BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Praktische Rechtsprobleme der Auftragsdatenverarbeitung

Linux Tag 2012, 23.05.2012

Sebastian Creutz

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

- Schwerpunkte
  - Was ist Auftragsdatenverarbeitung
  - Einführung ins Datenschutzrecht
  - ADV in der EU/EWR
  - ADV in Drittland
  - Praktische
  - Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

1. Was ist Auftragsdatenverarbeitung

1.1 Was ist Auftragsdatenverarbeitung

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

BILD Zeitung am 25.06.2010:

DATENSKANDAL!

Post soll Arbeitslosen-Briefe öffnen

http://www.bild.de/politik/2010/politik/post-soll-arbeitslosen-briefe-oeffnen-13069520.bild.html

(Viel Lärm um nichts: Das ist als Auftragsdatenverarbeitung zulässig.)

1.2 Was ist Auftragsdatenverarbeitung

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

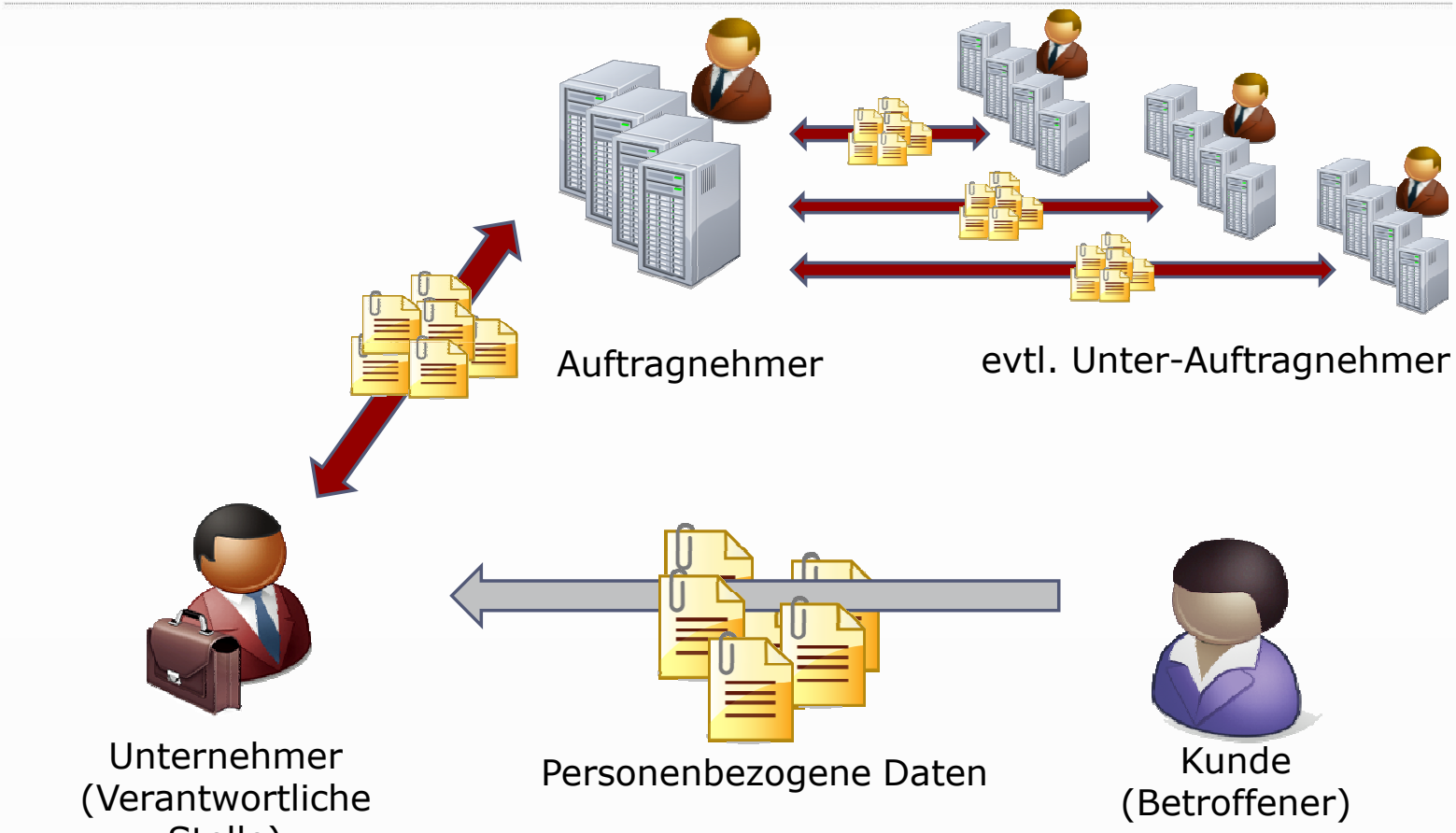
- Gesetzliche Definitionen:
  - § 11 Abs. 1 S. 1 BDSG:

    „Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich."
  - Art. 2 e) Europäische Richtlinie 95/46/EG:

    "Auftragsverarbeiter" (ist) die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

1.3 Was ist Auftragsdatenverarbeitung

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft



1.4 Was ist Auftragsdatenverarbeitung

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Abgrenzung zur Funktionsübertragung: Wenn der Dienstleister voll selbständig agiert und Herr der Daten ist.

Bsp: Möbel Höffner - Deutsche Post Marketing GmbH

ACHTUNG: Er muss die Daten dann auch selbst erheben, sonst gebe ich unbefugt Daten weiter.

1.5 Was ist Auftragsdatenverarbeitung

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

ADV:

➔ Die Datenverarbeitung wird durch einen Anderen in meinem Auftrag vorgenommen.

➔ Ich bleibe verantwortlich !!!

Achtung:

Gilt auch, wenn bei Prüfung oder Wartung von Systemen durch Dritte ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5)

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

2. Einführung ins Datenschutzrecht

2.1 Einführung ins Datenschutzrecht

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Geschichte des Datenschutzes:

- 1970 – Hessisches Landesdatenschutzgesetz
- 1977 – Bundesdatenschutzgesetz
- 1983 – Volkszählungsurteil
- 1995 – EU Richtlinie
- 2001 – Datenschutznovelle zur Umsetzung der Richtlinie
- 2009 – Verschärfungen des BDSG, insbesondere zur Auftragsdatenverarbeitung

2.2 Einführung ins Datenschutzrecht

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Datenschutz in Deutschland, Europa und der Welt:

- Deutschland: BDSG (strenge Umsetzung der RiL)
- EU/EWR (EU + NO, IS, LI): Datenschutzrichtlinie
- CH und andere Länder*: eigene Gesetze mit gleichem Schutzniveau
- USA: kein Datenschutzrecht, aber mit Safe Harbour gleiches Schutzniveau möglich
- ROW: kein ausreichender Datenschutz

* Argentinien, Australien, Guernsay, Isle of Man, Jersey, Canada

2.3 Einführung ins Datenschutzrecht

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Was ist geschützt?

- Personenbezogene Daten, § 3 Abs. 1 BDSG:

  Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
- Bestimmbarkeit genügt, nach Auffassung der Datenschutzbehörden auch, wenn nur für Dritten bestimmbar (IP Adressen!)

2.4 Einführung ins Datenschutzrecht

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Welches Recht gilt?

- Innerhalb der EU/EWR: Sitzprinzip:

  Wenn Sitz innerhalb der EU/des EWR, dann gilt Recht des Sitzes, nicht deutsches Recht.
- Ansonsten (bei sog. Drittländern): Territorialprinzip:

  Es gilt deutsches Recht, wenn in Deutschland Daten erhoben, verarbeitet oder genutzt werden.

  Entscheidend: Werden deutsche Nutzer angesprochen?

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

3. ADV in der EU/EWR

3.1 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Relevante Normen:

- § 11 BDSG: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
- § 9 BDSG: Technische und organisatorische Maßnahmen
- Anlage zu § 9 BDSG

3.2 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Anforderungen vor und nach Vertragsschluss, § 11 Abs. 2 S. 4 BDSG:

- Umfassende Prüfpflicht vor Vertrag (nicht zwingend vor Ort)
- Umfassende Prüfpflicht während Vertrag
- Dokumentationspflicht

3.3 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Anforderungen des § 11 BDSG an den Vertrag:

- Schriftform: auf Papier mit Unterschrift
- Ziff. 1: Was wird gemacht und wie lange?
- Ziff. 2: Von wem werden welche Daten warum und wie erhoben, verarbeitet oder genutzt?
- Ziff. 3: Was ist technisch und organisatorisch zum Schutz der Daten zu unternehmen? dazu sogleich
- Ziff. 4: Wie wird sichergestellt, dass die Rechte auf Berichtigung, Löschung und Sperrung von Daten (§ 20) umgesetzt werden?

3.4 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Anforderungen des § 11 BDSG an den Vertrag:

- Ziff. 5: Pflichten des Auftragnehmers:
  - Bestellung Datenschutzbeauftragter
  - Verpflichtung aller Mitarbeiter auf Datengeheimnis (§ 5)
  - Information bei behördlicher Kontrolle
  - Prüfungen des Auftragnehmers
- Nr. 6: Dürfen Subunternehmer eingeschaltet werden?
- Ziff. 7: Wie kontrolliert der Auftraggeber?
- Ziff. 8: Bei Verstößen ist der Auftraggeber zu informieren

3.5 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Anforderungen des § 11 BDSG an den Vertrag:

- Ziff. 9: Wie erteilt der Auftraggeber Weisungen zur ADV, wie muss der Auftragnehmer mit Weisungen umgehen?
- Ziff. 10: Was passiert nach Vertragsende mit den Daten? Löschung oder Rückgabe?

3.6 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

§ 9, technisch-organisatorische Maßnahmen:

- Zutrittskontrolle: Wie wird sichergestellt, dass kein Unbefugter räumlichen Zutritt zum System hat?
- Zugangskontrolle: Wie wird sichergestellt, dass kein Unbefugter System nutzen kann?
- Zugriffskontrolle: Wie wird sichergestellt, dass Berechtigte ausschließlich im Rahmen ihrer Berechtigung agieren?
- Weitergabekontrolle: Wie wird sichergestellt, dass Daten bei Transport nicht unbefugt genutzt usw. werden?

3.7 ADV in der EU/EWR

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

§ 9, technisch-organisatorische Maßnahmen:

- Eingabekontrolle: Wie wird sichergestellt, dass Änderungen nachträglich geprüft werden können?
- Auftragskontrolle: Wie wird sichergestellt, dass Daten nur im Rahmen des Auftrags verarbeitet werden?
- Verfügbarkeitskontrolle: Wie wird sichergestellt, dass Daten nicht zufällig zerstört werden?
- Trennungskontrolle: Wie wird sichergestellt, dass Daten mit verschiedenem Zweck getrennt verarbeitet werden?

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

4. ADV in Drittland

4.1 ADV in Drittland

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Relevante Normen:

- § 4 b: Übermittlung personenbezogener Daten ins Ausland
- § 3 Abs. 4 und 8: Definitionen

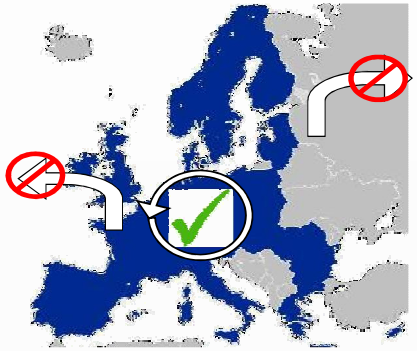
4.2 ADV in Drittland

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

§ 11 BDSG gilt nicht, denn:

- § 3 Abs. 8: Dienstleister im Drittland ist Dritter
- Übermittlung an Dritte im Drittland nur nach Interessenabwägung nach § 4 b Abs. 2 und 3

➔ Fazit?!: ADV in Drittland unmöglich?!



4.3 ADV in Drittland

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

EU-Standardvertragsklauseln:

- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:01:DE:HTML
- Ermöglichen ADV auch im Drittstaat
- Datenschutzbehörden: Regelungen des § 11 Abs. 2 zusätzlich zu vereinbaren.

4.4 ADV in Drittland

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Sondersituation USA:

- Safe Harbour: http://export.gov/safeharbor/
- Freiwillige Selbstzertifizierung durch US-Dienstleister
- ABER: Keine flächendeckende Kontrolle

➔ Prüfpflichten des Auftraggebers vor Datenübermittlung

➔ Auch wenn § 11 nicht gilt, muss Entsprechendes schriftlich vereinbart werden.

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

5. Praktische Relevanz

5.1 Praktische Relevanz

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Als Auftraggeber (Kunde):

- Prüfpflicht VOR Vertragsschluss über T-O-M
- SCHRIFTLICHER Vertrag, d.h. auf Papier mit Unterschrift (126 BGB) oder qualifizierte elektronische Signatur
- Vertrag muss Maßgaben nach § 11 Abs. 2 regeln
- Regelmäßige Prüfpflicht über T-O-M

5.2 Praktische Relevanz

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Als Auftragnehmer (Dienstleister):

- In erster Linie ist AG verantwortlich.
- ABER: mehr und mehr AG verlangen ADV-Vereinbarung

➔ Folgen:

- Möglicher Wettbewerbsvorteil
- Verträge standardisieren, Verhandlungen reduzieren
- Prüfpflichten des AG durch Zertifizierung lösen
- Mit eigenen Subunternehmern schriftlich ADV vereinbaren

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

6. Praktische Anwendungsfälle

6.1 Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Host Provider, insbesondere Cloud Computing:

- Wo stehen die Server? In EU/EWR oder Drittland? Je nachdem § 11 BDSG oder Standardvertragsklauseln
- Problem USA: Patriot Act, Anbieter behalten sich Weitergabe vor ➔ Keine zulässige ADV?

6.2 Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Google Analytics/ IVW, generell Trafficmeasurement:

- Langer Streit zwischen Google und Datenschutzbehörde
- IP-Adressen sind nach Auffassung der Datenschützer personenbezogen
- Google verarbeitete und speicherte IP in USA
- Lösung:
  - Anonymisierung der IP auf EU-Servern, erst dann Transfer
  - ADV-Vereinbarung: http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.de/de/de/intl/de/analytics/tos.pdf

6.3 Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Wartung und Service:

- § 11 Abs. 5 BDSG
- Im Einzelfall sind T-O-M anzupassen und AG kann ggf. Maßnahmen übernehmen

6.4 Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Freelancer:

- Wenn Arbeit mit anderen als vom Auftraggeber gestellten Einrichtungen.
- Nicht bei Telearbeit von festen Arbeitnehmern.

6.5 Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Callcenter, Kundenbetreuung:

- Nicht Marktforschung ohne feste Vorgaben

6.6 Praktische Anwendungsfälle

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Innerhalb von Konzernen:

- Bei Weitergabe eines Konzernunternehmens an anderes ADV
- Auch bei rechtlich selbständiger IT Abteilung
- Hier Binding Corporate Rules möglich:
  http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm#

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft

Sebastian Creutz
Rechtsanwalt

BARTELS KIM WOLLENHAUPT
Rechtsanwälte Partnerschaft
Invalidenstr. 115, 10115 Berlin
creutz@allmedialaw.de
www.allmedialaw.de

[ALLITLAW]
[ALLIPLAW]
[ALLMEDIALAW]