IT-Outsourcing aus der Perspektive einer bDSB

Bettina Robrecht
Datenschutzbeauftragte
17. März 2012

schufa

Agenda

I. Überblick: Definitionen und anwendbares Recht
II. Outsourcing innerhalb der EU/EWR
III. Outsourcing außerhalb der EU/EWR
IV. Pflichten des auslagernden Unternehmens
V. Arbeitshilfen
VI. Ausblick
VII. Fazit

I. Überblick: Definitionen und anwendbares Recht (1)

- Verantwortliche Stelle (§ 3 Abs. 7 BDSG): jede Person oder Stelle, die personenbezogene (pb) Daten für sich selbst erhebt, verarbeitet oder nutzt (kein Konzernprivileg)

- Empfänger (§ 3 Abs. 8 Satz 1 BDSG): jede Person oder Stelle, die pb Daten erhält

- Dritter (§ 3 Abs. 8 Satz 2 BDSG): jeder außerhalb der verantwortlichen Stelle,
  aber: nicht der Betroffene und nicht Stellen, die im Inland oder EU/EWR pb Daten im Auftrag erheben, verarbeiten oder nutzen
  also: Stellen außerhalb der EU/EWR, die pb Daten im Auftrag erheben, verarbeiten oder nutzen, sind danach Dritte

- EWR: EU plus Norwegen, Island und Liechtenstein, die die Datenschutzrichtlinie übernommen haben

I. Überblick: Definitionen und anwendbares Recht (2)

Ermittlung des anwendbaren Rechts bei internationalem Kontext:

§ 1 Abs. 5 BDSG in Umsetzung von Art. 4 Abs. 1 der EU-Datenschutzrichtlinie 95/46/EG

Satz 1: BDSG findet keine Anwendung, sofern eine in einem anderen EU/EWR-Staat belegene Stelle pb Daten in Deutschland (D) erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung in D

Satz 2: BDSG findet Anwendung, sofern eine Stelle außerhalb der EU/EWR pb Daten im Inland erhebt, verarbeitet oder nutzt

Satz 4: Ausnahme: reiner Transit

Satz 5: § 38 Abs. 1 Satz 1 BDSG (Aufsicht) bleibt unberührt, d. h. ungeachtet des anwendbares Rechts bleibt die Zuständigkeit der Aufsichtsbehörden unberührt

Agenda

I. Überblick: Definitionen und anwendbares Recht

II. Outsourcing innerhalb der EU/EWR

III. Outsourcing außerhalb der EU/EWR

IV. Pflichten des auslagernden Unternehmens

V. Arbeitshilfen

VI. Ausblick

VII. Fazit

II. Outsourcing innerhalb D/EU/EWR

Abgrenzung zwischen Funktionsübertragung oder Auftragsdatenverarbeitung
→ entscheidend Art und Umfang der Datenverarbeitung

- Auftragsdatenverarbeitung: Weisungsgebundenheit, Auslagerung von Hilfsfunktionen
- Funktionsübertragung: Entscheidungsbefugnis des AN, weitergehendes Eigeninteresse des AN, Erfüllung eigener Geschäftszwecke

Wenn ADV, dann erhöhte Anforderung an Vertragsgestaltung nach § 11 Abs. 2 BDSG

- § 11 Abs. 2 BDSG geändert durch BDSG-Novelle II: „zehn-Punkte-Katalog“
- neben vertraglichen Anforderungen Pflicht zur Überprüfung der TOM durch Auftraggeber vor Aufnahme der DV und dann regelmäßig
- Bußgeldbewehrung (§ 43 Abs. Abs. 1 Nr. 2b BDSG)
- Anpassung von Altverträgen: nach h. M. wohl erforderlich,

II. Outsourcing innerhalb D/EU/EWR

Wenn Funktionsübertragung, dann AN = Dritter nach § 3 Abs. 8 Satz 2 BDSG,

- Übermittlungsvoraussetzungen (insb. §§ 28, 32 BDSG) zu prüfen
- Transparenzvorschriften beachten (Information des Betroffenen, §§ 4 Abs. 3, 33 BDSG)
- anwendbares Recht nach § 1 Abs. 5 BDSG zu ermitteln
- Auftragnehmer wird selbst verantwortliche Stelle gegenüber dem Betroffenen

→ Abgrenzung schwierig, frühzeitige Einbindung von Rechtsabteilung und Datenschutz

Agenda

I. Überblick: Definitionen und anwendbares Recht
II. Outsourcing innerhalb der EU/EWR
III. Outsourcing außerhalb der EU/EWR
IV. Pflichten des auslagernden Unternehmens
V. Arbeitshilfen
VI. Ausblick
VII. Fazit

III. Outsourcing außerhalb EU/EWR (1)

- Außerhalb EU/EWR greift Privilegierung der ADV nicht (§ 3 Abs. 8 Satz 2 BDSG) d.h. AN ist Dritter (auch ausländische Konzernunternehmen)

- Zweistufige Zulässigkeitsprüfung
    a) Übermittlungsvoraussetzungen, insb. § 28 BDSG (§ 4b Abs. 1 BDSG) (bei Mitarbeiterdaten zusätzlich § 32 BDSG)
    b) Voraussetzungen des Drittlandtransfers, §§ 4b Abs. 2 Satz 2, 4c BDSG

- § 4b Abs. 2 Satz 2 BDSG:
    a) ausreichendes Datenschutzniveau gewährleistet?
    b) Angemessenheit zu bestimmen nach § 4b Abs. 3 BDSG
    c) durch EU-Kommission anerkannt: Argentinien, Australien, Guernsey, Isle of Man, Jersey, Kanada, Schweiz
    d) USA: Safe Harbor-Abkommen (unternehmensspezifisch)

III. Outsourcing außerhalb EU/EWR (2)

Zulässigkeit nach § 4c BDSG:

Abs. 1 i.d.R. bei Outsourcing-Projekten nicht einschlägig/nicht praktikabel

- Einwilligung des Betroffenen, Vertragserfüllung, lebenswichtige Interessen etc.

einschlägig Abs. 2

- Genehmigung der Aufsichtsbehörden, wenn die verantwortliche Stelle ausreichende Garantien zum Schutz des Persönlichkeitsrechts vorweist; ausreichende Garantien können sich entweder aus Vertrag oder verbindliche Unternehmensregelungen ergeben

III. Outsourcing außerhalb EU/EWR (3)

Ausreichende Garantien aus Vertrag = Standardvertragsklauseln (SVK)

1. „Controller to Controller“

a) SVK vom 15.6.2001

b) ergänzt durch „Alternative SVK“ vom 27.12.2004

→ Wahlrecht zwischen beiden SVK,

→ allerdings Alternative SVK nach Ansicht der AB nicht für den Datentransfer für Beschäftigtendaten geeignet

III. Outsourcing außerhalb EU/EWR (4)

Fortsetzung Standardvertragsklauseln

2. „Controller to Processor“ (entspricht Auftragsdatenverarbeitung)

a) SVK vom 27.12.2001

- Schwäche: keine Regelungen zu Unteraufträgen

b) abgelöst durch Neue SVK vom 5.2.2010

- insb. Regelungen für Unteraufträge
- allerdings mit Anforderungen, die über § 11 BDSG hinausgehen

→ kein Wahlrecht

→ Anpassung von Altverträgen, wenn Änderungen an der DV erfolgen oder der Datenimporteur Unteraufträge erteilt

Bei Verwendung der unveränderten SVK = Genehmigung der Datenübermittlung durch AB („Ermessensreduzierung auf Null“)

Bei Änderungen der SVK = Genehmigungserfordernis durch die AB

III. Outsourcing außerhalb EU/EWR (5)

Ausreichende Garantien:

2. Verbindliche Unternehmensregeln (Binding Corporate Rules, BCR)

a) anwendbar nur innerhalb eines Konzerns

b) anders als bei Vertragsklauseln keine Standardverträge, d. h. in jedem Fall Genehmigungserfordernis (Zeit einplanen!)

c) aber Hilfestellung in Form von WP der Artikel-29-Gruppe (WP 74, 108 und 154)

Agenda

I. Überblick: Definitionen und anwendbares Recht
II. Outsourcing innerhalb der EU/EWR
III. Outsourcing außerhalb der EU/EWR
IV. Pflichten des auslagernden Unternehmens
V. Arbeitshilfen
VI. Ausblick
VII. Fazit

IV. Pflichten des auslagernden Unternehmens

insb. nach § 11 Abs. 2 BDSG, aber im Grunde übertragbar

Sorgfältige Auswahl -> frühzeitige Einbindung des bDSB

Prüfung der Einhaltung der technisch-organisatorischen Maßnahmen beim AN

- Initial vor Aufnahme der DV
- Form nicht vorgeschrieben
- Dokumentenbasiert: Zertifikate (ISO 27001 etc.) oder
- Vorort-Audit

- Danach regelmäßige Folgeaudits
- Intervall nach Kritikalität (analog Revisionsprüfungen)

IV. Pflichten des auslagernden Unternehmens

Sonderfall „Cloud Computing“

- Was für eine Cloud? (Public/Private/Hybrid)
- Welche(r) Anbieter? (Inland/Ausland/Drittland)
- Wo sind meine Daten? (wo und wen und wann prüfe ich?)

Agenda

I. Überblick: Definitionen und anwendbares Recht
II. Outsourcing innerhalb der EU/EWR
III. Outsourcing außerhalb der EU/EWR
IV. Pflichten des auslagernden Unternehmens
V. Arbeitshilfen
VI. Ausblick
VII. Fazit

V. Arbeitshilfen

Arbeitshilfen der Aufsichtsbehörden zu den SVK

- Working Paper der Artikel 29-Gruppe (insb. WP 161, 176, 179)

- „Handreichung des Düsseldorfer Kreises zur Internationalen Auftragsdatenverarbeitung“ (Beschluss vom 19./20.4.2007), allerdings noch bezogen auf die alten SVK (dagegen: Stellungnahme der BITKOM vom 22.4.2008)

- „Datenschutzkonforme Gestaltung und Nutzung von Cloud Computing“ (Entschließung der 82. Konferenz der Datenschutzbeauftragtes des Bundes und der Länder vom 28./29.9.2011)

Agenda

I. Überblick: Definitionen und anwendbares Recht
II. Outsourcing innerhalb der EU/EWR
III. Outsourcing außerhalb der EU/EWR
IV. Pflichten des auslagernden Unternehmens
V. Arbeitshilfen
VI. Ausblick
VII. Fazit

VI. Ausblick

Entwurf der EU-Datenschutzgrundverordnung vom 25.1.2012 (1)

Datenschutz und Datensicherheit als Teil der Unternehmensstrategie

Art. 20 „Strategien und Maßnahmen“ die sicherstellen, dass pb Daten im Einklang mit der VO verarbeitet werden

Art. 30 Datensicherheit

Art. 31 Meldepflichten bei Verletzung des Schutzes pb Daten

Art. 33 Datenschutz-Folgenabschätzung

Art. 34 Vorherige Genehmigung und Zurateziehung der Aufsichtsbehörde

VI. Ausblick

Entwurf der EU-Datenschutzgrundverordnung (2)

Übermittlung in Drittländer nach wie vor nur unter engen Voraussetzungen (Art. 40 ff)

Art. 41 Angemessenheitsentscheidung

Art. 42 Datenübermittlung aufgrund geeigneter Garantien

Art. 43 Datenübermittlung aufgrund verbindlicher Unternehmensrichtlinien

Art. 44 Ausnahmen (Einwilligung etc.)

VI. Ausblick

Entwurf der EU-Datenschutzgrundverordnung (3)

Zuständigkeit der Aufsichtsbehörde (Art. 46 ff.)

Art. 51 Zuständigkeit bei internationalem Kontext (Sitz der Hauptniederlassung)

Art. 53 Befugnis, Datenverarbeitung vorübergehend oder dauerhaft zu verbieten oder Drittlandtransfer zu untersagen

Art. 55 ff: Zusammenarbeit und Kohärenz

Agenda

I. Überblick: Definitionen und anwendbares Recht
II. Outsourcing innerhalb der EU/EWR
III. Outsourcing außerhalb der EU/EWR
IV. Pflichten des auslagernden Unternehmens
V. Arbeitshilfen
VI. Ausblick
VII. Fazit

VII. Fazit

- kein Königsweg für internationale Outsourcing-Projekte
- Wirtschaftliche Vorteile sind gegen rechtliche Risiken abzuwägen
- neben der materiellrechtlichen Zulässigkeit Schwerpunkt Datensicherheit (technisch-organisatorische Maßnahmen)
- Herausforderungen bei der Prüfung der Partners
- Zusätzliche Dynamik durch Cloud Computing
- Keine Abhilfe durch EU-Datenschutz-Grundverordnung in Sicht

… noch Fragen?