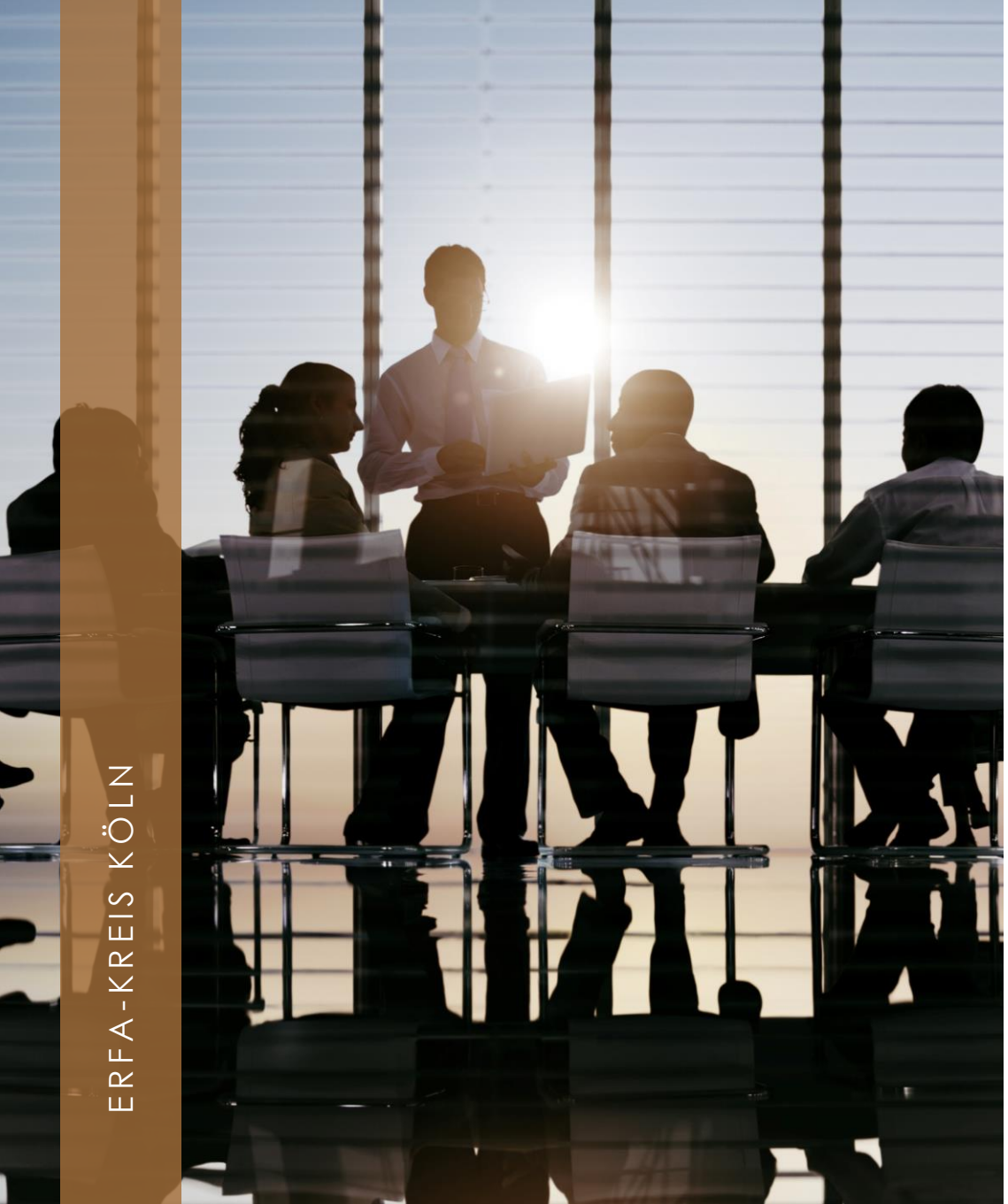
03. November 2023

ANWENDUNGSHINWEISE DER DSK ZUM ANGEMESSENHEITSBESCHLUSS DER KOMMISSION ZUM EU-US DATA PRIVACY FRAMEWORK

CBH RECHTSANWÄLTE



ERFA-KREIS KÖLN

CBH
RECHTSANWÄLTE

Köln, 03.11.2023

DSK zum Angemessenheits-beschluss der Kommission zum EU-US Data Privacy Framework

- **Referent:**
  Dr. Sascha Vander, LL.M.
  RA und FA IT-Recht
  CBH Rechtsanwälte, Köln
  s.vander@cbh.de

Überblick

I. Einleitung

1. Zweckbestimmung der Anwendungshinweise

- Erläuterung Hintergründe und Inhalte des Angemessenheitsbeschlusses
- Adressaten
  - Verantwortliche
  - Betroffene Personen
- Beleuchtung Reichweite und Anwendungsbereich
- Bewertung alternativer Übermittlungsinstrumente
- Umfang und Durchsetzung von Rechten betroffener Personen

I. Einleitung

2. Aufbau

- Allgemeine Informationen
- Informationen für Datenexporteure
  - Anwendungsbereich
  - Wesentliche inhaltliche Vorgaben
  - Überwachung zertifizierter Stellen
- Informationen für betroffene Personen zu Rechtsschutzmöglichkeiten
- Datenübermittlung in die USA auf Grundlage anderer Übermittlungsinstrumente
- Ausblick

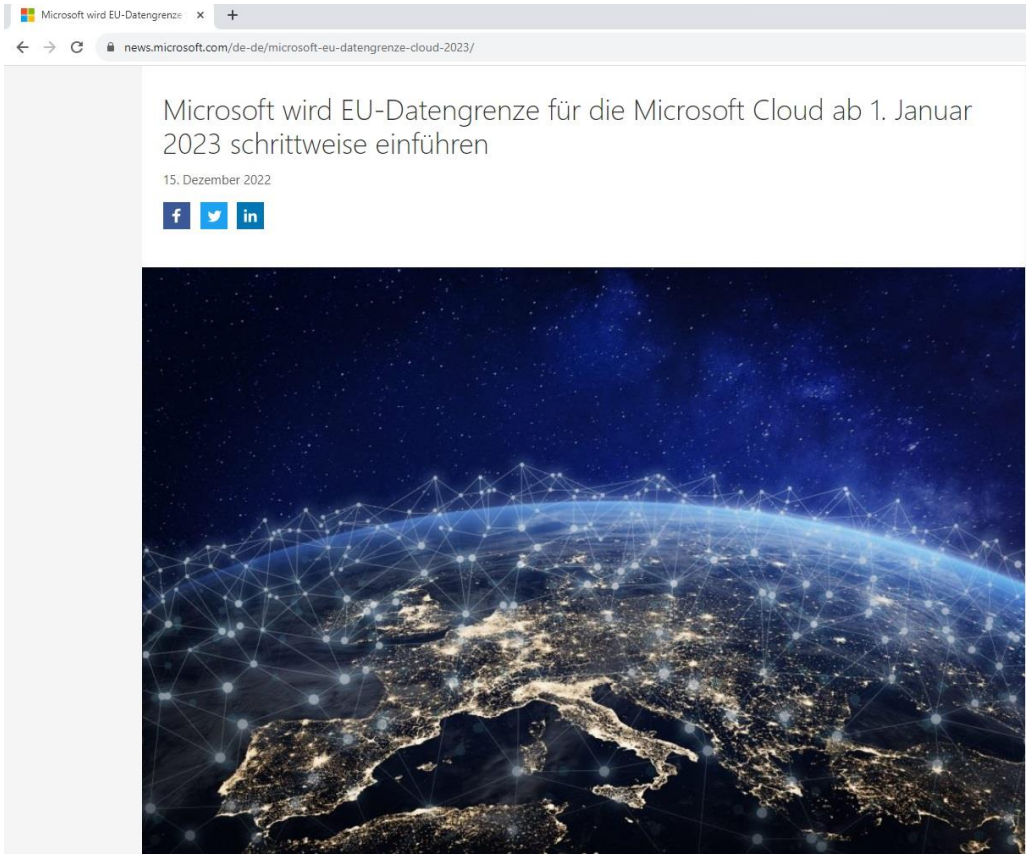
II. Allgemeine Informationen

1. Übermittlungsbegriff

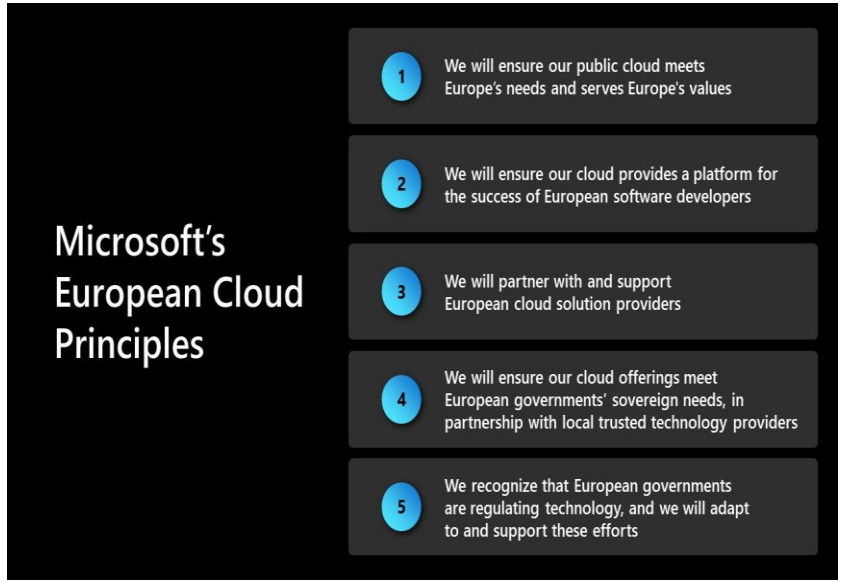
- Bezug auf EDSA-Leitlinien 05/2021 zu Art. 44 ff. DS-GVO („Transfer“)
- Zielgerichtete und absichtliche Vorgänge
- Aber auch: Einräumung einer faktischen Zugriffsmöglichkeit aus Drittland
  - ➢ Fall mit hoher Praxisrelevanz: Zugriff für administrative und/oder Support-Zwecke
  - ➢ **Problem: RZ-Standort von US-Anbietern in Europa ist kein Freibrief!!!**

II. Allgemeine Informationen

1. Übermittlungsbegriff



https://news.microsoft.com/de-de/microsoft-eu-datengrenze-cloud-2023/



II. Allgemeine Informationen

1. Übermittlungsbegriff

- Bezug auf EDSA-Leitlinien 05/2021 zu Art. 44 ff. DS-GVO („Transfer“)
- Zielgerichtete und absichtliche Vorgänge
- Aber auch: Einräumung einer faktischen Zugriffsmöglichkeit aus Drittland
  - ➢ Fall mit hoher Praxisrelevanz: Zugriff für administrative und/oder Support-Zwecke
  - ➢ **Problem: RZ-Standort von US-Anbietern in Europa ist kein Freibrief!!!**

2. Zweistufige Prüfung

- Stufe 1: Allgemeine datenschutzrechtliche Rechtfertigung (+/-)
- Stufe 2: **nur wenn (+)**, zusätzliche Anforderungen nach Art. 44 DS-GVO
- Merke: Auslandsübermittlungslegitimation nach Art. 44 ff. DS-GVO allein hilft nicht!

II. Allgemeine Informationen

3. Vor- und Entstehungsgeschichte

- Safe Harbor (2000) – Schrems I (2015)
- Privacy Shield (2016) – Schrems II (2020)
  - Kernproblem 1: US-Sicherheitsgesetze / Executive Order 12333
  - Kernproblem 2: Mangelnder Rechtsschutz für betroffene Personen
- **EU-US Data Privacy Framework (2023) – Schrems III (???)**
- Grundsätzliche Einigung Kommissions-Präsident und US-Präsident (03/2022)
- Executive Order 14086 / „Regulation" US-Justizministerium zur Umsetzung (10/2022)
- Kommissions-Entwurf Angemessenheitsbeschluss EU-US DPF (12/2022)
- Annahme und Inkrafttreten Angemessenheitsbeschluss (C(2023) 4745 final) am 10.07.2023
  - https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

III. Informationen für Datenexporteure

1. Anwendungsbereich

- **Zertifizierbarkeit (persönlicher Anwendungsbereich)**
  - US-Organisationen
  - aber nur, wenn unter Aufsicht von
    - FTC – Federal Trade Commission
    - DOT – Department of Transportation
    - Öffnungsmöglichkeiten für weitere US-Behörden (derzeit aber nur FTC/DOT)
    - **Sonderproblem**: Begrenzte Zuständigkeiten der FTC gemäß 15 U.S.C. § 45 für z.B. Banken, Versicherungsgewerbe, TK-Netzbetreiber mit Folge möglichen Zertifizierungsausschlusses
  - **Merke: EU-US DPA ist kein allgemeiner Freibrief für alle US-Unternehmen!**
  - **Merke: Kein umfassender Angemessenheitsbeschuss für die gesamten USA, sondern lediglich sektoraler Charakter**

III. Informationen für Datenexporteure

1. Anwendungsbereich

- **Verfahren für Zertifizierung**
  - Grundsatz der Selbstzertifizierung
  - Übermittlung Basisinformationen an Department of Commerce (DOC)
    - Name, Zweck der Datenverarbeitung, Datenkategorien, gewählte Überprüfungsmethode, zuständige Stelle für Durchsetzung
  - Prüfung durch DOC (wohl eher Formalprüfung)
  - Veröffentlichung der Selbstverpflichtung zur Einhaltung der Vorgaben des EU-US DPF durch das zertifizierende Unternehmen (z.B. auf Website)
  - Aufnahme zertifiziertes Unternehmen in Data Privacy List (DPF-Liste) durch DOC
    - https://www.dataprivacyframework.gov/s/
    - **Merke: Datenübermittlung auf Basis EU-US DPF nur an Unternehmen in Liste!**
  - Jährliche „Neu-Zertifizierung“ mit Verpflichtungserklärung gegenüber DOC und Prüfung durch DOC

III. Informationen für Datenexporteure

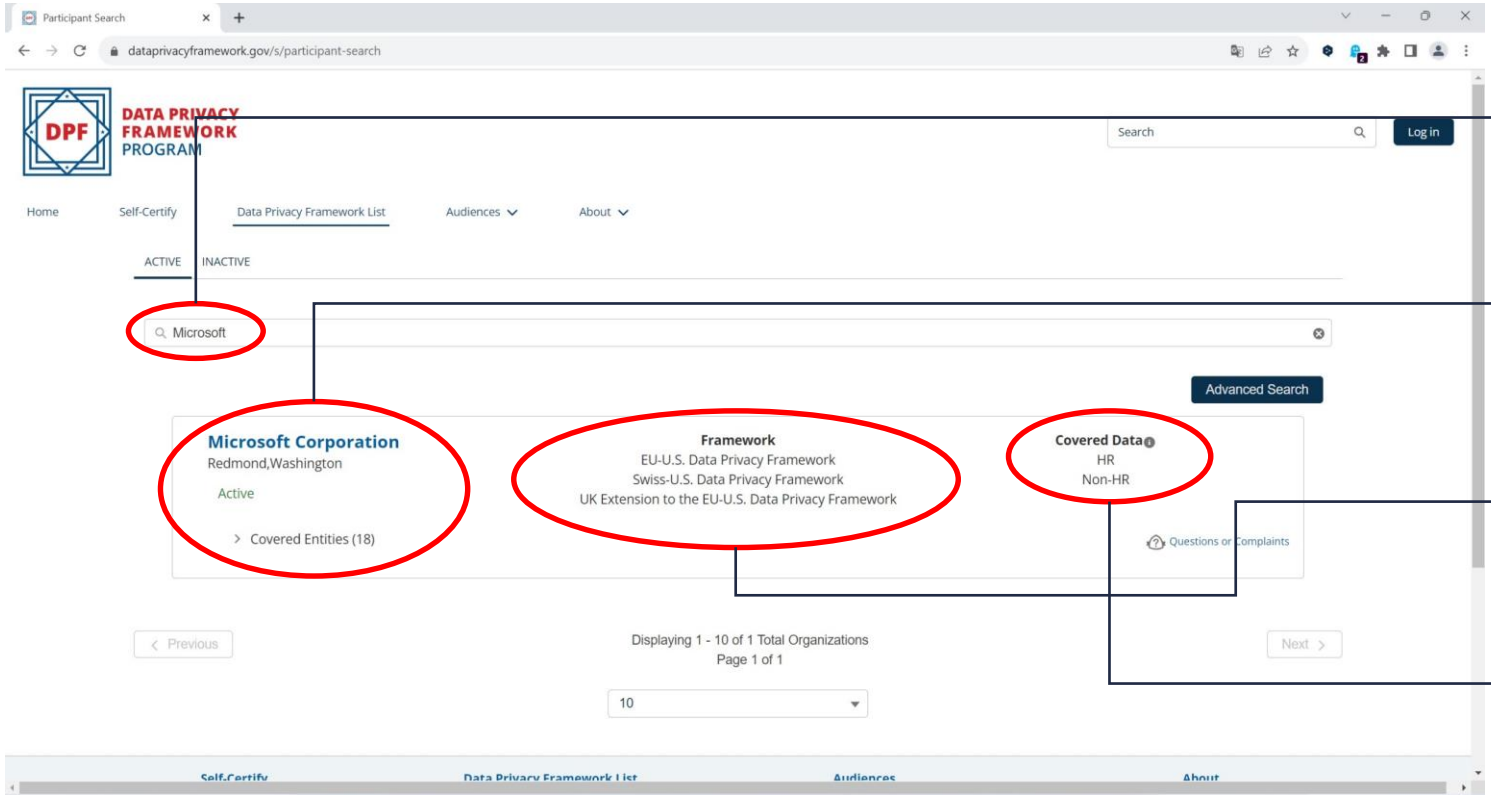
1. Anwendungsbereich

- **Gegenstand legitimierter Datenübermittlungen**
  - Grundsätzlich alle Übermittlungen aus EU/EWR an in DPF-Liste aufgeführte US-Organisationen
  - „Journalistische Ausnahme“
    - DV im Zusammenhang mit journalistischen Aktivitäten / Medienarchiven
    - Keine Übermittlung auf Grundlage DPF möglich (Anwendungsausschluss)
  - Beschäftigtendaten (HR)
    - **Vorsicht**: Zertifizierung bezieht sich nicht automatisch auf Beschäftigtendaten; dann können HR-Daten nicht auf Grundlage EU-US DPF übermittelt werden!!!
    - **Hinweis: Ist in DPF-Liste kenntlich gemacht!** Eintrag in Rubrik Covere Data: „HR Data“ (im Regelfall zusätzlich zu „Non-HR“)

III. Informationen für Datenexporteure

1. Anwendungsbereich

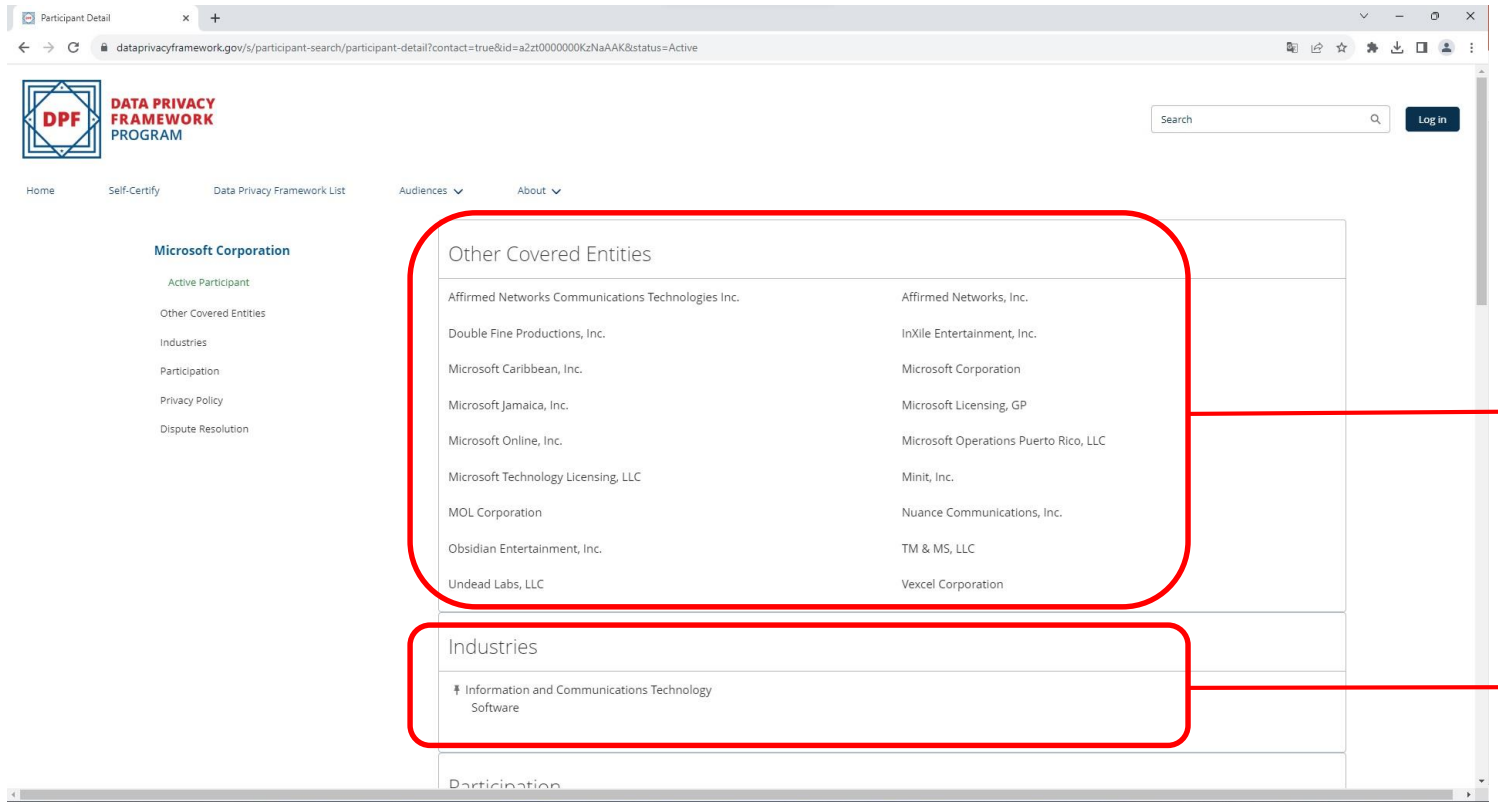
– Beispiel Auszug DPF Liste



III. Informationen für Datenexporteure

1. Anwendungsbereich

– Beispiel Auszug DPF Liste



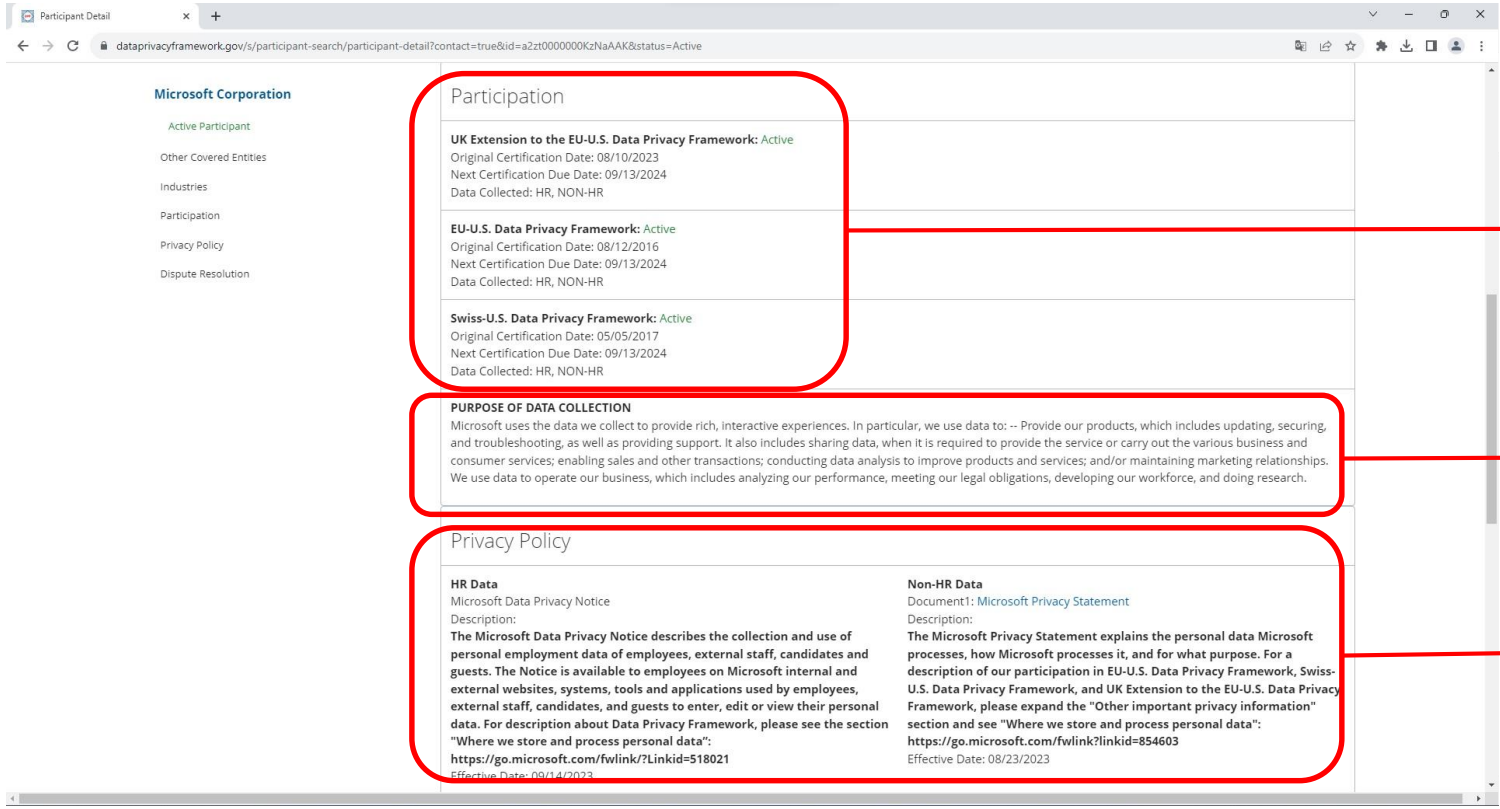
Verbundene Unternehmen

Branche

III. Informationen für Datenexporteure

1. Anwendungsbereich

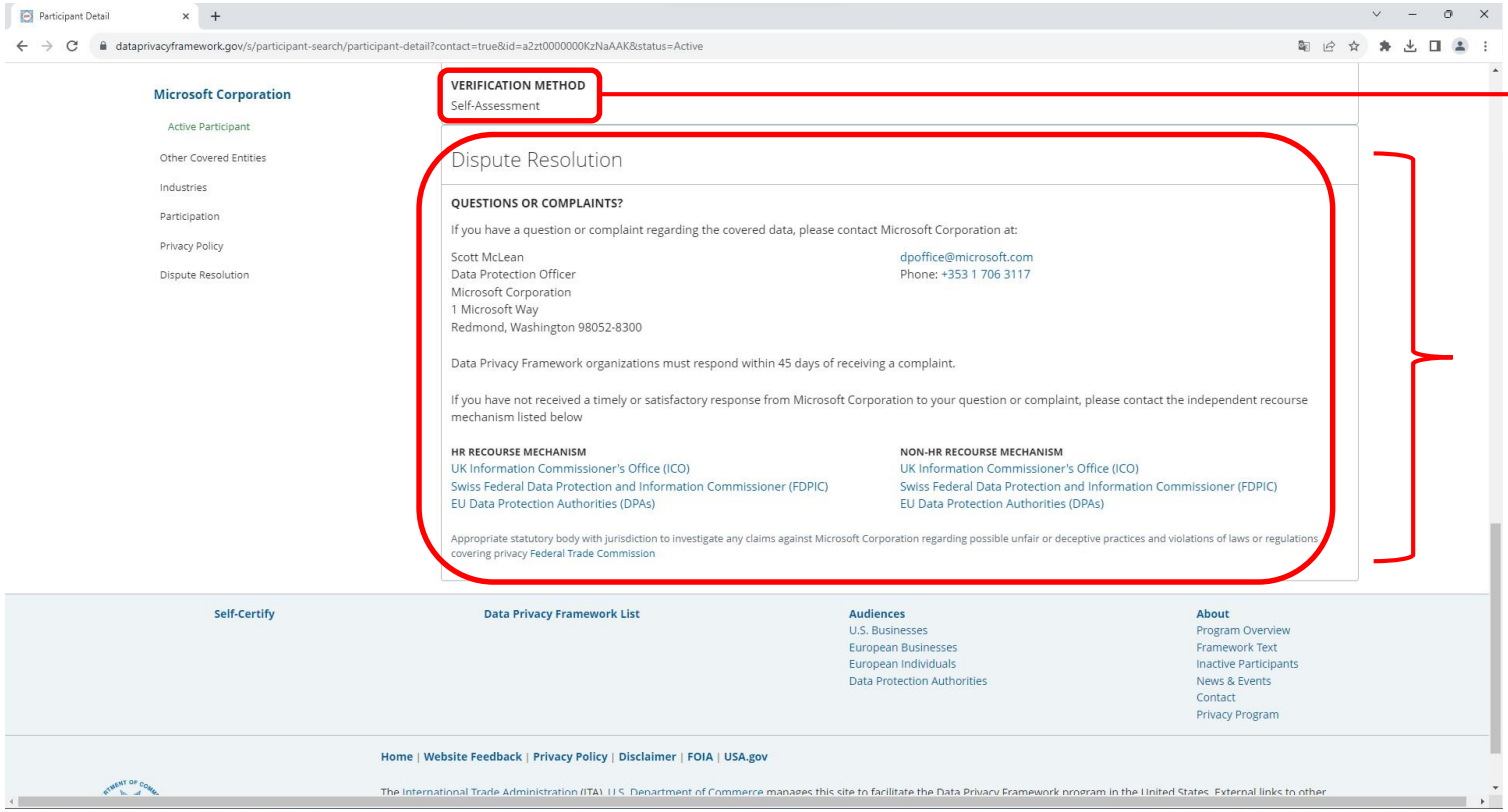
– Beispiel Auszug DPF Liste



III. Informationen für Datenexporteure

1. Anwendungsbereich

– Beispiel Auszug DPF Liste



Art der Verifikation

Streitbeilegung

AP Unternehmen

Zuständigkeit Behörden (HR und Non-HR)

III. Informationen für Datenexporteure

2. Wesentliche Inhalte EU-US DPF

- **Vorgaben für zertifizierte Datenimporteure in den USA**
  - Ausgangspunkt und Grundlage der Selbstzertifizierung ist Verpflichtung auf sog. **EU-US DPF Principles**
    - Prinzipien bilden als Annex I einen Teil des Angemessenheitsbeschlusses
    - Umfangreicher Katalog an Vorgaben und „Spielregeln“
    - Inhaltliche Nähe zur DS-GVO, allerdings mit Sonderthemen
  - Begriffsbestimmungen
    - Personenbezogene Daten, besondere Kategorien, Verarbeitung, Verantwortlicher, Auftragsverarbeiter
    - Definitionen entsprechend DS-GVO
  - Rechtmäßigkeit der Verarbeitung
    - Keine enumerativ aufgeführten Rechtsgrundlagen
    - Sog. „Notice and Choice-Mechanismus“ i.S. Information mit Opt-Out

III. Informationen für Datenexporteure

2. Wesentliche Inhalte EU-US DPF

- **Vorgaben für zertifizierte Datenimporteure in den USA**
  - Transparenz
    - „Choice"-Mechanismus
    - Veröffentlichung von Informationen zur Umsetzung und Implementierung datenschutzrechtlicher Pflichten inkl. EU-US DPF
  - Grundsatz der Zweckbindung
    - Festlegung bei Erhebung
    - Weitere Verwendung nur wenn mit ursprünglichem Zweck vereinbar
  - Grundsätze der Datenminimierung, Speicherbegrenzung, Richtigkeit und Erforderlichkeit

III. Informationen für Datenexporteure

2. Wesentliche Inhalte EU-US DPF

- **Vorgaben für zertifizierte Datenimporteure in den USA**
  - ➢ Verarbeitung besonderer Kategorien personenbezogener Daten
    - Opt-in für Zweckänderung oder Weiterübermittlung an Dritte
  - ➢ Weiterübermittlungen an dritte Stelle in den USA oder anders Drittland
    - Vertragliche Vereinbarung mit Dritten zur Sicherstellung des gleichen Schutzes wie beim Importeur
    - **Wichtig**: **Kettenwirkung EU-US DPF Legitimation bei entsprechenden Vereinbarungen** (relevant vor allem für große Cloud-Anbieter mit einer Vielzahl von Unterauftragnehmern)

III. Informationen für Datenexporteure

2. Wesentliche Inhalte EU-US DPF

- **Vorgaben für zertifizierte Datenimporteure in den USA**
  - Datensicherheit
    - **TOM** einzuführen und einzuhalten (ähnlich Art. 32 DS-GVO)
    - Schutz vor Verlust, Missbrauch, unberechtigtem Zugang, Offenlegung, Veränderung oder Löschung
  - Rechenschaftspflicht
    - Verantwortlichkeit für Einhaltung EU-US DPF ab Zertifizierung
    - Dokumentation mit Nachweiseignung
    - Merke: Rückgriff auf Dokumentation für Exporteur ggf. Kontrollmittel
    - Betroffenenrechte
  - Berichtigung, Ergänzung, Löschung und Auskunft
    - Sonderbeschränkungen Auskunftsrecht: Aufwand außer Verhältnis zu Risiko für die Privatsphäre; Verlangen einer nicht übermäßig hohen Gebühr

III. Informationen für Datenexporteure

2. Wesentliche Inhalte EU-US DPF

- **Überwachung zertifizierter Stellen in den USA**
  - FTC (vgl. Annex IV zum Angemessenheitsbeschluss)
    - Einholung von Informationen zur Sachverhaltsaufklärung und Problemklärung, z.B. Überprüfung Datenschutzrichtlinien der zertifizierten Organisationen
    - Erlass und Überwachung von Vollstreckungsanordnungen
      - Verstöße gegen Anordnungen können Sanktioniert werden (50.120 US$ pro Verstoß bzw. pro Tag bei fortgesetztem Verstoß)
      - Anordnungen werden auf Website der FTC veröffentlicht
      - Beachte: FTC ist in Vergangenheit (unter Privacy Shield und Safe Harbor) wiederholt tätig geworden und hat erhebliche Strafzahlungen verhängt
  - DOT (vgl. Annex V zum Angemessenheitsbeschluss)
    - Befugnisse nach dem Vorbild für FTC ausgestaltet
    - Unterlassungsanordnungen und Geldstrafen von bis zu 37.377 US$ je Verstoß

IV. Abgrenzung: Andere Übermittlungsinstrumente

1. Übermittlung an nicht zertifizierte Stellen

- Allgemeine Grundsätze
  - Merke: Keine Zertifizierung = kein Rückgriff auf EU-US DPF
  - Aber: Mangelnde Zertifizierung lässt sonstige Übermittlungsinstrumente unberührt (EU-US DPF ist nur ein (!) mögliches Instrument von vielen)
- Praktische Auswirkungen
  - Übermittlungsinstrumente ggf. kumulativ einsetzen, um Datenübermittlung zusätzlich abzusichern
  - Befund in der Praxis: Aufgrund langer „Hängepartie“ haben die Akteure ganz weitgehend auf Standardvertragsklauseln umgestellt bzw. diese etabliert
  - **Empfehlung: Datenexport in die USA – soweit möglich – zusätzlich (!) mit EU-US DPF hnterlegen**

IV. Abgrenzung: Andere Übermittlungsinstrumente

2. Auswirkungen EU-US DPF auf Standardvertragsklauseln?

- Allgemeine Grundsätze
  - Stehen grundsätzlich unabhängig nebeneinander
  - Können isoliert oder auch kumuliert zur datenschutzrechtlichen Rechtfertigung einer Datenübermittlung in die US verwendet werden
- Besondere Herausforderung bei Nutzung Standardvertragsklauseln
  - Bewertung der Rechtslage und Rechtspraxis im Drittland
  - **Sog. Transfer Impact Assessment (TIA) in der Praxis sehr schwierig**
  - **Mögliche Entschärfung und „Problemlösung“ durch EU-US DPF???**

IV. Abgrenzung: Andere Übermittlungsinstrumente

2. Auswirkungen EU-US DPF auf Standardvertragsklauseln?

DSK
DATENSCHUTZKONFERENZ

(sog. Transfer Impact Assessment – TIA)[91] und ggf. die Ergreifung geeigneter zusätzlicher Maßnahmen (sog. „supplementary measures“).[92]

Nach Mitteilung der EU-Kommission gelten alle von der US-Regierung im Bereich der nationalen Sicherheit implementierten Schutzmaßnahmen unabhängig von den verwendeten Übermittlungsinstrumenten für alle Datenübermittlungen im Rahmen der Datenschutz-Grundverordnung an US-Unternehmen.[93] Deshalb können Datenexporteure im Rahmen der Datenübermittlung mithilfe geeigneter Garantien (Art. 46 DS-GVO) die von der EU-Kommission im Angemessenheitsbeschluss ausgeführten Bewertungen für ihr Transfer Impact Assessment berücksichtigen.

TIA (insoweit):

„*Die Ausführungen der Kommission im Angemessenheitsbeschluss zum EU-US DPF werden zu Eigen gemacht*“

V. Fazit und Ausblick

1. Auswirkungen EU-US DPF

- Hohe Praxisrelevanz
- Rein formale Rechtfertigung: „Liste checken und gut!“
- US-Unternehmen machen intensiv von Zertifizierung Gebrach (vgl. DPF-Liste)
- Praxistauglichkeit EU-US DPF abzuwarten, insbesondere Rechtsbehelfe und Rechtsdurchsetzung
- **Damoklesschwert Schrems III**

2. DSK Anwendungshinweise

- Vielfach reine Inhaltsbeschreibung des EU-DS DPF
  - Kaum Wertungen
  - Kaum Praxistipps (vgl. kurz und knapp FAQ zum EU-US DPF der GDD v. 25.7.2023)
- Detailaspekte zutreffend in den Fokus gerügt
  - **Beschränkter Anwendungsbereich für zertifizierte US-Unternehmen**
  - **Beschränkter Geltungsbereich bzw. Ausnahmen für Teilbereiche**

CBH
RECHTSANWÄLTE

Ansprechpartner

Dr. Sascha Vander, LL.M.

Rechtsanwalt / Partner
Fachanwalt für Informationstechnologierecht

Schwerpunkt: IT-Recht

T +49 221 95 190-60
E s.vander@cbh.de

CBH
RECHTSANWÄLTE

Expertise

- IT-Vertragsrecht
- Softwarerecht
- E-Commerce
- Datenschutzrecht
- Wettbewerbsrecht

Vita

Dr. Sascha Vander wurde 2006 als Rechtsanwalt zugelassen und ist seit Beginn seiner anwaltlichen Tätigkeit mit IT-rechtlichen Fragen befasst. Er berät schwerpunktmäßig in den Bereichen IT-Projekte, Software- und Lizenzrecht, E-Commerce und Datenschutzrecht sowie zu IT-spezifischen Fragen des allgemeinen Zivil- und Wirtschaftsrechts. Sein Tätigkeitsgebiet umfasst zudem den Bereich des Gewerblichen Rechtsschutzes.

Mitgliedschaften

Dr. Sascha Vander ist Mitglied des Fachausschusses für Informationstechnologierecht des Kölner Anwalt Verein und stellvertretender Leiter des Erfa-Kreises Köln der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD). Er ist zudem Mitglied des Kölner Arbeitskreises EDV & Recht und der Deutschen Gesellschaft für Recht und Informatik.

Referenzen

CBH Rechtsanwälte zählen zu den gemäß Kanzleimonitor 2019/2020, 2020/2021, 2021/2022 mehrfach empfohlenen Sozietäten für IT-Recht.

Der Kanzleimonitor 2019/2020, 2020/2021, 2021/2022 weist Herrn Dr. Vander als mehrfach empfohlenen Rechtsanwalt für IT-Recht aus. Zudem zählt er gemäß Handelsblatt zu „Deutschlands Beste Anwälte“ für Datenschutzrecht, IT-Recht und Gewerblichen Rechtsschutz.

Dr. Sascha Vander absolvierte den Masterstudiengang „Informationsrecht“ am Zentrum für Informationsrecht der Heinrich-Heine-Universität Düsseldorf und war dort mehrere Jahre als Lehrbeauftragter tätig. Zudem publiziert er regelmäßig in Fachzeitschriften, wirkt an Buchveröffentlichungen mit und hält Fachvorträge.