BlnBDI
Gardain

28. März 2007

22421.18.16

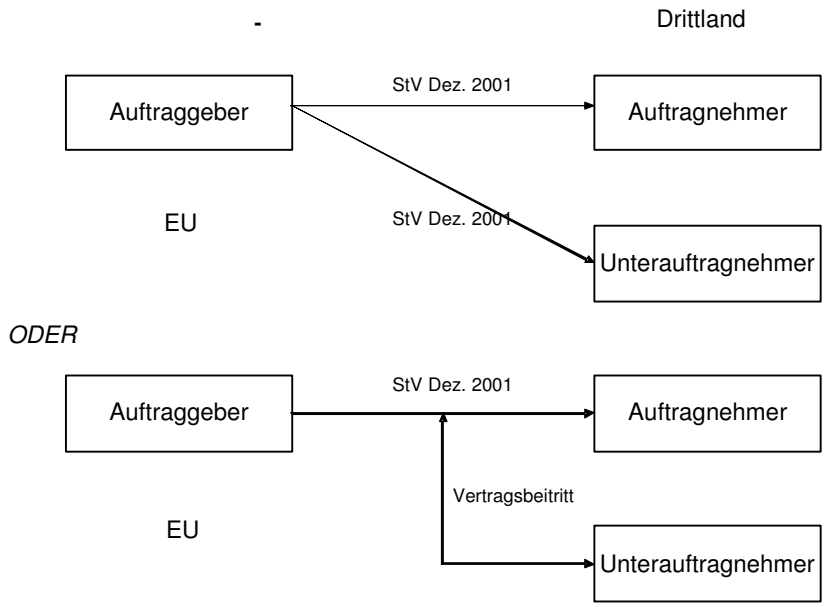
Fallgruppen zur internationalen Auftragsdatenverarbeitung

Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung

Einleitung

Die folgende Darstellung beinhaltet die häufigsten Fallkonstellationen der internationalen Auftragsdatenverarbeitung und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Alle Grafiken stammen vom Regierungspräsidium Darmstadt, Dezernat Datenschutz.

Fallgruppe A



Regierungspräsidium Darmstadt, Dezernat Datenschutz

Konstellation:

Der Auftraggeber ist in der EU/EWR ansässig, während der Auftragnehmer und der von ihm beauftragte Unterauftragnehmer im Drittland ansässig sind.

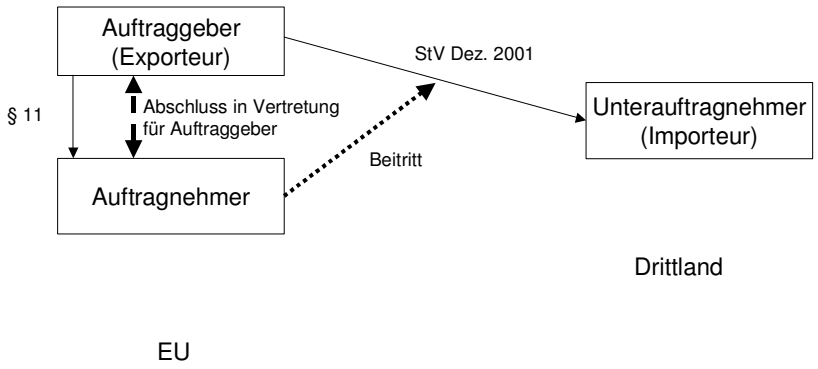
Besonderheit:

Die Pflichten des Auftragnehmers sind an den Unterauftragnehmer "weiterzuleiten".

Bewertung:

Der Auftraggeber hat einen weiteren "Drittstaatenvertrag" mit dem Unterauftragnehmer zu schließen, oder der Unterauftragnehmer muss dem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer beitreten.

Fallgruppe B



Konstellation:

Der Auftraggeber und der Auftragnehmer sind in der EU/EWR ansässig. Es wird ein Unterauftragnehmer im Drittland eingeschaltet, der die Daten vom Auftragnehmer erhält.

Besonderheit:

Der Abschluss eines Standardvertrags zwischen Auftragnehmer in der EU/EWR und dem Unterauftragnehmer im Drittland ist nicht sachgerecht, weil der Auftragnehmer (anders als der Datenexporteur in den Standardverträgen) nicht verantwortliche Stelle ist. Der Auftragnehmer hat dann selbst keine vertraglichen Rechte oder Pflichten.

Bewertung:

Der Auftraggeber ist als Datenexporteur i.S.d. §§ 4b, 4c einzustufen, der Unterauftragnehmer als Datenimporteur. Beide müssen daher Vertragsparteien des Standardvertrages vom Dez. 2001 sein. Ein Beitritt des Auftragnehmers in der EU/EWR zum Vertrag ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

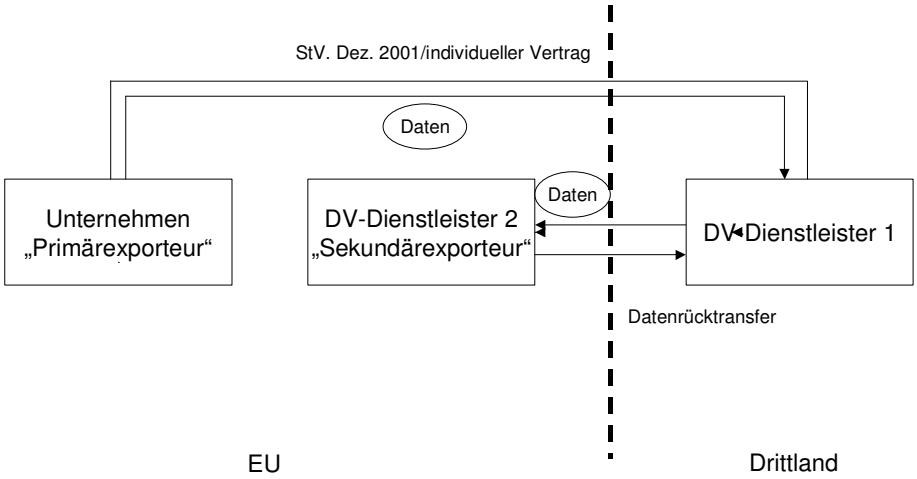
Erläuterung der Bewertung zur Fallgruppe B:

Da u.U. wegen der möglichen Vielzahl von Auftraggebern entsprechend viele Standardverträge mit den Unterauftragnehmern abgeschlossen werden müssten, ist es praktikabel und akzeptierbar, dass der Auftragnehmer im Auftrag (oder besser: in Vertretung) der Auftraggeber einen Standardvertrag (Auftragsdatenverarbeitung) mit dem Unterauftragnehmer abschließt. Dass auch der EU/EWR-Auftragnehmer dem Vertrag zwischen Auftraggeber und Drittstaaten-Unterauftragnehmer beitritt, ist jedenfalls sinnvoll. Bei einem Beitritt besteht keine Genehmigungspflicht nach § 4 c Abs. 2 BDSG, und zwar unabhängig davon, ob er durch eine gesonderte Vereinbarung erfolgt oder als Vertragsergänzung in den "Drittstaatenvertrag" integriert wird.

Folgender Text kann für einen derartigen Beitritt verwendet werden:

"Die vorstehenden Regelungen gelten mit folgender Maßgabe auch für den DV-Dienstleister in Europa [Name, Sitz], der insoweit dem Vertrag beitritt. Da der Datenexporteur einen Datenverarbeitungsdienstleistungsvertrag mit [Name des DV-Dienstleisters in Europa] geschlossen hat (als Auftragsdatenverarbeitung gemäß § 11 BDSG / Art. 2e, 17 Abs. 3 EG-Datenschutzrichtlinie 95/46/EG und den hierzu erlassenen nationalen Vorschriften) und der Datenimporteur als "Unterauftragnehmer" (oder: Subunternehmer) für [Name des DV-Dienstleisters in Europa] fungiert, ist der/die [Name des DV-Dienstleisters in Europa] gegenüber dem Datenexporteur primär verantwortlich, dass der Datenimporteur die Pflichten gemäß diesem Vertrag erfüllt. Der [Name des DV-Dienstleisters in Europa] hat zu diesem Zweck entsprechende abgeleitete Kontrollpflichten gegenüber dem Datenimporteur und kann hierfür die in diesem Vertrag beschriebenen Kontrollbefugnisse des Datenexporteurs wahrnehmen. Dieser bleibt verpflichtet, die Ausübung der Kontrollbefugnisse zu überwachen, und kann jederzeit auch selbst diese Kontrolle gegenüber dem Unterauftragnehmer ausüben."

Fallgruppe C



Konstellation:

Ein in der EU/EWR ansässiges Unternehmen beauftragt einen im Drittstaat ansässigen DV-Dienstleister mit der Verarbeitung personenbezogener Daten und schließt mit diesem den Standardvertrag vom Dezember 2001 (Controller - Processor) oder einen entsprechenden individuellen Vertrag. Der DV-Dienstleister im Drittstaat schaltet einen DV-Dienstleister in der EU/EWR ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat (rück-) transferiert.

Besonderheit:

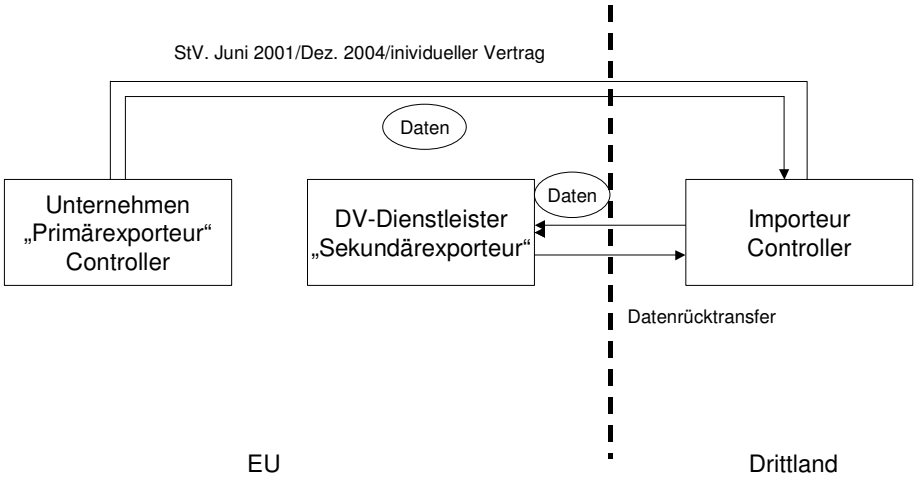
Der Dienstleister in der EU (DV-Dienstleister 2) erhält Daten vom DV-Dienstleister im Drittland (DV-Dienstleister 1). Ein Vertrag besteht nur zwischen dem Unternehmen und dem DV-Dienstleister 1.

Bewertung:

Es besteht keine Notwendigkeit einer eigenständigen vertraglichen Regelung nach § 4 c Abs. 2 BDSG zwischen dem EU-/EWR-Dienstleister und dem Drittland-Unternehmen. Ein Beitritt des EU-/EWR-Dienstleisters zum "Drittstaatenvertrag" ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

Fallgruppe D



Konstellation:

Ein in der EU/EWR ansässiges Unternehmen übermittelt Daten an ein Unternehmen im Drittstaat und schließt mit diesem den Standardvertrag vom Juni 2001 oder Dezember 2004 (Controller - Controller) oder einen entsprechenden, individuellen Vertrag. Das Unternehmen im Drittstaat schaltet einen DV-Dienstleister in der EU/EWR ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat (rück-)transferiert.

Besonderheit:

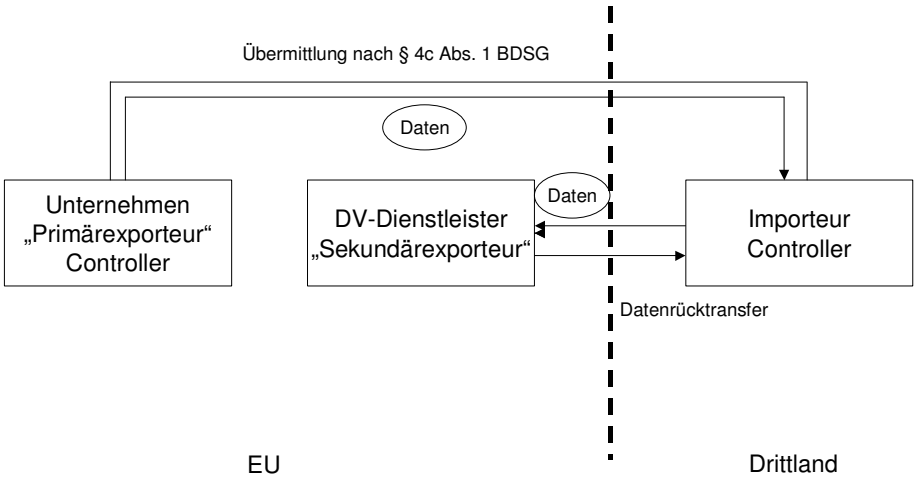
Es besteht nur ein Vertragsverhältnis zwischen dem Controller in der EU und dem Controller im Drittland.

Bewertung:

Es besteht (wie bei Fallgruppe C) keine Notwendigkeit einer eigenständigen vertraglichen Regelung nach § 4c Abs. 2 BDSG zwischen dem EU-/EWR-Dienstleister und dem Drittlandunternehmen. Ein Beitritt zum "Drittstaatenvertrag" ist jedenfalls sinnvoll.

Näheres hierzu: s. Erläuterungen.

Fallgruppe E



Konstellation:

Wie in Fallgruppe D, aber zwischen dem in der EU/EWR ansässigen Unternehmen und dem Unternehmen im Drittstaat wird kein "Drittstaaten-Vertrag" gemäß § 4c Abs. 2 BDSG abgeschlossen, weil eine der Katalogausnahmen des § 4c Abs. 1 BDSG gegeben ist.

Besonderheit:

Es besteht nur ein Vertragsverhältnis zwischen dem Controller in der EU und dem Controller im Drittland.

Bewertung:

Es besteht (wie bei Fallgruppen C und D) keine Notwendigkeit einer eigenständigen vertraglichen Regelung zwischen dem EU-/EWR-Dienstleister und dem Drittlandunternehmen.

Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zu den Fallgruppen C, D und E:

Die Fallgruppen C, D und E sind dadurch gekennzeichnet, dass die Daten von einer verantwortlichen Stelle, die quasi der "Primär-Exporteur" ist, in ein Drittland transferiert und hierbei die Voraussetzungen des § 4c BDSG erfüllt wurden.

Der DV-Dienstleister in der EU/EWR ist quasi der "Sekundär-Exporteur". Ungeachtet der grundsätzlichen Frage, inwieweit EU/EWR-Auftragnehmer überhaupt verantwortlich sind für das Vorliegen der Voraussetzungen der §§ 4b, 4c BDSG (s. hierzu Näheres zu den Fallgruppen F bis I), ist jedenfalls in den Fallgruppen C, D und E keine eigenständige vertragliche Regelung im Sinne des § 4c Abs. 2 BDSG zwischen dem EU/EWR-Dienstleister und dem Drittstaaten-Unternehmen erforderlich.

Offensichtlich ist dies bei der **Fallgruppe C**, bei der sich der eigentliche Auftraggeber in der EU/EWR befindet. Da Zweck und Umfang der zulässigen Datenverarbeitung, die einzuhaltenden Datensicherheitsmaßnahmen etc. bereits in dem Vertrag zwischen dem EU/EWR-Auftraggeber und dem Drittstaaten-Auftragnehmer geregelt sind, besteht weder ein Erfordernis noch ein Spielraum für den EU/EWR-Unterauftragnehmer für eigenständige Vorgaben gegenüber dem Drittstaatenunternehmen bzgl. der dortigen Datenverarbeitung.

Würde man einen individuellen -genehmigungsbedürftigen- Vertrag mit dem EU/EWR-Unterauftragnehmer für erforderlich halten (die Standardverträge passen hier nicht), dann würde dies sogar die Gefahr bergen, dass Regelungen getroffen werden, die dem Vertrag zwischen dem EU-Auftraggeber und dem Drittstaaten-Unternehmen widersprechen.

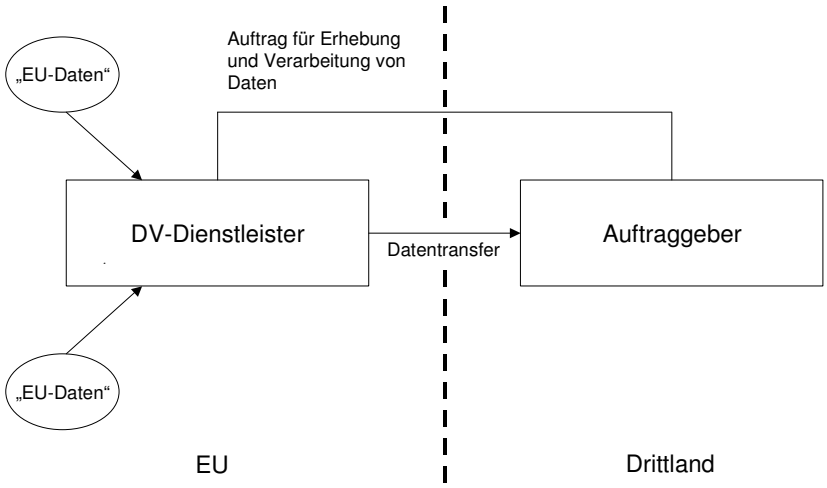
Gleiches gilt für die **Fallgruppe D**. Wenngleich sich hier - im Unterschied zu C - der "Auftraggeber" im Drittstaat befindet, wurden doch auch hier bereits umfassende Regelungen zur Gewährleistung ausreichender Datenschutzgarantien im Drittstaat getroffen, sodass für den EU/EWR-Auftragnehmer kein Erfordernis und kein Spielraum für eigene Vorgaben bestehen. Ein Beitritt des EU/EWR-Auftragnehmers zu dem Vertrag zwischen dem "Primär-Datenexporteur" und dem Datenimporteur ist in den Fallgruppen C und D sinnvoll. Wenn kein DV-Dienstleistungsvertrag existiert, der den Vorgaben des § 11 BDSG entspricht, kann diese Lücke durch Beitritt zum Vertrag geschlossen werden.

In der **Fallgruppe E** besteht zwar kein Vertrag zwischen dem "Primär-Datenexporteur" und dem Datenimporteur zur Gewährleistung ausreichender Datenschutzgarantien (ein Beitritt

scheidet daher aus), allerdings wäre es nicht gerechtfertigt, an den "Sekundär-Datenexporteur" strengere Anforderungen zu stellen als an den "Primär-Datenexporteur".

Der Abschluss eines -genehmigungsbedürftigen- Vertrags im Sinnes des § 4c Abs. 2 BDSG zwischen EU-Auftragnehmer und Drittstaatenunternehmen ist auch in der Fallgruppe E nicht erforderlich.

Fallgruppe F



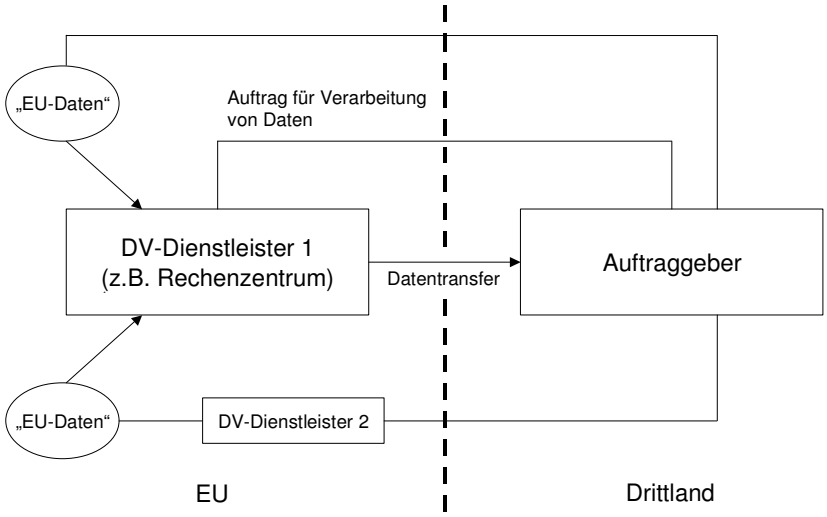
Konstellation:
Ein in der EU/EWR ansässiger DV-Dienstleister wird von einem in einem Drittland ansässigen Unternehmen beauftragt, in der EU/EWR personenbezogene Daten zu erheben und zu verarbeiten und dann an den Auftraggeber im Drittstaat zu transferieren.

Besonderheit:
Der Auftraggeber im Drittland beauftragt den DV-Dienstleister in der EU/EWR auch zusätzlich mit Datenerhebungen in der EU/EWR. Der DV-Dienstleister bleibt zwar auch Datenverarbeiter, kennt die Daten aber selbst (im Unterschied zur Fallgruppe G).

Bewertung:
Der DV-Dienstleister ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 i.V.m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. U.U. trifft ihn aber eine "Remonstrationspflicht". Bezüglich der selbst erhobenen Daten muss er eine summarische Plausibilitätsprüfung vornehmen.

Näheres hierzu: s. Erläuterungen.

Fallgruppe G



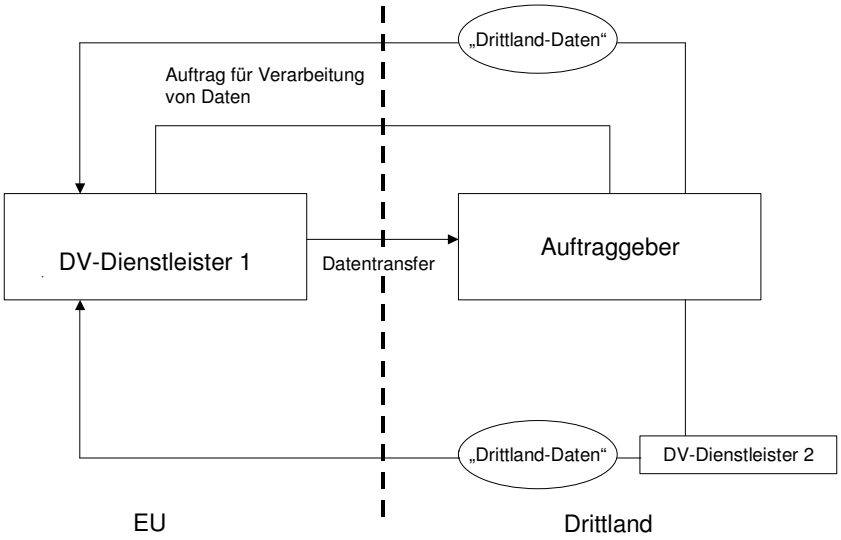
Konstellation:
Ein in der EU/EWR ansässiger DV-Dienstleister 1 wird von einem in einem Drittland ansässigen Unternehmen beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber zu transferieren. Die Daten stammen aus der EU/ dem EWR. Sie wurden hier entweder vom Auftraggeber selbst oder in dessen Auftrag von einem DV-Dienstleister 2 erhoben.

Besonderheit:
Die Daten für den DV-Dienstleister 1 in der EU/EWR kommen vom Auftraggeber aus dem Drittland sowie vom europäischen DV-Dienstleister 2.

Bewertung:
Der DV-Dienstleister 1 ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 i.V.m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister 1 hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. U.U. trifft ihn aber eine "Remonstrationspflicht".

Näheres hierzu: s. Erläuterungen.

Fallgruppe H



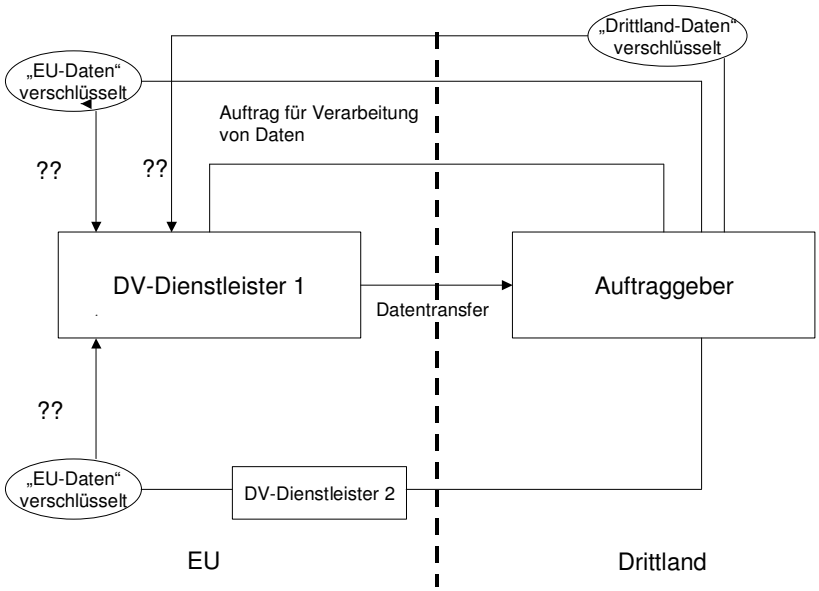
Konstellation:
wie Fallgruppe G, aber die Daten stammen nicht aus der EU/EWR, sondern aus dem Drittland. Sie werden in der EU/EWR nur verarbeitet und dann zurückübermittelt.

Besonderheit:
Die aus dem Drittland stammenden Daten wurden nach dortigem Recht zulässig erhoben. Nach deutschem Recht wäre die Erhebung unzulässig gewesen.

Bewertung:
Der DV-Dienstleister ist für die von ihm durchgeführte Datenverarbeitung verantwortlich (§ 11 i.V.m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie). Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich. Er ist Adressat der übrigen Vorschriften des BDSG. Der DV-Dienstleister hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. U.U. trifft ihn aber eine "Remonstrationspflicht".

Näheres hierzu: s. Erläuterungen.

Fallgruppe I



Konstellation:

Wie Fallgruppe G oder H, aber der EU/EWR-Dienstleister erhält die Daten in verschlüsselter Form und kann von dem Inhalt keine Kenntnis nehmen.

Besonderheit:

Der DV-Dienstleister in der EU/EWR kennt die Daten aus dem Drittland nicht (Black Box-Konstellation).

Bewertung:

Deutsches materielles Recht gilt weder für die DV-Dienstleister noch für den Auftraggeber, wenn der deutsche AN nicht auf die vom AG übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System oder verschlüsselt erfolgt, ohne dass der AN über den Schlüssel verfügt).

Näheres hierzu: s. Erläuterungen.

Erläuterung der Bewertung zu den Fallgruppen F, G, H, I:

Nach § 1 Abs. 5 Satz 2 BDSG findet dieses Gesetz Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Für die Verarbeitung durch den DV-Dienstleister in Deutschland gilt somit das BDSG. Der DV-Dienstleister ist grundsätzlich nur für die Datensicherheit der von ihm durchgeführten Datenverarbeitung nach Maßgabe der Regelungen in § 11 i. V. m. § 9 BDSG, Art. 17 Europäische Datenschutzrichtlinie verantwortlich. Im Übrigen bleibt der Auftraggeber im Drittland selbst verantwortlich.

Bei den Fallgruppen F, G, H und I gibt es keine "Primär-Datenexporteure", die für das Vorliegen der Voraussetzungen des § 4c BDSG beim Drittstaaten-Auftraggeber zu sorgen haben. Die Frage der eigenen Verantwortlichkeit des EU/EWR-Auftragnehmers wird hier also besonders virulent. Fraglich ist, ob ihn weitere (über die vorgenannten hinausgehenden) Pflichten treffen.

Hinsichtlich der **Fallgruppen F bis I** ist zu fragen, ob sich für den Auftragnehmer aus § 1 Abs. 5 Satz 2 BDSG die Pflicht ergibt zu prüfen und sicherzustellen, dass beim (Rück-) Transfer der Daten die Voraussetzungen des § 4c BDSG (bzw. des § 4b BDSG) erfüllt werden. Würde man eine solche Pflicht annehmen, müsste der Auftragnehmer eine umfassende Prüfung der gesamten Datenverarbeitung vornehmen, also eine umfassende Prüfung des Zwecks der gesamten Datenverarbeitung sowie des Kontextes und der Umstände der Datenverarbeitung. Die bloße Vereinbarung mit dem Auftraggeber im Drittstaat, dass die Daten von jenem nur zu dem Zweck weiterverarbeitet werden dürfen, zu dem der Auftragnehmer die Daten erhalten hat, würde keinesfalls reichen. Eine Verantwortung gemäß §§ 4b, 4c BDSG würde vielmehr eine eigenständige umfassende Prüfung durch den Auftragnehmer erfordern. Dieser kennt aber höchstwahrscheinlich nur einen kleinen Ausschnitt der Datenverarbeitung und des Verwendungszusammenhanges. Die Rechtmäßigkeit der Verarbeitung von Daten im Konzernzusammenhang etwa wird er oft nur schwerlich beurteilen können. Er kann im Unterschied zu den Fallgruppen A - E gerade nicht auf einen vorhandenen Regelungsrahmen verweisen oder Bezug nehmen.

Deshalb ist zu konstatieren, dass es in den meisten Fällen für den Auftragsverarbeiter in Deutschland (EU/EWR) unmöglich sein dürfte, eine umfassende Prüfung i.S.d. §§ 4b, 4c BDSG vorzunehmen, um beurteilen zu können, ob eine Katalogausnahme gegeben ist, oder um vertragliche Regelungen i.S.d. § 4 c Abs. 2 BDSG treffen zu können. Bezüglich etwaiger

vertraglicher Regelungen i.S.d. § 4c Abs. 2 BDSG wäre im übrigen unklar, welche konkrete Rolle mit welchen Pflichten der Auftragsverarbeiter hierin übernehmen sollte (Einstandspflicht für Betroffenenrechte wie Auskunfts- und Haftungsanspruch?).

Aus alledem ergibt sich, dass der Auftragsverarbeiter in Deutschland (EU/EWR) keine Verantwortung i.S.d. §§ 4b, 4c BDSG hat. Der Gesetzgeber hat in § 1 Abs. 5 BDSG der Stelle im Drittstaat selbst die umfassende Verantwortung für die Vereinbarkeit der Datenverarbeitung mit dem BDSG zugewiesen, nicht dem Auftragsverarbeiter, dessen sich der Auftraggeber im Drittstaat bedient.

Den Auftragnehmer in Deutschland trifft aber eine qualifizierte Remonstrationspflicht entsprechend § 11 Abs. 3 Satz 2 BDSG sowie unter Umständen eine Pflicht zur materiellen Plausibilitätsprüfung bezüglich der von ihm selbst in Deutschland vorgenommenen Datenerhebungen, -verarbeitungen und -nutzungen.

Daraus ergeben sich folgende Konsequenzen:

a) **Fallgruppe F**

Wenn der DV-Dienstleister die Daten selbst zu erheben hat, so ist damit in aller Regel eine inhaltliche Kenntnisnahme der Daten verbunden. Daher hat der DV-Dienstleister summarisch auf Plausibilität zu prüfen, ob die Datenerhebung und -verarbeitung und die diesbezüglichen Weisungen des Auftraggebers mit dem BDSG vereinbar sind. Wenn nein, gelten die unter b) genannten Anforderungen.

b) **Fallgruppe G**

Die DV-Dienstleistung wird häufig in der Rechenzentrums-Dienstleistung bestehen, so dass eine inhaltliche Kenntnisnahme der Daten durch den Auftragsverarbeiter nicht vorgesehen ist. Der Auftragsverarbeiter hat lediglich für die Datensicherheit zu sorgen, er hat keine Prüfungspflicht bzgl. der Vereinbarkeit der Datenverarbeitung mit dem BDSG.

Soweit ihm jedoch (aufgrund besonderer Hinweise Dritter o. ä.) bekannt wird, dass die Datenverarbeitung gegen das BDSG verstößt, hat er eine qualifizierte Remonstrationspflicht entsprechend § 11 Abs. 3 Satz 2 BDSG. Gleiches gilt in den Einzelfällen, bei denen dem Auftragsverarbeiter bekannt wird, dass offensichtlich (eindeutig) kein angemessenes Datenschutzniveau (ausreichende Datenschutzgarantien) beim Auftraggeber besteht und auch eindeutig kein Ausnahmetatbestand i.S.d. § 4c Abs. 1 BDSG gegeben ist.

In diesen Fällen, in denen der Auftraggeber einen gravierenden Missstand trotz Hinweisen des Auftragsverarbeiters nicht abstellt, ist eine Hinweis-/Anzeigepflicht des Auftragsverarbeiters gegenüber der Datenschutzaufsichtsbehörde gegeben. Gegebenenfalls besteht somit unter Umständen die Pflicht des Auftragsverarbeiters, die weitere Ausführung des Auftrages einzustellen. Dann entscheidet die Aufsichtsbehörde, wie weiter zu verfahren ist.

c) Die **Fallgruppe H** bedarf besonderer Betrachtung:
In Drittstaaten können bestimmte Verarbeitungen personenbezogener Daten explizit vorgeschrieben sein, die in Deutschland unzulässig wären (z. B. die Verarbeitung der Sozialversicherungsnummern von Kunden, die die Funktion eines Personenkennzeichens haben). Zwar gilt das BDSG grundsätzlich unabhängig davon, ob die Betroffenen Personen in Deutschland ansässig sind oder nicht. Allerdings wird mit der Sondervorschrift des § 1 Abs. 5 Satz 2 BDSG der reguläre Anwendungsbereich des BDSG ohnehin ausgedehnt, so dass hier eine Relativierung möglich erscheint. Ob der Gesetzgeber bzw. die Europäische Datenschutzrichtlinie bei der Regelung des § 1 Abs. 5 Satz 2 BDSG (bzw. Art. 4 Abs. 1 c) Richtlinie) einen "EU/EWR-Bezug" der Daten stillschweigend unterstellt hat, bleibt unklar.

Die Lösung besteht darin, dass zwar aus § 1 Abs. 5 Satz 2 BDSG keine umfassende Geltung des deutschen Datenschutzrechts abzuleiten wäre, aber Verarbeitungen, die eindeutig gegen unseren "ordre public" verstoßen (z. B. bei Menschenrechtsverletzungen), unzulässig sind, auch wenn die Daten keinerlei EU/EWR-Bezug aufweisen. Demzufolge besteht die qualifizierte Remonstrationspflicht des Auftragsverarbeiters (s. o. b)) nur bei derartigen Verstößen.

d) **Fallgruppe I**
Hier muss der Auftraggeber nicht die Regelungen des BDSG beachten, weil die Situation vergleichbar ist mit der Transitregelung des § 1 Abs. 5 Satz 4 BDSG. Es besteht auch keine weitere (über die technisch-organisatorische hinausgehende) Verantwortlichkeit des EU/EWR-Auftragnehmers. Der Grundsatz lautet hier: Deutsches materielles Datenschutzrecht gilt nicht, wenn der deutsche Auftragnehmer nicht auf die vom Auftraggeber übermittelten Daten zugreifen kann (weil die Datenverarbeitung im geschlossenen System / Black Box oder verschlüsselt erfolgt).