Drittes Kapitel: Die Zulässigkeitsvoraussetzungen einer Übermittlung personenbezogener Daten in ein Drittland

Die besonderen Rechtmäßigkeitsvoraussetzungen für die Übermittlung personenbezogener Daten in ein Drittland ergeben sich aus den in Kapitel IV zusammengefassten Artikeln 25 und 26 der Richtlinie 95/46/EG.

A. Der Aufbau der Zulässigkeitsprüfung eines Drittländertransfers

Die Artikel 25 und 26 der Richtlinie weisen jeweils in ihrem Absatz 1 darauf hin, dass sie die Zulässigkeit des Datenexports vorbehaltlich der aufgrund der anderen Richtlinienbestimmungen erlassenen mitgliedstaatlichen Vorschriften festlegen. Die Rechtmäßigkeit der Übermittlung in ein Drittland richtet sich somit nicht nur nach den Voraussetzungen dieser beiden Spezialvorschriften. Der Transfer muss darüber hinaus den Anforderungen entsprechen, die an eine inländische Übermittlung gestellt werden.

Abgesehen von den im Rahmen einer Verarbeitung anfallenden Pflichten der verantwortlichen Stelle, den Rechten des Betroffenen sowie der Berücksichtigung sonstiger Verarbeitungsmodalitäten ist also zunächst zu prüfen, ob die konkrete Verarbeitung der Daten überhaupt zulässig ist. Die Zulässigkeit ist in Artikel 7 der Richtlinie in Form eines Verbots mit Erlaubnisvorbehalt geregelt, sodass auch die Übermittlung personenbezogener Daten in ein Drittland durch einen der in Artikel 7 der Richtlinie abschließend aufgezählten Erlaubnistatbestände legitimiert sein muss. Erst im Anschluss daran werden die besonderen Rechtmäßigkeitsvoraussetzungen der Artikel 25 und 26 der Richtlinie relevant.

Gemäß Artikel 25 Absatz 1 der Richtlinie ist eine „Übermittlung personenbezogener Daten (...) in ein Drittland (...) zulässig (...), wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.“ Der Artikel 26 Absatz 1 der Richtlinie listet demgegenüber einzelne Tatbestände auf, die eine Übermittlung trotz eines mangelhaften Schutzniveaus in dem betreffenden Drittland unter bestimmten Umständen zulassen. Unbeschadet des Artikels 26 Absatz 1 wird dem für die Verarbeitung Verantwortlichen in Artikel 26 Absatz 2 der Richtlinie schließlich die Möglichkeit eröffnet, die Genehmigung eines Mitgliedstaates für eine Übermittlung in ein unsicheres Drittland einzuholen. Voraussetzung für die Erteilung der Übermittlungserlaubnis ist, dass „der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet“.

Entsprechend den Überschriften der Richtlinienbestimmungen legt der Artikel 25 die Grundsätze zum Drittländertransfer fest, während der

Artikel 26 sich mit den Ausnahmen befasst. Die Reihenfolge der Vorschriften in der Richtlinie bestätigt diese Rangfolge ebenso wie der Wortlaut der Absätze 1 und 2 des Artikels 26, die jeweils unter bestimmten Umständen Datenübermittlungen in solche Drittländer erlauben, die „kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleiste(n)". Ein rechtssystematisches Vorgehen erfordert daher zunächst eine Prüfung des Schutzniveaus im Sinne des Artikels 25, während die Ausnahmen des Artikels 26 der Richtlinie entsprechend ihrer numerischen Reihenfolge nur bei einer fehlenden Angemessenheit zur Anwendung kommen.[257]

In der Literatur wird diese Prüfungsreihenfolge indessen teilweise infrage gestellt. Zwar besteht Einigkeit darüber, dass die Regelung des Artikels 26 Absatz 2 nur relevant wird, sofern eine Übermittlung nicht schon gemäß den Artikeln 25 oder 26 Absatz 1 der Richtlinie zulässig ist. Das Verhältnis der beiden letzten Vorschriften zueinander wird jedoch unterschiedlich beurteilt.

So komme dem Artikel 26 Absatz 1 der Richtlinie unter praktischen Gesichtspunkten bei der Zulässigkeitsprüfung der Vorrang zu. Sei einer der dort aufgezählten Tatbestände erfüllt, erübrige sich grundsätzlich eine Analyse des Schutzniveaus. Die Angemessenheitsprüfung entscheide mithin lediglich darüber, ob der Transfer gemäß Artikel 26 Absatz 2 der Richtlinie genehmigt werden müsse.[258] Für diese Systematik spreche ferner, dass die Tatbestände des Artikels 26 Absatz 1a) bis c) der Richtlinie den tatsächlichen Regelfall der Übermittlungen in Dritt-

[257] So z. B. dargestellt von *WP 12*, S. 32; *Abel*, BDSG, S. 57; *Bachmeier*, RDV 1995, S. 49, S. 52; Roßnagel (- *Brühann*), 2.4, Rn. 51; *Büllesbach* in: Datenverkehr ohne Datenschutz?, S. 51, S. 60; *Draf*, S. 56 ff.; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, vor Art. 25, Rn. 3; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 2 f.; *Franzen*, DB 2001, S. 1867, S. 1869; *Giesen*, DuD 1996, S. 394; *Heil*, DuD 1999, S. 458; *Hobert*, S. 95; *Hoeren*, S. 269 f.; *Hoeren/Queck*, S. 275; *Jacob* in: Datenverkehr ohne Datenschutz?, S. 25, S. 26 f.; *Koch*, S. 331; *Löw*, S. 90; *Moos* in: Kröger/Gimmy, S. 3, S. 14; *Mütsch*, DuD 1994, S. 187, S. 189; *Palm*, CR 1998, S. 65, S. 72 f.; *Schild*, EuZW 1996, S. 549, S. 553; *Stein* in: Festschrift f. Rudolf, S. 513, S. 519; *Tinnefeld/Ehmann*, Datenschutzrecht, S. 68; *Wülfing/Dieckert*, S. 125 f. Für die entsprechenden Vorschriften des BDSG (§ 4b und c): *Räther/Seitz*, MMR 2002, S. 425, S. 426; *Rittweger/Weiße*, CR 2003, S. 142, S. 145 f.; *Schaffland/Wiltfang*, BDSG, 5001, § 4c, Rn. 1.

[258] *Wuermeling*, Handelshemmnis Datenschutz, S. 102; *ders.*, MMR 9/2000, S. XX, im Hinblick auf die Bedeutung der Safe Harbor Privacy Principles; so auch die Gewichtung bei *Kopp*, DuD 1995, S. 204, S. 209; für das Verhältnis zwischen § 4b Absatz 2 und § 4c BDSG offenbar auch *Börner* u. a., S. 101, die die Tatbestände des § 4c Absatz 1 BDSG „unabhängig von einem angemessenen Datenschutzniveau" anwenden wollen.

länder bildeten. Die Richtlinie sei insofern missverständlich konstruiert.[259]

Die Struktur des Artikels 26 Absatz 1 der Richtlinie bestätigt die Annahme einer Vorrangstellung. Der Aufbau der Bestimmung ist dem Tatbestand des Artikels 7 der Richtlinie nachgebildet, der die generellen Zulässigkeitsbedingungen für eine Verarbeitung personenbezogener Daten aufstellt. Es liegt daher die Schlussfolgerung nahe, dass der Artikel 26 Absatz 1 der Richtlinie die zunächst abschließenden Erlaubnistatbestände für einen Drittländertransfer aufzählt. Nur ausnahmsweise wäre mithin darüber hinaus ein Transfer zulässig, sofern das betreffende Drittland über ein angemessenes Schutzniveau verfügte.

Da sich eine Angemessenheitsprüfung im Rahmen des Artikels 25 Absatz 1 der Richtlinie recht aufwendig gestalten kann, mag eine vorrangige Behandlung der Tatbestände des Artikels 26 Absatz 1 in der Praxis durchaus sinnvoll sein. Rechtsdogmatisch verkehrt sie jedoch den Charakter der Vorschriften über den Drittländertransfer, der gemäß der Begründung des Rates zum gemeinsamen Standpunkt in der Schaffung einer „gewisse(n) Undurchlässigkeit“[260] des auf dem Binnenmarkt geltenden Datenschutzsystems besteht. Diese Absicht wird nur deutlich, wenn das Erfordernis eines angemessenen Schutzniveaus in außereuropäischen Empfängerstaaten als Grundregel aufgefasst wird und nicht in seinem Rang hinter den Öffnungsklauseln des Systems zurücksteht.

Das bestätigt auch der Blick auf die historische Entwicklung der Drittländerregelung. Der erste Vorschlag zur Richtlinie sah noch keine Ausnahmen im Sinne des Artikels 26 Absatz 1 der Richtlinie zu dem Erfordernis eines angemessenen Schutzniveaus vor.[261] Selbst in dem zweiten Vorschlag war der Ausnahmenkatalog noch kürzer als in der endgültigen Richtlinie gefasst.[262] Mit der kontinuierlichen Abschwächung des Grundsatzes der Angemessenheit sollte einer Handelsbarriere im Ver-

[259] Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 1; *ders.*, CR 2000, S. 472, S. 473; *ders.* in: Datenverkehr ohne Datenschutz?, S. 177, S. 180 f.
[260] *Begründung des Rates zum gemeinsamen Standpunkt*, ABl. EG Nr. C 93 vom 13.4.1995, S. 19, S. 20.
[261] Artikel 24 des *Vorschlags für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (90/C 277/03)*, KOM (90) 314 endg. – SYN 287, von der Kommission vorgelegt am 27. Juli 1990, ABl. EG Nr. C 277 vom 5.11.1990, S. 3.
[262] Artikel 26 des *geänderten Vorschlags für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (92/C 311/04)*, KOM (92) 422 endg. – SYN 287, gemäß Artikel 149 Absatz 3 des EWG-Vertrages von der Kommission vorgelegt am 16. Oktober 1992, ABl. EG Nr. C 311 vom 27.11.1992, S. 30.

hältnis zu Drittstaaten vorgebeugt werden.[263] Es ist jedoch nicht ersichtlich, dass zugleich eine Umkehr der Gewichtung zwischen den Bestimmungen der Artikel 25 und 26 Absatz 1 der Richtlinie zueinander intendiert war.

Zudem darf auch die Relevanz der Ausnahmetatbestände des Artikels 26 Absatz 1 der Richtlinie für die Privatwirtschaft nicht überbewertet werden.[264] Zwar mag eine Mehrheit der denkbaren Sachverhaltsvarianten[265] erfasst sein. Viele weltweit tätige Unternehmen sind aber dennoch auf die Herstellung eines angemessenen Schutzniveaus in ihrem Wirkungsbereich angewiesen,[266] da sowohl der konzerninterne Datenaustausch als auch die zentrale Verarbeitung von Personal- und Kundendaten in außereuropäischen Rechenzentren[267] sowie die Verwendung der Daten zu Sekundärzwecken,[268] insbesondere zum Direktmarketing,[269] nur sehr fragmentarisch Berücksichtigung in dem Ausnahmenkatalog gefunden haben. Solchen Verantwortlichen nützt der Artikel 26 Absatz 1 der Richtlinie daher nur bedingt.

Neben dem Wortlaut und der Richtliniensystematik sprechen mithin auch teleologische Aspekte sowie die Relevanz in der Wirtschaftsrealität für den Vorrang des Artikels 25 der Richtlinie. Die Vorschriften ü-

---

[263] Z. B. *Klug*, BDSG, S. 132.
[264] So auch *Eul/Godefroid*, RDV 1998, S. 185, S. 188 f.
[265] *Gounalakis/Mand*, CR 1997, S. 497, S. 502; *Schaar*, Datenschutz im Internet, Rn. 866; *Weber*, CR 1995, S. 297, S. 299 und S. 303, sieht die typischen Fälle des Drittländertransfers abgedeckt.
[266] Vgl. dazu *Büllesbach* in: Datenverkehr ohne Datenschutz?, S. 51, S. 60 f.; *Däubler*, RDV 1998, S. 96, S. 97, geht sogar davon aus, dass etwa 90% der grenzüberschreitenden Datenübermittlungen innerhalb multinationaler Unternehmen oder Konzerne stattfinden.
[267] *Büllesbach*, RDV 2002, S. 55, S. 58; *ders.*, CR 2000, S. 544, S. 552.
[268] *Simitis*, CR 2000, S. 472, S. 473; *ders.* in: Datenverkehr ohne Datenschutz?, S. 177, S. 182.
[269] *Wuermeling*, CR 2001, S. 303, S. 307; missverständlich jedoch *Hobert*, S. 95 f., der offenbar Arbeitnehmer- und Marketingdaten grundsätzlich vom Anwendungsbereich des Artikels 26 Absatz 1 der Richtlinie ausgenommen sieht.

ber den Drittländertransfer werden dementsprechend im Folgenden in ihrer numerischen Reihenfolge vorgestellt.

B. Die gemeinsamen Voraussetzungen der Artikel 25 und 26 der Richtlinie

Sowohl der Artikel 25 als auch der Artikel 26 der Richtlinie setzen eine „Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland“ voraus.

I. Der Verpflichtete der Vorschriften

Der Verpflichtete der mitgliedstaatlichen Datenschutzvorschriften, die in Umsetzung der Artikel 25 Absatz 1 und 26 Absatz 1 und 2 der Richtlinie erlassen wurden, ist in Entsprechung zu den übrigen Richtlinienbestimmungen der für die Verarbeitung Verantwortliche. Er darf personenbezogene Daten nur unter den in diesen Vorschriften genannten Voraussetzungen in ein Drittland übermitteln. Sofern eine der Zulässigkeitsbedingungen nicht erfüllt ist und insbesondere die Angemessenheit des Schutzniveaus nicht positiv festgestellt wurde, sprechen die Bestimmungen ein unmittelbares Übermittlungsverbot aus. Der Verantwortliche kann sich folglich nicht auf ein noch schwebendes Verfahren der Europäischen Kommission zur Entscheidung über die Angemessenheit des Schutzniveaus in dem jeweiligen Drittland berufen.

Nicht in allen Mitgliedstaaten sind indessen die Verantwortlichen der Übermittlung zugleich zu der selbstständigen Beurteilung des Schutzniveaus befugt. In Österreich,[270] Portugal[271] und Spanien[272] entscheiden die nationalen Datenschutzbeauftragten über das Vorliegen der Angemessenheit, während in Griechenland[273] sogar jede einzelne Übermittlung einer Erlaubnis der Kontrollstelle bedarf. Diesen strengeren Ansatz hat die Europäische Kommission allerdings in ihrem ersten Bericht über die Durchführung der Richtlinie aufgrund seiner handelshemmenden Wirkung und im Hinblick auf die angestrebte Harmonisierung des Datenverkehrs mit Drittländern zu Recht kritisiert.[274] Zugleich signalisiert der Bericht jedoch umgekehrt, dass das z. B. im deutschen Bundesdatenschutzgesetz[275] gewählte Verfahren einer Beurteilung des Schutzniveaus allein durch den für die Verarbeitung Verantwortlichen

[270] § 12 Absatz 2 Satz 2.
[271] Artikel 19 Absatz 3.
[272] Artikel 33 Absatz 1 und 2.
[273] Artikel 9.
[274] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 20.
[275] § 4b Absatz 2.

nicht ausreichend sei. Da die Richtlinie keine eindeutige Aussage zu der Frage der zuständigen Beurteilungsinstanz enthält, bleibt abzuwarten, welche der divergierenden nationalen Regelungen der Mitgliedstaaten sich endgültig durchsetzen wird.

II. Die Übermittlung personenbezogener Daten in ein Drittland

Die Artikel 25 und 26 der Richtlinie regeln den Transfer personenbezogener Daten in ein Drittland.

Gemäß Artikel 2a) der Richtlinie geht es sonach um die Übermittlung von „Informationen über eine bestimmte oder bestimmbare natürliche Person". Das Ziel des Transfers muss ein Drittland sein, also ein Land, das weder der Europäischen Union noch dem Europäischen Wirtschaftsraum angehört.

Ungeachtet des Adressaten liegt eine Übermittlung im Sinne der Artikel 25 und 26 der Richtlinie grundsätzlich bei jedem Transfer personenbezogener Daten über die europäischen Grenzen hinweg durch einen für die Verarbeitung Verantwortlichen vor. Die Daten können sowohl an einen Empfänger im Sinne einer Bekanntgabe weitergegeben als auch an eine eigene Datenbank versandt werden.[276] Voraussetzung ist allein der grenzüberschreitende Datenverkehr,[277] durch den die personenbezogenen Daten des Betroffenen den Geltungsbereich des Gemeinschaftsrechts verlassen.

Auf den äußeren Vorgang der Übermittlung kommt es dabei nicht an. Es macht folglich keinen Unterschied, ob die Daten tatsächlich aktiv verschickt werden, also per Post, E-Mail oder auf einem ähnlichen Wege das Drittland erreichen, oder ob die importierende Stelle die Daten von einem in der Europäischen Union lokalisierten Terminal abruft.[278] Da die personenbezogenen Informationen auch in diesem Fall mindestens durch die Kenntnisnahme der außereuropäischen Stelle in das Drittland gelangen, ist die Gefährdungslage für das Persönlichkeitsrecht des Betroffenen bei beiden Sachverhalten identisch.

[276] Vgl. dazu Gliederungspunkt B.II.2.d. des zweiten Kapitels.
[277] Vgl. dazu Erwägungsgrund (56) der Richtlinie, der den „grenzüberschreitende(n) Verkehr von personenbezogenen Daten" quasi als Synonym für die Übermittlung personenbezogener Daten in Drittländer verwendet.
[278] Vgl. dazu Gliederungspunkt B.II.2.d. des zweiten Kapitels.

Teilweise wird angenommen, dass auch ein von dem Betroffenen selbst veranlasster Transfer von den Artikeln 25 und 26 der Richtlinie geregelt werde.[279] Fraglich ist jedoch, wer in einer solchen Konstellation der Verpflichtete des Übermittlungsverbots sein sollte. Wie bereits an anderer Stelle am Beispiel der Datenübertragung im Rahmen eines Website-Besuchs erörtert, trägt der außereuropäische Empfänger sogar bei einer grenzüberschreitenden Erhebung die Verantwortung für den Transfer der Daten nur, sofern er auf ein in der Europäischen Union belegenes Mittel zurückgreift.[280] Sodann handelt es sich jedoch nicht mehr um eine Übermittlung des Betroffenen.

Andererseits ergäbe es keinen Sinn, dem Betroffenen selbst die Übermittlung seiner Daten in ein unsicheres Drittland zu verbieten. Auch die Eröffnung des sachlichen Anwendungsbereichs der Richtlinie gemäß Artikel 3 wäre kaum zu begründen. Die eigenverantwortliche Übermittlung des Betroffenen unterliegt daher nicht den Bestimmungen der Artikel 25 und 26 der Richtlinie.

Wohl aber hat die verantwortliche Stelle die Vorschriften zum Drittländertransfer bei einer Übermittlung an den Betroffenen zu beachten. Zwar dient ein solcher Transfer im Zweifel dem Schutzbedürfnis des Betroffenen, da die Weitergabe der Daten regelmäßig dem Recht auf Information oder dem Auskunftsbegehren abzuhelfen bestimmt ist. Zudem wird der Betroffene selten ein berechtigtes Interesse daran nachweisen können, seine personenbezogenen Informationen nicht zu erhalten. Andererseits könnten die Daten auf dem Übertragungsweg aufgrund von Sicherheitsmängeln in dem betreffenden Drittland gefährdet sein, sodass eine Prüfung gemäß den Artikeln 25 und 26 der Richtlinie unentbehrlich ist.

III. Die Daten als Gegenstand einer Verarbeitung

Die Vorschriften zum Drittländertransfer setzen ferner voraus, dass die übermittelten Daten bereits Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen.

Die erste Tatbestandsvariante ist erfüllt, sofern die Daten bereits vor dem Transfer in einem Mitgliedstaat verarbeitet werden. Einer Literaturmeinung[281] zufolge bezögen sich die Artikel 25 und 26 der Richtlinie

[279] So Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 6; *Draf*, S. 60; *WP 4*, S. 10.
[280] Siehe dazu Gliederungspunkt B.II.2.a.(3). des zweiten Kapitels.
[281] So aber *Draf*, S. 57 f.

sogar auf manuelle Verarbeitungen, bei denen keine Speicherung der Daten in einer Datei vorgesehen sei. Das ergebe sich aus Artikel 2b) der Richtlinie, dessen Legaldefinition der Verarbeitung auch diesen Vorgang als Verarbeitung im Sinne der Richtlinie bezeichne.

Es ist jedoch nicht ersichtlich, warum die Drittländerregelung über den sich aus Artikel 3 ergebenden sachlichen Anwendungsbereich der Richtlinie hinausgehen sollte.[282] Die bloße Wahl des Wortes „verarbeiten“ kann diese Annahme jedenfalls nicht rechtfertigen. Anderenfalls würde jede Vorschrift, die ausdrücklich von einer Verarbeitung spricht, den Anwendungsbereich der Richtlinie erweitern und sonach die Funktion des Artikels 3 der Richtlinie aushöhlen.

Unter die erste Tatbestandsvariante werden daher nur solche Verarbeitungsvorgänge subsumiert, die im Rahmen des Anwendungsbereichs der Richtlinie stattfinden.

Die zweite Tatbestandsvariante setzt voraus, dass die Daten erst nach der Übermittlung verarbeitet werden. Ein eigenständiger Regelungsbereich kommt dieser Alternative nur zu, sofern eine Übermittlung von Daten keine Verarbeitung gemäß Artikel 2b) der Richtlinie ist. Anderenfalls wären die Daten bereits zum Zeitpunkt der Übermittlung „Gegenstand einer Verarbeitung“.

Eine Verarbeitung im Sinne des Artikels 2b) der Richtlinie bezeichnet „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“.

In der sich der Legaldefinition anschließenden Aufzählung von Beispielen für Verarbeitungsvorgänge ist ausschließlich die „Weitergabe durch Übermittlung“ genannt. Die Formulierung deutet insbesondere darauf hin, dass der Tatbestand der Weitergabe nur bei einer Übermittlung personenbezogener Daten erfüllt ist.[283] Ebenfalls kann sich daraus jedoch ergeben, dass umgekehrt jede Übermittlung eine Weitergabe von Daten voraussetzt, also eine Bekanntgabe der personenbezogenen Informationen an einen mit dem für die Verarbeitung Verantwortlichen nicht identischen Adressaten.

[282] Vgl. dazu Gliederungspunkt A. des zweiten Kapitels.
[283] *Dressel*, S. 246.

Auf eine innereuropäische Übermittlung mag das tatsächlich zutreffen. Wie an anderer Stelle jedoch bereits dargestellt,[284] ist entsprechend dem äquivalenten Schutzbedürfnis des Betroffenen eine Übermittlung von Daten in ein Drittland auch dann gegeben, wenn der für die Verarbeitung Verantwortliche die personenbezogenen Informationen an die eigene Anschrift in dem Drittland transferiert. Eine grenzüberschreitende Übermittlung setzt daher nicht zwingend eine Weitergabe voraus.

Die Tatsache der ausschließlichen Nennung der „Weitergabe durch Übermittlung“ in der Legaldefinition des Artikels 2b) der Richtlinie schadet dieser Auslegung nicht, da sich die Aufzählung der Verarbeitungsvorgänge nicht als abschließend versteht. Darüber hinaus steht außer Frage, dass eine Übermittlung personenbezogener Daten in ein Drittland ein „Vorgang (...) im Zusammenhang mit personenbezogenen Daten“ ist. Zwar nimmt *Kaspersen* an, dass eine Übermittlung deswegen keine Verarbeitung sein könne, weil sie nicht auf die Bedeutung und den Inhalt der Daten gerichtet sei.[285] Der Hintergrund dieser Ansicht erschließt sich jedoch nicht, da einerseits Artikel 2b) der Richtlinie diese Merkmale nicht voraussetzt. Auf der anderen Seite ist nicht nachvollziehbar, inwieweit im Vergleich zu einer Übermittlung beispielsweise eine bloße Aufbewahrung der Daten, die ausdrücklich in Artikel 2b) der Richtlinie erwähnt ist, dieser Anforderung eher gerecht würde.

Bei einer Übermittlung handelt es sich also bereits um eine Verarbeitung im Sinne der Richtlinie, sodass die zweite Tatbestandsvariante in sich widersprüchlich ist.

Deshalb wird vertreten, dass der Formulierung eine klarstellende Funktion im Hinblick auf die Anwendbarkeit des Artikels 25 der Richtlinie auf die eigenständige Übermittlung der Daten durch den Betroffenen zukomme.[286] Wie bereits erläutert, gelten die Vorschriften über den Drittländertransfer für diesen Sachverhalt jedoch nicht.[287]

Alternativ ist zu erwägen, dass die erste Variante nur zur Anwendung kommen soll, sofern die Daten Gegenstand einer über die bloße Übermittlung hinausgehenden Verarbeitung sind. Dazu müsste es jedoch eine Form der Datenerfassung geben, die keine Verarbeitung im Sinne

[284] Siehe dazu Gliederungspunkt B.II.2.d. des zweiten Kapitels.
[285] *Kaspersen* in: *e*Directives, S. 119, S. 122.
[286] So Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 8.
[287] Vgl. Gliederungspunkt B.II. dieses Kapitels.

des Artikels 2b) der Richtlinie wäre. Als solche scheidet die Erhebung von vornherein aus, da sie ausdrücklich als Verarbeitungsvorgang definiert ist. Somit darf der Übermittlung kein von dem zurechenbaren Willen der verantwortlichen Stelle getragenes Beschaffen personenbezogener Informationen vorausgehen, durch das die verantwortliche Stelle Kenntnis von den betreffenden Daten erhält oder die Verfügung über sie begründet.[288]

In Betracht kommt hiernach nur ein seitens des Betroffenen aufgedrängter Datenzuwachs, dem auch nachträglich[289] von dem in der Europäischen Union ansässigen Datenempfänger keine Zweckbestimmung beigemessen wurde. Stets unterlägen die Daten jedoch spätestens zum Zeitpunkt der Übermittlung mindestens dem Übertragungszweck, sodass sie entweder rückwirkend erhoben oder jedenfalls vor dem Transfer im Sinne des Artikels 2b) der Richtlinie genutzt würden.

Der Übermittlung von Daten durch einen für die Verarbeitung Verantwortlichen geht demzufolge generell eine weitere Verarbeitung in der Europäischen Union voraus.

Fände indessen keine Verarbeitung in der Europäischen Union vor der Ankunft der Daten in dem Drittland statt, tauchten überdies Probleme bei der Frage des sachlichen Anwendungsbereichs der Richtlinie auf, der das Vorliegen einer Verarbeitung gerade verlangt. Zwar ist entsprechend dem Sitzprinzip grundsätzlich keine Verarbeitung innerhalb der Europäischen Union erforderlich.[290] Da die Tatbestände der Artikel 25 und 26 der Richtlinie jedoch einen Transfer von den Mitgliedstaaten in ein Drittland voraussetzen, muss die Richtlinie bereits zum Zeitpunkt der Grenzüberschreitung sachlich und örtlich anwendbar sein.

Teilweise wird sogar davon ausgegangen, dass Artikel 25 Absatz 1 der Richtlinie mit der zweiten Tatbestandsvariante über den sachlichen Anwendungsbereich der Richtlinie hinausginge, um der besonderen Risikolage des Drittländertransfers Rechnung zu tragen.[291] Das wäre plausibel, wenn entweder Artikel 3 der Richtlinie einen Hinweis auf derartige Ausnahmen enthielte oder die Richtlinie auch an anderer Stelle ähnliche Erweiterungen des Anwendungsbereichs vornehmen würde.

---

[288] So die Definition des Begriffs der Erhebung bei Simitis u. a. (- *Dammann*), BDSG-Dokumentation, § 3, Rn. 108.
[289] Kilian/Heussen (- *Weichert*), Nr. 132, Rn. 96.
[290] Vgl. dazu Gliederungspunkt B.I. des zweiten Kapitels.
[291] So Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 5.

Da das nicht der Fall ist, widerspricht diese Ansicht jedoch der Richtliniensystematik, nach welcher der Anwendungsbereich ausschließlich in den allgemeinen Bestimmungen festgelegt ist. Davon abgesehen enthalten die Artikel 25 und 26 der Richtlinie gemäß ihrem eigenen Wortlaut die Voraussetzungen eines Drittländertransfers vorbehaltlich der Beachtung der aufgrund der anderen Richtlinienbestimmungen erlassenen einzelstaatlichen Vorschriften. Dazu zählen im Zweifel auch die Regeln über den Anwendungsbereich der Richtlinie beziehungsweise der sie umsetzenden nationalen Gesetze.

Eine Erweiterung des Anwendungsbereichs ist demnach nicht vorgesehen, aber auch entbehrlich. Ohnehin liegen die Voraussetzungen des Tatbestandes des Artikels 3 Absatz 1 der Richtlinie stets entweder aufgrund der Übermittlung oder wegen einer dieser vorausgehenden Verarbeitung der Daten vor.

Insgesamt ergibt sich, dass für die zweite Tatbestandsvariante kein eigenständiger Regelungsbereich existiert.[292]

[292] *Draf*, S. 58; *Koenig/Röder*, CR 2000, S. 668, dort Fn. 84; *Wuermeling*, Handelshemmnis Datenschutz, S. 85 ff.