Datenschutzgrundverordnung und Privacy Shield – Auswirkungen auf Cloud-Anwendungen

RA Dr. Jan K. Köcher
Datenschutzauditor, DFN-CERT
koecher@dfn-cert.de

Cloud-Dienste

- **Auftragsverarbeitung für den Verantwortlichen?**
- **Gemeinsame Verarbeitung?**
- **Auftragsverarbeiter ist in Wahrheit der Verantwortliche?**
- **Übermittlung in Drittstaaten?**

Prüfungsraster

- **Rechtsgrundlage für Verantwortlichen**
- **Auftragsverarbeitung:**
- Rechtmäßigkeit Auftragsdatenverarbeitung
- Rechtsgrundlage Verarbeitung im Verhältnis zur betroffenen Person für den Auftragnehmer
- Rechtsgrundlage Übermittlung vom Auftraggeber zum Auftragnehmer
- **Gemeinsame Verarbeitung**
- Rechtmäßigkeit Gemeinsamer Verarbeitung
- Rechtsgrundlage Übermittlung zwischen den Verantwortlichen
- **Auftragsverarbeiter ist Verantwortlicher**
- Art. 28 Abs. 10 EU-DSGVO, gilt als Verantwortlicher
- **Übermittlung in Drittstaaten?**
- Zulässigkeit nach Art. 44-49 EU-DSGVO

Rechtsgrundlagen

Art. 6 Abs. 1 a): Einwilligung der betroffenen Person

Art. 6 Abs. 1 b): Zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich / Vorvertragliche Maßnahmen auf Anfrage der betroffenen Person

Art. 6 Abs. 1 c): Zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich

Art. 6 Abs. 1 e): Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

- **Hochschulen:** Art. 6 Abs. 1 e) i.V.m Art. 6 Abs. 3 i.V.m. Hochschulgesetz, -zulassungsgesetz, Satzungen, VOen
- **Forschung:** Wann im öffentlichen Interesse?

Art. 6 Abs. 1 f): Berechtigtes Interesse, nicht bei überwiegendem Interesse des Betroffenen

- Nicht für Behörden in Erfüllung ihrer Aufgaben!

Besondere Kategorien

Verbot der Verarbeitung Art. 9 Abs. 1 EU-DSGVO:
Rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

Ausnahmen:

- Einwilligung
- Erforderlichkeit nach Arbeits- und Sozialrecht (Öffnungskl.)
- Mitgliederverwaltung Kirchen, Gewerkschaften, etc.
- Daten, die die Person offensichtlich öffentlich gemacht hat
- Gesundheitsvorsorge, Arbeitsmedizin
- **Archivzwecke und wissenschaftliche Forschung (Öffnungsklausel)**

Auftragsverarbeitung

Abgrenzung Verantwortlicher zu Auftragsverarbeiter?

- **Art. 4 Nr. 8 EU-DSGVO: Auftragsverhältnis**
- **Verantwortlicher und kein Auftragsverarbeiter:**
- Wenn durch die betreffende Stelle Zweck und Mittel der Verarbeitung bestimmt werden (Arg. Art. 4 Nr. 7 und Art. 28 Abs. 10 EU-DSGVO)
- **Auftragsverarbeitung schwer vorstellbar:**
- Wenn die Zwecke bestimmt werden! Die Zwecke einer Verarbeitung werden normalerweise durch den Auftraggeber bestimmt

Auftragsverarbeitung

Art. 28 und 29: Wie bisher

- **Auswahl geeigneter Verarbeiter**
- **Vertragsgrundlage mit inhaltlichen Mindestvoraus-setzungen in Art. 28 Abs. 3**
- **Pflichten:**
- Verarbeitung nur auf dokumentierte Weisung
- Verpflichtung Personal zur Vertraulichkeit
- Erforderliche TOM nach Art. 32
- Regelung zur Befugnis Unterauftragsverarbeitung
- TOM Unterstützung Erfüllung Betroffenenrechte
- Unterstützung Verantwortlicher Sicherheit Art. 32 ff
- Löschung bzw. Rückgabe der Daten
- Ermöglichung und Unterstützung von Prüfungen
- Hinweispflicht bei rechtswidriger Weisung
- **Schriftlichkeit:** auch elektronisches Format
- **Standardvertragsklauseln**

Kettenauftragsverarbeitung

Voraussetzung Unterauftragsverarbeitung

- **Art. 28 Abs. 2: Nur mit vorheriger Genehmigung**
- Gesonderte schriftliche Genehmigung
- Allgemeine schriftliche Genehmigung
- Informationspflicht bei allg. Genehmigung

- **Art. 28 Abs. 4: Vertrag mit Unterauftragnehmer**
- Die selben Datenschutzverpflichtungen wie im Vertrag mit dem Verantwortlichen
- Haftung des ersten Auftragnehmers bei Nichteinhaltung

Rechtmäßigkeit Übermittlung

Wegfall der bisherigen Privilegierung?

- **Bisher:** Keine rechtfertigungsbedürftige Übermittlung innerhalb der EU

- **EU-DSGVO:**
- Gemäß Art. 4 Nr. 10 ist der Auftragsverarbeiter nicht Dritter
- ABER: Es fehlt die bisherige Rechtsfolge, weil eine Übermittlung nicht mehr von der Eigenschaft als Dritter abhängt
- Für weitere Privilegierung: Bayerisches LDA https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf

Gemeinsame Verantwortung

NEU Art. 26 Gemeinsam für die Verarbeitung Verantwortliche

Transparenz: Gemeinsame Festlegung, wer welche Pflichten aus der DSGVO erfüllt, insb.:

Informationspflichten
Betroffenenrechte

Unabhängig von Vereinbarungen: Der Betroffene kann gegenüber beiden Verantwortlichen seine Rechte geltend machen

Übermittlung in ein Drittland

Art. 44: Grundsätze

- **Daten:** Werden bereits verarbeitet oder werden für eine Verarbeitung in das Drittland übermittelt
- **Bestimmungen:** Einhaltung der EU-DSGVO auch bei Weiterübermittlung innerhalb/anderes Drittland
- **ErwG 102:** Int. Abkommen zwischen EU und Drittländern über die Übermittlung einschließlich geeigneter Garantien, werden von der EU-DSGVO nicht berührt!(Lex TTIP, CETA)

Gestufte Zulässigkeit

- **Art. 45 Angemessenheitsbeschluss**
- **Art. 46: Datenübermittlung vorbehaltlich geeigneter Garantien**
- **Art. 49 Ausnahmen für bestimmte Fälle**

Übermittlung in ein Drittland

Art. 45: Angemessenheitsbeschluss

- **Beschluss der Kommission bezogen auf das Drittland, ein Gebiet, ein oder mehrere spezifische Sektoren**

  Beispiele: Kanada, Schweiz, Argentinien, Israel, Neuseeland, Uruguay, USA – **Privacy Shield!**

- **Folge:** Eine Übermittlung bedarf keiner besonderen Genehmigung

Übermittlung in ein Drittland

Art. 46: Vorbehaltlich geeigneter Garantien
Geeignete Garantien + durchsetzbare Rechte und wirksame Rechtsbehelfe

Ohne Genehmigungserfordernis DS-Aufsicht:

- Rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen
- Binding Corporate Rules, Art. 47
- Standarddatenschutzklauseln
- CoC und Genehmigter Zertifizierungsmechanismus

Mit Genehmigungserfordernis DS-Aufsicht:

- Vertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern mit denen im Drittland

Übermittlung in ein Drittland

Art.49: Ausnahmen für bestimmte Fälle

- **Ausdrückliche Einwilligung** (nicht Behörden)
- **Zur Erfüllung eines Vertrags oder für vorvertragliche Maßnahmen auf Antrag der betroffenen Person erforderlich** (nicht Behörden)
- **Zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich** (nicht Behörden)
- **Erforderlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen**

DFN CERT®

DFN Deutsches Forschungsnetz

Vielen Dank
für die Aufmerksamkeit

RA Dr. Jan K. Köcher
koecher@dfn-cert.de