

Datenschutzverträge, Standardvertragsklauseln und Haftung

RA Dr. Michael M. Pachinger, CIPP/E
16. Österreichischer IT-Rechtstag 2022
Wien, 06.05.2022

AUSTRIA BELGIUM BULGARIA CHINA CZECH REPUBLIC FRANCE
GERMANY HUNGARY ITALY POLAND ROMANIA SLOVAKIA SPAIN TURKEY

[scwp.com](https://www.scwp.com)

Pachinger

Datenschutz-Verträge

Verantwortlicher – Auftragsverarbeiter –
Joint Controller

- Rollenverteilung
- Vertragsgestaltung
- Vertragsklauseln
- Vertragsmuster
- Standardvertragsklauseln

Beispiele
Querverweise
Praxistipps

ÜBERSICHT

- Verantwortung / Haftung
- EDPB Guidelines 07/2020 „*concepts of controller and processor*“
- Gemeinsam Verantwortliche
 - Vertragsgestaltung
 - Spezialaspekt Weiterverarbeitung
- Auftragsverarbeitung
 - Einzelne Spezialaspekte
 - Vertragsgestaltung
- Standardvertragsklauseln Drittländer (SCC)

VERANTWORTUNG

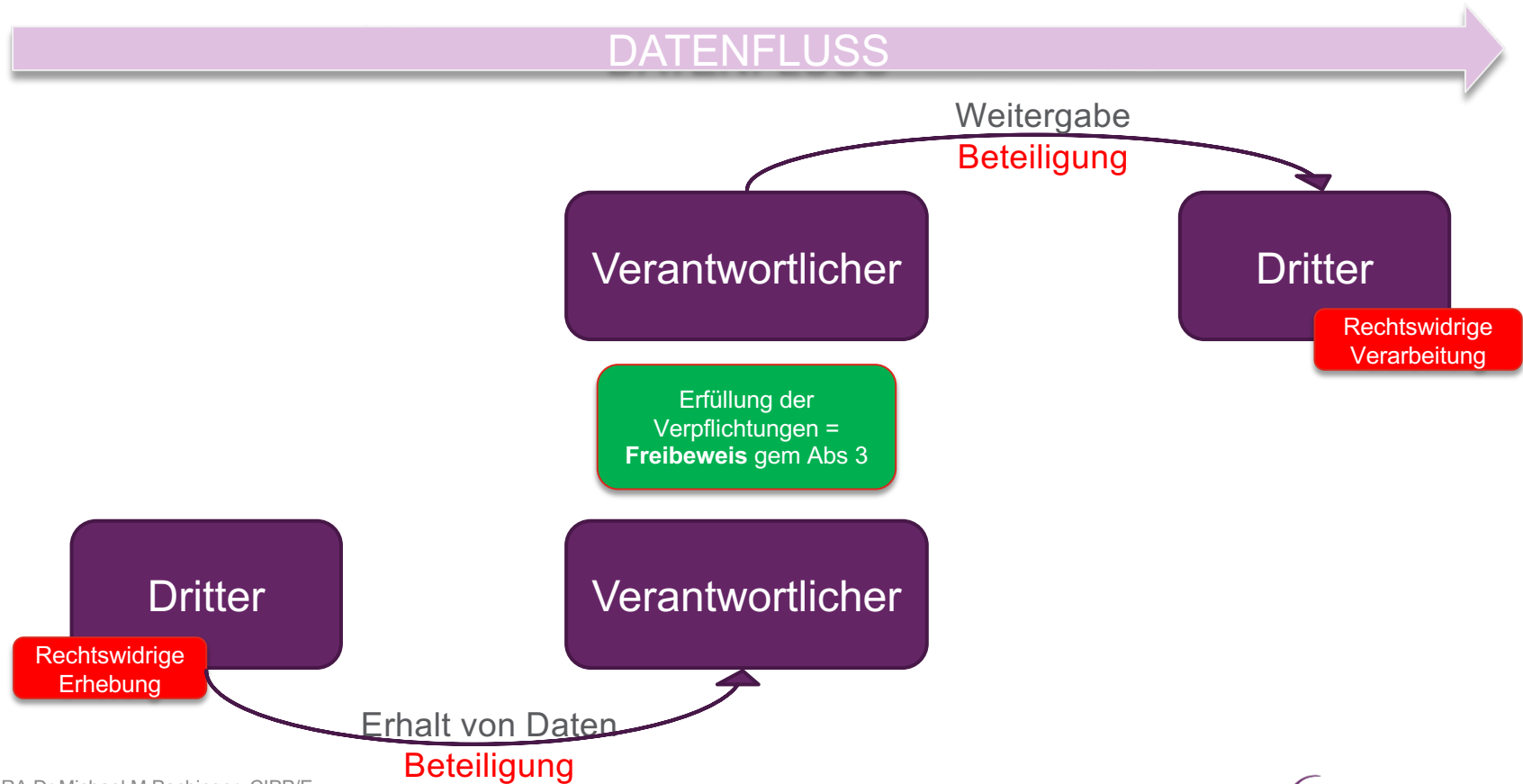
SELBSTVERANTWORTUNG (ART 24, 25, 32)

- Sicherstellung und Nachweis (Art 24, 25)
- angemessene **technische** und **organisatorische Maßnahmen** zur wirksamen Umsetzung der Grundsätze der DSGVO und zwar unter Berücksichtigung
 - der *Art, des Umfangs, der Umstände, des Zwecks der Verarbeitung*
- Pflicht zur Gewährleistung eines **angemessenes Schutzniveaus**, unter Berücksichtigung (Art 32)
 - von *Art, Umfang, Umstände und Zwecke der Verarbeitung* sowie
- Eintrittswahrscheinlichkeit des Risikos / Risikobewertung (Art 35)

HAFTUNG & SCHADENERSATZ

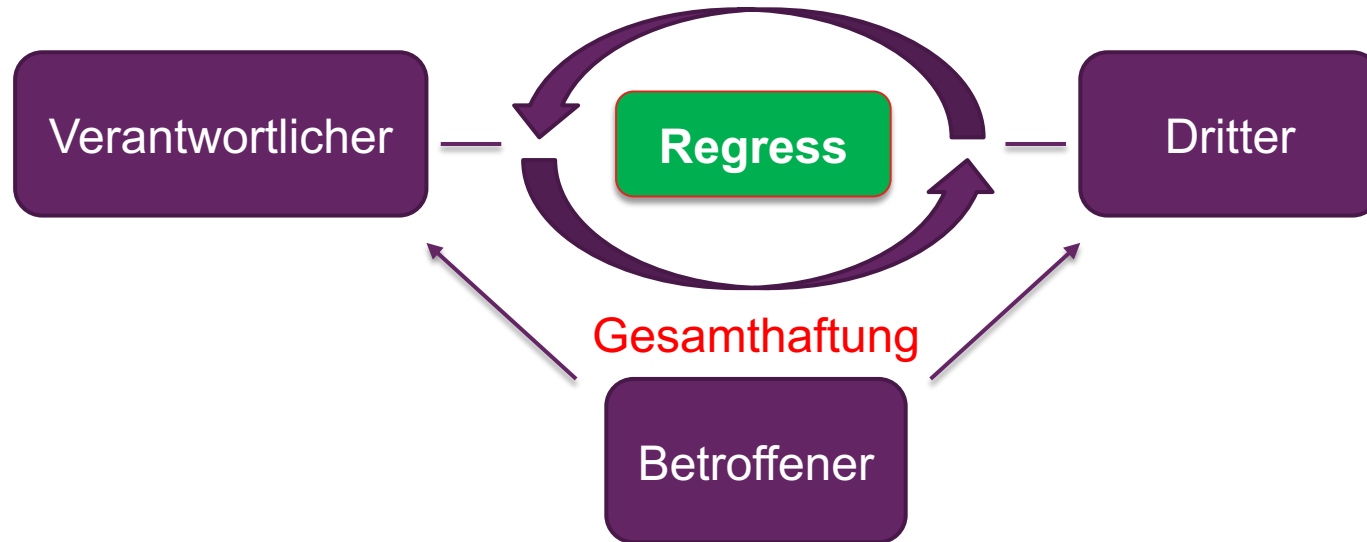
- Anspruch auf Schadenersatz gegen V oder AV
 - Jeder an einer Verarbeitung Beteiligter haftet!
- Verstoß gegen die DSGVO
 - „nicht im Einklang mit der Verordnung“
 - auch: präzisierende Rechtsvorschriften der MS
- Materieller / Immaterieller Schaden
 - alle zurechenbaren Nachteile, geschützte Rechtsgüter (ErwGr 75)
- Haftungsbefreiung: in keinerlei Hinsicht für Schaden verantwortlich!
 - „Verantwortungszusammenhänge“

HAFTUNG & SCHADENERSATZ (BETEILIGUNG)



GESAMTHAFTUNG (REGRESS)

- Mehrere V oder AV haften für gesamten Schaden
- Innenausgleich/Regress



NACHWEIS UND VERTRAGSRECHT (I)

- Grundsatz der Rechenschaftspflicht (Art 5 Abs 2)
- VGV
 - Informationspflichten, Betroffenenrechte
 - Wiedergabe tatsächlicher Funktionen und Zurverfügungstellung
- AVV
 - Kriterien der Verarbeitung nachweisbar dokumentiert
- SCC (Drittländer)
 - Klausel 14: Umstände der Übermittlung, Gepflogenheiten
 - Beurteilung qua Transfer Impact Assessment (TIA)

NACHWEIS UND VERTRAGSRECHT (II)

- Datenschutzverträge als wichtige Nachweise für
 - Entlastungsbeweis und für
 - Erfüllung der Verarbeitungsgrundsätze
 - Transparenz
 - Fairness (Treu und Glauben)
 - Rechtmäßigkeit
- Konzipierung der Verträge **nach Treu und Glauben**

EDPB GUIDELINES 07/2020 V2.0,
ADOPTED ON 07 JULY 2021

VERANTWORTLICHER (ART 4 Z 7)

- Relevante Fragen
 - Warum wird Verarbeitung durchgeführt? Wer hat sie veranlasst?
 - Warum? → Zweck → dem Verantwortlichen vorbehalten
 - Wie? → Mittel (essenzielle / nicht essenzielle)
- Funktionales Konzept vs formale Bezeichnung
 - Realität abbilden:

*„It is not possible either to become a controller or to escape controller obligations simply by **shaping the contract** in a certain way where the **factual circumstances** say something else“ (Rz 26)*
- Bezug zur Datenverarbeitung
 - eine / eine Reihe von Verarbeitungstätigkeit(en) oder Bereich davon

AUFTRAGSVERARBEITER (ART 4 Z 8)

- 2 Grundvoraussetzungen
 - Separate Entität (im Vergleich zum Verantwortlichen)
 - Mitarbeiter als Teil des Verantwortlichen
 - Abteilungen untereinander idR nicht als Auftragsverarbeiter
 - Verarbeitung pb Daten im Auftrag des Verantwortlichen
- Analyse der konkreten Aktivitäten – Dienstleistung auf Datenverarbeitung gerichtet ist?

*„In practice, where the provided service is not **specifically targeted at processing personal data** or where such processing does not constitute a **key element of the service**, the service provider may be in a position to independently determine the purposes and means to that processing which is required in order to provide the service.“
(Rz 25)*

■ Gemeinsam Verantwortliche?

- kumulatives Zusammenwirken
 - Mitentscheidung über Zielrichtung/Modalitäten (Relevanzschwelle)
 - Gemeinsame / konvergierende Entscheidungen
- Maßgeblich:
 - nicht tatsächliche Mitwirkung bei einzelnen Datenverarbeitungen
 - Veranlassung oder direkte Mitgestaltung – zB als Auftraggeber
- Gemeinsamer Zweck

*„...use of a **common data processing system** or **infrastructure** will not in all cases lead to qualify the parties involved as joint controllers ... the existence of a mere **commercial benefit** for the parties involved is **not** sufficient to **qualify as a purpose** of processing) “
(Rz 68)*

- Sachverhalt
 - Hacker dringen in Infrastruktur des Telekomanbieters COSMOTE
 - Sensible Daten, 10 Mio Betroffene; Geldbuße EUR 6 Mio
- Rechtliche Beurteilung
 - Keine ausreichenden TOM beim Verantwortlichen (Anonym., DSFA)
 - Unzureichend klar definierte Rollenverteilung mit Filiale OTE Group
 - 3,2 Mio EUR Sanktion für Filiale qua Beitrag zur Infrastruktur
 - *„Zuteilung der Verantwortung und Zusammenarbeit hätte auf Vereinbarung gem Art 26 oder auf einer Vereinbarung oder anderem Rechtsinstrument gem Art 28 beruhen müssen“*

GEMEINSAM VERANTWORTLICHE

VGV-Vertragsgestaltung



VGW – VERTRAGSGESTALTUNG (I)

- Allgemein
 - gemeinsame Entscheidung
 - konvergierende Entscheidungen
 - für Verarbeitung notwendig, ergänzen sich
 - wirken sich auf Zwecke und Mittel aus
 - **Datenverarbeitung ohne Beteiligung der jeweils anderen Partei** im Hinblick auf Zwecke und Mittel **nicht möglich**
 - „*inseparable, ie inextricably linked*“ (EDPB Guidelines 07/2020 V2.0, Rz 55)
 - Zusammenarbeit in komplexen Akteurs-Netzwerken, zB Personalvermittlung, Ärzte

VGV – VERTRAGSGESTALTUNG (II)

- Phasen der Verarbeitungsvorgänge
 - dsb jüngst in E zu Google Analytics (D155.027):

„... die **datenschutzrechtliche Verantwortung** bei einem Verarbeitungsvorgang (aus rechtlicher Sicht) trotzdem „**teilen**“ lässt, es also je nach **Phase des Verarbeitungsvorgangs unterschiedlichen Grad der Verantwortung** geben kann...“
 - Vgl auch Guidelines 7/2020 EDSA, Rz 63 ff mwN
- Zuordnung der Verantwortlichkeiten
 - faktische Gegebenheiten („*operative agreement*“)
 - Tatsächliche Funktionen und Beziehungen zur betroffenen Person

VGW – VERTRAGSGESTALTUNG (III)

- Zuordnung der Verantwortlichkeiten im Innenverhältnis
- Achtung: Betroffene Person → Rechte bei und gegenüber jedem einzelnen Verantwortlichen (Art 26 Abs 3)
- EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, Rz 34:

*“... **arrangement** of the joint controllers regarding their **respective responsibilities** ... **data subject’s rights**, especially concerning the answer to **access requests**, does **not affect** the rights of the data subjects towards the controller to whom they address their request.”*

Spezialaspekt



- Andere Zwecke aller oder eines Verantwortlichen
 - Festlegungen zu zweckändernder Weiterverarbeitung der zunächst zu gemeinsamen Zwecken erhobenen Daten
 - neue Zwecke, die einem Akteur oder mehreren Akteuren dienen
- Sperrwirkung (Art 26 // Art 6 Abs 4 DSGVO)?
 - Nein, aber: Offenlegung der Feststellungen gegenüber Betroffenen als "Modellierung" der Erwartungshaltung; für weitere Verarbeitung zu berücksichtigen (ErwGr 50 S 6 DSGVO; Schulz)
 - To-Do:
 - Evaluierung, ob Aussagen zu Zweckänderung in VGv aufzunehmen
 - Strategische Erwägungen je nach Interessenlage

Praxisbeispiel



- Sachverhalt
 - Beklagte gab in Datenschutzerklärung nicht an, dass Google Analytics verwendet wird

- Rechtliche Beurteilung
 - Gemeinsame Verantwortlichkeit nach Art 26 DSGVO
 - Zwecke / Mittel der Datenverarbeitung tw von Google vorgegeben
 - keine Auftragsverarbeitung nach Art 28 DSGVO
 - Verarbeitung mit Google Analytics **einheitlicher Lebenssachverhalt**
 - verschiedene **Aspekte der Verarbeitung** machen **nur als Ganzes Sinn**
 - Beteiligte können nicht innerhalb einer Verarbeitungstätigkeit zwischen Verantwortlichem und Auftragsverarbeiter springen

AUFTRAGSVERARBEITUNG

Einzelne Spezialaspekte



VERTRAG VS ANDERES RECHTSINSTRUMENT? (I)

- Grundlage für Verarbeitung durch Auftragsverarbeiter ist Vertrag oder „*anderes Rechtsinstrument*“ (Art 28 Abs 3 S 1 DSGVO)
- EDPB (Guidelines 07/2020 v2.0, Rz 102):
 - „...*the contract or the other legal act under Union or Member State law must be binding on the processor with regard to the controller*“
 - Legal Act:
 - nationales Gesetz (national law, primary or secondary) oder
 - anderes Rechtsinstrument (other legal instrument)
- Praxis:
 - Telos: Möglichkeit, auf AV einzuwirken, Verpflichtungen auferlegen
 - Daher: nicht nur gesetzliche Vorschriften!

VERTRAG VS ANDERES RECHTSINSTRUMENT? (II)

- Rechtliche verbindliche Akte, einseitig bindende Verpflichtungen
- zB einseitig verpflichtende Erklärungen (Garantieerklärungen bei Standardleistungen, *Hartung in Kühling/Bucher*, Art 28 Rz 63)
- Praxis-Bsp: Online-Umfrage-Applikation (Auftragsverarbeiter) elektronisch zur Verfügung gestellte einseitige Erklärung mit Inhalt des Art 28 Abs 3 DSGVO
- Gültigkeit/Wirksamkeit
 - Art 28 Abs 9 DSGVO: schriftlich, elektronisches Format
 - „EDPB recommends ensuring that the necessary signatures are included in the legal act“ (Rz 101)
 - Praxis-Tipp: Unterschrift / elektron. Signatur in Erklärung aufnehmen!

AV – GESETZLICH ANGEORDNET

- Auftragsverarbeitung gesetzlich vorgesehen
 - COVID-19-Impfpflichtgesetz: “... *Bundesminister im Wege der ELGA GmbH als dessen Auftragsverarbeiterin*” (§ 6 Abs 6 COVID-19-IG)
- Vertrag zusätzlich erforderlich?
 - “*If the legal act does not include all the minimum required content, it must be **supplemented** with a **contract/another legal act** that includes the missing elements.*” (EDPB Guidelines 07/2020 V 2.0, Rz 102)
 - “... *gesetzliche Anordnung entbindet nicht davon, die Vorgaben des Art 28 Abs 3 DSGVO einzuhalten bzw einen AVV abzuschließen*” (dsb, Newsletter 1/2022; Stellungnahme zum COVID-19-IG)

AUFTRAGSVERARBEITER – WEITERVERARBEITUNG?

- Weiterverwendung Daten (Kunde, Auftraggeber) für eigene Zwecke
 - zB Analyse, Verbesserung v Cloud-Services, Sicherheit etc
- CNIL v 12.01.2022: Ja, aber strenge Voraussetzungen:
 - Klare Spezifizierung, wie und warum Daten weiterverwendet werden
 - Explizite & ausreichende Erlaubnis des Verantwortlichen
 - Kompatibilitätstest – neuer Zweck (Art 6 Abs 4)
 - Geeignete Garantien (Anonym.) ev kompatibel, Marketing des AV nicht
 - Nicht erfüllt: V hat Erlaubnis zu verweigern
 - Erfüllt: V kann zustimmen oder nicht
 - Information an Betroffene (zB Widerspruchsrecht)
 - AV als neuer V: DSGVO-Pflichten, insbes RGL/Info an Betroffene

- Unterstützungspflichten (Art 28 Abs 3 lit e DSGVO)
 - Unterstützung bei der Wahrnehmung der Rechte der betroffenen Person, zB fristgerechte Beauskunftung;
 - „Rechte und Freiheiten anderer“ gem Art 15 Abs 4 DSGVO
 - Achtung: auch Rechte des Auftragsverarbeiters berücksichtigen!
- *EDPB* (Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, Rz 169):

*“Others” means any other person or entity apart from the data subject ... Hence, the **rights/freedoms** of the **controller/processor** (trade secrets /intellectual property for example) **might come into consideration**. If the EU legislator had wanted to exclude controllers/processors rights/freedoms, it would have used the term “**third party**”, defined in Art. 4(10) GDPR.*

AVV-Vertragsgestaltung



SCC AUFTRAGSVERARBEITER

7.6.2021

DE

Amtsblatt der Europäischen Union

L 199/21

ANHANG

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

AVV ODER SCC? (I)

- Art 28 Abs 6 & 7 DSGVO: individueller Vertrag oder SCC
 - Freiwilligkeit / Wahlmöglichkeit
 - (Legalisierungs-)Wirkung Art 1 SCC: „*erfüllen Anforderungen DSGVO*“
- „Ganz oder gar nicht“
 - Klauseln nicht ändern, nur Ergänzung/Aktualisierung der in Anhängen gegebenen Informationen (Klausel 2a)
 - Dh nicht selektiv, nur insgesamt zu nutzen
 - Widerspruch zu Art 28 Abs 6 DSGVO ("ganz oder teilweise")
 - ErwGr 5: “*SCC insgesamt oder teilweise verwenden*”

- Einbindung in Vertrag
 - Art 2 SCC: "... SCC können in Verträgen... verwendet werden"
 - Klausel 2 SCC: "... SCC in umfangreichen Vertrag aufzunehmen... weitere Klauseln/zusätzliche Garantien nur, sofern diese **weder unmittelbar noch mittelbar im Widerspruch** zu Klauseln stehen oder Grundrechte/Grundfreiheiten der betroffenen Person beschneiden"
 - Ergänzungen, solange den SCC weder direkt noch indirekt widersprochen wird

AVV ODER SCC? (III)

- „Mängel/Ergänzungsbedarf“ (*Moos, Gosch, Datenschutz-Notizen, Pachinger*)
 - Klausel 7.1 b): Kein Recht, Weisung vorläufig auszusetzen
 - Klausel 7.5 (Sensible Daten): keine Spezifizierung zusätzlicher Garantien (auch nicht in Anlage) vorgesehen
 - Klausel 7.6 c), d) (Auditregelung): Mitwirkungspflichten nicht konkret
 - Klausel 7.6 d): Keine Frist zur Vorankündigung eines Audits, keine Vorgabe, Betriebsablauf nicht zu stören, keine Kostenregelung, kein Verbot externer Prüfer, die in Wettbewerbsverhältnis
 - Klauseln 7.7 (Sub-AV): Widerspruchsfrist – Wirkung nicht geregelt
 - Klausel 7.8 b) (Drittland): Zustimmung AV + Erfüllung SCC – keine Schrems II Problematik
 - Keine Erwähnung der Beauftragung durch gemeinsam Verantwortliche

AVV ODER SCC? (IV)

- Vorteile:
 - Rechtssicherheit (aber: Anhänge I-IV befüllen!)
 - Muster als Kompromiss (kommt nicht von einer Partei!)
- Nachteile:
 - Interessen der Parteien verwirklicht? Ergänzungsbedarf?
- Praxis:
 - SCC als Ausgangsbasis, Vertragsmuster für Standardverarbeitungen (*Gosch, jusIT 5/2021*)
 - Nicht geeignet für umfangreichere/komplexere Verarbeitungen (*Moos, DSB 09/2021*)
 - Mittelweg: nur einzelne Klauseln in eigenen, individuellen Vertrag; nicht als SCC bezeichnen! (*Datenschutz-Notizen 18.01.2022*)

STANDARDVERTRAGSKLAUSELN DRITTLÄNDER (SCC)

7.6.2021

DE

Amtsblatt der Europäischen Union

L 199/37

ANHANG

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

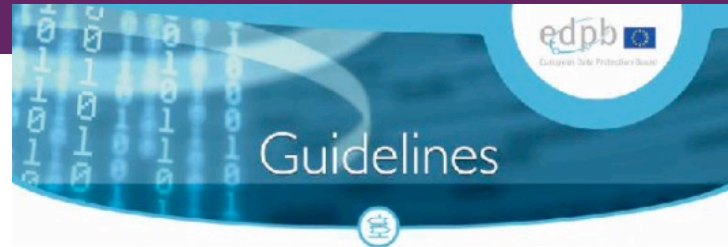
SCC – MUST-KNOW (I)

- **Achtung – Fristen:**
 - 27.06.2021: wirksam / in Kraft
 - 27.09.2021: neue SCC müssen für neue Prozesse verwendet werden
 - **27.12.2022**: **alte SCC** bei laufenden Prozessen **ersetzen**
- **Modularer Aufbau**
 - MODUL 1: Übermittl Verantwortl an Verantwortl (C2C)
 - MODUL 2: Übermittl Verantwortl an Auftragsverarbeiter (C2P)
 - MODUL 3: Übermittl Auftragsverarb an Auftragsverarb (P2P)
 - MODUL 4: Übermittl Auftragsverarb an Verantwortl (P2C)

SCC – MUST-KNOW (II)

- Risikobasierter Ansatz – ErwGr 20 & Fn 12
- Schrems II
 - Klausel 14, Prüfung Umstände & Angemessenheit lit b) - d), TIA
- ErwGr 9: SCC Drittländer erfüllen auch Art 28 Abs 3 und 4 DSGVO
- Achtung – Anwendbarkeit vs Art 3 DSGVO:
 - ErwGr 7: SCC nur insoweit, als Verarbeitung durch Datenimporteur nicht unter DSGVO fällt
 - Art 1 (1): SCC als geeignete Garantien für Übermittlung eines Exporteurs an Verantwortlichen / (Unter-)Auftragsverarbeiter, dessen Verarbeitung nicht dieser Verordnung unterliegt (Importeur)

SCC – CHAPTER V „TRANSFER OF DATA“



Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

Adopted on 18 November 2021

SCC – CHAPTER V „TRANSFER OF DATA“

- „Transfer of Data“ – 3 cumulative criteria (for given processing!):
 - Controller or Processor subject to GDPR
 - Exporter discloses or makes available data to importer
 - Importer is in 3rd country (or int. Org), ***irrespective of whether or not this importer is subject to the GDPR***
- Consequences:
 - Controller or processor in „transfer situation“ have to comply with Chapter V
 - As to transfer tools - content of safeguards:
 - Transfer by processor not the same as transfer by controller
 - Transfer to a controller in 3rd country **less protection/safeguards needed if subject to GDPR!**
 - SCC/Adhoc clauses: **„Art 3(2) situation to be taken into account in order not to duplicate GDPR obligations but rather address elements/principles that are ‘missing’ and needed to fill the gaps“**
 - Tools should address measures to be taken in case of conflict of laws GDPR/3rd country
 - **New set of SCC** in cases where importer is subject to GDPR for processing re Art 3 (2)

SCC – LÖSCHEN & ANONYMISIEREN

- SCC Drittländer – Klausel 8:
 - Modul 1 (C2C) „Einhaltung Speicherbegrenzung“
 - „Löschung oder Anonymisierung“
 - Module 2-4: „**Löschung oder Rückgabe**“ (wie Art 28 DSGVO)
 - Recht zur Anonym. könnte nur einzelvertraglich vereinbart werden → Controller hat Verantwortung/Pflicht, Validität d Anonym.verf bei AV zu prüfen
- Modul 1:
 - Verantw. Datenimporteur:
 - muss Anforderungen an Anonym. selbst prüfen, da entscheidet (RGL, Art 13, DSFA)
 - Ähnliche Prüfpflichten, als hätte man Anonymisierung in Modulen 2-4 vereinbart (in anderen Modulen: Verantwortlicher durch Vertragsgestaltung Prüfung entziehen)
 - Verantw. Datenexporteur – Prüfpflicht?
 - Gem Klausel 8 Abs 1 versichern, davon überzeugt zu haben, dass Datenimporteur Pflichten aus Klauseln, dh auch 8.4, nachkommt.
 - Eigene Prüfpflicht verletzt, gg **Haftung beider!**

TO-DO'S

- Gliederung in Phasen
 - Vorvertrag, Verhandlung, Durchführung/Erneuerung
- Frist 27.12.2022
 - Neue SCC & Etablierung TIA
- Erarbeitung Klausel-Katalog
 - Verantwortlicher / Auftragsverarbeiter / Joint Controller
 - „*Must have*“, „*nice to have*“, „*akzeptable/nicht akzeptable Klauseln*“
- Drittparteien-Audits / Zertifizierungen
 - Key-Lieferanten, kritische Dienstleister
 - Zweck: Beschleunigung der Vertragsgestaltung

KONTAKT



Michael M. Pachinger

Dr. iur., CIPP/E

Rechtsanwalt, Partner

Avocat inscrit (Paris), Abogado inscrito (Valencia)

Univ.- & FH-Lektor, EuroPriSe Legal Expert

European Trademark & Design Attorney



Michael M. Pachinger
SCWP Schindhelm
Data Protection Lawyer
of the Year in Austria



@MichaelMPachin1



[Dr. Michael M. Pachinger, CIPP/E | LinkedIn](#)



Newsletter: Aktuelles zum IT- und Datenschutzrecht
m.pachinger@scwp.com