

Cloud Computing & die Relevanz der Datenschutzgrundverordnung

Christopher Götz, LL.M.
(New York)

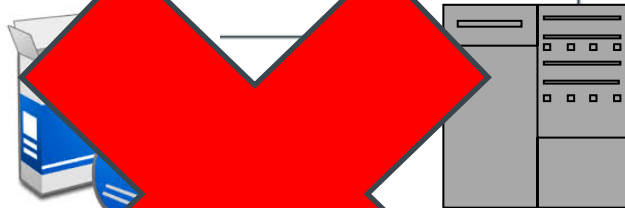
München, den 26. April
2018

Cloud Computing & Datenübermittlung

Moderne u. leistungsfähige IT-Systeme zur Datenverarbeitung



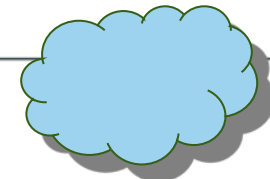
Aufbau eigener IT-Infrastruktur



Beauftragung
Unternehmen

- Aufbau der IT-Infrastruktur
- evtl. Softwareerstellung
- Wartung der IT-Systeme
- regelmäßigen Upgrades

Rückgriff auf Systeme Dritter



Cloud Computing & Hosting durch Service Provider (z.B. MS Office 365, Salesforce, Workday, AWS)

- Anbindung an Internet genügt
- Hohe Skalierbarkeit
- Niedrigere Kosten bei oftmals höherer Sicherheit
- **Achtung: ständiger Datentransfer**

Fragen

- „Verbot mit Erlaubnisvorbehalt“ – gilt dieser Grundsatz auch für eine Datenübermittlung bzw. das Abfragen von Daten, insbesondere im Rahmen von Cloud Computing?
- Bei Konzernunternehmen: Gibt es ein Konzernprivileg?
- Welche Relevanz hat die Auftragsdatenverarbeitung?
- Gelten Besonderheiten bei Datenübermittlungen in einen Drittstaat?

„Verbot mit Erlaubnisvorbehalt“

■ **Datenschutzrechtlicher Grundsatz (Art. 6 Abs.1 lit a – f DSGVO):**

„**Verarbeitung**“ von **personenbezogenen Daten** einer *natürlichen Person*

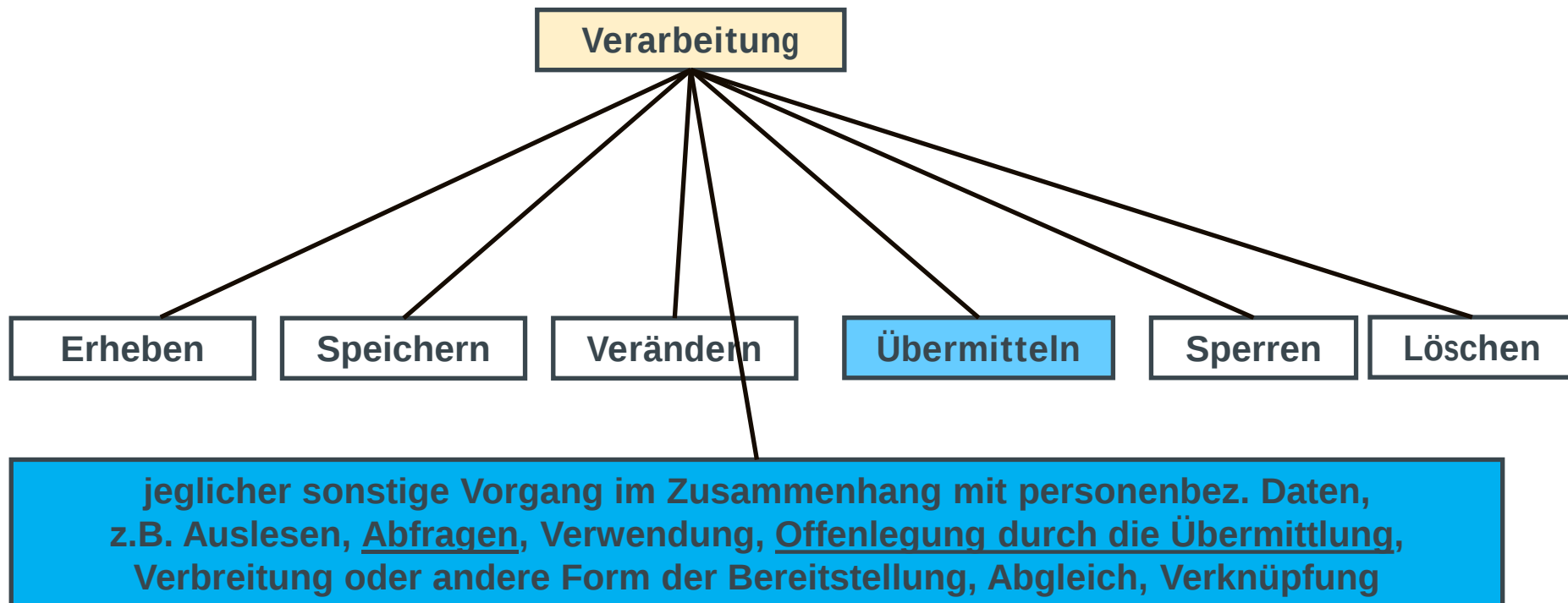
(Betroffene) ist **nur rechtmäßig, soweit**

- **Einwilligung** des Betroffenen oder
- **Erlaubnistatbestand**

vorliegt.

„Verarbeitung“

- „Verarbeitung“ = Datenübermittlung?
- Definition Artikel 4 Nr. 2 DSGVO:



Personenbezogene Daten, Art. 4 Nr. 1 DSGVO

■ Personenbezogene Daten:

- „Informationen, die sich auf eine
 - „identifizierte“ oder eine (durch Zusatzwissen eines Dritten) „identifizierbare“
 - natürliche Person (keine juristische!) beziehen (sog. Betroffener)
- **Beispiele :**
 - Beschäftigtendaten (Name, Adresse, Konto,)
 - Daten von Geschäftspartnern (wie z.B. Kunden, Lieferanten)
 - Dynamische IP Adresse, eindeutige Geräteerkennung
 - DNA

Rechtmäßigkeit der Datenübermittlung

■ Konsequenz:

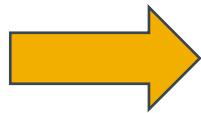
Datenübermittlung nur rechtmäßig, soweit

- **Einwilligung** des Betroffenen oder
 - **Erlaubnistatbestand vorliegt**
(Art. 6 Abs.1 lit a – f EU-DSGVO) !
-
- Bei Verstoß drohen **Sanktionen von bis zu 4% des weltweiten Jahresumsatzes oder EUR 20 Millionen**
 - Gilt grds. auch für **Cloud Computing!**

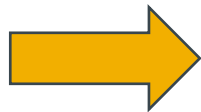
Rechtmäßigkeit der Datenübermittlung

Problem: Feststellung eines Erlaubnistatbestands regelmäßig kompliziert bzw. mit Güterabwägung verbunden;
Einholen einer Einwilligung häufig nicht praktikabel & mit Risiken verbunden!

Frage: **Ausnahmen zu vorgenanntem Erlaubnisvorbehalt?**



„Konzernprivileg“?



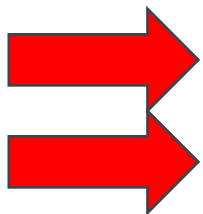
Auftragsdatenverarbeitung, Art. 28 EU-DSGVO?

„Konzernprivileg“?

- Das **einzelne Konzernunternehmen** ist für **datenschutzrechtliche Betrachtung maßgebend!** → **Kein Konzernprivileg!**

- Aber möglicherweise Erlaubnistatbestand Art. 6 lit. f EU-DSGVO („berechtigtes Interesse“) iVm Erwägungsgrund 48?

*„Verantwortliche, die Teil einer **Unternehmensgruppe** [...] sind, können ein **berechtigtes Interesse** **haben**, personenbezogene Daten **innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.**“*



Güterabwägung mit Interessen des Betroffenen nötig!

Spezialvorschrift: Art. 88 DSGVO iVm. § 26 BDSG-neu!

Rechtmäßigkeit der Datenübermittlung

Problem: Feststellung eines Erlaubnistatbestands regelmäßig kompliziert bzw. Einholen einer Einwilligung häufig nicht praktikabel!

Frage: Ausnahmen zu vorgenanntem Erlaubnisvorbehalt?

 „Konzernprivileg“?

 Auftrags(daten)verarbeitung

Auftrags(daten)verarbeitung

■ Privilegierung der Auftragsverarbeitung!

- Datentransfer (von Auftraggeber zu Auftragnehmer bedarf weder eines Erlaubnistatbestands noch einer Einwilligung!
- Verarbeitung bzw. Nutzung der übermittelten Daten durch den Auftragnehmer bedarf ebenso wenig einer Rechtfertigung!

(hM Literatur & Auffassung der Bay. Landesdatenschutzbehörde)

(Beachte: Daten müssen selbstverständlich von der Verantwortlichen Stelle rechtmäßig erhoben worden sein und von ihr grds. verarbeitet werden dürfen)

■ Voraussetzung der Privilegierung:

- Vollständig **weisungsgebundene** Datenverarbeitung
- **Auftrags(daten)verarbeitungsvertrag** (vgl. Art. 28 Abs. 3 lit. a – h)



Im Rahmen von Cloud Computing höchste Relevanz!

Auftragsverarbeitungsvertrag – Mindestinhalt

- Gegenstand und Dauer des Auftrags
- Umfang, Art, Zweck d. Verarbeitung/Art der Daten/Betroffenenkreis
- Technische und organisatorische Sicherheitsmaßnahmen
- Berechtigung zur Unterbeauftragung (back2back!)
- Weisungsgebundenheit & Verschwiegenheit
- Unterstützung des Verantwortlichen in Bezug auf
 - Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte & Einhaltung der TOMs,
 - Meldepflichten ggüber Behörden und Betroffenen (Art. 33, 34),
 - Datenschutzfolgeabschätzung (Art. 35, 36 DSGVO)
- Kontrollrechte des Auftraggebers (Audit Recht) sowie Duldungs- und Mitwirkungspflichten des Auftraggebers
- Mitteilungspflichten bei Verstößen
- Rückgabe/Löschung von Daten nach Auftragsbeendigung

Auftragsverarbeitungsvertrag -- zusätzliche Inhalte

■ Verarbeitung besonderer Kategorien von Daten

➤ § 22 Abs. 2 BDSG – neu!

➤ Besondere Kategorien von Daten:

- u.a. Gewerkschaftszugehörigkeit, biometrische Daten, genetische Daten, Gesundheitsdaten, sexuelle Orientierung, politische Meinung

➤ „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person“ zu treffen, „wie z.B.“:

- Besondere technische und organisatorische Maßnahmen
- **Verschlüsselung** der Datenübermittlung
- **Sensibilisierung der an Verarbeitungsvorgängen Beteiligten**
- **Beschränkung des Zugangs zu** den personenbezogenen **Daten** bei der verantwortlichen Stelle und **beim Auftragsverarbeiter**

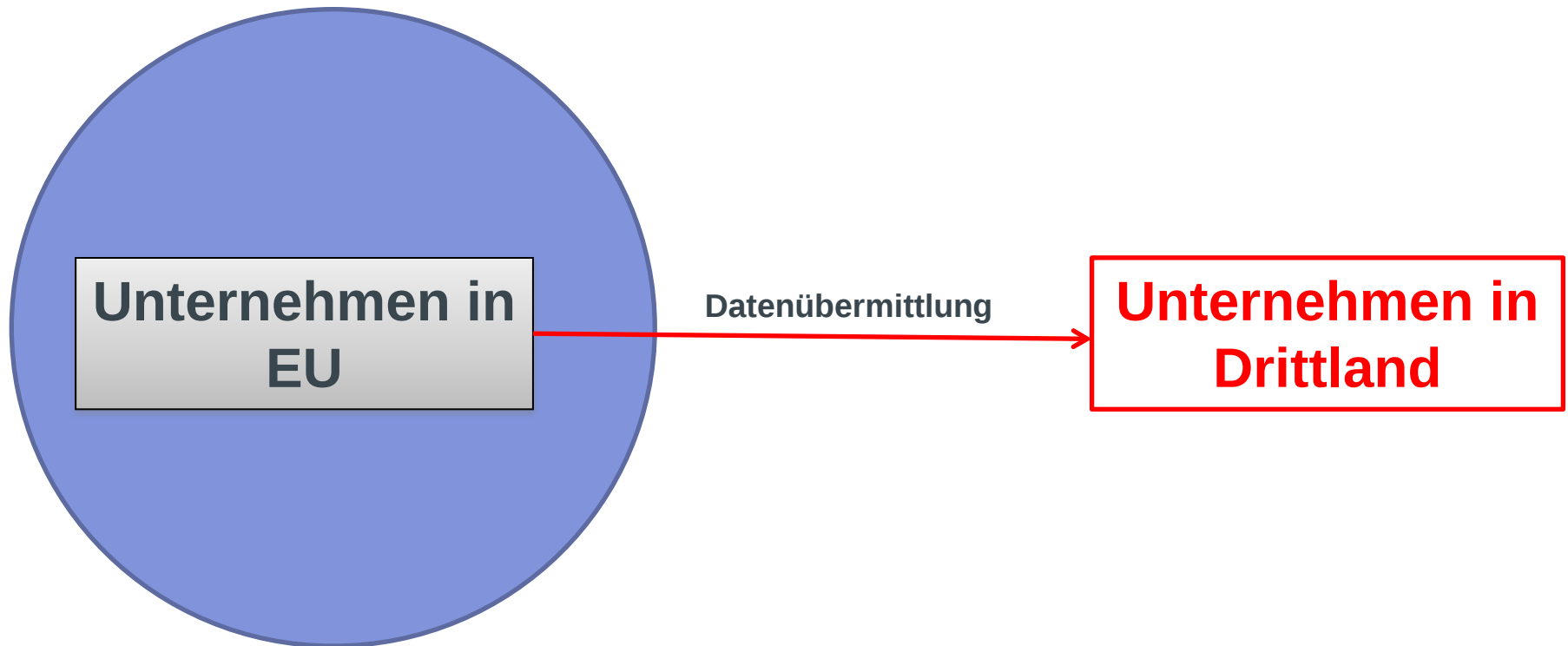
Besonderheit: Finanzsektor (§§25 a, 25b KWG, MaRisk)

- Sofern Cloud Computing “wesentliche Auslagerung”: zusätzlich folgende Mindestinhalte (AT 9 MaRisk)
 - Klare Leistungsbeschreibung
 - **Informations- und Prüfungsrechte der Internen Revision u. externer Prüfer**
 - **Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der BaFin**
 - Weisungsrechte (soweit erforderlich)
 - Beachtung datenschutzrechtlicher Bestimmungen
 - Kündigungsrechte und angemessene Kündigungsfristen
 - Regelungen zur Weiterverlagerung unter Beachtung der Auslagerungsanforderungen
 - **Informationspflicht über geschäftsgefährdende Entwicklungen**
 - **Exitregelung, die geordnete Überführung auf Institut / Dritten sicherstellt**

Auftrags(daten)verarbeitung

- **Auftragsverarbeiter** nicht nur vertraglich, sondern auch **kraft Gesetzes** verpflichtet,
„Geeignete Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung zu ergreifen“ (Art. 32 DSGVO)
- **Gesamtschuldnerische Haftung** Auftraggeber **und** Auftragsverarbeiter!
 - Befreiung von Schadensersatzansprüchen nur bei Nachweis, dass in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich, Art. 82 DSGVO

Besonderheiten bei Datentransfer in Drittland



Datenübermittlung an Cloud Computing - Provider in Drittland

■ Zwei - Stufen Prüfung

1. Stufe:

Erlaubnistatbestand / Einwilligung (Art. 6 DSGVO) bzw.

Auftragsdatenverarbeitung im Sinne des § 28 DSGVO (!)

2. Stufe:

Angemessenes Datenschutzniveau in Drittland

— Wie wird dieses sichergestellt?

Angemessenheit des Datenschutzniveaus

- Möglichkeit der EU-Kommission verbindlich (positiv) festzustellen, ob Drittstaaten über angemessenes Datenschutzniveau verfügen (Art. 45 DSGVO)



adäquates Datenschutzniveau festgestellt für:

- Argentinien, Australien, Israel, Kanada, Schweiz
- Neuseeland, Uruguay
- Andorra, Färöer Inseln, Guernsey, Isle of Man, Jersey
- USA: nur wenn Cloud Provider „Privacy Shield“ zertifiziert ist



nicht positiv festgestellt für:

- (u.a.) China, Indien, Brasilien, Japan, Russland

EU-Standardvertragsklauseln

- **Standardvertragsklauseln**, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 erlassen werden = „geeignete Garantie“ (Art. 46 Abs. 2 lit c DSGVO)
- Aktuell drei EU – Standardverträge, die auf Basis der aktuellen Datenschutzrichtlinie erlassen wurden:
 - **Standardvertrag I** („Controller-to-Controller“)
 - **Standardvertrag II** („Controller-to-Controller“)
 - **Standardvertragsklauseln für "Auftragsdatenverarbeiter"** („Controller-to-Processor“)

EU-Standardvertragsklauseln

■ Können aktuelle EU-Standardvertragsklauseln nach dem 25. Mai 2018 weiterhin verwendet werden?

➤ Ja

➤ Erw.Gr. 171 Satz 4:

„Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission ... bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.“

Kettenauftragsdatenverarbeitung bei grenzüberschreitendem Sachverhalt

In diesem Kontext praxisrelevant:

Anwendung der „**EU-Standardvertragsklauseln für Auftragsdatenverarbeiter**“ in Fällen der

- Kettenauftragsdatenverarbeitung bei grenzüberschreitendem Sachverhalt
- **Frage:** Wer schließt mit wem den Vertrag?
 - Zwei Fälle zu unterscheiden

Datenübermittlung trotz fehlendem angemessenem Datenschutzniveau, Art. 49 DSGVO

- Explizite Einwilligung in Datenübermittlung, nachdem betroffene Person über die für sie bestehenden Risiken derartiger Datenübermittlungen in ein Drittland ohne angemessenes Datenschutzniveau unterrichtet wurde
- Übermittlung für die Erfüllung eines Vertrags zwischen Betroffenen und Verantwortlichen erforderlich
- Übermittlung zum Vertragsabschluss oder Erfüllung eines im Interesse des Betroffenen von dem Verantwortlichen mit einer anderen (nat./jur.) Person geschlossenen Vertrags erforderlich
- im öffentlichen Interesse /Übermittlung zur Durchsetzung von Rechtsansprüchen

Fragen?



Christopher Götz, LL.M. (New York)

Counsel, IT

Simmons & Simmons LLP

DD 0 89 208077 63 32

M 0151 1624 4050

christopher.goetz@

simmons-simmons.com

simmons-simmons.com
elexica.com

This document is for general guidance only. It does not contain definitive advice. SIMMONS & SIMMONS and S&S are registered trade marks of Simmons & Simmons LLP. Simmons & Simmons is an international legal practice carried on by Simmons & Simmons LLP and its affiliated practices. Accordingly, references to Simmons & Simmons mean Simmons & Simmons LLP and the other partnerships and other entities or practices authorised to use the name "Simmons & Simmons" or one or more of those practices as the context requires. The word "partner" refers to a member of Simmons & Simmons LLP or an employee or consultant with equivalent standing and qualifications or to an individual with equivalent status in one of Simmons & Simmons LLP's affiliated practices. For further information on the international entities and practices, refer to simmons-simmons.com/legalresp. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS. It is authorised and regulated by the Solicitors Regulation Authority. A list of members and other partners together with their professional qualifications is available for inspection at the above address.