



**ZENDAS**

Zentrale Datenschutzstelle der  
baden-württembergischen Universitäten

# **EU-U.S. Data Privacy Framework (**DPF**)- Die **p**lagenden **F**ragen**

**Fortbildung**

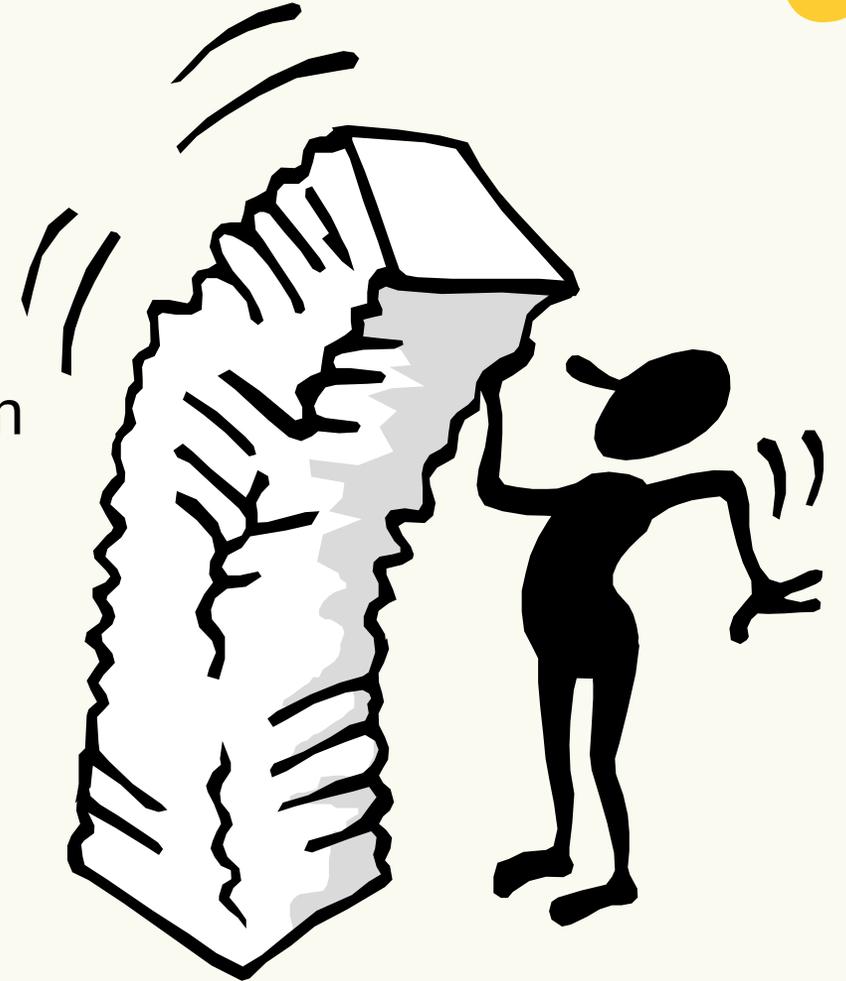
# 1. Was ist ein Angemessenheitsbeschluss und welche Wirkung hat er?

- Beschluss der EU-Kommission, dass „das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland [...] ein angemessenes Schutzniveau bietet.“ (Art. 45 Abs. 1)
- Unmittelbar geltendes Recht, egal was Datenschützer, Aufsichtsbehörden und nationale Gerichte denken. Verwerfungskompetenz liegt ausschließlich beim EuGH.
- Datenübermittlungen sind auf Basis des Beschlusses ohne weitere Maßnahmen zulässig und bedürfen keiner anderen Rechtsgrundlage aus Art. 46-50 (Art. 45 Abs. 3).
- Vorteil DPF gegenüber SCC: Kein Transfer Impact Assessment (TIA) und keine zusätzlichen Schutzmaßnahmen
- DPF: [https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en)



## 2. Wie ist der Angemessenheitsbeschluss zum DPF aufgebaut?

- 62 Seiten Erwägungsgründe
- 1,5 Seiten Angemessenheitsbeschluss
- Ca. 70 Seiten Anlagen, darunter 30 Seiten Prinzipien und Verfahrensgrundsätze, dann ca. 40 Seiten Schreiben diverser US-Einrichtungen



### 3. Sind die USA jetzt ein sicheres Drittland?

- Nein. Es ist kein Angemessenheitsbeschluss, der für ein Land oder Gebiet gilt, sondern ein **sektoraler** Angemessenheitsbeschluss.

“The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation” (Annex I, I.1.)

- Gilt nur für Organisationen, die auf der Liste des DPF stehen:

<https://www.dataprivacyframework.gov/s/>

- **Achtung:** Bei Beschäftigtendaten immer erst prüfen, ob sich Zertifizierung auf der Liste auch auf diese Datenkategorie bezieht.
- Gültig ab 10.07.2023



## 4. Unter welchen Voraussetzungen kommen Organisationen auf die Liste des DPF?

- a) Organisation unterliegt der Aufsicht der Federal Trade Commission oder des U.S. Department of Transportation oder einer anderen US-Aufsichtseinrichtung, die die Einhaltung der datenschutzrechtlichen Prinzipien überwacht.
- b) Sie verpflichtet sich öffentlich zur Einhaltung der Prinzipien (Annex I, II.).
- c) Sie macht Ihre Datenschutzerklärung im Einklang mit diesen Prinzipien öffentlich bekannt.
- d) Sie setzt die Prinzipien vollständig um.

(Annex I, I.2.)

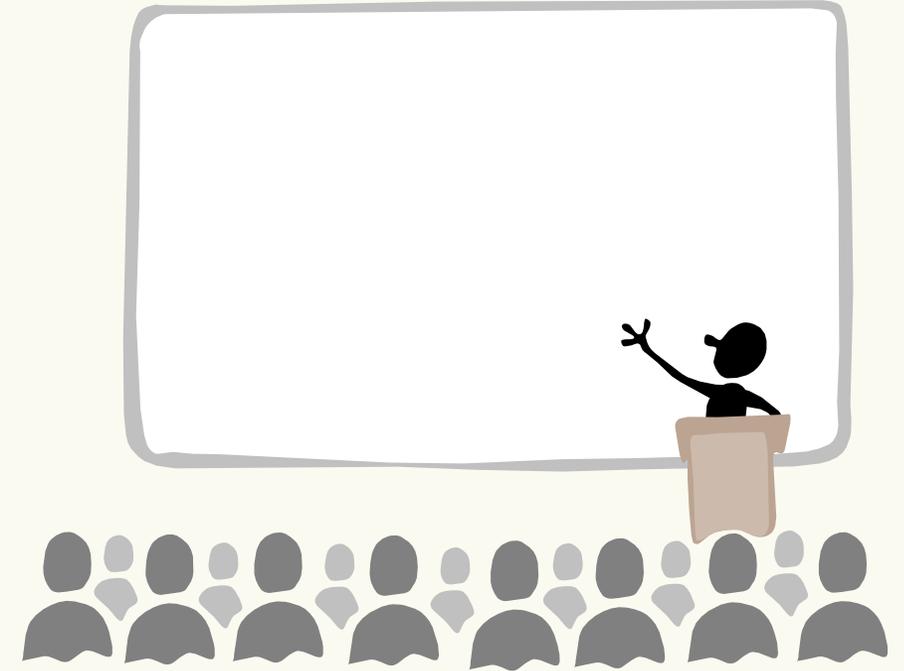
## 4. Unter welchen Voraussetzungen kommen Organisationen auf die Liste des DPF?

- Selbstzertifizierungsmechanismus (jährliche Erneuerung)
- **Achtung:** gilt nur für „commercial organizations participating in the EU-US Data Privacy Framework“ ([https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en));
- Organisationen, die bislang auf der Privacy-Shield-List stehen, werden automatisch ab dem 17.07.23 auf der DPF-Liste stehen (sofern sie dies nicht zuvor widerrufen) (vgl. Annex I, III.6.e.); dreimonatige „Anpassungsfrist“

Hintergrund: Kritikpunkte des EuGH in Schrems II wandte sich vor allem gegen die Rechtslage in den USA, nicht gegen die Anforderungen der Privacy-Shield-Liste.

## 5. Können auch US-Universitäten auf die Liste des DPF?

- Wenn sie der Aufsicht des FTC oder des U.S. Department of Transportation unterliegen.
- Auf der Liste ist keine aufgeführt.
- *Glocker, Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework, RDi 2023, 465 (470): „[...] öffentliche Einrichtungen wie forschende Universitäten [können sich nicht selbst zertifizieren]“*



## 6. Braucht man noch einen AVV, wenn der Auftragsverarbeiter in den USA sitzt?

10

Ja. Unabhängig davon, ob der Auftragsverarbeiter am DPF teilnimmt oder nicht, bedarf es eines AVV (Annex I III.10.a.i DPF).



## 7. Sind die SCC überflüssig geworden?

Nein.

- Notwendig für Organisationen, die nicht auf der DPF-Liste stehen.
- Grundsatz der Vertragsfreiheit: Selbst mit Organisationen, die auf der DPF-Liste stehen, könnten SCC als Transfertool genutzt werden. (das ergibt sich aus Punkt 7 dieser FAQ: [https://ec.europa.eu/commission/presscorner/detail/de/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752); DPF fließt dann nach Meinung der EU offenbar positiv in die dann vorzunehmende TIA ein: Änderungen im US-Recht auf Basis der Executive Order beziehen sich danach auf alle Transfermechanismen)



## 8. Welche Auswirkungen hat der Angemessenheitsbeschluss beim Einsatz von SCC?

- Im Rahmen des Transfer Impact Assessment (Klausel 14) muss Rechtslage im Drittland beurteilt werden.
- Quelle für Beurteilung der Rechtslage kann ein Angemessenheitsbeschluss sein (siehe EDSA 01/2020, Anhang 3, Rn. 44, 2. Spiegelstrich).
- **Executive Order 14086** ist Grundlage für Änderung der Rechtslage in den USA.
- EU-Kommission bringt im **Angemessenheitsbeschluss** zum Ausdruck, dass die neue Rechtslage nicht (mehr, weil die Kritiken des EuGH in Schrems II aufgegriffen wurden) im Widerspruch zu den Grundprinzipien der EU steht. **Und weil die Änderung eben bedingt ist durch die EO 14086 und nicht durch den DPF, gilt die Änderung der Rechtslage gerade auch für Unternehmen, die nicht auf der DPF-Liste stehen.**
- (Schrems II hatte Überwachungsbefugnisse durch Behörde für nationale Sicherheit und Rechtsschutz dagegen kritisiert; genau diese Punkte ändert die Executive Order 14086 – nach Meinung der EU-Kommission zum Positiven)



## 8. Welche Auswirkungen hat der Angemessenheitsbeschluss beim Einsatz von SCC?

- Nur die Änderung der Rechtslage in den kritisierten Punkten war aber nicht ausreichend, um vollständig ein der EU entsprechendes Datenschutzniveau herzustellen.
- Deshalb bedarf es entweder der Selbstverpflichtung der Organisationen (und damit verbunden des Eintrags in die DPF-List) oder des Abschlusses der SCC.

## 9. Wenn SCC abgeschlossen wurden, treten diese automatisch außer Kraft?

- Nur wenn vertragliche (z.B. in einem abgeschlossenen AVV) geregelt ist, dass bei Inkrafttreten eines Angemessenheitsbeschlusses dieser automatisch als Grundlage für den Datentransfer genutzt werden soll.

Oder

- Wenn die Zustimmung zu den SCC von einer Vertragspartei widerrufen werden (Klausel 16e).

Ansonsten:

- SCC gelten vorrangig weiter.



# 10. Braucht man noch ein TIA, wenn man Übermittlungen auf DPF stützt?

Nein, weil die Anforderung danach aus den SCC kommt.

Anmerkung:

GDD bezeichnet die Notwendigkeit der TIA bei SCC in Frage 8 ihrer "FAQ zum Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework" (für uns nicht nachvollziehbar) als „nicht eindeutig“ geklärt.

<https://www.gdd.de/wp-content/uploads/2023/07/Stellungnahme-zum-Angemessenheitsbeschluss-der-EU-Kommission.pdf>



# 11. Welche Auswirkungen hat der Angemessenheitsbeschluss beim Einsatz einer Einwilligung?

- Einwilligung nach Art. 49 Abs. 1 lit. a DS-GVO kommt in Betracht, wenn Empfänger nicht auf DPF-Liste steht, keine SCC abgeschlossen werden und es sich lediglich um einen Einzelfall handelt.

Beispiel: [https://www.zendas.de/themen/drittlandstransfer/uebermittlung\\_zeugnisse\\_drittland.html](https://www.zendas.de/themen/drittlandstransfer/uebermittlung_zeugnisse_drittland.html)

- Inhalt: Aufklärung über für die betroffene Person bestehenden möglichen Risiken
- Rechtslage hat EO 14086 geändert, aber das alleine reicht nicht aus, um ein der EU entsprechendes Datenschutzniveau zu erreichen. Daher sind die Risiken jetzt zwar nicht mehr, dass es unverhältnismäßige Überwachungsmaßnahmen und fehlende Rechtsschutzmöglichkeiten gibt.



# 11. Welche Auswirkungen hat der Angemessenheitsbeschluss beim Einsatz einer Einwilligung?

„Risiko-Text“ **vor** Angemessenheitsbeschluss:

- Die Befugnisse der US-amerikanischen Behörden hinsichtlich des Zugriffs auf Daten, die aus der Europäischen Union in dieses Drittland übermittelt werden, sind nicht auf das zwingend erforderliche Maß beschränkt. Den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des us-amerikanischen Rechts wird Vorrang eingeräumt, was Eingriffe in die Grundrechte der Personen ermöglicht, deren Daten in die Vereinigten Staaten übermittelt werden.
- Es bestehen darüber hinaus keine ausreichenden effektiven Rechtsschutzmöglichkeiten für betroffene Personen, insbesondere sind den betroffenen Personen keine Rechte verliehen, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können.



# 11. Welche Auswirkungen hat der Angemessenheitsbeschluss beim Einsatz einer Einwilligung?

„Risiko-Text“ **nach** Angemessenheitsbeschluss:

Die Rechtslage in den USA sieht (im Gegensatz zu früher) nach einer Executive Order des Präsidenten vom 07.10.2022 Einschränkungen hinsichtlich der Befugnisse von U.S.-amerikanischen Behörden vor und gibt auch dahingehend Rechtsschutzmöglichkeiten, die die EU als ausreichend erachtet hat. Jedoch existieren möglicherweise andere Vorschriften nicht, die in der EU die Datenverarbeitung (einschränkend) regeln. Welche Regelungen dies genau betrifft, ist vom jeweiligen U.S.-Bundesstaat abhängig.

Es gibt insbesondere möglicherweise keine dem EU-Recht entsprechende Regelungen zur

- Zweckbindung, d.h. die Daten dürfen für andere Zwecke verarbeitet und damit ggf. auch an weitere Stellen übermittelt werden,
- Speicherbegrenzung, d.h. die Daten können länger verarbeitet werden als für den konkreten Zweck erforderlich,
- Sicherheit der Verarbeitung, d.h. keine oder andere Vorschriften, wie insbesondere Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet werden,
- Verarbeitung durch Auftragnehmer des Datenimporteurs,
- Meldung von Verletzungen des Schutzes personenbezogener Daten.
- Sicherstellung der Betroffenenrechte, wie Auskunft, Berichtigung oder Löschung



## 12. Welche Auswirkungen hat die EO 14086/ das DPF auf den CLOUD-Act?

- Teilweise Äußerungen von US-Tochterunternehmen, sie würden sich an Patriot Act (Vorläufer des CLOUD Act) gebunden sehen und müssten ggf. Daten in die USA übermitteln.
- Rechtsprechung gegen das Unternehmen Microsoft, das sich (ziemlich erfolgreich) weigerte, in Irland gespeicherte Daten herauszugeben. Kurz bevor Supreme Court entschied, hat Gesetzgebung CLOUD-Act mit eindeutiger Regelung erlassen.

Ausführlich: [https://www.zendas.de/themen/cloud\\_computing/patriot\\_act.html](https://www.zendas.de/themen/cloud_computing/patriot_act.html)

### Datenschutzrechtlich:

**Ausschlussgrund für die Beauftragung mangels ausreichender Gewähr trotz Privacy Shield?**



# 12. Welche Auswirkungen hat die EO 14086/ das DPF auf den CLOUD-Act?

## 18 U.S.C. § 2713:

A **provider of electronic communication** service or **remote computing service** shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located **within** or **outside** of the United States. (Hervorhebung durch ZENDAS)

Ein **Anbieter elektronischer Kommunikationsdienste** oder **Remote-Computing-Dienste** muss die in diesem Kapitel enthaltenen Verpflichtungen zur Aufbewahrung, Sicherung oder Offenlegung des Inhalts einer drahtgebundenen oder elektronischen Kommunikation und aller Aufzeichnungen oder anderer Informationen über einen Kunden oder Abonnenten erfüllen, die sich im Besitz, Gewahrsam oder unter der Kontrolle eines solchen Anbieters befinden, unabhängig davon, ob sich diese Kommunikation, Aufzeichnung oder andere Informationen **innerhalb** oder **außerhalb** der Vereinigten Staaten befinden.

Full Text: <https://www.justice.gov/criminal-oia/page/file/1152896/download>



# 12. Welche Auswirkungen hat die EO 14086/ das DPF auf den CLOUD-Act?

Was hat sich jetzt daran durch EO 14086/ DPF geändert?

**NICHTS!**

- CLOUD-Act unverändert in Kraft.
- EG 96: „Darüber hinaus kann der Zugang zu Teilnehmerinformationen, Verkehrsdaten und gespeicherten Kommunikationsinhalten, die sich im Besitz von Internet-Diensteanbietern, Telefongesellschaften und anderen Drittanbietern befinden, zu Strafverfolgungszwecken auf der **Grundlage des Stored Communications Act (18 U.S.C. §§ 2701-2713)** gewährt werden. [...]“ (Hervorhebung durch ZENDAS, übersetzt mit DeepL)



# 12. Welche Auswirkungen hat die EO 14086/ das DPF auf den CLOUD-Act?

*Q2: Does the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) affect the EU-U.S. DPF?*

- The CLOUD Act involves data transfers for law enforcement purposes. It does not conflict with the EU-U.S. DPF, which provides a legal basis under EU law for transfers of personal data from the European Union to participating organizations in the United States. The EU-U.S. DPF is unrelated to, and unaffected by, the CLOUD Act.

<https://www.dataprivacyframework.gov/s/article/FAQs-General-dpf>



# 12. Welche Auswirkungen hat die EO 14086/ das DPF auf den CLOUD-Act?

**Welchen Schluss zieht man jetzt aber aus der Tatsache des Angemessenheitsbeschlusses?**

- a. Ausschlussgrund für die Beauftragung mangels ausreichender Gewähr trotz DPF
- b. Befugnisse des CLOUD-Acts werden durch Angemessenheitsbeschluss „abgesegnet“

U.E. spricht viel für b:

- Anders als bei Privacy Shield (12.07.16-16.07.20) war CLOUD-Act (23.03.18) **beim Erlass des Angemessenheitsbeschlusses** schon bekannt. Jetzt kann man nicht mehr argumentieren „Kommission hätte nie Angemessenheitsbeschluss erlassen, wäre CLOUD-Act schon in der Welt gewesen“, im Gegenteil: Ausweislich EG 96 war CLOUD-Act bewusst.
- Wertungswidersprüche: Übermittlung an Unternehmen in USA (auf DPF-Liste) wäre zulässig, nicht aber an europäische Tochter? In beiden Fällen ist die gleiche Regel des CLOUD-Act anwendbar (18 U.S.C. § 2713).
- Annex VI legt dar, welchen Behördenzugriff und Rechtsschutz es bei Strafverfolgungszwecken gibt. Kommission hat mit Angemessenheitsbeschluss gerade festgestellt, dass das verhältnismäßig ist.

[https://www.zendas.de/themen/cloud\\_computing/patriot\\_act.html/](https://www.zendas.de/themen/cloud_computing/patriot_act.html/)



## 13. Sind die Prinzipien und Verfahrensgrundsätze in Ordnung?

- Man hat die Prinzipien und Verfahrensgrundsätze des Privacy Shield übernommen und dadurch allen darunter zertifizierten Unternehmen die Aufnahme in die DPF-Liste ermöglicht.

### **Ist das eigentlich so in Ordnung?**

- EU und USA haben – nach Schrems II notgedrungen – einen Nachfolger gesucht. EuGH hat sich bislang nicht mit den Prinzipien inhaltlich auseinandergesetzt und in Schrems I (C-362/14, Rz. 81) festgestellt, das System der Selbstzertifizierung sei kein Verstoß gegen die Verpflichtung zu einem angemessenen Schutzniveau.

Es gibt damit schlichtweg keine Aussage „EuGH hat die Prinzipien des Privacy Shield für ausreichend“ gewertet.



## 13. Sind die Prinzipien und Verfahrensgrundsätze in Ordnung?

### Kritik (noch zur Entwurfsfassung des DPF):

„Diese Prinzipien sind eine pragmatischere, „abgespeckte“ Version der Rechte und Pflichten der DS-GVO. Nahezu jede der zentralen Pflichten der DS-GVO, wie sie in dem Arbeitspapier WP 254 der Art. 29-Datenschutzgruppe niedergelegt sind, findet sich zumindest der Begrifflichkeit nach in den Prinzipien wieder, jedoch stets in einer wirtschaftsfreundlicheren Ausgestaltung.“

*Glocker: EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmaß, ZD 2023, 189*

### Zur endgültigen Fassung:

*Glocker, Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework, RDi 2023, 465 ff.*



## 14. Wird das DPF wieder vom EuGH für ungültig erklärt?

Es gibt Kritikpunkte (Auswahl):

- Anforderungen aus Schrems-II-Urteil wurden zwar aufgegriffen: Zugriffe der US-Geheimdienste nur, wenn „verhältnismäßig“ zum Schutz der nationalen Sicherheit. Aber: Differenzen bei Auslegung des Begriffs „Verhältnismäßig“.
- Keine wirklichen Rechtsbehelfe für EU-Bürger, da kein Zugang zu einem unabhängigen Gericht.
- Änderungen im US-Recht basieren auf einer präsidentialen Executive Order (14086), die relativ einfach wieder aufgehoben werden kann.

([https://](https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities)

[www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities](https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities)

)



# 14. Wird das DPF wieder vom EuGH für ungültig erklärt?

Lesenswerte Zusammenstellung der Kritikpunkte:

„Der TLfDI weicht vom Votum der DSK ab und nimmt Stellung!“

([https://tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen\\_2023/230904\\_PM\\_DPF.pdf](https://tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2023/230904_PM_DPF.pdf))

Kritik:

Regelmäßig fehlende Verantwortlichkeit des US-Unternehmens; Verpflichtungen muss Verantwortlicher umsetzen; fehlende Regelungen des DPF in diesem Verhältnis bedeuten, dass der Verantwortliche sich im Verhältnis zum Datenimporteur nur auf vertragliche Regelungen berufen kann (Auftragsverarbeitung), z.B. bei Erfüllung Betroffenenrechte.

Dr. Lutz Hasse: „Unternehmen etwa sollten vor diesem Hintergrund abwägen, ob sie sensible Daten – auch Kundendaten – in die USA transferieren oder bis zur Entscheidung des EuGH vorsorglich nicht. Denn die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, ist danach recht hoch.“

Dr. Lutz Hasse  
Thüringer Landesbeauftragter für den Datenschutz  
und die Informationsfreiheit



## 14. Wird das DPF wieder vom EuGH für ungültig erklärt?

- Phillippe Latombe, franz. Parlamentarier, hat Eilrechtsschutz geltend gemacht (Pressemitteilung: [https://www.politico.eu/wp-content/uploads/2023/09/07/4\\_6039685923346583457.pdf](https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf)); wies EuGH am 12.10.2023 wegen fehlender Dringlichkeit als unbegründet zurück. Außerdem fehle eine hinreichende Darlegung, inwieweit und welche seiner Daten in USA verarbeitet würden (<https://curia.europa.eu/juris/document/document.jsf?text=&docid=278542&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=225583>)
- Klage noyb angekündigt

# 14. Wird das DPF wieder vom EuGH für ungültig erklärt?

Es wird kein „Schrems III“-Entscheidung geben.



GERICHTSHOF  
DER EUROPÄISCHEN UNION



## PRESSEMITTEILUNG Nr. 1/23

Luxemburg, den 9. Januar 2023

### **Den anonym geführten Vorabentscheidungsverfahren, die ab dem 1. Januar 2023 eingeleitet werden, werden fiktive Namen zugeordnet**

*Zweck dieser Maßnahme ist, dass Verfahren, die aus Gründen des Schutzes personenbezogener Daten anonym geführt werden, leichter bezeichnet und identifiziert werden können*

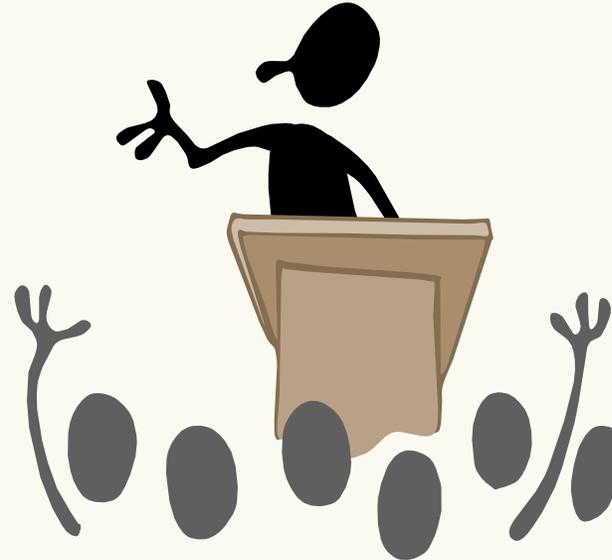
Ab dem 1. Januar 2023 werden allen neuen, anonym geführten Verfahren, in denen sich natürliche Personen gegenüberstehen (deren Namen seit dem 1. Juli 2018 aus Gründen des Schutzes personenbezogener Daten durch Initialen ersetzt werden) oder in denen natürliche Personen juristischen Personen gegenüberstehen, deren Namen nicht unterscheidungskräftig sind, mit Hilfe eines IT-basierten Generators fiktive Namen zugeordnet. Diese Vorgehensweise wurde eingeführt, um anonym geführte Verfahren leichter zu identifizieren. So **bleiben diese Verfahren besser im Gedächtnis und können sowohl in der Rechtsprechung als auch in anderen Zusammenhängen einfacher zitiert werden.**





# ZENDAS

Zentrale Datenschutzstelle der  
baden-württembergischen Universitäten



**Info-Server:**  
[www.zendas.de](http://www.zendas.de)

# Vielen Dank.

Credit Line: Screen Beans Art © A Bit Better Corporation