



## Informationen zum Thema Datenschutz

Liebe Leserin, lieber Leser,

auch wenn das informationelle Selbstbestimmungsrecht schon seit Jahrzehnten besteht,

entwickelt sich der Datenschutz dynamisch weiter, da er auf technische und rechtliche Entwicklungen reagieren muss.

In Ihrer neuen Ausgabe finden Sie ganz aktuell Hinweise,

wie Sie es vermeiden können, durch Nutzung einer Künstlichen Intelligenz (KI) ungewollt zum Geheimnisverräter zu werden.

Nicht minder aktuell sind die Entwicklungen bei den Transfers personenbezogener Daten in die USA und beim neuen Data Privacy Framework (DPF).

Ich wünsche Ihnen viel Spass beim Lesen.

Detlef Riese  
Datenschutzbeauftragter

---

## Geheimnisverrat an die KI?

**Einen langen Text kürzen, Ergebnisse einer Besprechung zusammenfassen oder Programmcode schreiben – die Möglichkeiten eines KI-Dienstes wie ChatGPT scheinen fast grenzenlos. Doch leider sind auch die möglichen Risiken durch Künstliche Intelligenz (KI) weitreichend. Das darf niemand bei dem Hype um KI vergessen.**

### Der Hoffnungsträger KI

Künstliche Intelligenz gilt als eine Schlüsseltechnologie, die praktisch überall zum Einsatz kommen soll, ob in der Automobilbranche, im Maschinenbau oder im Dienstleistungsbereich, so der Digitalverband Bitkom.

Unternehmen erhoffen sich schnellere und präzisere Problemanalysen, beschleunigte Prozesse und einen geringeren Ressourcenverbrauch.



Aber auch im Personalbereich werden Vorteile gesehen, etwa die Vermeidung menschlicher Fehler und die Möglichkeit, durch KI Expertenwissen ins Unternehmen zu holen.

Durch KI können sich Beschäftigte auf andere Aufgaben konzentrieren, hoffen die Unternehmen.

Tatsächlich aber sollte man sich zuerst einmal auf die KI und ihre möglichen Risiken konzentrieren, bevor man durch Dienste wie ChatGPT Aufwände einsparen will.

### Das übersehene Risiko KI

Wie bei vielen neuen Technologien erzeugt KI auch Angst und Bedenken. Trotzdem werden ChatGPT & Co. munter genutzt, die Neugierde siegt, mögliche Bedenken werden beiseitegeschoben. Das kann aber mehr als riskant sein, für die eigene Privatsphäre, für den Datenschutz im Unternehmen sowie für die Betriebs- und Geschäftsgeheimnisse.

So hilfreich es erscheint, wenn ein Online-Dienst etwa einen langen Text zusammenfasst oder aus ein paar Notizen ein Besprechungsprotokoll erstellt: Die Inhalte der Notizen und Texte können personenbezogene und andere zu schützende Informationen enthalten. Wenn man zum Beispiel über die neue Produktplanung spricht und sich automatisiert das Protokoll der Planungssitzung erzeugen lässt, besteht die Gefahr, dass die Informationen abfließen, also das Unternehmen verlassen und Dritten bekannt werden könnten.

Letztlich könnte so die Nutzung der KI ungewollt Geheimnisse verraten, denn eine KI lernt von den Eingaben und Reaktionen der Nutzenden auf die Antworten. Lernen bedeutet aber auch, Informationen in den Datenbestand der KI aufzunehmen.

### KI braucht Regeln

In den meisten Unternehmen fehlen noch interne Richtlinien für den Umgang mit einer KI. Doch KI-Tools sollten nicht ohne jede Regelung zum Einsatz kommen, so wie beispielsweise die Nutzung einer Cloud nach internen Richtlinien erfolgen sollte.

Wer also einen KI-Dienst betrieblich nutzen will, sollte zuerst klären, ob das im Unternehmen erlaubt und gewünscht ist. Dann gilt es zu klären, zu welchem Zweck und mit welchen Daten der erlaubte KI-Dienst eingesetzt werden darf. Maßstab sollte dabei immer sein, die KI wie einen Dritten, der nicht zum Unternehmen gehört, anzusehen. Soll eine Information das Unternehmen nicht verlassen, gehört sie auch nicht in das Eingabefeld einer KI.

### Tipp: Auch bei KI gibt es Datenschutzeinstellungen

KI-Dienste wie ChatGPT bessern gegenwärtig bei ihren Datenschutzeinstellungen nach.



Es ist wichtig, sich auch hier mit den Einstellungen zu befassen und zum Beispiel die Übernahme der Eingaben in den Datenbestand der KI zu verbieten.

Gleichzeitig sollte man der KI trotzdem keine vertraulichen und sensiblen Daten anvertrauen, um jeden Geheimnisverrat zu vermeiden.

---

## Das EU-U.S. Data Privacy Framework



**Was lange währt, wird endlich gut. Dieses Motto gilt hoffentlich für das EU-U.S. Data Privacy Framework. Sie kennen dieses Stichwort noch gar nicht? Es geht um eine neue Rechtsgrundlage für Datenübermittlungen in die USA. Dabei gilt es einige Fallstricke zu beachten.**

**Der 16. Juli 2020 weckt böse Erinnerungen**

Der 16. Juli 2020 war für alle Unternehmen, die auf Datenübermittlungen in die USA angewiesen sind, ein schwarzer Tag. Denn damals erklärte der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der EU-Kommission zum „Privacy Shield“ für nichtig. Von diesem Tag an konnten Unternehmen Datenübermittlungen in die USA nicht mehr auf den Angemessenheitsbeschluss als Rechtsgrundlage stützen.

Das war schmerzlich, denn Datenübermittlungen auf seiner Basis verursachten nur einen geringen rechtlichen Aufwand. Alle denkbaren Alternativen, auf die sie von da an zurückgreifen mussten, waren für die Unternehmen dagegen zum Teil mit wahren Papierbergen verbunden.

### Der rechtliche Schwebezustand hat jetzt ein Ende

Seit dem 10. Juli 2023 gibt es wieder einen Angemessenheitsbeschluss der EU-Kommission, den Unternehmen für Datenübermittlungen in die USA nutzen können. Darin ist festgehalten, dass unter bestimmten Bedingungen in den US-Unternehmen ein angemessenes Datenschutzniveau herrscht.

Wohlgemerkt: unter bestimmten Bedingungen. Aber wenn sie erfüllt sind, funktioniert wieder alles so, wie man es vor dem 16. Juli 2020 mit dem „Privacy Shield“ gewohnt war. Unternehmen in der EU können also wieder personenbezogene Daten an ihre US-Geschäftspartner übermitteln, ohne dafür umfangreiche zusätzliche Datenschutzregelungen vereinbaren zu müssen.



### Der Jubel ist trotzdem eher verhalten

Die neuen Regelungen wurden in der Wirtschaft dankbar registriert. Immerhin bringen sie erhebliche Erleichterungen für den „Datenschutzalltag“. Echte Begeisterung spürt man allerdings nur selten. Eher herrscht eine gewisse Skepsis, was die Zukunft der neuen Regelungen angeht. Über kurz oder lang wird es auf irgendeinem Weg dazu kommen, dass der EuGH auch sie rechtlich überprüft. Werden sie dann Bestand haben?

### Die neuen Regelungen werden bis auf Weiteres tragfähig sein

So verständlich solche Befürchtungen sind – im Augenblick helfen die neuen Regelungen wirklich weiter.

Das Grundschema, nach dem sie funktionieren, ist relativ einfach: US-Unternehmen können sich in den USA in eine Art Datenschutzregister eintragen lassen. Es trägt die Bezeichnung „Data Privacy Framework List“. Dazu müssen sie ziemlich viele Voraussetzungen erfüllen. So müssen etwa ausreichende Datensicherungsmaßnahmen vorhanden sein.

Wenn ein US-Unternehmen diesen Zertifizierungsprozess erfolgreich abgeschlossen hat, können sich seine Geschäftspartner in der EU darauf verlassen, dass in diesem US-Unternehmen ein angemessenes Datenschutzniveau herrscht. Das bildet die rechtliche Basis dafür, dass die Übermittlung personenbezogener Daten dorthin zulässig ist.

### Für Personaldaten gelten Besonderheiten

Die Frage, ob auf dieser Basis auch eine Übermittlung von Personaldaten zulässig ist, lautet: „Ja, aber ...“. Die Übermittlung solcher Daten an ein US-Unternehmen setzt voraus, dass dieses Unternehmen zusätzliche Verpflichtungen einght. Dazu gehört insbesondere die Verpflichtung, mit den Datenschutz-Aufsichtsbehörden in der EU zusammenzuarbeiten.

### Die Zertifizierung ist jedes Jahr zu erneuern

US-Unternehmen, die auf der „Data Privacy Framework List“ stehen, müssen ihre Zertifizierung jedes Jahr erneuern lassen. Sonst werden sie von der Liste gestrichen. Deshalb müssen sich ihre Geschäftspartner in der EU jedes Jahr vergewissern, dass die Zertifizierung erneuert wurde. Im Augenblick richten alle betroffenen Unternehmen in der EU die dafür nötigen Abläufe ein, wenn sie nicht ohnehin schon vorhanden sind.



## Microsoft 365 bleibt eine Herausforderung

Viele Unternehmen hatten gehofft, dass der neue Angemessenheitsbeschluss alle vorhandenen Probleme bei Datenübermittlungen in die USA löst. Dies galt besonders für den Einsatz von Microsoft 365. Hier gießen jedoch die ersten Aufsichtsbehörden für den Datenschutz schon wieder Wasser in den Wein. Sie verweisen darauf, dass bei Microsoft 365 weiterhin unklar sei, welche Daten Microsoft in den USA verarbeitet und was dabei geschieht.

Ob diese Behauptung zutrifft, sei dahingestellt. Dass der neue Angemessenheitsbeschluss nicht von der Pflicht befreit, die Datenverarbeitung transparent zu gestalten, steht auf alle Fälle fest. Sofern es Unklarheiten gibt, bietet der Angemessenheitsbeschluss keine Hilfe. Hier gilt es also weiterhin, Lösungen zu finden.

---

## Impressum

Detlef Riese (ITDSC UG)

Datenschutzbeauftragter

**Anschrift:**

ITDSC UG • Bethanienstrasse 8 • 03172 Guben

Telefon: 03561 5595574 • E-Mail: [d.riese@itdsc.de](mailto:d.riese@itdsc.de)