Dresdner
Institut für
Datenschutz

DRITTLANDTRANSFER & TRANSFERFOLGENABSCHÄTZUNG

Handlungsempfehlungen für verantwortliche Stellen

Alexander Weidenhammer, Rechtsanwalt
Max Just, LL.M., Wirtschaftsjurist

INHALT

(1) Was bisher geschah

(2) Datenübermittlungen an Drittländer

a. Angemessenheitsbeschluss
b. Binding Corporate Rules
c. Standarddatenschutzklauseln und Transferfolgenabschätzung

45 - 60 Minuten

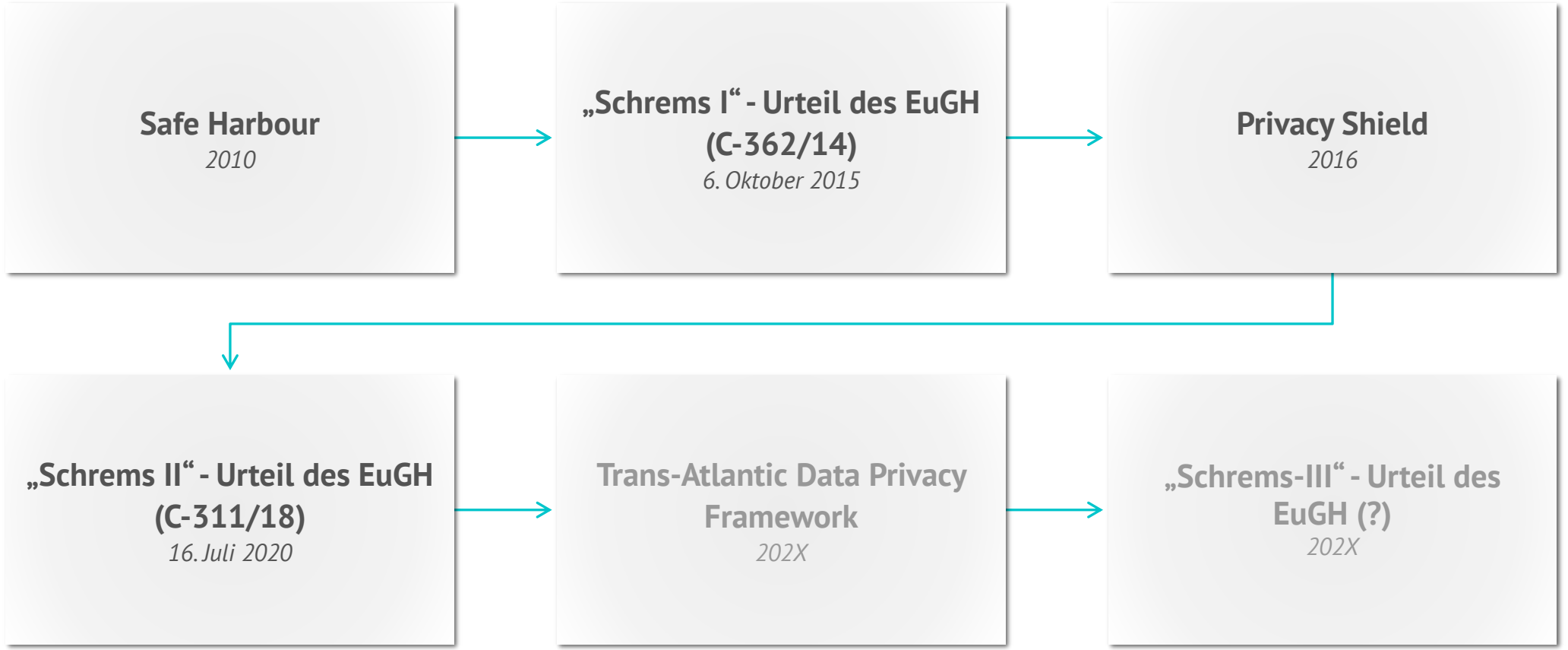
(3) Handlungsempfehlungen

(4) Weiterführende Informationen

(5) Fragen und Antworten

30 - 45 Minuten

WAS BISHER GESCHAH

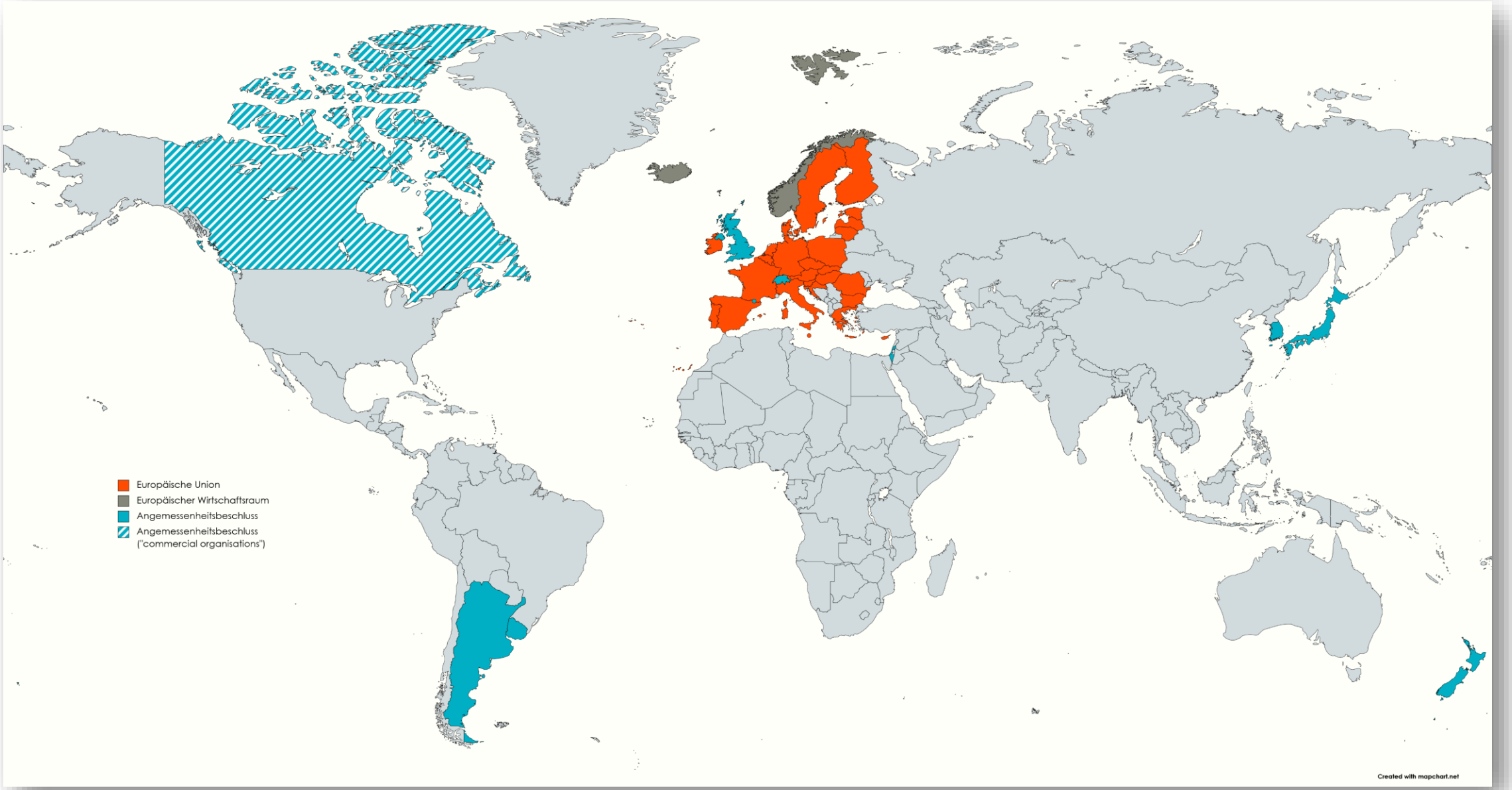


ÜBERMITTLUNGEN AN DRITTLÄNDER

- **„Drittländer“** im Sinne der DS-GVO bezeichnet Länder außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR).
- Rechtmäßigkeit der Datenverarbeitung richtet sich neben den allgemeinen Grundsätzen nach den besonderen Bestimmungen des **Kapitel V** der DS-GVO.
- Möglichkeiten der Datenübermittlung bei Vorliegen folgender Voraussetzungen:
  - Angemessenheitsbeschluss der Europäischen Kommission,
  - Binding Corporate Rules zwischen Unternehmen (*genehmigungspflichtig*),
  - Standarddatenschutzklauseln,
  - Genehmigte Verhaltensregeln,
  - Genehmigter Zertifizierungsmechanismus.
- Praktische Relevanz entfalten hauptsächlich das Vorliegen eines **Angemessenheitsbeschlusses** oder der Abschluss von **Standardvertragsklauseln**.

ANGMESSENHEITSBESCHLUSS

- Die Europäische Kommission kann gemäß Art. 45 Abs. 3 DS-GVO feststellen, dass personenbezogene Daten in einem bestimmten Drittland, Gebiet oder Sektor einem **mit dem europäischen Datenschutzrecht vergleichbaren Schutz** genießen.
- Angemessenheitsbeschlüsse bestehen **ausschließlich** für folgende Länder:
  - Andorra,
  - Argentinien,
  - Kanada („*commercial organisations*“),
  - Färöer,
  - Guernsey,
  - Israel,
  - Isle of Man,
  - Japan,
  - Jersey,
  - Neuseeland,
  - Südkorea,
  - Schweiz,
  - Vereinigtes Königreich,
  - Uruguay.



mapchart.net, CC BY-SA 4.0

BINDING CORPORATE RULES

- Binding Corporate Rules („*verbindliche interne Datenschutzvorschriften*“) legitimieren **interne Datenübermittlungen multinationaler Unternehmensgruppen**.
- Sie unterliegen bestimmten inhaltlichen Anforderungen sowie einem **Genehmigungsvorbehalt** der zuständigen Aufsichtsbehörde.
- Zu berücksichtigen ist der jeweilige **Anwendungsbereich** der Binding Corporate Rules, zum Beispiel *Controller – Controller* oder *Controller – Processor*.
- **Übersicht** genehmigter Binding Corporate Rules:
  - Vor dem 25. Mai 2018 (vor Anwendbarkeit der DS-GVO): Link – zum Beispiel: DocuSign, Mastercard, Salesforce, Twilio Ireland Limited, Zendesk International Limited.
  - Ab dem 25. Mai 2018 (mit Anwendbarkeit der DS-GVO): Link – zum Beispiel: Luxoft Group, Webhelp.

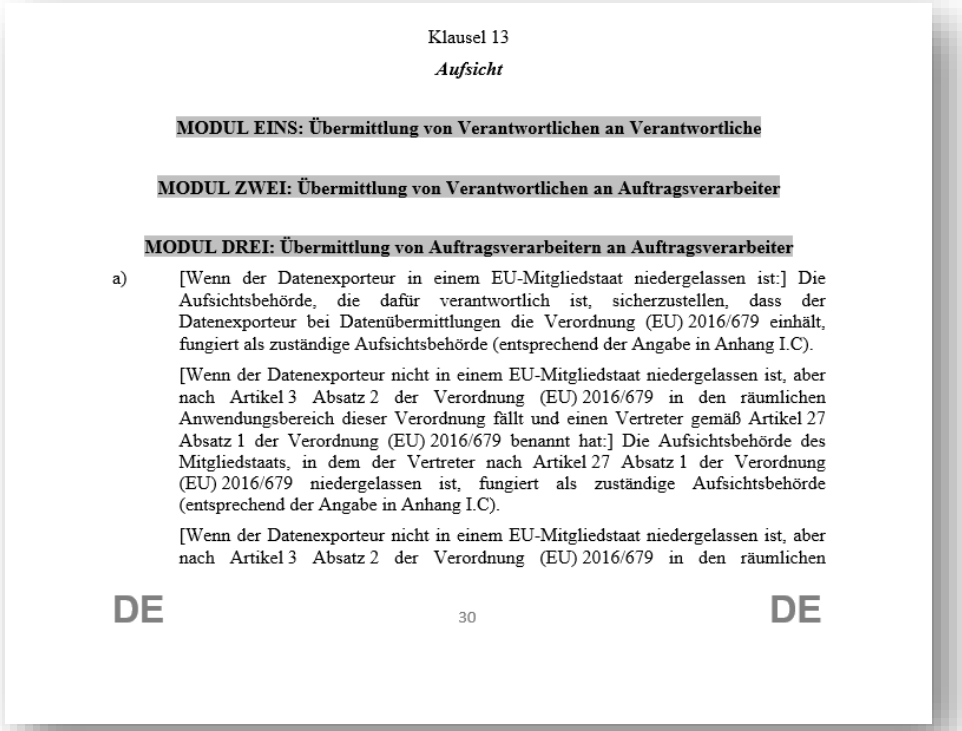
NICHT UMFASST SIND:

- **Adobe**,
- **Alphabet** (*Google*),
- **Amazon**,
- **Apple**,
- **Atlassian**,
- **Canva**,
- **Cisco**,
- **Citrix**,
- **Hubspot**,
- **LinkedIn**,
- **LogMeIn** (*GoToMeeting*),
- **Meta** (*Facebook, Instagram, WhatsApp*),
- **Microsoft**,
- **Rocket Science Group** (*Mailchimp*),
- **Slack**,
- **Twitter**,
- **Zoom**,
- **...**

STANDARDDATENSCHUTZKLAUSELN

- Standarddatenschutzklauseln („Standardvertragsklauseln“) gemäß Art. 46 Abs. 2 lit. c DS-GVO werden in einem **Prüfverfahren** durch die Europäische Kommission erlassen.
- **Vertragliche (Muster-)Vereinbarung** zwischen datenübermittelnder und datenempfangender Stelle (Verantwortlicher – Verantwortlicher, Verantwortlicher – Auftragsverarbeiter, neu: Auftragsverarbeiter – Auftragsverarbeiter).
- Neue Standarddatenschutzklauseln bieten einen **modularen Aufbau** und beinhalten den **risikobasierten Ansatz** – Vorprüfung durch Verantwortlichen, ob hierdurch ein angemessenes Datenschutzniveau erreicht werden kann (sonst kein Abschluss zulässig). → **„Transferfolgenabschätzung“**
- Bisherige Standarddatenschutzklauseln durften nur noch bis **September 2021** abgeschlossen werden, bis **27. Dezember 2022** sind auch in bereits bestehenden Vertragsverhältnissen die neuen Standarddatenschutzklauseln anzuwenden.

STANDARDDATENSCHUTZKLAUSELN



Klausel 13

Aufsicht

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

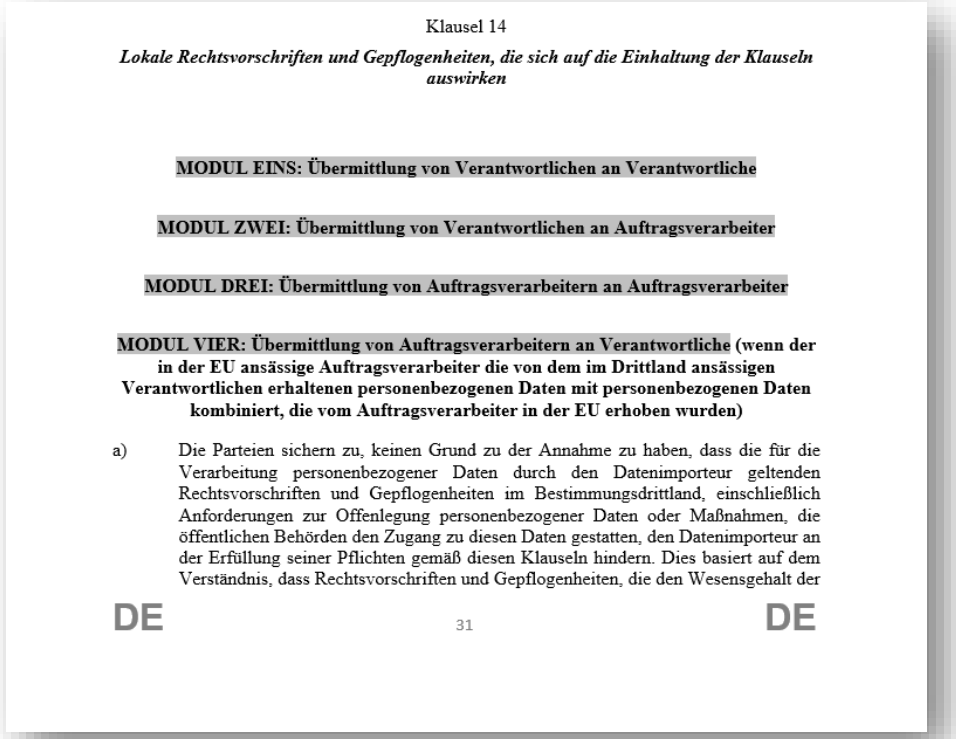
MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

a) [Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen

DE 30 DE



Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche (wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden)

a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der

DE 31 DE

TRANSFERFOLGENABSCHÄTZUNG

- Die Verpflichtung zur Durchführung einer Datentransferfolgenabschätzung ergibt sich unter anderem aus **Klausel 14** der Standardvertragsklauseln.
- Verpflichtende Inhalte:
  - Art der personenbezogenen Daten und Kreis der betroffenen Personen,
  - Häufigkeit und Dauer der Verarbeitungstätigkeit,
  - Getroffene technische und organisatorische Maßnahmen zur Sicherstellung eines hohen Datenschutzniveaus, z.B. durch Verschlüsselung **(!)**,
  - Betrachtung der Rechtslage im jeweiligen Drittland hinsichtlich des Datenschutzes,
  - Beurteilung von Alternativen innerhalb der EU / des EWR.
- Im Ergebnis ist sodann festzuhalten, weshalb ein Einsatz aus Sicht des Unternehmens datenschutzrechtlich **dennoch vertretbar** ist.
- Die Parteien haben sich bei der Durchführung gegenseitig zu unterstützen.

TRANSFERFOLGENABSCHÄTZUNG

- Unternehmen in Drittländern stellen zumeist gebündelte Informationen zur Durchführung einer Transferfolgenabschätzung bereit, z.B. **Atlassian**:
  - Hinweise zur Durchführung einer Transferfolgenabschätzung,
  - Vertrag zur Auftragsverarbeitung inklusive Standarddatenschutzklauseln,
  - Richtlinien für Anfragen von Strafverfolgungsbehörden,
  - Transparenzbericht.

Atlassians Reaktionen auf Behördenanfragen nach Nutzerdaten (international)

JAHR	ANTWORT	ANZAHL DER REAKTIONEN
2021	Einige Nutzerinhalte vorgelegt	0
	Nur Daten ohne Nutzerinhalte vorgelegt	0
	Keine zutreffenden Daten vorzulegen	0
	Anfrage abgelehnt und keine Daten beigefügt	3

Dieses Dokument ist als Anlage zur benannten Verarbeitungstätigkeit beizufügen, sofern eine Übermittlung personenbezogener Daten in ein Land außerhalb der EU / des EWR oder an eine internationale Organisation durchgeführt wird. Die Datenübermittlung findet wie folgt statt oder ist wie folgt geplant:

Name und Anschrift des Empfängers

Zweck der Übermittlung

Kategorien der von der Übermittlung betroffenen Personen und personenbezogener Daten

Beschreibung der Übermittlung

Bitte beschreiben Sie kurz die verwendeten Übertragungskanäle (z.B. per E-Mail, Schnittstelle, Cloud-Zugang), das Format (z.B. Art der Verschlüsselung) sowie den Speicherort der personenbezogenen Daten, ob durch den Empfänger gegebenenfalls weitere Übermittlungen vorgenommen werden und benennen Sie diese weiteren Empfänger (z.B. Unterauftragsverarbeiter).

Übermittlungsgrundlage

☐ Angemessenheitsbeschluss der Europäischen Kommission
☐ Standarddatenschutzklauseln / Standardvertragsklauseln
☐ Verbindliche interne Datenschutzvorschriften / Binding Corporate Rules
☐ Sonstiges:

Sofern als Übermittlungsgrundlage die Standardvertragsklauseln herangezogen werden, ist nach Klausel 14 dieser eine sogenannte Transferfolgenabschätzung („Transfer Impact Assessment") durchzuführen. Hierzu ist die Angabe weiterer Informationen erforderlich:

Relevante Rechtsvorschriften und Gepflogenheiten im Drittland sowie geltende Beschränkungen und Garantien

Maßnahmen, die im Bestimmungsland angewandt werden

Ergänzende technische und organisatorische Maßnahmen (TOM)

Dies können beispielsweise eigene Verschlüsselungsverfahren oder vorgenommene Pseudonymisierungen sein.

Begründung der Übermittlung / Ausschluss europäischer Alternativen

Dresdner Institut für Datenschutz

Step 3: Define the safeguards in place

				Reasoning
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?[7]	No		*The analysis needs to be done by the parent company, which is located in the US. This is also where the staff performing such analysis is located.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*n/a*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?[8]	No	*Ensure that data remains encrypted*	*All traffic over telecom lines is protected by state-of-the-art line encryption (VPN).*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*The parent company needs access to the HR data in clear text in order to be able to process it. Encryption is not possible.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial	Yes	*Ensure that the mechanism remains in place and is complied with*	*We have in place an IGDTA based on the new EU SCC, and we have no reason to believe that the parent company will not comply with them, to the extent that US law permits so. Regular audits confirm the adequacy of the data security agreed therein.*
Based on the answers given above, the transfer is:		**permitted, subject to Step 4**		

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction[9]

*Country-specific! The following factors have been drafted for **US law**; amend as necessary for other jurisdictions.*

				Reasoning
a)	Assess the probability that during the assessment period, the following *legal arguments* will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the			
		Probability†	Probability of possibility of a (successfull) request††	
	The data importer/recipient is no "Electronic Communications Service Provider"[11] with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	90%	10,00%	*In the context of the transfer, the parent company does not provide any cloud, data storage or communications service. It is using the data for its own purposes.*

David Rosenthal

HANDLUNGSEMPFEHLUNGEN

- **Evaluierung eingesetzter Dienstleister mit Bezug zu einem Drittland.**
  Dieser kann bereits dann gegeben sein, wenn es sich bei dem Dienstleister um ein Tochterunternehmen eines in einem Drittland ansässigen Mutterunternehmen handelt oder ein solches Unternehmen als Unterauftragsverarbeiter im Rahmen einer Auftragsverarbeitung tätig wird.

- **Betrachtung gleichwertiger Alternativen innerhalb der EU / des EWR.**
  Wirtschaftliche Aspekte allein schließen nicht automatisch eine Gleichwertigkeit aus. Gleichwertige Alternativen bestehen regelmäßig hinsichtlich der Nutzung von Microsoft Teams, Google Drive, Google Analytics, Zoom. Alternativen für Microsoft 365 sind umstritten. Hier erfolgt seitens der Aufsichtsbehörden eine Duldung.

- **Durchführung einer Datentransferfolgenabschätzung.**
  Diese ist für den jeweiligen Einzelfall unter Beachtung der zuvor aufgeführten Kriterien durchzuführen. Fällt diese positiv aus, kann ein Abschluss der neuen Standardvertragsklauseln erfolgen. Bestehen Zweifel, ist kein Einsatz des Dienstleisters möglich.

- **Auswahl der erforderlichen Module, Abschluss der Standardvertragsklauseln.**

WEITERE INFORMATIONEN

Unser Leitfaden:

Unsere Blog-Beiträge:

- „*Das EuGH-Urteil zum EU-US-Privacy Shield*“ *(2020)*
- „*Die neuen Standardvertragsklauseln*“ *(2021)*
- „*Übermittlung personenbezogener Daten in Drittländer*“ *(2022)*

Sie können unseren Blog auch als RSS-Feed abonnieren und erhalten so wöchentlich die aktuellsten Beiträge auf Ihren RSS-Reader.

Zeit für Ihre Fragen!

Dresdner
Institut für
Datenschutz