DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

BvD e.V.

BvD-Blitzlicht – Wie prüfe ich eine AVV datenschutzrechtlich? Was muss, was kann, was soll?

online, 25.08.2022

Dr. Jens Eckhardt
Rechtsanwalt und Fachanwalt für IT-Recht
Datenschutz-Auditor (TÜV)
Compliance-Officer (TÜV)

Wie prüfe ich eine AVV datenschutzrechtlich? Agenda

- **Was muss?**
- **Was soll?**
- **Was kann?**
- **Fragen und Diskussion**

Wie prüfe ich eine AVV datenschutzrechtlich? Was muss, was kann, was soll?

- **Ausgangspunkt**
  - **Kenntnis und Verständnis der Anforderungen der DS-GVO an Auftragsverarbeitung**
  - **Einordnung der tatsächlichen Konstellation**
  - **3 typische Gestaltungsvarianten** (AVV mit allen relevanten Inhalten **oder** AVV mit Verweis auf Anlagen bzw. Online-Dokumente oder Zertifizierungen **oder** AVV neben Hauptvertrag und damit mit Verweis auf Hauptvertrag)
  - Beachtung der Grenzen zur Rechtsberatung (Stichwort: Haftung des DSB)

- **Was muss?**
  - Vorgaben des Art. 28 DS-GVO (plus Art. 29 DS-GVO)
- **Was soll? -** kein Muss, aber geboten
  - praktische Konkretisierung der gesetzlichen Vorgaben (bspw. Art. 33 Abs. 2 DS-GVO)
  - auftragsspezifische Gestaltungen (bspw. nur Hosting, nur Wartung)
- **Was kann?**
  - Vereinbarung über Auftragsverarbeitung = Vertrag im Sinne des Zivilrechts
  - rechtlich Zulässiges und ohne Widerspruch zu Art. 28 DS-GVO (bspw. Haftung, Freistellung, Kündigungsregelungen)

Wie prüfe ich eine AVV datenschutzrechtlich? Was muss?

- **Verantwortlicher zu Auftragsverarbeiter**
  - **konstitutiv: Vereinbarung nach Maßgabe des Art. 28 DS-GVO**
  - Auftraggeber: Festlegung von Zwecke und Mittel
  - Weisungsgebundenheit des Auftragnehmers (Art. 29 DS-GVO)
  - Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern der EU-Kommission vom 04.06.2021
- **Rechtsgrundlage für die Offenlegung personenbezogener Daten**
  - Art. 28, 29 DS-GVO (umstritten)
  - Argumentationsansatz (u.a.): keine Offenlegung wegen Weisungsgebundheit
  - anderenfalls: „Herausforderung“ durch Art. 9 DS-GVO
- **Drittlandtransfer**
  - kein Bestandteil des Art. 28 DS-GVO
  - eigenständige Regelung in Art. 44 DS-GVO – eigenständiger Verstoß
  - **Achtung: NEUE SCC ab 27.12.2022 zwingend**
- **Rechtsfolgen**
  - gesamtschuldnerische Haftung im Außenverhältnis mit Exkulpationsmöglichkeit für Auftragsverarbeiter
  - Haftung des Auftraggebers für Auftragsverarbeiter (§ 278 BGB)

Wie prüfe ich eine AVV datenschutzrechtlich? Was muss?

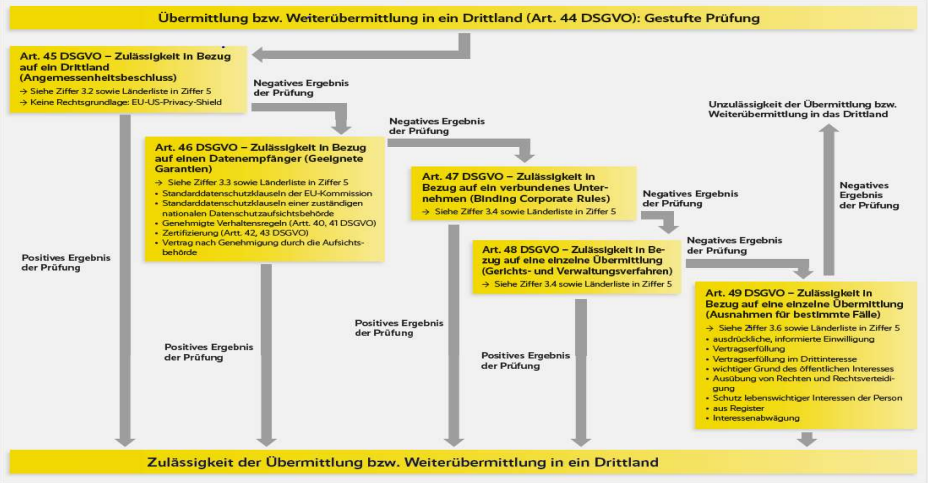
- **Auftragsverarbeitung**
  - **Weisungsgebundenheit (Art. 28, 29 DS-GVO)**:
    Entscheidungsspielraum eines Auftragsverarbeiters in Bezug auf Zweck und Mittel?
    - DSK (Kurzpapier 13) & Guidelines 07/2020 on the concepts of controller and processor in the GDPR & LfDI Baden-Württemberg, FAQ Verantwortlicher/Auftragsverarbeiter, Stand: 14.07.2021
    - keine (Mit-)Entscheidung in Bezug auf Zweck
    - (Mit-)Entscheidung in Bezug auf „nicht-wesentliche Mittel“
  - **Vereinbarung nach Maßgabe des Art. 28 DS-GVO - Auswahl an Themen**
    - Beurteilung der Anforderungen nach Art. 32 DS-GVO
    - Kontrollrecht vor Ort
    - Einbindung von IT-Dienstleistern = „weitere Auftragsverarbeitung“ mit Genehmigungspflicht?
    - Vorgabe der Vertragsinhalt aus AG-AN-Verhältnis für AN-UAN-Verhältnis?
    - Verweis auf andere Dokumente (dynamische Verweisungen oder Formmängel)
  - **Konsequenzen einer nicht ausreichenden Gestaltung nach Art. 28 DS-GVO?**
  - **Sonderthema: Melde- und Benachrichtigungspflicht nach Artt. 33, 34 DS-GVO**
    „Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.“ (Art. 33 Abs. 2 DS-GVO)

Wie prüfe ich eine AVV datenschutzrechtlich? *EXKURS:* Drittlandtransfer

- **Drittlandtransfer**
  - kein Bestandteil des Art. 28 DS-GVO
  - Eigenständige Regelung in Art. 44 DS-GVO – eigenständiger Verstoß

- **Anwendung der Regelungen über Drittlandübermittlung**
  *„Jedwede **Übermittlung** personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist **nur zulässig, wenn** der **Verantwortliche und der Auftragsverarbeiter** die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt **auch für die etwaige Weiterübermittlung** personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.“ **(Art. 44 DS-GVO)***
  - **Was ist ein Drittland?**
  - **Was bedeutet Übermittlung?**
    - Standort der Daten und/oder Sitz des empfangenden Unternehmens?
    - bspw.: Beispiele bei LfDI Baden-Württemberg, Orientierungshilfe vom 24.08.2020 (Ziffern II, IV)
    - „etwaige Weiterübermittlung … an ein anderes Drittland“
    - Vergabekammer BaWü, Beschluss v. 13.07.2022, 1 VK 23/22
  - ➔ **Konsequenz: zusätzliche (!) Zulässigkeitsprüfung**

Wie prüfe ich eine AVV datenschutzrechtlich?
EXKURS: Drittlandtransfer



Quelle: Eckhardt/Fuhlert, Datenverarbeitung in Drittstaaten, PrivacyXperts, ISBN: 978-3-8125-2900-6, Seite 38

Wie prüfe ich eine AVV datenschutzrechtlich?
Was muss?

- **Checkliste der Berliner Beauftragten für den Datenschutz und Informationsfreiheit**
  - **Pressemitteilung, 19.07.20222:** Webhoster mit unzureichenden Vereinbarungen über die Auftragsverarbeitung als Anlass für Prüfung der Vertragsmuster
    - Checkliste daher nur hierfür tauglich?
  - **Hinweise zur Nutzung der Checkliste Prüfung AVV, Version 1.0, 30.06.2022**
    - „keinen Anspruch auf Vollständigkeit und Richtigkeit“, aber abgestimmte Rechtsauffassung der an Erstellung mitwirkenden Aufsichtsbehörden
  - **Checkliste Prüfung AVV, Version 1.0, 30.06.2022**

Checkliste Prüfung AVV

Version 1.0, 30. Juni 2022

Vorgangsnummer:		Bezeichnung:	
Datum:		Bearbeiter:in:	

Nr.	Norm	Stichwort	Fundstelle in AVV	Erfüllt	Nicht erfüllt
1	Art. 28 Abs. 3 UAbs. 1 S. 1	AVV wird zwingend abgeschlossen und gilt zeitlich für alle Verarbeitungen		□ gesondert □ Teil der AGB □ zwingend in Bestellprozess □	□ nur optional □ AVV deckt zeitlich nicht alle Verarbeitungen von pbD ab, etwa nach Kündigung des AVV oder des Hauptvertrags fortgesetzte Verarbeitungen □
2	Art. 28 Abs. 3 UAbs. 1 S. 1	rechtlich bindend für die Auftragsverarbeiter		□ Vertrag □ sonstiges bindendes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, und zwar:	□
3	Art. 28 Abs. 9	AVV schriftlich/elektronisch		□ Papier mit Unterschriften (incl. aller Anlagen mit Pflicht-Inhalten) □ Papier mit Unterschriften wird ge-	□ Vertragsdokumente mit Pflicht-Inhalten werden □ im Bestellprozess □ im AVV nur referenziert

Wie prüfe ich eine AVV datenschutzrechtlich? Was muss?

- **Checkliste Prüfung AVV, Version 1.0, 30.06.2022 – Highlights**
  - **Prüfungsgegenstand: AVV und in Bezug genommene Dokumente (aus „Hinweise …")**
    - Formmangel in Bezug auf Pflichtinhalte = Formmangel der AVV
    - ergänzender pauschaler Verweis auf nicht formgerechte Inhalte = Formmangel der AVV (m.E. zweifelhaft)
  - **Weisungsrecht**
    - bei Verweisung auf Hauptvertrag ohne Festlegung im Hauptvertrag
    - neue Weisung im Change-Request-Verfahren: nur bzgl. Kosten, aber nicht bzgl. Ob
    - „auch für Datenexporte"
  - **Dedizierte Vorgaben zum Abschluss und zur Dokumentation der Vereinbarung**
  - **Kostenpflichtigkeit von Unterstützungspflichten** (bspw. bei Datenpannen, bei der Beantwortung von Betroffenenrechten oder die Ermöglichung von Kontrollen): Problem, falls ohne Ausnahme für Verstoß des Auftragsverarbeiters
  - **Unzulässigkeit von Vertraulichkeitsverpflichtungen** mit Ausschluss der Offenlegung gegenüber der Aufsichtsbehörde oder betroffenen Personen ausschließen
  - Klare **Definition der erfassten Verarbeitungen** in AVV
  - **Zulässigkeit von weisungswidrigen Verarbeitungen** nur bei Pflicht aufgrund Unionsrecht oder EU-Mitgliedsstaaten-Recht: Zulässigkeit aufgrund von bspw. US-Recht = Verstoß
  - Entscheidungshoheit des Auftraggebers, ob **Löschung oder Rückgabe**

Wie prüfe ich eine AVV datenschutzrechtlich? Agenda

- **Was muss?**
- **Was soll?**
- **Was kann?**
- **Fragen und Diskussion**

Wie prüfe ich eine AVV datenschutzrechtlich? Was soll?

- **Auftragsspezifische Beschreibungen des Gegenstands**
  - bspw. keine Verarbeitung personenbezogener Daten im eigentlichen Sinn sondern nur Unvermeidbarkeit des Zugriffs
  - Übernahme von Pflichten gegenüber den betroffenen Personen als Vertreter des Auftraggebers
- **(Un-)Zulässigkeit der Verarbeitung bzw. Transfer in Drittland**
- **Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DS-GVO)**

  *„(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten **meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde**, … .*

  *(2) Wenn dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt wird, **meldet er diese dem Verantwortlichen unverzüglich**.*

  (3) ….“
  - **Risiko für Auftragsverarbeiter: Fehlende Ausgestaltung des konkreten Meldeprozesses**
  - **Risiko für Auftragsverarbeiter: Keine eigene Beteiligung an der Meldung**

  ➔ **erforderlich: konkrete vertragliche Ausgestaltung**

Wie prüfe ich eine AVV datenschutzrechtlich? Agenda

- **Was muss?**
- **Was soll?**
- **Was kann?**
- **Fragen und Diskussion**

Haftung und Sanktionen

- **Ausgangspunkt**
  - **Häufig zu lesen zur Haftung:** *„Es gilt die Regelung des Art. 82 DS-GVO."*
  - **Anspruch gegen jeden Verantwortlichen und auch direkt gegen Auftragsverarbeiter**

    *„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz **gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.**" (Art. 82 Abs. 1 DS-GVO)*
  - **Gesamtschuldnerische Haftung im Außenverhältnis**

    *„Ist **mehr als ein** Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter **an derselben Verarbeitung** beteiligt und sind sie **gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich**, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter **für den gesamten Schaden**, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist." (Art. 82 Abs. 4 DS-GVO)*
  - **Keine Haftung ohne Verantwortung**

    *„Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass **er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich** ist." (Art. 82 Abs. 3 DS-GVO)*
  - **Auftragsverarbeitung**

    *„Ein **Auftragsverarbeiter** haftet für den durch eine Verarbeitung verursachten Schaden **nur dann, wenn** er **seinen speziell den Auftragsverarbeitern auferlegten Pflichten** aus dieser Verordnung nicht nachgekommen ist oder **unter Nichtbeachtung der rechtmäßig erteilten Anweisungen** des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat." (Art. 82 **Abs. 2** S. 2 DS-GVO)*

➔ **Bedürfnis nach vertraglichen Haftungs- und/oder Freistellungsregelungen?**
➔ **Kompetenzbereich des DSB?**

Wie prüfe ich eine AVV datenschutzrechtlich? Agenda

- **Was muss?**
- **Was soll?**
- **Was kann?**
- **Fragen und Diskussion**

Fragen und Diskussion!

Rechtsanwalt Dr. Jens Eckhardt
Fachanwalt für IT-Recht
Datenschutz-Auditor (TÜV)
Compliance-Officer (TÜV)

Immermann Straße 15
40210 Düsseldorf
Tel.: +49 211 – 17 52 06 60
Fax: +49 211 – 17 52 06 66
eckhardt@derra-d.de
www.derra.eu

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

Rechtsanwalt Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV) und Compliance-Officer (TÜV)

dmp Derra, Meyer & Partner PartG mbB – www.derra.eu – eckhardt@derra-d.de

Seit 2001 berät er bundesweit nationale und internationale Unternehmen zu den Themen Datenschutz, Informationstechnologie, Telekommunikation und Marketing. Die Beratung umfasst die gerichtliche Vertretung, Vertretung gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, die strategische Beratung bei der Einführung neuer Systeme, die Bewertung von bestehenden Systemen, das Outsourcing sowie die Vertragsgestaltung.

Funktionen als

- Dozent zum Datenschutzrecht der udis Ulmer Akademie für Datenschutz und IT-Sicherheit – gemeinnützige Gesellschaft mbH
- Mitglied im Vorstand des Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (Ressort Recht)
- Mitglied im Vorstand von EuroCloud Deutschland_eco e.V. (Ressort Recht)
- Dozent der DeutscheAnwaltAkademie Gesellschaft für Aus- und Fortbildung sowie Serviceleistungen mbH (Fortbildung im Bereich Fachanwalt IT-Recht)
- Lehrbeauftragter der SRH Fernhochschule Riedlingen zum Internet- und Medienrecht und Datenschutz sowie zum im Studiengang Medien und Kommunikation sowie Lehrauftrag zum Datenschutzrecht
- Anhörung durch die Datenschutzaufsichtsbehörden als Fachexperte für Werbung und Adresshandel
- Moderator und Referent verschiedener Datenschutzveranstaltungen und Autor von Fachbeiträgen zum Datenschutz-, IT-, Zivil- und Wettbewerbsrecht und zur Datenschutz-Grundverordnung, - auch zusammen mit Vertreter/innen deutscher Datenschutzaufsichtsbehörden

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

Auswahl der Veröffentlichungen:

- Schwartmann/Jaspers/Eckhardt, Kommentar zum TTDSG. 2022, C.F. Müller Verlag
- TTDSG leicht erklärt, 2021, PrivacyXperts Verlag
- DSGVO-Kompendium, Eckhardt/Kramer/Tausch, 2021, PrivacyXperts Verlag
- Datenverarbeitung in Drittstaaten, Eckhardt/Fuhlert, 2020, PrivacyXperts Verlag
- GDPR Playbook, 2020, eco - Verband der Internetwirtschaft e.V., Autor der Kapitel Cloud Computing und E-Mail-Marketing
- Datenschutz&Marketing – Praxisleitfaden, PrivacyXperts Verlag, 2019, ISBN 978-3-8125-2792-7
- Mit-Autor „Vernetzte und autonome Mobilität", eco Verband der deutschen Internetwirtschaft, 2019
- Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, C.H. Beck München, 2018
- „Wann ist ein Datum ein personenbezogenes Datum?", gemeinsam mit Dr. Brink (Landesbeauftragter für den Datenschutz Baden-Württemberg, ZD Editorial 1/2015 und ZD 2015, 205 ff.
- Leitfaden – Datenschutz und Cloud Computing, Mitautor und Leiter der Taskforce „Datenschutz" der AG „Rechtsrahmen im Cloud Computing", Trusted Cloud-Initiative des BMWi
- Bergmann/Möhrle/Herb, BDSG/DS-GVO , Mit-Autor, Boorberg Verlag
- Recht der elektronischen Medien, Kommentar, Mitautor, C. H. Beck München
- Handbuch IT- und Datenschutzrecht, Mitautor, Verlag C. H. Beck München
- Beck'scher OK, Wolff/Brink, BDSG/DS-GVO , Mit-Autor, C.H. Beck München
- Beck'scher TKG Kommentar, Mitautor, C. H. Beck München
- Big Data im Marketing – Chancen und Möglichkeiten für eine effektive Kundenansprache, 2015, Mitautor, Haufe Gruppe
- Digitalisierung und Transformation im Unternehmen, Mitautor, KS-Energy
- Leitfaden zu Durchsuchung und Beschlagnahme, Herausgeber und Mit-Autor, EuroCloud Deutschland_eco e.V.