage für IP-Adressen.

⚡ CDN und DNS-Anbieter

Content Delivery Networks (CDNs) sind aus modernen Webseiten kaum wegzudenken – sie beschleunigen die Auslieferung von Inhalten erheblich. Datenschutzrechtlich sind sie jedoch eine eigene Kategorie von Datenempfängern und oft problematisch.

Warum ist das problematisch?

Ein CDN-Anbieter wie Cloudflare sieht *jede* Anfrage an Ihre Webseite – bevor sie Ihren eigentlichen Server erreicht. Er kennt IP-Adresse, Browsertyp, Standort und Zeitpunkt jedes Besuchers. Auch wenn Cloudflare europäische Server betreibt: Das Unternehmen hat seinen Sitz in den USA und unterliegt US-amerikanischen Geheimdienstgesetzen.

Außerdem nutzt Cloudflare für jede Anfrage Cookies, was wegen § 25 TDDDG (Cookie-Paragraph) problematisch sein könnte.

```
Cloudflare · Anycast-Routing
────────────────────────────
IP 104.16.0.1 ist gleichzeitig aktiv in:
  🇩🇪 Frankfurt
  🇺🇸 New York
  🇸🇬 Singapur
  ...und ~300 weiteren Standorten

→ Geo-Datenbank zeigt: San Francisco
→ Tatsächlich antwortet: nächster Standort
────────────────────────────
```

Das Tool erkennt CDN-Anbieter anhand von Response-Headern (z. B. `cf-ray` für Cloudflare, `x-amz-cf-id` für Amazon CloudFront) und gibt eine datenschutzrechtliche Einschätzung.

📨 MX-Records: Wer verarbeitet Ihre E-Mails?

Ein oft übersehener Aspekt: Die MX-Records einer Domain verraten, welcher Anbieter eingehende E-Mails verarbeitet. Das ist nicht selten ein US-amerikanischer Konzern.

MX-Eintrag	Anbieter	Sitz
`aspmx.l.google.com`	Google Workspace	USA 🇺🇸
`mail.protection.outlook.com`	Microsoft 365	USA 🇺🇸
`mx.mailbox.org`	Mailbox.org	DE 🇩🇪
`mail.protonmail.ch`	ProtonMail	CH 🇨🇭
`mxext1.mailbox.org`	Mailbox.org	DE 🇩🇪

Wenn ein Unternehmen Google Workspace oder Microsoft 365 nutzt, werden alle eingehenden E-Mails – auch solche mit personenbezogenem Inhalt – über US-amerikanische Server geleitet. Dies ist datenschutzrechtlich zu dokumentieren und abzusichern.

📋 WHOIS und Registrar

Der Domain-Registrar ist das Unternehmen, bei dem eine Domain registriert ist. Auch hier verarbeitet ein Dritter Daten – und auch hier kann der Sitz des Registrars datenschutzrechtlich relevant sein.

Das Tool ermittelt automatisch:

- **Registrar** (z. B. GoDaddy, INWX, united-domains)
- **Registrierungsland**
- **Registrierungsdatum** und **Ablaufdatum**
- **DNSSEC-Status** (Schutz vor DNS-Manipulation)

Ein abgelaufenes Zertifikat oder fehlende DNSSEC-Konfiguration kann ein Hinweis auf mangelnde technische Sorgfalt sein – und damit indirekt auf Datenschutzrisiken.

🔒 Content Security Policy: Wer bekommt Besucherdaten?

Die Content Security Policy (CSP) ist ein HTTP-Sicherheitsheader, der definiert, von welchen externen Quellen eine Webseite Ressourcen laden darf. Für den Datenschutz ist er besonders aufschlussreich: Jede in der CSP aufgeführte externe Domain ist ein potenzieller Datenempfänger.

```
Beispiel CSP-Analyse
─────────────────────────────────
Externe Domains in der CSP:
  fonts.googleapis.com     ← Google (USA)
  www.google-analytics.com ← Google Analytics (USA)
  connect.facebook.net     ← Meta Pixel (USA)
  cdn.cookiebot.com        ← Cookiebot/Usercentrics (DK)
─────────────────────────────────
→ 3 von 4 Diensten in den USA!
→ Einwilligung und AVV prüfen
```

Diese Information ist Gold wert für eine **Datenschutz-Folgenabschätzung** (DSFA) oder ein Verzeichnis von Verarbeitungstätigkeiten (VVT).

🔌 Offene Ports und Dienste

Das Tool scannt die öffentlich erreichbaren Ports des Servers und greift dabei auf eine öffentliche Datenbank zurück. Ein echter Portscan wird also nicht durchgeführt, um die Stabilität der gescannten Webseite nicht zu beeinflussen. Unnötig offene Ports – etwa FTP (Port 21), Telnet (Port 23) oder unverschlüsselte Verwaltungsinterfaces – sind ein Sicherheitsrisiko und können auf mangelnde technische Schutzmaßnahmen nach Art. 32 DSGVO hinweisen.

```
Beispiel Port-Scan
────────────────────
Port     Dienst
────────────────────
80/tcp   http         ✓ erwartet
443/tcp  https        ✓ erwartet
22/tcp   ssh          ⚠ Verwaltungszugang öffentlich?
21/tcp   ftp          ❌ unverschlüsselt!
────────────────────
```

Datenschutzrechtliche Einordnung: USA vs. EU

Das Tool bewertet den Serverstandort automatisch:

Land / Region	Bewertung
🇩🇪 Deutschland	✅ Beste Datensicherheit – DSGVO + BDSG
🇪🇺 EU / EWR	✅ Sehr gut – DSGVO-Geltungsbereich
🇨🇭 🇬🇧 🇯🇵 u. a.	✅ Gut – EU-Angemessenheitsbeschluss vorhanden
🇺🇸 USA	⚠️ Risiko – Cloud Act, FISA 702, Executive Order 12333
Sonstige Drittländer	🔍 Prüfen – Art. 44 ff. DSGVO, nationale Geheimdienstgesetze beachten

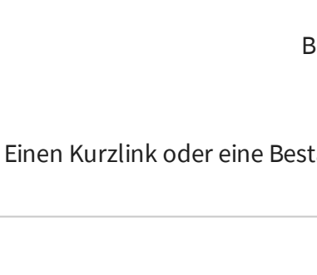
Problematische US-Gesetze im Überblick

Die folgenden Gesetze stehen der DSGVO entgegen und sorgen für **Probleme bei der Datensicherheit** mit US-Amerikanischen Anbietern.

Cloud Act (2018): Erlaubt US-Behörden, von US-Unternehmen die Herausgabe von Daten zu verlangen – unabhängig davon, ob die Daten auf Servern in Europa liegen.

FISA Section 702:

Wer schreibt hier?



Mein Name ist Klaus Meffert. Ich bin promovierter Informatiker und beschäftige mich seit über 30 Jahren professionell und praxisbezogen mit Informationstechnologie. In IT & Datenschutz bin ich auch als Sachverständiger tätig. Ich stehe für pragmatische Lösungen mit Mehrwert. Meine Firma, die IT Logic GmbH, berät Kunden und bietet Webseiten-Checks sowie optimierte & sichere Lösungen an (mit und ohne KI).

Bitte nutzen Sie bei Verwendung meiner Ergebnisse die Quellenangabe oder verlinken Sie gut wahrnehmbar auf diesen Artikel:

Quelle: Klaus Meffert, Dr. DSGVO Blog, Link: https://dr-dsgvo.de/webseiten-analyse-tool-wer-steckt-wirklich-hinter-einer-webseite

Einen Kurzlink oder eine Bestätigung für Ihre Quellenangabe erhalten Sie kurzfristig auf Anfrage. Ein Teilen oder Verteilen dieses Beitrags ist natürlich ohne weiteres möglich und gewünscht.