ChatGPT über Microsoft Azure: Digitales Wunder oder unsicher?

Veröffentlicht am 10. März 2026 von Dr. DSGVO · Zuletzt aktualisiert am 16. März 2026 · Lesezeit: 12 Minuten

Standardansicht: Dr. DSGVO Newsletter **nicht** erkannt. Erweiterte Funktionen nur für Abonnenten:
Artikel als PDF · Mehr Inhalte & kompakte Kernaussagen · Webseiten-Checks · Offline-KI Live

*Kategorien: **Datenschutz***

Einige deutsche Anbieter behaupten, die Nutzung von ChatGPT auf einem deutschen Server sei sicher und DSGVO-konform. DSGVO-konform mag offiziell stimmen, aber Sicherheit ist nicht vorhanden. US-Rechtsvorschriften zwingen Microsoft und andere US-Unternehmen zur Zusammenarbeit mit US-Behörden, ohne dass wir etwas davon mitbekommen dürfen (das nennt sich "Spionage gegen Ausländer" oder "Sicherheitsinteressen der USA").

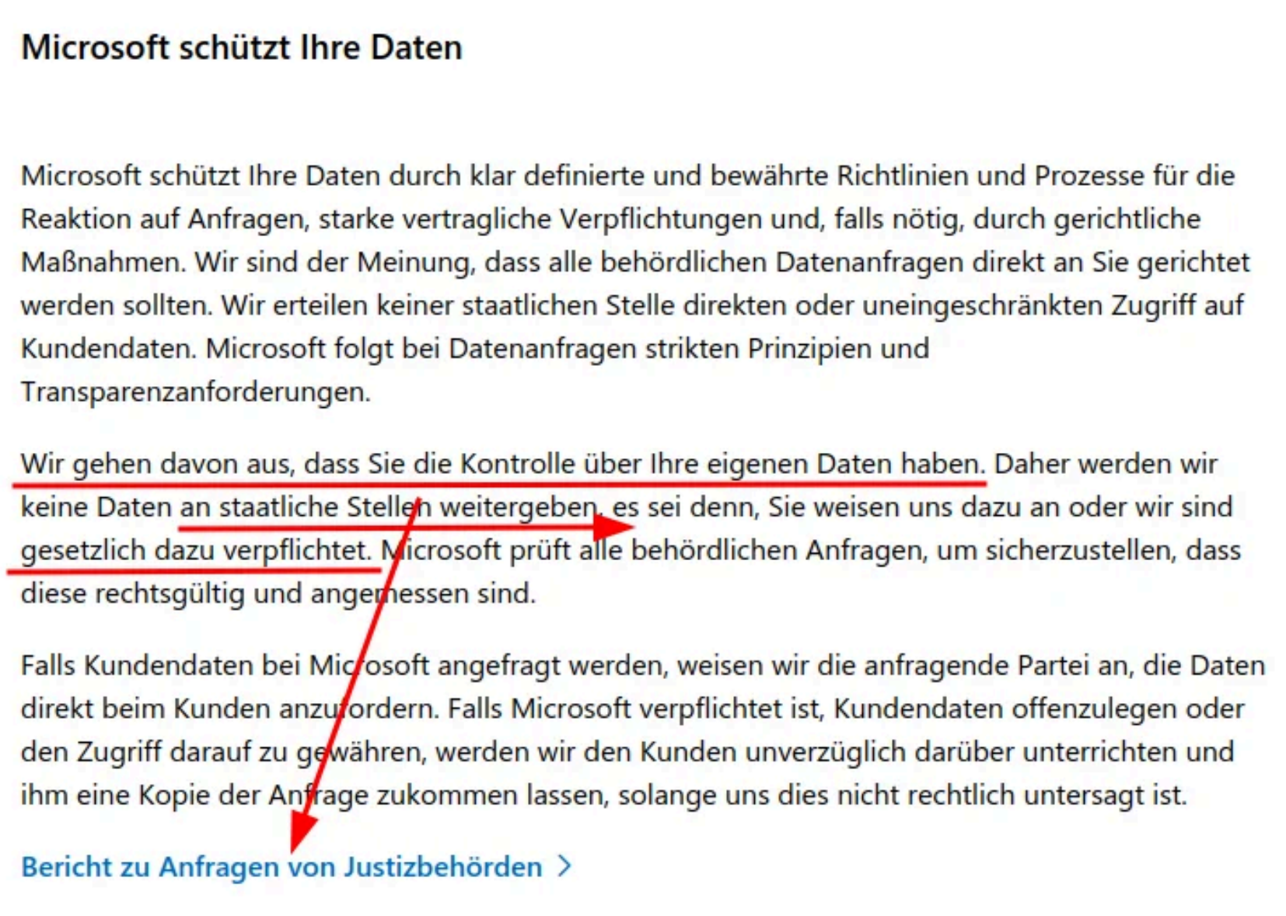
"Wir wollen unbedingt ChatGPT nutzen, also muss es sicher sein. Und wenn es nicht sicher ist, definieren wir es als sicher."

Das geht ganz einfach: ChatGPT auf einem Tenant (Server) in Deutschland oder Europa in der Azure Cloud hosten. Also in einem angeblich sicheren Datenraum, der nur einem selbst gehören würde. Immerhin steht der Server ja in Deutschland und ist somit angeblich sicher.

Bullshit.

Tatsächlich gibt es Unternehmen aus Deutschland, die das oder etwas ähnliches als Lösung verkaufen. Statt ChatGPT wird ann wahlweise Claude oder Gemini, und statt Azure wahlweise AWS eingesetzt.

Zu ChatGPT in der Azure Cloud schreibt Microsoft:



Microsoft schützt Ihre Daten

Microsoft schützt Ihre Daten durch klar definierte und bewährte Richtlinien und Prozesse für die Reaktion auf Anfragen, starke vertragliche Verpflichtungen und, falls nötig, durch gerichtliche Maßnahmen. Wir sind der Meinung, dass alle behördlichen Datenanfragen direkt an Sie gerichtet werden sollten. Wir erteilen keiner staatlichen Stelle direkten oder uneingeschränkten Zugriff auf Kundendaten. Microsoft folgt bei Datenanfragen strikten Prinzipien und Transparenzanforderungen.

Wir gehen davon aus, dass Sie die Kontrolle über Ihre eigenen Daten haben. Daher werden wir keine Daten an staatliche Stellen weitergeben, es sei denn, Sie weisen uns dazu an oder wir sind gesetzlich dazu verpflichtet. Microsoft prüft alle behördlichen Anfragen, um sicherzustellen, dass diese rechtsgültig und angemessen sind.

Falls Kundendaten bei Microsoft angefragt werden, weisen wir die anfragende Partei an, die Daten direkt beim Kunden anzufordern. Falls Microsoft verpflichtet ist, Kundendaten offenzulegen oder den Zugriff darauf zu gewähren, werden wir den Kunden unverzüglich darüber unterrichten und ihm eine Kopie der Anfrage zukommen lassen, solange uns dies nicht rechtlich untersagt ist.

Bericht zu Anfragen von Justizbehörden >

Quelle: Microsoft, 06.03.2026

Der Text gibt Anlass zum Nachdenken. WIr nehmen ihn Satz für Satz auseinander. Was hier nicht diskutiert ist, sind sogenannte KI-Anonymisierer, die angeblich automatisiert Texte anonymisieren, bevor sie ins unsichere ChatGPT geschickt werden. Das ist ebenso Bullshit. Vorab ein Bonbon (gilt für alle Cloud-Dienste von US-Unternehmen):

DAS DILEMMA FÜR EU-UNTERNEHMEN

Zahlen in USD = freiwillige Unterwerfung unter US-Recht

Viele EU-Unternehmen zahlen ihre Cloud-Rechnungen in USD – oft ohne zu wissen, dass sie damit einen **Jurisdiktions-Nexus** zur US-Finanzaufsicht herstellen. Wer in EUR zahlt, ist nicht vollständig geschützt: Microsofts eigene Bankverbindungen laufen über US-Institute. Der Hebel liegt **nicht beim Kunden, sondern bei Microsoft**. OFAC kann Microsoft zwingen, einem EU-Kunden **den Zugang zu sperren**.

USD-Zahlung → direkter Nexus · EUR-Zahlung → indirekter Nexus via MS · Zugang kann gesperrt werden: kein Datenschutzrecht greift · Völlig unabhängig von FISA/CLOUD Act

Betrifft alle US-Anbieter, nicht nur Microsoft oder andere KI-Anbieter.

Die folgenden Ausführungen betreffen in Teilen speziell Microsofts Datenschutzversprechen. Im Kern gelten die Kritikpunkte für **alle US-Unternehmen**, die teils sogar auf (fragwürdige) Versprechen verzichten und ebenso unsicher oder noch unsicherer sind (falls es für "unsicher" überhaupt eine Steigerung gibt).

Microsoft-Datenschutzversprechen – was wirklich gemeint ist

Die folgende Zitate beziehen sich allesamt auf die Microsoft Seite zum Azure Datenschutz.

Original: *„Microsoft schützt Ihre Daten durch klar definierte und bewährte Richtlinien und Prozesse für die Reaktion auf Anfragen, starke vertragliche Verpflichtungen und, falls nötig, durch gerichtliche Maßnahmen."*

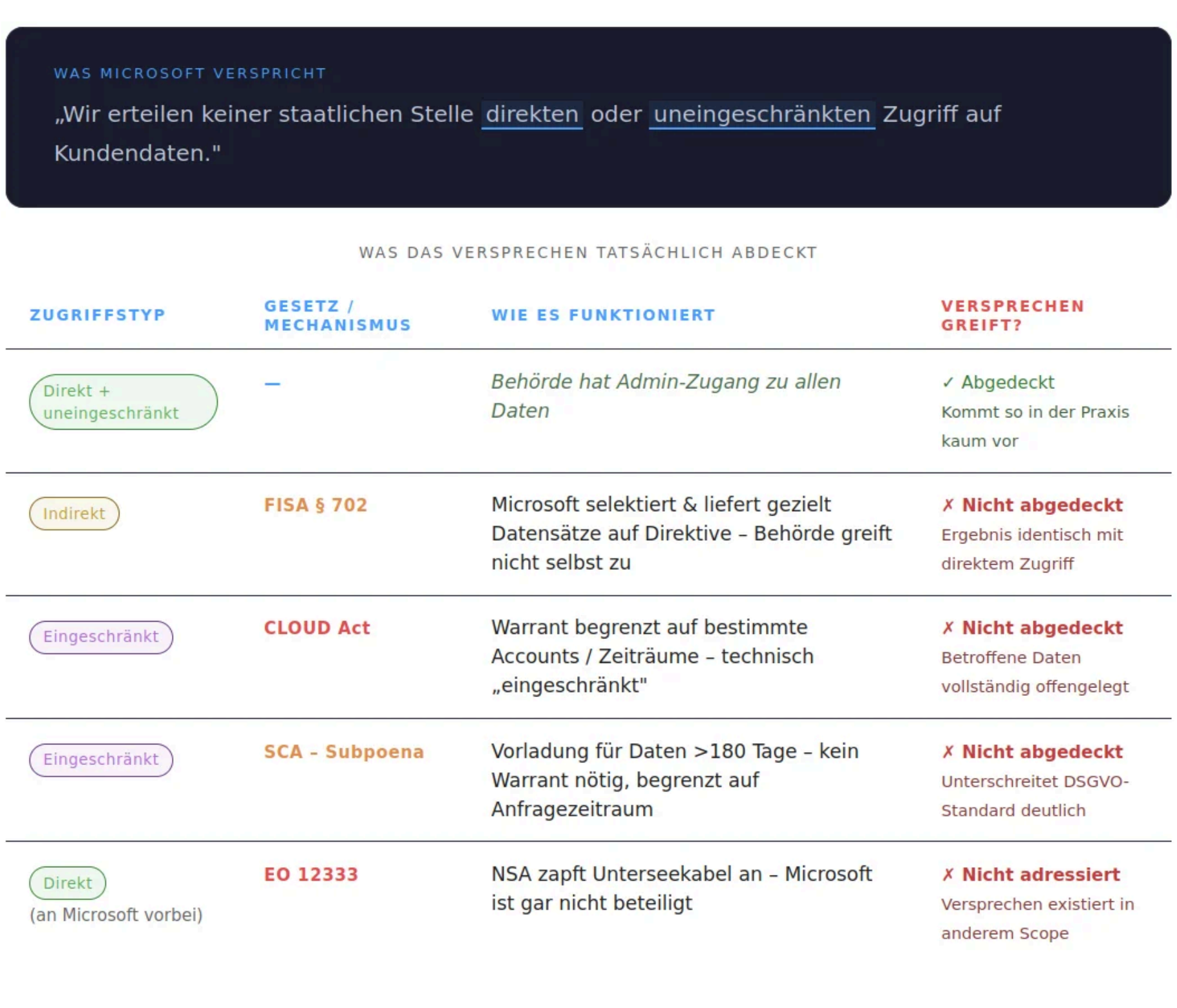
Realität: Microsoft ist als US-Unternehmen nach **FISA Section 702** und dem **CLOUD Act** gesetzlich verpflichtet, auf behördliche Anordnung Kundendaten herauszugeben – unabhängig von eigenen Richtlinien oder Verträgen. Vertragliche Zusagen (z. B. SCCs) werden durch einen US-Warrant schlicht überschrieben. Gerichtliche Maßnahmen *gegen* US-Behörden sind strukturell aussichtslos.

Original: *„Wir sind der Meinung, dass alle behördlichen Datenanfragen direkt an Sie gerichtet werden sollten."*

Realität: Diese Meinung ist rechtlich irrelevant. Nach **FISA Section 702** werden Anfragen nicht an den Kunden, sondern direkt und geheim an Microsoft gestellt. Der Kunde wird bewusst umgangen – und Microsoft darf ihn kraft Geheimhaltungspflicht nicht informieren.

Original: *„Wir erteilen keiner staatlichen Stelle direkten oder uneingeschränkten Zugriff auf Kundendaten."*

Realität: Nach **EO 12333** kann die NSA Daten abgreifen, *bevor* sie überhaupt bei Microsoft ankommen – durch Anzapfen von Unterseekabeln. Microsoft muss gar keinen Zugriff „erteilen", weil die Daten außerhalb seiner Kontrolle abgefangen werden. Zudem erlaubt EO 12333 die massenhafte Weitergabe dieser Daten an 16 weitere US-Behörden – ohne Gerichtsbeschluss.



WAS MICROSOFT VERSPRICHT

„Wir erteilen keiner staatlichen Stelle direkten oder uneingeschränkten Zugriff auf Kundendaten."

WAS DAS VERSPRECHEN TATSÄCHLICH ABDECKT

ZUGRIFFSTYP	GESETZ / MECHANISMUS	WIE ES FUNKTIONIERT	VERSPRECHEN GREIFT?
Direkt + uneingeschränkt	–	*Behörde hat Admin-Zugang zu allen Daten*	✓ Abgedeckt Kommt so in der Praxis kaum vor
Indirekt	FISA § 702	Microsoft selektiert & liefert gezielt Datensätze auf Direktive – Behörde greift nicht selbst zu	✗ Nicht abgedeckt Ergebnis identisch mit direktem Zugriff
Eingeschränkt	CLOUD Act	Warrant begrenzt auf bestimmte Accounts / Zeiträume – technisch „eingeschränkt"	✗ Nicht abgedeckt Betroffene Daten vollständig offengelegt
Eingeschränkt	SCA – Subpoena	Vorladung für Daten >180 Tage – kein Warrant nötig, begrenzt auf Anfragezeitraum	✗ Nicht abgedeckt Unterschreitet DSGVO-Standard deutlich
Direkt (an Microsoft vorbei)	EO 12333	NSA zapft Unterseekabel an – Microsoft ist gar nicht beteiligt	✗ Nicht adressiert Versprechen existiert in anderem Scope

„Kein direkter oder uneingeschränkter Zugriff" – das Versprechen definiert die einzige Zugriffsvariante weg, die niemand fordert. Alle anderen bleiben unbeantwortet.

Zugriff auf Daten ist möglich, trotz Versprechen.

Das Versprechen schützt gegen genau **einen Zugriffstyp** – den direkten, uneingeschränkten – der in der Praxis so gut wie nie vorkommt. Alle realen Zugriffsmechanismen unter US-Recht sind entweder **indirekt** (Microsoft liefert selbst) oder **formell eingeschränkt** (auf bestimmte Daten begrenzt), aber für die Betroffenen **in der Wirkung identisch**: ihre Daten landen bei US-Behörden – ohne ihr Wissen, ohne Rechtsschutz.

Original: *„Microsoft folgt bei Datenanfragen strikten Prinzipien und Transparenzanforderungen."*

Realität: Die Transparenz endet dort, wo US-Recht beginnt. Unter **FISA Section 702** und dem **SCA** (Stored Communications Act) besteht eine gesetzlich erzwungene Geheimhaltungspflicht. Microsoft kann und darf betroffene Kunden in vielen Fällen nicht informieren – Transparenz wird strukturell unmöglich gemacht.

Original: *„Wir gehen davon aus, dass Sie die Kontrolle über Ihre eigenen Daten haben."*

Realität: EU-Kunden haben de facto keine Kontrolle über ihre Daten. Der EuGH hat in **Schrems I & II** festgestellt, dass US-Überwachungsgesetze (insbesondere FISA 702) mit den EU-Grundrechten unvereinbar sind, weil sie Betroffenen keinen wirksamen Rechtsschutz gewähren. Nicht-US-Bürger haben keinerlei einklagbare Rechte gegenüber US-Behörden. Microsoft geht eben nur davon aus, dass Sie die Kontrolle über Ihre Daten haben – wohlwollend, dass jederzeit das Gegenteil der Fall sein kann.

Original: *„Daher werden wir keine Daten an staatliche Stellen weitergeben, es sei denn, Sie weisen uns dazu an oder wir sind gesetzlich dazu verpflichtet."*

Realität: Die Ausnahme „gesetzlich dazu verpflichtet" ist der Normalfall, nicht die Ausnahme. **CLOUD Act**, **FISA 702** und **SCA** schaffen weitreichende gesetzliche Herausgabepflichten. Der Zusatz „oder Sie weisen uns dazu an" verschleiert, dass Microsoft diese Daten auch ohne jede Kundenanweisung herausgeben muss – und muss er das, darf er den Kunden nicht einmal informieren.

Original: *„Microsoft prüft alle behördlichen Anfragen, um sicherzustellen, dass diese rechtsgültig und angemessen sind."*

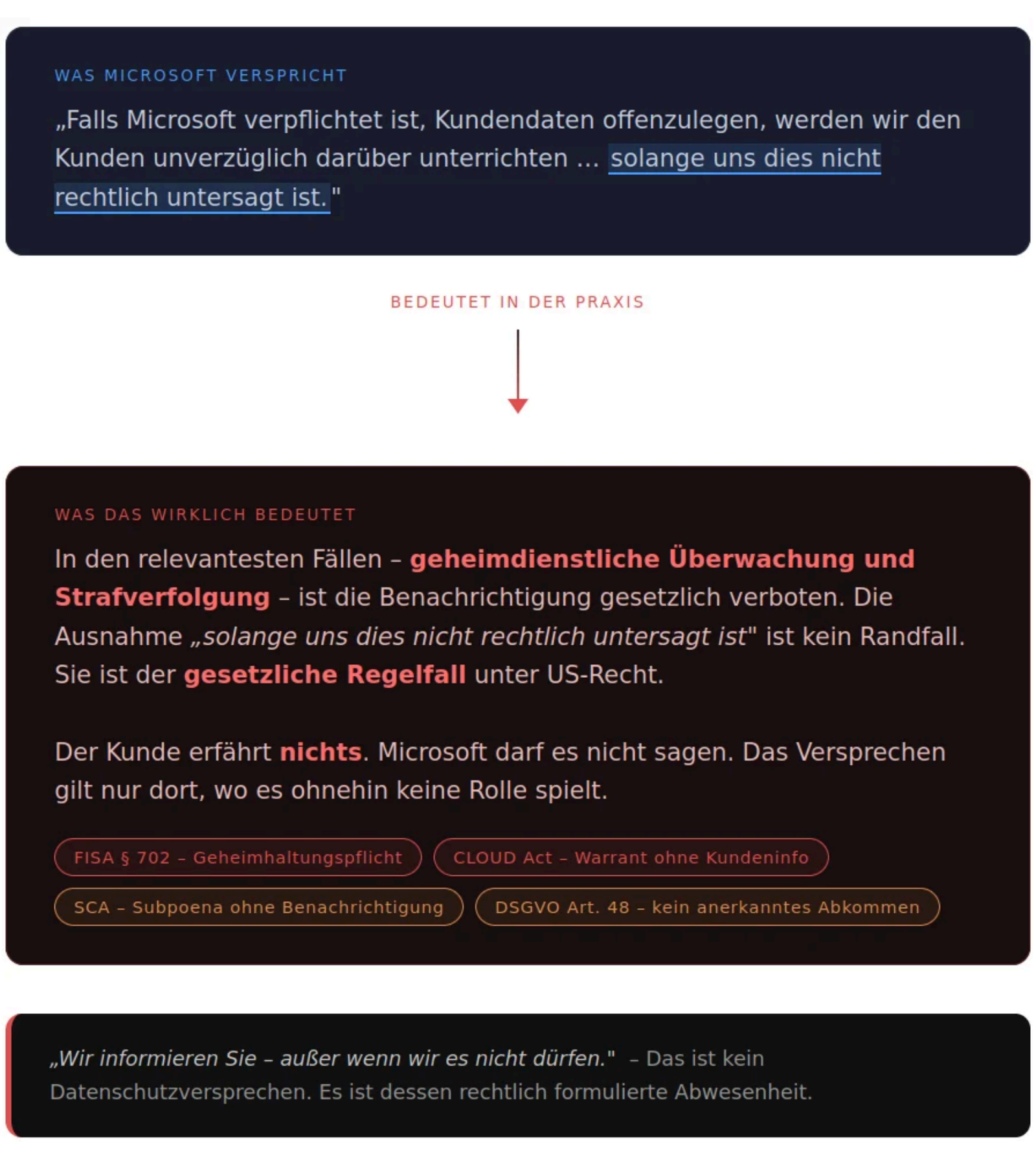
Realität: Die Prüfung erfolgt ausschließlich nach **US-Recht** – nicht nach der DSGVO. Was nach US-Recht „rechtsgültig" ist (z. B. ein CLOUD-Act-Warrant oder eine FISA-702-Direktive), verstößt nach **DSGVO Art. 48** gegen EU-Recht, da kein anerkanntes internationales Abkommen zugrunde liegt. Microsoft ist strukturell nicht in der Lage, beide Rechtsordnungen gleichzeitig zu erfüllen.

Original: *„Falls Kundendaten bei Microsoft angefragt werden, weisen wir die anfragende Partei an, die Daten direkt beim Kunden anzufordern."*

Realität: Unter **FISA Section 702** ist genau das ausgeschlossen. Die Behörde wendet sich per Direktive an Microsoft – nicht an den Kunden. Microsoft hat keine rechtliche Handhabe, die NSA oder das DOJ auf den Kunden zu verweisen.

Original: *„Falls Microsoft verpflichtet ist, Kundendaten offenzulegen oder den Zugriff darauf zu gewähren, werden wir den Kunden unverzüglich darüber unterrichten und ihm eine Kopie der Anfrage zukommen lassen, solange uns dies nicht rechtlich untersagt ist."*

Realität: Der Nachsatz „solange uns dies nicht rechtlich untersagt ist" macht die gesamte Zusage wertlos. Unter **FISA 702**, **SCA** und **CLOUD Act** ist die Benachrichtigung des Kunden regelmäßig gesetzlich verboten. In den praktisch relevantesten Fällen – geheimdienstliche Überwachung und Strafverfolgung – erfährt der Kunde nichts. Die Benachrichtigungszusage gilt damit nur für den rechtlich uninteressanten Ausnahmefall.



WAS MICROSOFT VERSPRICHT

„Falls Microsoft verpflichtet ist, Kundendaten offenzulegen, werden wir den Kunden unverzüglich darüber unterrichten … solange uns dies nicht rechtlich untersagt ist."

BEDEUTET IN DER PRAXIS

WAS DAS WIRKLICH BEDEUTET

In den relevantesten Fällen – **geheimdienstliche Überwachung und Strafverfolgung** – ist die Benachrichtigung gesetzlich verboten. Die Ausnahme *„solange uns dies nicht rechtlich untersagt ist"* ist kein Randfall. Sie ist der **gesetzliche Regelfall** unter US-Recht.

Der Kunde erfährt **nichts**. Microsoft darf es nicht sagen. Das Versprechen gilt nur dort, wo es ohnehin keine Rolle spielt.

FISA § 702 – Geheimhaltungspflicht · CLOUD Act – Warrant ohne Kundeninfo · SCA – Subpoena ohne Benachrichtigung · DSGVO Art. 48 – kein anerkanntes Abkommen

„Wir informieren Sie – außer wenn wir es nicht dürfen." – Das ist kein Datenschutzversprechen. Es ist dessen rechtlich formulierte Abwesenheit.

Microsofts Datenschutzversprechen: Kritischer Kern.

> **Fazit:** Die Datenschutzversprechen von Microsoft sind nach strenger Betrachtung keine rechtlich durchsetzbaren Garantien, sondern Absichtserklärungen, die unter US-Recht systematisch ausgehöhlt werden. Sie stehen im direkten Widerspruch zu **DSGVO Art. 44 ff.** (Drittlandtransfers) und **Art. 48** (behördliche Zugriffsanordnungen) und vermitteln EU-Kunden ein falsches Sicherheitsgefühl.

US-Spionage per Gesetz

Die DSGVO ist unvereinbar mit US-Rechtsvorschriften. US-Unternehmen müssen sich entscheiden:

1. DSGVO einhalten und Probleme mit der amerikanischen Justiz oder Regierung bekommen
   ODER stattdessen
2. DSGVO ignorieren und die amerikanische Justiz oder Regierung zufrieden stellen.

Beides gleichzeitig gleich nicht, wie eine Prüfung der US-Rechtsvorschriften zeigt.

Die wichtigsten US-Rechtsgrundlagen, die uns deutsche und andere Ausländer (aus US-Sicht) betreffen, sind folgende.

1. FISA Section 702

- Erlaubt der US-Regierung, US-Anbieter per Direktive zu zwingen, Kommunikation ausländischer Zielpersonen herauszugeben
- Keine individuelle richterliche Genehmigung pro Zielperson, Massenzugriff möglich
- Führt zu "incidental collection" von EU-Bürgerdaten
- Zweimal vom EuGH für unvereinbar mit EU-Grundrechten erklärt (Schrems I & II)
- Anbieter dürfen Betroffene nicht informieren (Geheimhaltungspflicht)

2. Executive Order 12333 (EO 12333)

- Gibt US-Geheimdiensten weitreichende Befugnis zur "Signals Intelligence" weltweit – ohne Gerichtsbeschluss
- Erlaubt der NSA, massenhaft private Daten ohne Warrants mit 16 anderen Behörden zu teilen
- Kernproblem laut EuGH: Massenüberwachung durch Anzapfen von Unterseekabeln, Daten werden abgegriffen bevor sie in den USA ankommen
- Kein effektiver Rechtsschutz für Nicht-US-Bürger

3. CLOUD Act (2018)

- Ermöglicht US-Strafverfolgungsbehörden, Daten von US-Unternehmen im Ausland per Warrant anzufordern
- Kollidiert direkt mit DSGVO Art. 48: EU-Daten dürfen nur auf Basis eines anerkannten internationalen Abkommens an Drittstaaten übermittelt werden – ein CLOUD Act Warrant ist kein solches
- US-Anbieter stecken im Dilemma: CLOUD Act befolgen = DSGVO-Verstoß; verweigern = US-Contempt of Court
- Standard Contractual Clauses (SCCs) lösen das Problem nicht – ein Warrant überschreibt vertragliche Zusagen

4. SCA – Stored Communications Act (1986)

- Regelt die freiwillige und erzwungene Herausgabe gespeicherter digitaler Kommunikation (E-Mails, Cloud-Daten) durch ISPs
- Für Inhalte unter 180 Tagen ist ein Warrant nötig – für ältere Daten reicht teils eine Vorladung (Subpoena), was DSGVO-Standards deutlich unterschreitet
- Veraltet (1986), von modernen Cloud-Diensten längst überholt; schafft Rechtsunsicherheit für internationale Anbieter
- Bildet die Grundlage des CLOUD Act – dessen Probleme (s.o.) bauen direkt darauf auf
- Kein Äquivalent zu DSGVO-Betroffenenrechten (Auskunft, Löschung etc.)

Kurz zusammengefasst:

Alle vier Regelwerke ermöglichen US-Behörden den Zugriff auf EU-Personendaten ohne ausreichenden Rechtsschutz für Betroffene – im direkten Widerspruch zu DSGVO Art. 44 ff. (Drittlandtransfers) und Art. 48

Ganzen Artikel jetzt über kostenfreien Dr. DSGVO Newsletter lesen.
Weitere Extras für Abonnenten:
Viele Artikel in PDF-Form · Kompakte Kernaussagen für Beiträge · Offline-KI · Freikontingent+ für Website-Checks
Schon Abonnent? Link im Newsletter anklicken & diese Seite auffrischen.
↓
Newsletter abonnieren

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/microsoft-datenschutz-in-der-cloud-wegen-serverstandort-eu

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.