Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU

Positionspapier

Brüssel, 14. Juli 2014

Zusammenfassung

Dieses Papier soll Organen und Einrichtungen der EU Hilfestellung bei der Auslegung und Anwendung der in der Verordnung (EG) Nr. 45/2001 niedergelegten Vorschriften für internationale Übermittlungen personenbezogener Daten bieten.

Organe und Einrichtungen der EU müssen aus verschiedenen Gründen wie der grenzüberschreitenden Zusammenarbeit und der Nutzung transnationaler Dienste zunehmend personenbezogene Daten an Drittländer oder internationale Organisationen übermitteln.

Der „Grundsatz des angemessenen Schutzes“ (Artikel 9 Absätze 1 und 2) ist bei der internationalen Übermittlung von Daten unbedingt zu wahren. Dieser Grundsatz verlangt, dass das Grundrecht auf Datenschutz auch dann garantiert ist, wenn personenbezogene Informationen in Länder außerhalb der EU oder an Einrichtungen übermittelt werden, die nicht dem EU-Recht unterworfen sind. Für die Verarbeitung Verantwortliche sollten das von dem Empfänger der Daten gebotene Schutzniveau genau prüfen; seine Angemessenheit ist anhand der Art der am Bestimmungsort geltenden Datenschutzvorschriften und anhand der Mittel zu beurteilen, mit denen ihre wirksame Anwendung gewährleistet wird (Aufsicht und Durchsetzung).

In Fällen, in denen die Europäische Kommission eine „Angemessenheitsentscheidung“ erlassen hat (Artikel 9 Absatz 5), muss die Angemessenheit nicht weiter geprüft werden. Übermittlungen sind auch dann zulässig, wenn der für die Verarbeitung Verantwortliche Vorkehrungen trifft, die ausreichende Garantien bieten (Artikel 9 Absatz 7). Schließlich dürfen Übermittlungen ohne besondere Garantien auch unter außergewöhnlichen Umständen erfolgen, sofern eine konkrete Ausnahmeregelung gilt (Artikel 9 Absatz 6).

In Fällen, in denen Organe oder Einrichtungen der EU im Einklang mit EU-Rechtsvorschriften oder bilateralen Abkommen zu internationalen Übermittlungen verpflichtet sind und dabei als für die Verarbeitung Verantwortliche auftreten und in denen dem Empfängerland von der Kommission kein angemessenes Schutzniveau bescheinigt wurde, sollte das Instrument im Idealfall die Maßnahmen vorsehen, mit denen sich die Einhaltung von Artikel 9 der Verordnung gewährleisten lässt. Zu diesem Zweck sollte vor der Annahme eines solchen Rechtsinstruments gemäß Artikel 28 Absatz 2 der Verordnung der EDSB konsultiert werden.

Je nach Art der Durchführung der Übermittlung kann der EDSB als Kontrollstelle fungieren, und dies insbesondere, wenn der EDSB vorab nicht konsultiert oder um eine Genehmigung ersucht wurde in Fällen, in denen dies eigentlich zu erwarten gewesen wäre. Gegebenenfalls können wir auch Inspektionen vornehmen oder unsere Durchsetzungsbefugnisse nutzen.

Inhalt

Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU

1. Einführung

In Wahrnehmung ihrer Aufgaben müssen Organe und Einrichtungen der EU zunehmend personenbezogene Daten an Drittländer[1] oder internationale Organisationen übermitteln, und zwar aus Gründen wie der grenzüberschreitenden Zusammenarbeit[2] und der Nutzung transnationaler Dienste.[3] Die rasche technologische Entwicklung, einschließlich Cloud Computing und mobile Anwendungen[4], schafft neue Herausforderungen, denen begegnet werden muss, um zu gewährleisten, dass die Grundrechte der Menschen in vollem Umfang geachtet werden. Artikel 9 der Verordnung (EG) Nr. 45/2001 („Verordnung“) enthält die Vorschriften für derartige Übermittlungen unter Berücksichtigung von Artikel 25 und 26 der Richtlinie 95/46/EG („Richtlinie“).

Das vorliegende Papier soll den für die Verarbeitung Verantwortlichen von Organen und Einrichtungen der EU technische und praktische Hilfestellung bei der Auslegung und Anwendung dieser Übermittlungsvorschriften bieten.

Der bestehende EU-Rechtsrahmen für den Datenschutz, einschließlich der Richtlinie, wird derzeit überarbeitet. In dem von der Europäischen Kommission vorgelegten Vorschlag wurden die Vorschriften über internationale Übermittlungen deutlich weiterentwickelt. Kapitel V des Vorschlags kann als gelungener Beitrag zu mehr weltweitem Datenschutz betrachtet werden[5], da dort nicht nur der Grundsatz des „angemessenen Schutzes“ aufgestellt[6], sondern auch mehr Spielraum für die Gewährleistung angemessener Garantien bei Datenübermittlungen eingeräumt wird[7]. Damit eröffnen sich größere Möglichkeiten für spezifische Lösungen (z. B. verbindliche unternehmensinterne Vorschriften), mit denen sich spürbare Fortschritte in Richtung praxisnaher Gewährleistung des Schutzes für natürliche Personen erzielen lassen.

---

[1] Länder, die nicht dem Europäischen Wirtschaftsraum (EWR) angehören.

[2] Siehe folgende Vorabkontrollstellungnahmen des EDSB: Betrugsuntersuchungen bei der EIB (2009-0459), Übermittlung von BFT Inspektionsberichten (2011-0615), Einfrieren von Vermögenswerten durch die Kommission (2010-0426), interne und externe Untersuchungen von OLAF (2005-418, 2007-47, 2007-48, 2007-49, 2007-50, 2007-72), Frontex Gemeinsame Rückführungsaktionen (2009-0281), abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/priorchecking/OpinionsPC.

[3] Siehe: Konsultation zur Übermittlung personenbezogener Daten an American Express Corporate Travel SA (AMEX) – EFSA (2009-390), abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Prioritychecks/Consultations/2010/10-12-21_EFSA_AMEX_DE.pdf , Konsultation zur Übermittlung von Daten von EIB-Bediensteten an die OECD (2013-0089), abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Prioritychecks/Consultations/2013/13-03-21_Consultation_EIB_FR.pdf

[4] Spezifische Leitlinien zu Cloud Computing und mobilen Geräten sind derzeit in Vorbereitung.

[5] Für detailliertere Kommentare des EDSB siehe: Stellungnahme des Europäischen Datenschutzbeauftragten vom 7. März 2012 zum Datenschutzreformpaket („EDSB-Stellungnahme zum Reformpaket“), abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf)

[6] Siehe Artikel 40 und 41 des Vorschlags.

[7] Siehe Artikel 42 und 43 des Vorschlags.

Die derzeitige in der Verordnung niedergelegte Regelung ist zwar durch die Überarbeitung des Datenschutzregelwerks nicht unmittelbar betroffen, doch hat der EDSB zumindest eine Änderung angeregt, die dann gleichzeitig mit den anderen Vorschriften in Kraft treten sollte.[8] In den kommenden Jahren wird daher nach wie vor die Verordnung die Vorschriften für internationale Übermittlungen vorgeben. Bei Bedarf werden wir in diesem Papier jedoch vorgeschlagene Entwicklungen betrachten.

So dürfte beispielsweise der in den bestehenden Vorschriften implizit vorhandene Grundsatz der Rechenschaftspflicht im neuen Datenschutzregelwerk vermutlich gestärkt werden. In Anbetracht dessen wenden wir im Einklang mit unserer Leitlinie zu Konsultationen im Bereich Aufsicht und Durchsetzung bei unserer Beratung von Organen und Einrichtungen bezüglich ihrer Verpflichtungen diesen Grundsatz bereits an.[9]

Wenn also ein Organ oder eine Einrichtung der EU personenbezogene Daten gemäß Artikel 9 der Verordnung übermittelt, sollte gewährleistet sein, dass es/sie seinen/ihren Pflichten aus der Verordnung nachkommt, bevor die Übermittlung oder Reihe von Übermittlungen stattfindet. In derartigen Fällen sollten die für die Verarbeitung Verantwortlichen ihre DSB von Anfang an konsultieren und um Rat fragen. Inzwischen hat der EDSB Hinweise zur Auslegung und Anwendung der bestehenden Vorschriften formuliert[10], die für die Verarbeitung Verantwortlichen in einer Reihe von Fällen an die Hand gegeben wurden. Das vorliegende Papier baut auf diesen Erfahrungen auf und soll für die Verarbeitung Verantwortlichen das Instrumentarium bieten, mit dem sie die für sie beste Lösung beurteilen können.

2. Allgemeiner Überblick

Wie nachstehend noch näher erörtert, enthält Artikel 9 der Verordnung den allgemeinen „Grundsatz des angemessenen Schutzes“. Dabei handelt es sich um den Hauptgrundsatz für den internationalen Datenverkehr, der auch in den Artikeln 25 und 26 der Richtlinie verankert ist. In Artikel 9 ist ferner festgelegt, wie das von einem Drittland oder einer internationalen Organisation gebotene Schutzniveau beurteilt werden sollte, welche Informationspflichten gegenüber der Kommission und/oder dem EDSB von dem für die Verarbeitung Verantwortlichen zu erfüllen sind und welche Ausnahmen von dem allgemeinen Grundsatz gelten.[11]

Der Grundsatz des angemessenen Schutzes verlangt, dass das Grundrecht auf Datenschutz auch dann gewahrt wird, wenn personenbezogene Daten an eine Partei übermittelt werden, die nicht in den Anwendungsbereich der Verordnung und der Richtlinie fällt. Auch wenn es bei den Grundsätzen und in der Praxis des Datenschutzes weltweit immer mehr Kohärenz und Konvergenz gibt, kann doch nicht

[8] Stellungnahme des EDSB zum Reformpaket (siehe Fußnote 5).

[9] Leitlinie zu Konsultationen in den Bereichen Überwachung und Durchsetzung, 23. November 2012, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/12-11-23_Policy_on_Consultations_DE.pdf

[10] Siehe die Liste der beim EDSB eingegangenen Konsultationen in Anhang 3.

[11] Siehe den vollständigen Wortlaut von Artikel 9 in Anhang 1.

in allen Fällen von einer vollständigen Angemessenheit ausgegangen werden. In vielen Fällen liegt das von Drittländern und internationalen Organisationen gebotene Datenschutzniveau deutlich unter dem der Europäischen Union oder ist gar nicht vorhanden. Bevor eine Übermittlung an ein Drittland oder eine internationale Organisation durchgeführt wird, sollte der für die Verarbeitung Verantwortliche daher den betroffenen Personen angemessenen Schutz gewährleisten.

Gemäß Artikel 9 Absatz 1 ist ein Austausch personenbezogener Daten mit Drittländern und internationalen Organisationen zulässig, wenn ein angemessenes Schutzniveau gewährleistet ist. Übermittlungen sind ferner zulässig, wenn der für die Verarbeitung Verantwortliche Vorkehrungen trifft, die angemessene Garantien bieten (Artikel 9 Absatz 7). Schließlich sind Übermittlungen ohne besondere Garantien unter außergewöhnlichen Umständen zulässig, sofern eine spezifische Ausnahme greift (Artikel 9 Absatz 6).[12]

3. Vorab zu klärende Punkte

3.1. Begriff der „Übermittlung personenbezogener Daten“

Weder in der Richtlinie noch in der Verordnung findet sich eine Bestimmung des Begriffs „Übermittlung personenbezogener Daten“. In der Verordnung wird der Begriff auch in anderen Bestimmungen verwendet, die sich mit dem Datenverkehr innerhalb oder zwischen Organen oder Einrichtungen der EU und mit der Übermittlung an Empfänger in der EU befassen, die ebenfalls der Richtlinie unterworfen sind.[13] Unter diesen Umständen kann zunächst einmal davon ausgegangen werden, dass der Begriff in seiner natürlichen Bedeutung verwendet wird und Daten bezeichnet, die sich zwischen verschiedenen Verwendern „bewegen“ oder „bewegen“ dürfen. In der Wirklichkeit ist die Angelegenheit jedoch nicht immer so klar.

Der EDSB hat gefordert, im Zuge der Datenschutzreform eine Definition dieses Begriffs zu erarbeiten[14], da dieser sich in bestimmten Fällen als problematisch erwiesen hat, deren Lösung bisher dem Gerichtshof oder dem Gesetzgeber überlassen blieb.

Das einzige Urteil, in dem der Gerichtshof den Begriff „Übermittlung“ erörtert hat, erging in der Rechtssache Lindqvist[15] und hat einen nur begrenzten Anwendungsbereich. Der Gerichtshof geht dort unter anderem der Frage nach, ob *allein die Tatsache*, dass personenbezogene Daten in eine Internetseite einstellt werden, die bei einem Host-Service-Provider gespeichert ist, der in demselben Mitgliedstaat (wie Frau Lindqvist) oder in einem anderen Mitgliedstaat ansässig ist, eine Übermittlung im Sinne von Artikel 25 der Richtlinie darstellt. Der Gerichtshof befand (Randnr. 71), dass *„(…) keine „Übermittlung von Daten in ein Drittland“ im Sinne von Artikel 25 der Richtlinie 95/46 vorliegt, wenn eine sich in einem Mitgliedstaat aufhaltende Person in eine Internetseite, die bei ihrem in demselben*

[12] Siehe eine kurze Checkliste in Anhang 2.
[13] Siehe die Artikel 7 und 8 der Verordnung.
[14] Stellungnahme des EDSB zum Reformpaket (Fußnote 5), S. 18, Punkt 108.
[15] Rechtssache C-101/01, *Lindqvist*, Slg. 2003, S. I-12971.

oder einem anderen Mitgliedstaat ansässigen Host-Service-Provider gespeichert ist, personenbezogene Daten aufnimmt und diese damit jeder Person, die eine Verbindung zum Internet herstellt, einschließlich Personen in Drittländern, zugänglich macht".

Diese Schlussfolgerung des Gerichtshofs muss vor dem Hintergrund der Rechtssache betrachtet werden. Der Gerichtshof kam unter Berücksichtigung der „*Umstände wie denen des Ausgangsverfahrens*" zu seiner Bewertung. Er äußerte sich nicht zu anderen Arten von Verarbeitung (anders beispielsweise von ihrem Umfang, ihrem Zweck, ihrem Ziel, ihren Risiken usw. her), sondern nur zu der unter den Umständen des Ausgangsverfahrens erfolgenden Einstellung personenbezogener Daten in eine Internetseite, die im Übrigen einem rein lokalen Zweck diente (Frau Lindqvist wollte lediglich die anderen Mitglieder ihrer Gemeinde informieren). Die Schlussfolgerung des Gerichtshofs zum Begriff „Übermittlung" sollte daher nicht einfach und automatisch auf Fälle angewandt werden, die völlig andere Merkmale aufweisen.

Es kommt natürlich auch vor, dass personenbezogene Daten an einen Empfänger in einem Drittland in der *Absicht* übermittelt werden, diese Informationen dem Empfänger zur Verfügung zu stellen. Desgleichen kann es Fälle geben, in denen die Veröffentlichung personenbezogener Daten im Internet mit dem *Ziel* erfolgt, die breite Öffentlichkeit zu informieren, und zwar nicht nur lokal oder innerhalb der EU, sondern auch in Drittländern; dies trifft beispielsweise auf das online zugängliche Personalverzeichnis der Kommission zu. Diese Fälle mögen unterschiedlich behandelt werden, wie wir noch sehen werden[16], doch ist ihnen gemeinsam, dass bestimmte Informationen *absichtlich* Empfängern in einem Drittland bereitgestellt werden und dass sie beide über das reine Hochladen dieser Informationen für begrenzte Zwecke hinausgehen.

Vor diesem Hintergrund und obwohl es noch keine offizielle Definition des Begriffs „Übermittlung personenbezogener Daten" gibt, sollten für die Verarbeitung Verantwortliche bedenken, dass dieser Begriff in der Regel die folgenden Elemente beinhaltet: *Mitteilung, Weitergabe oder sonstige Bereitstellung personenbezogener Daten, vorgenommen mit dem Wissen oder in der Absicht eines der Verordnung unterworfenen Übermittlers, dass der/die Empfänger Zugriff darauf hat/haben*.[17]

Der Begriff würde daher sowohl „beabsichtigte Übermittlungen" als auch den „zugelassenen Zugriff" auf die Daten durch den/die Empfänger abdecken.[18] Aufgrund der Bedingungen „Wissen" und „Absicht" wären Fälle des ungesetzlichen Zugriffs (z. B. Hacking) ausgeschlossen. Auf der anderen Seite würde allein die Tatsache, dass Informationen auf dem Weg zu ihrem Bestimmungsort aufgrund der Struktur von

[16] Siehe weiter unten ab Punkt 6.

[17] Diese Elemente gelten nicht nur für Übermittlungen an Drittländer und internationale Organisationen (Artikel 9), sondern auch für Übermittlungen innerhalb oder zwischen Organen oder Einrichtungen der Union (Artikel 7) und für Übermittlungen an Empfänger, die der Richtlinie unterworfen sind (Artikel 8).

[18] Push- und Pull-Systeme: Dies sind zwei unterschiedliche Methoden der internetgestützten Kommunikation. In einem „Push"-System geht die Kommunikation von dem Veröffentlichenden oder Zentralserver (für die Verarbeitung Verantwortlicher) aus. Dies könnte man als „beabsichtigte Übermittlung" personenbezogener Daten bezeichnen. In einem „Pull"-System geht das Ersuchen um die Übermittlung von Informationen vom Empfänger aus. Dies könnte man als „zugelassenen Zugriff" auf personenbezogene Daten bezeichnen.

Netzen internationale Grenzen überschreiten (könnten), nicht automatisch die Anwendung des Begriffs auslösen.

Internationale Übermittlungen personenbezogener Daten können also in verschiedenen (physischen und digitalen) Umgebungen erfolgen, wie z. B.:

- Versand personenbezogener Daten durch ein Organ oder eine Einrichtung der EU (für die Verarbeitung Verantwortlicher) an einen Empfänger außerhalb der EU per Post oder E-Mail;

- „Pushen" von Daten aus der Datenbank eines für die Verarbeitung Verantwortlichen in der EU an einen Empfänger außerhalb der EU;

- Gewährung des Zugriffs auf eine Datenbank („Pullen") eines für die Verarbeitung Verantwortlichen in der EU für einen Empfänger außerhalb der EU;

- direkte Online-Erhebung von Daten einer natürlichen Person in der EU durch einen Auftragsverarbeiter außerhalb der EU im Namen eines für die Verarbeitung Verantwortlichen in der EU;

- Veröffentlichung personenbezogener Daten im Internet durch einen für die Verarbeitung Verantwortlichen in der EU.

Der Begriff „Übermittlung" würde somit auf jeden Fall auch bestimmte in Artikel 2 Buchstabe b der Verordnung erwähnte Verarbeitungsvorgänge umfassen, so z. B. „Weitergabe durch Übermittlung" und „Verbreitung oder jede andere Form der Bereitstellung". Dies bedeutet, dass eine „Übermittlung personenbezogener Daten" nicht nur mit Artikel 9, sondern auch mit anderen relevanten Bestimmungen der Verordnung in Einklang stehen müsste wie den Bestimmungen über Datenqualität und rechtmäßige Verarbeitung (siehe hierzu auch weiter unten Punkt 3.3).

In Anbetracht des Stands der Diskussion über diesen Begriff und die Auswirkungen auf konkrete Fälle wird für die Verarbeitung Verantwortlichen geraten, bei schwerwiegenden Zweifeln den EDSB zu Rate zu ziehen.

3.2. Anwendungsbereich von Artikel 9

Artikel 9 findet Anwendung auf Übermittlungen personenbezogener Daten an Empfänger, die nicht Organe und Einrichtungen der EU und nicht der Richtlinie unterworfen sind. Somit erfasst er nicht Empfänger in Ländern des Europäischen Wirtschaftsraums (ERW)[19], es sei denn, die Übermittlungen erfolgen in Bereichen, die von der Richtlinie ausgenommen sind (früherer zweiter und dritter Pfeiler des EU-Rechts; siehe weiter unten Punkt 7).

Wie bereits kurz erwähnt, enthält die Verordnung noch zwei weitere Bestimmungen im Zusammenhang mit Übermittlungen, nämlich die Artikel 7 und 8. Für beide Bestimmungen gibt es keine Parallelvorschriften in der Richtlinie. Artikel 7 gilt für die Übermittlung personenbezogener Daten innerhalb oder zwischen Organen oder

[19] Die ERW-Länder sind die EU-Mitgliedstaaten sowie Island, Liechtenstein und Norwegen.

Einrichtungen der EU. Ein solcher Fall wäre beispielsweise eine Übermittlung zwischen zwei in Brüssel ansässigen Generaldirektionen der Kommission. Ein weiterer Fall wäre eine Übermittlung zwischen dem Europäischen Auswärtigen Dienst und einer der EU-Delegationen auf der ganzen Welt (auch wenn sich diese Delegationen in Drittländern befinden, gehören sie doch zu den EU-Organen und unterliegen damit der Verordnung). Artikel 8 gilt für Übermittlungen an Empfänger, die nicht Organe oder Einrichtungen der EU sind und die der Richtlinie 95/46/EG unterworfen sind.

Es sei darauf hingewiesen, dass seit der Annahme des Vertrags von Lissabon immer dann, wenn Organe und Einrichtungen der Gemeinschaft erwähnt werden, nunmehr Organe oder Einrichtungen der EU gemeint sind (beispielsweise in Artikel 3). Dies trifft nicht auf die Organe und Einrichtungen zu, für die derzeit eine besondere Datenschutzregelung gilt, wie z. B. Europol und Eurojust (siehe weiter unten Punkt 7).

3.3. Wahrung anderer rechtlicher Bedingungen

Datenübermittlungen gelten als Verarbeitungstätigkeiten und müssen daher gemäß Kapitel II der Verordnung rechtmäßig sein.

In Artikel 5 sind die verschiedenen Voraussetzungen aufgeführt, unter denen personenbezogene Daten verarbeitet werden dürfen. Dies bedeutet, dass der für die Verarbeitung Verantwortliche vor einer Übermittlung prüfen sollte, ob eine der dort genannten rechtlichen Voraussetzungen erfüllt ist. Dabei sind zwei verschiedene Schritte zu absolvieren: a) Die Verarbeitungstätigkeit vor der Übermittlung muss rechtmäßig sein (Erhebung, Speicherung usw.) und b) die eigentliche Übermittlung muss rechtmäßig sein (muss eine angemessene Rechtsgrundlage haben und im Einklang mit dem ursprünglichen Zweck der Verarbeitung stehen).

Darüber hinaus müssen die für die Verarbeitung Verantwortlichen dem Grundsatz der Datenqualität Genüge tun (Artikel 4). Dabei geht es um Anforderungen im Zusammenhang mit Zweckbindung, Datenminimierung, Fristen für die Datenaufbewahrung und sachlicher Richtigkeit der übermittelten Daten.

Darüber hinaus sind noch andere relevante Bestimmungen der Verordnung einzuhalten, wie

- das allgemeine Verbot der Verarbeitung besonderer Datenkategorien, sofern keine Ausnahme gilt;
- die Verpflichtung zur Information der betroffenen Person über die Empfänger;
- die Wahrung der Rechte der betroffenen Person in allen Phasen der Übermittlung, also ihres Rechts auf Auskunft, Berichtigung und Löschung vor Durchführung der Übermittlung;
- die Sicherheit der Verarbeitung (Bewertung des mit der Übermittlung verbundenen Risikos und Ergreifung angemessener Sicherheits- und organisatorischer Vorkehrungen);
- die Klärung der Frage, ob eine Vorabkontrolle erforderlich ist (siehe weiter unten Punkt 8).

3.4. Überwachung von Übermittlungen als bewährte Vorgehensweise

Generell dürfte es sich bewähren, wenn die Organe und Einrichtungen der EU ein internes Überwachungs- und Registrierungssystem für Übermittlungen gemäß Artikel 9 einrichten.[20] Es sollte nicht nur Übermittlungen nach Feststellung der Angemessenheit erfassen, sondern auch, was noch wichtiger wäre, Übermittlungen aufgrund von Ausnahmen (Artikel 9 Absätze 6 und 7). Siehe weiter unten Punkt 6. Auf diese Weise lässt sich die interne Verwaltung internationaler Übermittlungen unterstützen und die Rechenschaftspflicht und die Einhaltung der Verordnung wirksam gewährleisten.

4. Angemessener Schutz

4.1. Anwendbarkeit

Gemäß Artikel 9 Absatz 1 der Verordnung werden *„personenbezogene Daten […] an Empfänger, die nicht Organe oder Einrichtungen der Gemeinschaft sind und die nicht den aufgrund der Richtlinie 95/46/EG erlassenen Rechtsvorschriften unterliegen, nur übermittelt, wenn ein angemessenes Schutzniveau in dem Land des Empfängers oder innerhalb der empfangenden internationalen Organisation gewährleistet ist und diese Übermittlung ausschließlich die Wahrnehmung von Aufgaben ermöglichen soll, die in die Zuständigkeit des für die Verarbeitung Verantwortlichen fallen"*.[21]

Dieser allgemeine Grundsatz besagt, dass personenbezogene Daten nur dann von einem Organ oder einer Einrichtung der EU an ein Drittland oder eine internationale Organisation[22] übermittelt werden dürfen, wenn dort ein angemessenes Schutzniveau gewährleistet ist. Weiter heißt es in dieser Bestimmung, dass die Übermittlung „*ausschließlich die Wahrnehmung von Aufgaben ermöglichen soll, die in die Zuständigkeit des für die Verarbeitung Verantwortlichen fallen*". Dieser Ansatz ist restriktiver als der der Richtlinie und stützt sich auf die Eigenart der der Verordnung unterliegenden öffentlichen Organe und Einrichtungen, denen es nicht gestattet ist, außerhalb ihres Zuständigkeitsbereichs tätig zu werden.

Besteht in dem Land des Empfängers kein angemessenes Datenschutzniveau, dürfen Übermittlungen im Übrigen nur dann vorgenommen werden, wenn der für die Verarbeitung Verantwortliche angemessene Garantien vorsieht (siehe weiter unten Punkt 6.2) oder wenn eine der in Artikel 9 Absatz 6 aufgeführten Ausnahmen greift (siehe weiter unten Punkt 6.1).

---

[20] Bei einigen Organen oder Einrichtungen könnte es ratsam sein, ein zentrales Register der Übermittlungen zu führen. So hat der EDSB beispielsweise OLAF in Anbetracht der Sensibilität der Daten und des Verarbeitungszwecks geraten, ein zentrales Übermittlungsregister zu führen (Arbeitsunterlage *OLAF Operations: International Transfers of Personal Data*, 13. Februar 2006).

[21] Siehe ferner Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60, Artikel 13 Absatz 1 Buchstabe d.

[22] In den Artikeln 25 und 26 der Richtlinie werden nur Übermittlungen an Drittländer, nicht jedoch Übermittlungen an internationale Organisationen erwähnt.

4.2. Begriff der „Angemessenheit“

In Artikel 9 ist nicht definiert, was unter „Angemessenheit“ oder „angemessenem Schutzniveau“ zu verstehen ist. In Artikel 9 Absatz 2 finden sich jedoch ein paar Elemente, die bei der Beurteilung der „Angemessenheit“ berücksichtigt werden sollten. Dort heißt es, dass das von einem Drittland oder einer internationalen Organisation gebotene Schutzniveau „*anhand aller Umstände einer Datenübermittlung oder einer Reihe von Datenübermittlungen*“ zu beurteilen ist. Weiter wird dort gefordert: *„(…) Besonders zu berücksichtigen sind dabei die Art der Daten, der Zweck und die Dauer des geplanten Verarbeitungsvorgangs oder der geplanten Verarbeitungsvorgänge, das Drittland oder die internationale Organisation der Endbestimmung, die in dem betreffenden Drittland oder der betreffenden internationalen Organisation geltenden allgemeinen und sektoriellen Rechtsvorschriften sowie die in diesem Land oder in dieser internationalen Organisation geltenden Standesregeln und Sicherheitsmaßnahmen*“. Diese Aufzählung ist nicht erschöpfend; je nach Lage des Falls können noch weitere Elemente von Belang sein.

Die Beurteilung der Angemessenheit erfordert daher eine Evaluierung oder „Risikobewertung“ des geplanten Verarbeitungsvorgangs an sich (z. B. Art der Daten, Zweck und Dauer des/der Verarbeitungsvorgangs/Verarbeitungsvorgänge) und der für den Empfänger geltenden rechtlichen Regelungen oder Maßnahmen (z. B. allgemeine und sektorielle Rechtsvorschriften, Standesregeln und Sicherheitsmaßnahmen).[23] „Angemessenheit“ ist ein funktionales Konzept; dies bedeutet, dass bei jeder Beurteilung der Angemessenheit die an der Endbestimmung geltenden Vorschriften und die Möglichkeiten zu bedenken sind, deren wirksame Anwendung zu gewährleisten. Diese Grundsätze bilden den „Kern“ des Datenschutzes und sind von der Artikel 29-Datenschutzgruppe folgendermaßen beschrieben worden[24]:

„1) **Der Grundsatz der Beschränkung der Zweckbestimmung** – Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie (*wie auch in Artikel 20 der Verordnung*) aufgeführten Gründe notwendigen Fälle.

2) **Der Grundsatz der Datenqualität und -verhältnismäßigkeit** – Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Die Daten sollten

[23] Eine Bestimmung dieser Risiken dürfte vor allem in den Fällen von Bedeutung sein, in denen keine Angemessenheitsentscheidung ergangen ist und in denen der für die Verarbeitung Verantwortliche die Angemessenheit beurteilt oder angemessene Garantien bietet. Je größer das Risiko, desto strenger das Erfordernis einer Analyse des Schutzes.

[24] Siehe: Artikel 29-Datenschutzgruppe, Arbeitsunterlage *Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU*, (WP 12), angenommen am 24. Juli 1998, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf.
Die Artikel 29-Datenschutzgruppe hat bei der Ermittlung der in der Rechtsordnung des Empfängers zu bewertenden Elemente eine aktive Rolle gespielt. Dieses Dokument war die Grundlage aller Angemessenheitsentscheidungen der Europäischen Kommission sowie von Instrumenten, die bei fehlender Angemessenheit „angemessene Garantien“ bieten, wie Standardvertragsklauseln und verbindliche unternehmensinterne Vorschriften.

angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv sein.

3) **Der Grundsatz der Transparenz** – Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie (*bzw. Artikel 12 Absatz 2 und Artikel 20 der Verordnung*) möglich.

4) **Der Grundsatz der Sicherheit** – Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5) **Das Recht auf Zugriff, Berichtigung und Widerspruch –** Die betroffene Person muss das Recht haben, eine Kopie[25] aller sie betreffenden Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten haben mit Artikel 13 der Richtlinie (*bzw. Artikel 20 der Verordnung*) im Einklang zu stehen.

6) **Beschränkungen der Weiterübermittlung in andere Drittländer** – Weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland (d. h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen von diesen Rechten haben mit Artikel 26 Absatz 1 der Richtlinie (*bzw. Artikel 9 Absatz 6 der Verordnung*) im Einklang zu stehen."

Außerdem müssen verfahrensrechtliche Mechanismen / Durchsetzungsmechanismen gewährleistet sein. Daher verfolgt ein Datenschutzsystem oder ein gut entwickeltes Konzept für den Schutz der Privatsphäre im Wesentlichen drei Ziele:

„1) Gewährleistung einer **guten Befolgungsrate** der Vorschriften. (Kein System kann eine 100 %ige Einhaltung garantieren, aber einige sind besser als andere). Ein gutes System zeichnet sich im Allgemeinen dadurch aus, dass sich die für die Verarbeitung Verantwortlichen ihrer Pflichten und die betroffenen Personen ihrer Rechte und der Mittel für deren Wahrnehmung sehr stark bewusst sind. Die Existenz wirksamer, abschreckender Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicherzustellen; ebenso relevant sind natürlich auch Systeme der direkten Überprüfung durch Behörden, Wirtschaftsprüfer oder unabhängige Datenschutzbeauftragte.

[25] Gemäß Artikel 13 der Verordnung *kann* das Recht auf Auskunft das Recht auf eine Kopie der Daten beinhalten (diese Fußnote findet sich in WP 12 nicht).

2) **Unterstützung und Hilfe für einzelne betroffene Personen** bei der Wahrnehmung ihrer Rechte. Der Einzelne muss seine Rechte rasch und wirksam, ohne überhöhte Kosten durchsetzen können. Dafür muss es eine Art institutionellen Mechanismus geben, der eine unabhängige Prüfung von Beschwerden ermöglicht.

3) Gewährleistung **angemessener Entschädigung** für die geschädigte Partei bei Verstoß gegen die Bestimmungen. Für dieses Schlüsselelement muss ein System unabhängiger Schlichtung vorhanden sein, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht."

Wir fassen zusammen: In einem angemessenen System werden diese Grundsätze inhaltlich wie in der praktischen Umsetzung und bei Bedarf auch in der Durchsetzung anerkannt. Gewährleistet werden kann dies nicht nur durch die Existenz von Rechtsvorschriften und Verfahren, einschließlich Justiz- oder Datenschutzbehörden mit Abhilfebefugnissen, mit denen im Interesse der betroffenen Personen die Einhaltung der Vorschriften wiederhergestellt werden kann, sondern auch durch andere „Maßnahmen", die ein sichereres Datenschutzumfeld schaffen, wie z. B. Verhaltenskodizes, interne Vorschriften, Sicherheitskontrollen und Auditmechanismen, sofern alle oben erwähnten wesentlichen Elemente gegeben sind.

5. Beurteilung der Angemessenheit

Die Beurteilung des Schutzniveaus in einem bestimmten Land oder Wirtschaftszweig kann auf verschiedenen Ebenen und mit unterschiedlichen rechtlichen Wirkungen vorgenommen werden, und zwar durch die für die Verarbeitung Verantwortlichen selbst, durch Datenschutzbehörden oder die Europäische Kommission. Im letztgenannten Fall stehen dann am Ende für die Mitgliedstaaten und die Organe und Einrichtungen der EU verbindliche Angemessenheitsentscheidungen (siehe Artikel 25 Absatz 4 und Artikel 25 Absatz 6 der Richtlinie).

Liegt keine verbindliche Entscheidung vor, lässt die Richtlinie unterschiedliche Lösungen zu: Eine Mehrheit von Mitgliedstaaten unterliegt einer zentralen Beurteilung durch eine Datenschutzbehörde, während andere Mitgliedstaaten von den für die Verarbeitung Verantwortlichen zumindest eine Erstbewertung erwarten, wie sie auch in Artikel 9 der Verordnung vorgesehen ist. Das Organ oder die Einrichtung der EU ist somit als für die Verarbeitung Verantwortlicher rechenschaftspflichtig und hat vor der Durchführung einer Datenübermittlung die Angemessenheit zu prüfen. Hierauf wird nachstehend näher eingegangen.

5.1. Angemessenheitsentscheidung der Europäischen Kommission

Artikel 9 Absatz 5 der Verordnung besagt: „*Die Kommission stellt gemäß Artikel 25 Absätze 4 und 6 der Richtlinie 95/46/EG fest, ob ein Drittland oder eine internationale Organisation ein angemessenes Schutzniveau gewährleistet oder nicht, und die Organe und Einrichtungen der Gemeinschaft treffen die erforderlichen Maßnahmen, um den Entscheidungen der Kommission nachzukommen*".

Artikel 25 Absatz 6 der Richtlinie lautet: „*Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner*

innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen, die es (...) eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne von Absatz 2 gewährleistet". Eine Angemessenheitsentscheidung, die gemäß Artikel 25 Absatz 6 angenommen wurde, ist für alle Mitgliedstaaten verbindlich und führt zum „freien Datenverkehr" mit dem betreffenden Drittland. Diese Entscheidungen gelten auch für Organe und Einrichtungen der EU.

Die Europäische Kommission hat bereits eine Reihe von Angemessenheitsentscheidungen angenommen; daher sollten für die Verarbeitung Verantwortliche, die Übermittlungen in ein Drittland vornehmen müssen, zunächst einen Blick auf die Liste der Länder mit angemessenem Schutzniveau werfen[26].

> Zum Zeitpunkt der Abfassung dieses Papiers sind dies folgende Länder: Andorra, Argentinien, Kanada (privater Sektor), Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, US Safe Harbor (bestimmte Tätigkeiten des privaten Sektors) und Uruguay.

Der Anwendungsbereich einer Angemessenheitsentscheidung kann verschieden aussehen. Einige decken die Datenschutzregelungen eines Landes ab (z. B. Argentinien oder Schweiz), während andere nur bestimmte Kategorien der Verarbeitung personenbezogener Daten (z. B. US Safe Harbour, Kanada) erfassen. Dies sollte vor einer Übermittlung berücksichtigt werden.

Zusammenfassend gilt also: Ist das Schutzniveau beim Empfänger „angemessen", kann ein freier Verkehr personenbezogener Daten stattfinden und muss der für die Verarbeitung Verantwortliche bezüglich der Datenübermittlung keine weiteren Maßnahmen ergreifen, sofern alle anderen Aspekte der Verordnung eingehalten werden.

5.2. Beurteilung der Angemessenheit durch den für die Verarbeitung Verantwortlichen

Liegt keine Angemessenheitsentscheidung der Kommission vor, sollte der für die Verarbeitung Verantwortliche grundsätzlich das betreffende Datenschutzsystem (Rechtsvorschriften und andere Maßnahmen) unter Berücksichtigung der Gegebenheiten des Einzelfalls auf seine Angemessenheit prüfen. Dabei sollte er sich auf die spezifischen Merkmale (Garantien und/oder Risiken) der betreffenden Übermittlung oder Reihe von Übermittlungen konzentrieren. Dazu gehören die Arten von Daten, Zweck und Dauer des geplanten Verarbeitungsvorgangs sowie die Empfänger im Drittland oder der internationalen Organisation der Endbestimmung.

Wie bereits erwähnt, sind bei einer Beurteilung der Angemessenheit sowohl inhaltliche Aspekte als auch die tatsächliche Praxis zu berücksichtigen (objektiver und funktionaler Ansatz). Dies bedeutet, dass die Umsetzung einiger Maßnahmen zu überprüfen ist, bevor mit Sicherheit gesagt werden kann, ob tatsächlich ein

[26] Die Liste der Länder (oder Sektoren innerhalb eines Drittlands, wie z. B. US Safe Harbour), deren Schutzniveau als angemessen gilt, kann von der folgenden Website abgerufen werden: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

angemessenes Schutzniveau gewährleistet ist. Dies ist Sache des für die Verarbeitung Verantwortlichen. In der Praxis wird es jedoch für den für die Verarbeitung Verantwortlichen nicht immer möglich sein, bezüglich eines Drittlands oder einer internationalen Organisation die Angemessenheit vollständig zu beurteilen. In derartigen Fällen sollte der für die Verarbeitung Verantwortliche davon ausgehen, dass das Schutzniveau nicht angemessen ist und andere, nachstehend erörterte Optionen in Erwägung ziehen.

Auf jeden Fall sind diese spezifischen Angemessenheitsbeurteilungen klar von den Angemessenheitsentscheidungen der Kommission zu unterscheiden, weil nämlich Erstere keinen Einfluss auf eine künftige Beurteilung des Datenschutzregelwerks des betreffenden Drittlands oder der betreffenden internationalen Organisation oder auf dessen Angemessenheit durch die Kommission haben. Darüber hinaus sind sie nicht generell gültig.

Mit Blick auf den Grundsatz der Rechenschaftspflicht sollte der für die Verarbeitung Verantwortliche, soweit dies relevant ist, die Schritte sorgfältig dokumentieren, mit denen er Angemessenheit gewährleistet, und eine entsprechende Risikobewertung durchführen.[27]

5.3. Rolle des EDSB bei der Beurteilung der Angemessenheit

- Angemessenheitsentscheidung der Europäischen Kommission

Hat die Kommission eine Angemessenheitsentscheidung erlassen, ist von den für die Verarbeitung Verantwortlichen kein bestimmtes Verfahren einzuhalten und muss der EDSB nicht unterrichtet werden. Im Rahmen unserer Überwachungs- und Aufsichtspflichten und im Einklang mit Artikel 9 Absatz 5 können wir jedoch fallweise beschließen, von für die Verarbeitung Verantwortlichen Informationen anzufordern.

- Beurteilung der Angemessenheit durch den für die Verarbeitung Verantwortlichen

Jede von dem für die Verarbeitung Verantwortlichen vorgenommene Analyse sollte genau dokumentiert und dem EDSB auf Verlangen vorgelegt werden.

Vor dem Hintergrund der Leitlinie zu Konsultationen im Bereich Aufsicht und Durchsetzung sollte der DSB des Organs oder der Einrichtung der EU stets konsultiert und in die Analyse einbezogen werden. Darüber hinaus sind die für die Verarbeitung Verantwortlichen aufgefordert, den EDSB zu konsultieren, wenn die Angelegenheit a) eine gewisse Neuheit oder Komplexität aufweist (bezüglich der der DSB oder das

[27] Hat die Regierung oder die zuständige Behörde des Drittlands Erläuterungen und/oder Zusicherungen bezüglich der Auslegung und Anwendung ihres verbindlichen Rechts oder nicht verbindlicher Vorgaben vorgelegt, kann dies entscheidenden Einfluss auf die Beurteilung der Angemessenheit haben. In der Beurteilung muss jedoch darauf hingewiesen werden, dass sie sich auf diese Erläuterungen und Zusicherungen stützt, und dass sie daher nur gilt, wenn diese eingehalten werden.

Organ echte Zweifel hegen) oder b) sich eindeutig auf die Rechte der betroffenen Person auswirkt (aufgrund der mit der Verarbeitung verbundenen Risiken usw.).[28]

6. Abweichungen

Selbst wenn das empfangende Land oder die empfangende internationale Organisation kein angemessenes Schutzniveau bietet, können in bestimmten Fällen Übermittlungen vorgenommen werden, wenn eine der in Artikel 9 Absatz 6 und/oder Artikel 9 Absatz 7 der Verordnung dargestellten Situationen gegeben ist.

Die erste Art von Ausnahmen ist in Artikel 9 Absatz 6 in einer begrenzten Auflistung konkreter Situationen geregelt. Trifft eine der dort aufgeführten Situationen zu, sind im Prinzip keine weiteren Maßnahmen erforderlich (siehe weiter unten Punkt 6.1).

Die zweite Art von Ausnahmen ist Gegenstand von Artikel 9 Absatz 7 und umfasst Übermittlungen an einen Empfänger in einem Land oder einer internationalen Organisation, das/die kein angemessenes Schutzniveau gewährleistet. Solche Übermittlungen dürfen nur erfolgen, wenn der für die Verarbeitung Verantwortliche angemessene Garantien bietet (siehe weiter unten Punkt 6.2).

6.1. Spezifische Abweichungen (Ausnahme von Erfordernis der Angemessenheit)

In Artikel 9 Absatz 6 sind verschiedene Situationen dargestellt, in denen eine Übermittlung an eine Endbestimmung mit nicht angemessenem Schutzniveau stattfinden könnte. Diese Möglichkeiten sollten restriktiv ausgelegt und angewandt werden.

Es sei darauf hingewiesen, dass die Nutzung von *Ausnahmen an sich* noch nicht gewährleistet, dass die Rechte der betroffenen Person im empfangenden Drittland oder der empfangenden internationalen Organisation gewahrt sind. Daher wird empfohlen, dass für die Verarbeitung Verantwortliche *„den Lösungen den Vorzug geben sollten, die den Betroffenen garantieren, dass die Grundrechte und Garantien, die sie bei der Verarbeitung ihrer Daten in der EU genießen, auch nach Übermittlung der Daten in ein Drittland gewährleistet sind"*.[29]

Insbesondere Übermittlungen personenbezogener Daten, die als *„wiederholt, massiv oder strukturell"*[30] bezeichnet werden könnten, sollten gemäß einem spezifischen Rechtsrahmen und nicht im Wege von Ausnahmen erfolgen. Die Ausnahmen sollten grundsätzlich nur bei gelegentlichen Übermittlungen zum Einsatz kommen.

Ein Rückgriff auf die Ausnahmen sollte auf jeden Fall niemals dazu führen, dass möglicherweise Grundrechte von betroffenen Personen verletzt werden. Daher sollte in den wenigen Fällen, in denen der Rückgriff auf Ausnahmen gerechtfertigt ist, der für die Verarbeitung Verantwortliche durch Vorkehrungen gewährleisten, dass der Empfänger bestimmte Grundsätze des Datenschutzes einhält. Diese Garantien können

[28] Siehe weiter oben Fußnote 9.
[29] Artikel 29-Datenschutzgruppe *Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995*, WP 114, S. 10.
[30] Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket.

in unterschiedlicher Form abgegeben werden (Absichtserklärung, Briefwechsel usw.). Der Inhalt der Garantien hängt natürlich von den Umständen der Übermittlung ab, beispielsweise von den verschiedenen Risikoniveaus.

Es kann jedoch vorkommen, dass andere Lösungen (wie Angemessenheitsentscheidungen oder angemessene Garantien) unangemessen oder unmöglich sind, und dann muss der für die Verarbeitung Verantwortliche die in Artikel 9 Absatz 6 der Verordnung vorgesehenen Ausnahmen heranziehen. Die in dieser Bestimmung aufgeführten Ausnahmen sind eindeutig als Alternativen gekennzeichnet und lassen sich folgendermaßen darstellen:

a) „[D]ie betroffene Person [hat] ohne jeden Zweifel ihre Einwilligung zu der geplanten Übermittlung gegeben".

> Diese Grundlage wird ebenso wie Artikel 5 Buchstabe d der Verordnung normalerweise von Organen und Einrichtungen der EU nur wenig genutzt. Sie sollten nämlich über spezifische gesetzliche Aufträge zur Verarbeitung personenbezogener Daten verfügen, die nur zur Wahrnehmung von Aufgaben übermittelt werden dürfen, für die der für die Verarbeitung Verantwortliche zuständig ist. In Anbetracht der Definition der „Einwilligung der betroffenen Person" in Artikel 2 Buchstabe h der Verordnung dürfte eine „Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt" nur unter außergewöhnlichen Umständen gegeben sein. Im Beschäftigungsbereich muss außerdem eine „ohne Zwang"[31] gegebene Einwilligung nach strengen Kriterien geschützt werden. Damit muss die Verwendung dieser Option jedoch nicht völlig ausgeschlossen sein. So kann beispielsweise eine betroffene Person selber das Organ oder die Einrichtung der EU um eine Übermittlung bitten (z. B. von Beurteilungsberichten an einen außerhalb der EU ansässigen künftigen Arbeitgeber). Eine Einwilligung „für den konkreten Fall" impliziert, dass sie nicht für mehrere Verarbeitungszwecke gleichzeitig gegeben worden sein kann. Die betroffene Person muss außerdem gemäß Artikel 11 der Verordnung über die Einzelheiten der Übermittlung sowie über etwaige Risiken unterrichtet werden.

b) „[D]ie Übermittlung [ist] für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich".

> Die Organe und Einrichtungen der EU (für die Verarbeitung Verantwortliche) dürfen in den verschiedensten Bereichen Verträge unterzeichnen; dazu gehören Forschungsprojekte, Praktika, Übersetzungen, technische Unterstützung, Beratung, Konferenz- und Werbedienstleistungen. Dazu können auch Verträge mit natürlichen Personen gehören. Übermittlungen an ein Drittland oder eine internationale Organisation können in diesen Fällen für die Erfüllung des Vertrags mit der betroffenen Person erforderlich sein. Im

[31] Artikel 29-Datenschutzgruppe (2001), *Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten*, WP 48, 13. September 2001.

Fall eines Vertrags mit einem Forscher kann eine Übermittlung beispielsweise bei einer Auslandsreise erfolgen, wenn das Organ oder die Einrichtung der EU personenbezogene Informationen an einen in einem Drittland ansässigen Forschungspartner übersendet. Ein weiteres Beispiel wäre eine Überweisung an eine Person auf ein ausländisches Bankkonto. Ähnliche Übermittlungen sind in einer vorvertraglichen Phase zulässig, sofern sie für die Durchführung von Maßnahmen erforderlich sind, die die betroffene Person beantragt hat.

c) „[D]ie Übermittlung [ist] zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person zwischen dem für die Verarbeitung Verantwortlichen und einem Dritten geschlossen wird".

Dies könnte beispielsweise auf Ad hoc-Reiseversicherungsverträge mit in einem Drittland niedergelassenen Privatunternehmen zutreffen. In diesem Fall wäre die betroffene Person keine Vertragspartei, aber der Vertrag würde in ihrem Interesse abgeschlossen (z. B. für einen Beamten auf Dienstreise).

d) „[D]ie Übermittlung [ist] für die Wahrung eines wichtigen öffentlichen Interesses oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben".

Das „wichtige öffentliche Interesse" sollte einem politischen Interesse oder einer gesetzlichen Verpflichtung des Sendenden (Organ oder Einrichtung der EU) und nicht nur des Empfängers entsprechen. Liegt keine spezifische gesetzliche Verpflichtung vor, muss das öffentliche Interesse „wichtig" und die Übermittlung „erforderlich" sein, damit diese Ausnahme greift. Dies sollte fallweise entschieden werden. Der Fall würde beispielsweise eintreten, wenn eine EU-Einrichtung wie OLAF eine Betrugsuntersuchung durchführt und dabei personenbezogene Daten (wie Beweise) an ein Drittland übermitteln muss. In Anbetracht der Schutzwürdigkeit der Daten wäre die Nutzung dieser Ausnahme in derartigen Fällen grundsätzlich auf außergewöhnliche oder gelegentliche Übermittlungen beschränkt. Sollten die Übermittlungen als „wiederholt, massiv oder strukturell" bezeichnet werden können (auch wenn sie zu einer einzigen Untersuchung oder einem einzigen Fall gehören), wäre eine eher systemische und stärker schützende Lösung erforderlich, um unverhältnismäßige Risiken für die Grundrechte und Freiheiten der betroffenen Person zu vermeiden. Dann wäre es angeraten, als Rechtsgrundlage für die Übermittlungen die in Artikel 9 Absatz 7 erwähnten „ausreichenden Garantien" zu nehmen (siehe weiter unten Punkt 6.2).

Der EDSB erhielt eine Konsultation von OLAF zu einer Reihe von Standardklauseln, die für Vereinbarungen über die Verwaltungszusammenarbeit mit Drittlandsbehörden oder internationalen Organisationen verwendet werden sollten. Die Standardklauseln lehnten sich an die von der Kommission angenommenen Standardvertragsklauseln an (siehe weiter unten Punkt 6.2). Nach Auffassung des EDSB sollten diese Standardklauseln grundsätzlich auch für Übermittlungen im Rahmen der Ausnahmen von Artikel 9 Absatz 6 verwendet werden, sobald spezifische Risiken für die betroffenen Personen vorliegen. Dies könnte beispielsweise gegeben sein aufgrund der Art der betroffenen Daten (z. B. sensible Daten),

des Zwecks der Verarbeitung (z. B. Untersuchungen, die in strafrechtliche Ermittlungen münden können) oder des Rechtsrahmens im Bestimmungsland (z. B. überhaupt keine oder nur geringen Schutz bietende Datenschutzvorschriften).

Die Europäische Agentur für Flugsicherheit (EASA) führt Tätigkeiten durch (vor allem im Bereich Zertifizierung), die die Zahlung von Gebühren und Entgelten durch die Antragsteller zur Folge haben. Teile dieser Tätigkeiten können ganz oder teilweise außerhalb des Hoheitsgebiets der Mitgliedstaaten durchgeführt werden. Die dem Antragsteller in Rechnung gestellten Beträge umfassen auch die Reisekosten der Experten. Um die Ausgaben den einzelnen Personen zuordnen zu können, bitten die Antragsteller die EASA um die Namen der Experten und die Reisedaten. Da die Erbringung dieser Dienstleistungen zu den Kerntätigkeiten der EASA gehört, sollten nach Auffassung des EDSB diese Datenübermittlungen als für das Funktionieren dieser Einrichtung erforderlich betrachtet und damit als Ausnahme gemäß Artikel 9 Absatz 6 Buchstabe d behandelt werden. Wird jedoch eine Ausnahme angewandt, sind Garantien nicht zwangsläufig gewährleistet. Daher empfiehlt der EDSB die Aufnahme einer Klausel, der zufolge der Empfänger a) gesetzlich zur Anforderung dieser Daten befugt ist und b) die Daten nur für die Zwecke verwenden wird, für die sie übermittelt wurden. [32]

Die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht ist ein weiterer Anlass für eine Ausnahme. Diese könnte z. B. erforderlich sein, wenn in einem Drittland ein Gerichtsverfahren läuft und von einem Organ oder einer Einrichtung der EU Beweismittel angefordert werden, die personenbezogene Daten enthalten. Der für die Verarbeitung Verantwortliche muss in der Lage sein, die Notwendigkeit der Übermittlung nachzuweisen.

e) „[D]ie Übermittlung [ist] für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich“.

Diese Ausnahme würde beispielsweise greifen, wenn ein Beamter während einer Dienstreise einen Unfall erleidet und ein Krankenhaus in einem Drittland den ärztlichen Dienst des EU-Organs oder EU-Einrichtung um für die Versorgung des Beamten erforderliche medizinische Daten bittet. Der für die Verarbeitung Verantwortliche muss in der Lage sein, die Notwendigkeit der Übermittlung nachzuweisen.

[32] Siehe beispielsweise das Schreiben des EDSB vom 4. Oktober 2010 an den Datenschutzbeauftragten der Europäischen Agentur für Flugsicherheit zu internationalen Übermittlungen, abrufbar unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-10-04_Letter_DPO_EASA_EN.pdf

Das Europäische Parlament (EP) unterhält eine Datenbank, das sogenannte „Security Support System“, das in medizinischen Notfällen Unterstützung bei Dienstreisen ins Ausland leistet. Dazu kann auch die Übermittlung von Daten an Gesundheitsdienste in einem Drittland gehören. Die verarbeiteten personenbezogenen Daten umfassen unter anderem medizinische Informationen (bei einem Notfall, wenn also der Teilnehmer bewusstlos aufgefunden wird, z. B. die von ihm benötigten Medikamente, Angaben zu Allergien, der Blutgruppe). Nach Auffassung des EDSB fällt diese Verarbeitungstätigkeit unter Artikel 9 Absatz 6 Buchstabe e (sowie unter Artikel 9 Absatz 6 Buchstabe a, wenn man berücksichtigt, dass die betroffene Person die Angaben freiwillig gemacht hat).[33]

f) „[D]ie Übermittlung [erfolgt] aus einem Register, das gemäß dem Gemeinschaftsrecht zur Unterrichtung der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht [...]“.

Dies träfe beispielsweise auf einen außerhalb der EU gestellten Antrag eines EU-Bürgers auf Einsichtnahme in ein von einem Organ oder einer Einrichtung der EU geführtes öffentliches Register zu.[34] Ganz allgemein würde dies auch für die Veröffentlichung bestimmter personenbezogener Daten im Internet gelten, die von der Öffentlichkeit abgerufen werden können, wie das Handbuch der Kommissionsdienststellen. In diesem Fall sollte im Mittelpunkt der Analyse nicht der Begriff „Übermittlung“ stehen, sondern die Frage, ob die Veröffentlichung personenbezogener Daten rechtmäßig und verhältnismäßig ist.

6.2. Angemessene Garantien

Wie bereits festgestellt, kommt es vor, dass in dem Drittland oder der internationalen Organisation der Endbestimmung kein angemessenes Schutzniveau gewährleistet oder ein solches zumindest zweifelhaft ist. In einigen dieser Fälle dürfen möglicherweise keine Ausnahmen angewandt werden. Dann sollte der für die Verarbeitung Verantwortliche gemäß Artikel 9 Absatz 7 der Verordnung Garantien vorsehen, die den Schutz personenbezogener Daten gewährleisten.

Der Begriff „angemessene Garantien“ ist weder in der Richtlinie noch in der Verordnung definiert. Unter „angemessenen Garantien“ sollten daher Datenschutzgarantien verstanden werden, die für eine konkrete Situation geschaffen wurden und die es in der Rechtsordnung des Empfängers noch nicht gibt. Typische Beispiele angemessener Garantien sind die von der Kommission angenommenen

[33] Siehe: Vorabkontrollstellungnahme des EDSB vom 29. September 2009 (Fall 2009-0225) zum „Security Support System“ des Europäischen Parlaments.

[34] Artikel 2 Absatz 1 der Verordnung (EG) Nr. 1049/2001 lautet: „Jeder Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder Sitz in einem Mitgliedstaat hat vorbehaltlich der in dieser Verordnung festgelegten Grundsätze, Bedingungen und Einschränkungen ein Recht auf Zugang zu Dokumenten der Organe.“

Standardvertragsklauseln[35] oder verbindliche unternehmensinterne Vorschriften[36]. Mit diesen Instrumenten soll der Schutz hergestellt werden, der am Bestimmungsort der Daten fehlt.

6.2.1. Inhalt der angemessenen Garantien

Auch wenn in Artikel 9 Absatz 7 nicht genau ausgeführt wird, welche Garantien als „angemessen" bzw. „ausreichend" gelten würden, sollten die weiter oben unter Punkt 4.2 beschriebenen Angemessenheitselemente sorgfältig in Erwägung gezogen werden. Jedes Instrument, das als „angemessene Garantie" dienen soll, sollte eindeutig eine Beschreibung der vom Importeur (Empfänger) zu beachtenden Datenschutzgrundsätze sowie der Mittel enthalten, mit denen die für die Wirksamkeit dieses Schutzes erforderlichen Mechanismen gewährleistet werden.

Potenzielle Aufsichts- und Durchsetzungsmechanismen könnten Folgendes enthalten (ein Teil davon ist nur im Privatrecht von Belang – siehe Punkt 6.2.2):

- eine Drittbegünstigtenklausel (damit die betroffene Person in der Lage ist, gegen einen Verstoß gegen die vertraglichen Verpflichtungen des Importeurs oder Exporteurs vorzugehen);
- eine Klarstellung der Pflichten des Exporteurs und des Importeurs (z. B. Verpflichtung zur Beantwortung von Anfragen, Bereitstellung einer Kopie der Klauseln für die betroffene Person, Vorlage zur Überprüfung, Auditing usw.);
- eine Haftungsklausel (in den Standardvertragsklauseln der Kommission sind für die Konstellationen für die Verarbeitung Verantwortlicher/für die Verarbeitung Verantwortlicher bzw. für die Verarbeitung Verantwortlicher/Auftragsverarbeiter verschiedene Lösungen vorgesehen);
- die Verpflichtung des Importeurs zur Meldung von Sicherheitsverstößen an den Exporteur;
- Angaben zu Schlichtung und Gerichtsstand, falls eine Streitigkeit nicht gütlich beigelegt wird;
- Angaben zum anzuwendenden Recht (die Klauseln unterliegen dem Recht des Landes, in dem das Organ oder die Einrichtung der EU seinen/ihren Sitz hat). Diese Art von Klausel wird aufgenommen, um etwaige zivilrechtliche Probleme zwischen den Parteien im Falle einer Durchsetzung zu regeln;
- Informationen über die Zusammenarbeit mit Kontrollbehörden;
- Befugnis der Datenschutzbehörde zur Sperrung oder Aussetzung der Übermittlungen.

[35] Entscheidungen der Kommission 2001/497/EG und 2004/915/EG (zwischen für die Verarbeitung Verantwortlichen) und Entscheidung der Kommission 2002/16/EG (für die Verarbeitung Verantwortlicher an Auftragsverarbeiter). Die Entscheidung 2004/915/EG ist eine überarbeitete Fassung der Entscheidung 2001/497/EG. Die neueste Fassung wurde einer Reihe von Unternehmensverbänden vorgelegt und weist im Vergleich zur ersten einige Unterschiede auf. So enthält sie beispielsweise flexiblere Prüfungsanforderungen und detailliertere Vorschriften über das Recht auf Auskunft (siehe auch die Präambel der Entscheidung 2004/915/EG).

[36] Siehe einen Überblick über verbindliche unternehmensinterne Vorschriften, abrufbar unter: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

Wie bei den Standardvertragsklauseln ist eine Klausel mit Einzelheiten zu den Übertragungen oder Reihen von Übertragungen aufzunehmen. Darin sollten folgende Angaben enthalten sein: Datenkategorien, Zweck, Aufbewahrungsfrist, Details zu den Sicherheitsmaßnahmen, Informationsmechanismen und Ausübung der Rechte der betroffenen Person (Auskunft, Löschung, Widerspruch usw.).

Ist je nach Art der Übermittlung oder des Empfängers ein Vertrag nicht das geeignete Instrument[37] (siehe weiter unten Punkt 6.2.2), müssen andere sowohl für den für die Verarbeitung Verantwortlichen als auch für den Empfänger geltende Zusagen bezüglich Aufsicht und Durchsetzung formuliert werden, wie:

- Direktüberprüfung durch Behörden (z. B. gemeinsame Inspektionen, Audits durch unabhängige Stellen usw.) oder durch den für die Verarbeitung Verantwortlichen (z. B. Audits);
- Verpflichtung zur Benennung eines unabhängigen Datenschutzbeauftragten;
- unabhängige Untersuchung von Beschwerden (Benennung von Kontaktstellen für Anfragen);
- abschreckende Sanktionen, angemessene Entschädigung und Respektierung von Gerichtsentscheidungen;
- eine Klausel über Rechenschaftspflicht (Verpflichtung zur Vorlage von Nachweisen der Einhaltung der Vorschriften beim EDSB, entweder auf Ersuchen oder in regelmäßigen Abständen);
- Transparenz der Garantien (z. B. Veröffentlichung der Instrumente im Internet);
- Kündigung des Abkommens, der Vereinbarung usw. bei Verstößen.

Ist der Empfänger eine öffentliche Stelle, könnte er aufgefordert werden, verbindliche interne Vorschriften zu erlassen, damit die Einhaltung der Zusagen gewährleistet ist.

Außerdem sollte in den Maßnahmen darauf hingewiesen werden, dass der EDSB befugt ist, den Datenverkehr mit Drittländern oder internationalen Organisationen zum Schutz natürlicher Personen in folgenden Fällen zu verbieten oder auszusetzen:

a) wenn das Recht, dem der Datenimporteur unterliegt, von ihm das Abrücken von wichtigen Datenschutzgarantien verlangt, und zwar über die in einer demokratischen Gesellschaft erforderlichen Einschränkungen hinaus, wie sie in Artikel 20 der Verordnung geregelt sind, und wenn sich dieses Verlangen vermutlich stark nachteilig auf die durch die „angemessenen Garantien“ gebotenen Garantien auswirkt[38] oder

[37] Dies dürfte insbesondere für internationale Organisationen gelten, denen es Klauseln über Vorrechte und Befreiungen unmöglich machen, eine direkte Überprüfung durch Behörden, die Einhaltung von Entscheidungen von EU-Gerichten usw. zuzusagen. Bei der Ausarbeitung „angemessener Garantien“ muss dann der Fantasie etwas mehr Raum gelassen werden, da bisher die meisten Instrumente für kommerzielle Umgebungen entwickelt wurden.

[38] Siehe z. B. LIBE-Ausschuss, Untersuchung der massiven elektronischen Überwachung von EU-Bürgern, öffentliche Anhörung, Straßburg, 7. Oktober 2013, Beitrag von Peter Hustinx (EDSB), abrufbar unter: http://www.europarl.europa.eu/document/activities/cont/201310/20131009ATT72609/20131009ATT72609EN.pdf

b) wenn überzeugende Beweise vorliegen oder eine hohe Wahrscheinlichkeit dafür besteht, dass den „angemessenen Garantien“ nicht Genüge getan wird oder werden wird und dass die Fortsetzung der Datenübermittlung den betroffenen Personen einen unmittelbar bevorstehenden schweren Schaden zuzufügen droht.

Diese Maßnahmen erfolgen unbeschadet der Befugnisse des EDSB, gegenüber den beteiligten Organen und Einrichtungen der EU die Einhaltung der Verordnung durchzusetzen (siehe Punkt 9).

6.2.2. Form und Art des/der Instruments/Instrumente mit den angemessenen Garantien

Die Verordnung verlangt von dem Instrument mit den Garantien kein bestimmtes Format. Je nach den Gegebenheiten des Einzelfalls könnten die Garantien beispielsweise Bestandteil eines Vertrags oder einer verbindlichen Erklärung oder Entscheidung sein. Die Art des Rechtsinstruments hängt davon ab, ob das Organ oder die Einrichtung der EU im Bereich des Privatrechts oder des öffentlichen Rechts tätig wird.

Betätigt sich das Organ oder die Einrichtung der EU im Bereich des Privatrechts (z. B. Auslagern der Verwaltung von Dienstreisen, von IT-Dienstleistungen oder Schulungen) und ist der Empfänger der Daten in einem Drittland niedergelassen, dessen Schutzniveau als nicht angemessen erklärt wurde, könnte das Organ oder die Einrichtung der EU mit dem Empfänger einen Vertrags abschließen, der angemessene Garantien vorsieht.[39] Es könnten auch Standardvertragsklauseln der Kommission zum Einsatz kommen. In diesen Fällen muss gegebenenfalls der Verweis auf die Richtlinie durch einen Verweis auf die Verordnung ersetzt werden.[40]

Die Standardvertragsklauseln wurden ursprünglich für die Wirtschaft entworfen, daher finden sie bei Behörden vermutlich eher nur wenig Anwendung. Wird das Organ oder die Einrichtung der EU im Bereich des öffentlichen Rechts tätig (beispielsweise mit dem Aufbau eines Datenaustauschsystems mit Drittländern oder mit der Übermittlung von Strafverfolgungs-/Zolldaten) ist ein Vertrag nicht das geeignete Rechtsinstrument; in diesen Fällen ist eine andere Lösung anzustreben. Damit soll für die Einhaltung der Angemessenheitsgrundsätze gesorgt und darüber hinaus gewährleistet werden, dass die Garantien für den Empfänger bindend sind und wirksam durchgesetzt werden können.

Als erster Schritt sollten die angemessenen Garantien in den Korpus des internationalen Abkommens aufgenommen werden, wenn dieses das Mandat für die Übermittlung enthält (siehe Punkt 8).

---

[39] Neben einem Vertrag sind noch andere Mittel denkbar (so könnte der Empfänger beispielsweise eine Datenschutzerklärung formulieren und eine einseitige Erklärung abgeben, die eine Selbstverpflichtung bedeutet, entweder nach einzelstaatlichem Recht oder mithilfe des Grundsatzes des Vertrauensschutzes).

[40] In den am 15. Juni 2001 angenommenen Standardvertragsklauseln (Entscheidung der Kommission 2001/497/EG) gibt es einen solchen Verweis hauptsächlich in der Klausel 1 Buchstabe a), in der Anlage 2, in den einleitenden Absätzen, im Grundsatz 5, im Grundsatz 6, im Grundsatz 7 und im Grundsatz 9. Die Klausel 10 „Anwendbares Recht“ muss durch einen Verweis auf den Mitgliedstaat ergänzt werden, in dem das Organ oder die Einrichtung der EU seinen/ihren Sitz hat.

In manchen Fällen mag es aufgrund der Art der betreffenden internationalen Organisation oder des betreffenden Rechtsinstruments nicht möglich sein, „angemessene Garantien" in Form eines „verbindlichen Instruments" vorzusehen. In derartigen Fällen sollte eine andere Art von Schutzinstrument erwogen werden. Unter bestimmten außergewöhnlichen Umständen könnte beispielsweise eine Absichtserklärung angemessen sein.

Nach Auffassung des EDSB sollte „*die Möglichkeit der Verwendung nicht rechtverbindlicher Instrumente eindeutig begründet und streng auf Fälle begrenzt werden, in denen die Notwendigkeit des Rückgriffs auf diese Art nicht rechtsverbindlicher Instrumente nachgewiesen ist. […] Die Frage, ob es im öffentlichen Sektor erforderlich ist, auf ein nicht rechtsverbindliches Instrument zurückzugreifen, sollte mit Blick auf den Zweck der Verarbeitung und die Art der Daten einer genauen Prüfung unterzogen werden*".[41] Unabhängig von der Art des Instruments müssen die Maßnahmen ausreichen, um eine angemessene Umsetzung (und bei Bedarf Durchsetzung) der weiter oben unter Punkt 6.2.1 dargestellten Garantien zu gewährleisten.

6.3. Rolle des EDSB bei der Behandlung von Ausnahmen

Artikel 9 Absatz 8 der Verordnung besagt: „*Die Organe und Einrichtungen der Gemeinschaft unterrichten den Europäischen Datenschutzbeauftragten über alle Kategorien von Fällen, in denen sie die Absätze 6 und 7 angewandt haben.*" Wie nachstehend erläutert, findet die Unterrichtung je nach Art des Falls in unterschiedlicher Form statt.

- Ausnahmen gemäß Artikel 9 Absatz 6

Muss ein Organ oder eine Einrichtung der EU auf eine der in Artikel 9 Absatz 6 aufgeführten Ausnahmen zurückgreifen, hat es/sie den EDSB vorab (also bevor die Übermittlung stattfindet) nicht zu unterrichten. Auf Nachfrage sollte der für die Verarbeitung Verantwortliche jedoch dem EDSB im Rahmen von Aufsichts- oder Durchsetzungstätigkeiten Informationen erteilen. Auf jeden Fall sollte der DSB des Organs oder der Einrichtung der EU stets konsultiert und in die Entscheidung über die Anwendung einer Ausnahme einbezogen werden.

Vor dem Hintergrund der Leitlinie zu Konsultationen im Bereich Aufsicht und Durchsetzung wird den für die Verarbeitung Verantwortlichen nahegelegt, unter bestimmten, bereits weiter oben unter Punkt 5.3 (zweiter Anstrich) dargelegten Umständen den EDSB zu Rate zu ziehen.

- Ausnahmen gemäß Artikel 9 Absatz 7

Auch hier ist der DSB des Organs oder der Einrichtung der EU in die Analyse vor der Entscheidung über angemessene Maßnahmen einzubeziehen.

[41] Stellungnahme des EDSB zum Reformpaket (siehe Fußnote 5).

Vorherige Einbeziehung des EDSB: Bei der Entscheidung über eine Hinzuziehung des EDSB sind drei Optionen denkbar:

- Eine vorherige Genehmigung oder Konsultation ist nicht erforderlich, wenn Standardvertragsklauseln zum Einsatz kommen.

- Eine vorherige Genehmigung ist nicht erforderlich, doch könnte eine Konsultation erforderlich sein (Nachprüfen in der Leitlinie des EDSB zu Konsultationen im Bereich Aufsicht und Durchsetzung), wenn beispielsweise ein spezifisches verbindliches Instrument (im Gegensatz zu Standardvertragsklauseln) für den Einsatz entweder im privatrechtlichen der im öffentlich-rechtlichen Bereich von dem Organ oder der Einrichtung der EU entwickelt wird.

- Eine vorherige Genehmigung ist erforderlich in Ausnahmefällen, in denen sich die Übermittlungen auf spezifische Garantien stützen und nicht in einem rechtsverbindlichen Instrument geregelt sind.[42]

Wird ein Instrument mit spezifischen Garantien zur Konsultation und/oder Genehmigung eingereicht, sollte dem EDSB auch eine ausführliche Beschreibung der „Angemessenheits"prüfung zusammen mit den einschlägigen Unterlagen und der Bestätigung der Entwürfe der Instrumente/Maßnahmen vorgelegt werden, mit denen angemessene Garantien gewährleistet werden sollen.

Nach Erhalt der Konsultation oder des Antrags auf Genehmigung prüft der EDSB den Sachverhalt und die rechtlichen Aspekte des Falls und spricht gegebenenfalls Empfehlungen aus. Ist eine Genehmigung erforderlich, können wir eine Genehmigung der Übermittlung oder der Kategorie von Übermittlungen erteilen, sofern wir mit der Angemessenheit der von dem für die Verarbeitung Verantwortlichen gewährleisteten Garantien zufrieden sind. Sind die Garantien unserer Auffassung nach nicht in vollem Umfang angemessen, formulieren wir Empfehlungen, damit der Verordnung Genüge getan wird. Anschließend beginnt eine Follow-up-Phase.

7. Übermittlungen an Empfänger, die nicht der Richtlinie 95/46/EG unterworfen sind

Der Titel von Artikel 9 lautet: „Übermittlung personenbezogener Daten an Empfänger, die nicht Organe oder Einrichtungen der Gemeinschaft sind und die nicht der Richtlinie 95/46/EG unterworfen sind". Diese Empfänger könnten ihren Sitz in den EWR-Ländern haben, führen aber möglicherweise Tätigkeiten aus, die von der Anwendung der Richtlinie ausgenommen sind. Artikel 3 Absatz 2 der Richtlinie besagt nämlich: „*Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten, – die für die Ausübung von Tätigkeiten erfolgt, die nicht in*

[42] Siehe: Entscheidung des EDSB vom 13. Februar 2014 über die gemäß Artikel 9 Absatz 7 der Verordnung (EG) Nr. 45/2001 von OLAF über die Investigative Data Consultation Platform vorgenommenen Übermittlungen personenbezogener Daten, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_EN.pdf

den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich; (...)". Dies träfe beispielsweise auf Übermittlungen an Polizei- oder Justizbehörden zu.

Diese Ausschlüsse waren vor der Annahme des Vertrags von Lissabon erforderlich, stehen jetzt jedoch nicht mit dessen Artikel 16[43] sowie mit Artikel 8 der Charta der Grundrechte der Europäischen Union im Einklang.

Die Mitgliedstaaten unterliegen dem Übereinkommen Nr. 108[44] und haben häufig das Übereinkommen über den Anwendungsbereich der Richtlinie hinaus umgesetzt.[45] Die Richtlinie galt für das ganze Rechtssystem, nicht nur für die Bereiche des früheren ersten Pfeilers. In diesen Fällen konnte davon ausgegangen werden, dass auf einzelstaatlicher Ebene in den Bereichen des früheren zweiten und dritten Pfeilers des EU-Rechts ein „angemessenes" (oder sogar „gleichwertiges") Schutzniveau besteht. Daher können Übermittlungen im Einklang mit Artikel 9 vorgenommen werden, sofern sie Artikel 8 der Verordnung Genüge tun.

Wie bereits erwähnt, haben alle Mitgliedstaaten das Übereinkommen Nr. 108 des Europarats ratifiziert. Durch diese Ratifizierung ist eine Angemessenheitsvermutung entstanden, die in der Praxis mit dem betreffenden Mitgliedstaat überprüft werden muss.[46] Dazu gehört, dass die vom Empfänger verlangten konkreten Maßnahmen überprüft werden.[47] So sind beispielsweise folgende Fragen zu stellen: Hat die Polizei im Einklang mit dem Übereinkommen Nr. 108 spezifische Verpflichtungen bezüglich des Datenschutzes? Ist sie sich ihrer Datenschutzverpflichtungen hinreichend bewusst? Werden bei Verstößen Durchsetzungsmechanismen angewandt? Diese Analyse ist von dem für die Verarbeitung Verantwortlichen zu dokumentieren.
Diese Überprüfung wird auch empfohlen, weil a) das derzeit geltende Datenschutzinstrument der EU, das auf Polizei- und Justizbehörden Anwendung

[43] Siehe Stellungnahme des EDSB vom 14. Januar 2011 zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Gesamtkonzept für den Datenschutz in der Europäischen Union", Punkte 33.
[44] Das Übereinkommen Nr. 108 (Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten) wird derzeit überarbeitet. Nähere Informationen hierzu unter: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp
[45] Siehe „Analyse und Folgenabschätzung der Umsetzung der Richtlinie 95/46/EG in den Mitgliedstaaten", Begleitdokument zum „Ersten Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG)", KOM(2003) 265 endgültig, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.
Siehe ferner Anhang 3 „Datenschutz in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen" der Folgenabschätzung zum Datenschutzreformpaket, SEC(2012) 72 FINAL, Brüssel, 25. Januar 2012, S. 36, abrufbar unter: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf.
[46] Gemäß Artikel 9 Absatz 2 des Übereinkommens Nr. 108 sind Abweichungen von bestimmten Grundsätzen des Instruments zulässig, wenn „die Abweichung durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist: zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten".
[47] Das Übereinkommen Nr. 108 schafft an sich keine subjektiven Rechte für die betroffene Person und ist auch durch den Europäischen Gerichtshof für Menschenrechte nicht unmittelbar durchsetzbar.

findet (Rahmenbeschluss 2008/977), nicht alle Elemente behandelt, die für eine im WP 12 der Artikel 29-Datenschutzgruppe beschriebene Beurteilung der Angemessenheit von Belang sind und auch nicht rein EU-interne Situationen abdeckt[48], und b) es derzeit im EU-Datenschutzrecht keinen Rechtsakt gibt, der die Gemeinsame Außen- und Sicherheitspolitik abdeckt.[49]

Zu Europol und Eurojust ist anzumerken, dass sie nicht der Richtlinie, sondern einer besonderen Datenschutzregelung unterworfen sind.[50] Obwohl beide nunmehr Einrichtungen der EU sind, wäre aus diesem Grund eine Beurteilung der Angemessenheit erforderlich.

Dessen ungeachtet besteht, wie es häufig für Mitgliedstaaten im früheren zweiten und dritten Pfeiler der Fall ist, eine Angemessenheitsvermutung, weil ihr Datenschutzregelwerk im Großen und Ganzen mit der Richtlinie und der Verordnung in Einklang steht. In diesem Fall sollte der für die Verarbeitung Verantwortliche, wie bereits unter Punkt 5.2 erwähnt, eine Beurteilung der Angemessenheit durchführen, um zu kontrollieren, ob die Vorschriften tatsächlich eingehalten werden.

8. EU-Rechtsvorschriften und bilaterale Abkommen

Es kommt vor, dass Organe und/oder Einrichtungen der EU aufgrund von EU-Rechtsvorschriften oder bilateralen Abkommen internationale Übermittlungen vorzunehmen haben und dann als für die Verarbeitung Verantwortliche fungieren.[51] In einem solchen Fall sollte das Instrument idealerweise den geeigneten Rahmen enthalten, mit dem die Einhaltung von Artikel 9 der Verordnung gewährleistet werden kann.

Vor der Annahme eines solchen Rechtsinstruments sollte gemäß Artikel 28 Absatz 2 der Verordnung der EDSB konsultiert werden.
Wurde (im Fall eines bilateralen Abkommens) das Schutzniveau im Bestimmungsland von der Kommission nicht als angemessen bewertet, muss im Instrument angeben

---

[48] Siehe Stellungnahme des EDSB vom 14. Januar 2011 zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Gesamtkonzept für den Datenschutz in der Europäischen Union“, Punkte 35, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_DE.pdf.

[49] Siehe Stellungnahme des EDSB vom 24. November 2010 zur Mitteilung der Kommission an das Europäische Parlament und den Rat über die EU-Politik zur Terrorismusbekämpfung: wichtigste Errungenschaften und künftige Herausforderungen, Punkt 31, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-11-24_EU_counter-terrorism_DE.pdf

[50] Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamtes (Europol) (2009/371/JI), abrufbar unter: https://www.europol.europa.eu/sites/default/files/council_decision.pdf
Bestimmungen der Geschäftsordnung betreffend die Verarbeitung und den Schutz personenbezogener Daten bei Eurojust, ABl. C 68 vom 19.3.2005, S. 1, abrufbar unter: http://eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Data-Protection-Rules-2005-02-24-DE.pdf

[51] Siehe z. B. die mit Drittländern abgeschlossenen Abkommen mit Bestimmungen über die gegenseitige Amtshilfe im Zollbereich (siehe Anhang 3).

sein, ob Angemessenheit besteht (wie bereits unter Punkt 5.2 beschrieben) oder ob „angemessene Garantien“ formuliert wurden (wie bereits unter Punkt 6.2 beschrieben). In letzterem Fall sollten die angemessenen Garantien fester Bestandteil des Instruments sein, beispielsweise in Form eines Anhangs. Hierbei handelt es sich um eine besondere Art von verbindlichem Rechtsinstrument, das sich nicht nur mit dem Inhalt des eigentlichen Abkommens, sondern auch mit den entsprechenden Datenschutzaspekten befasst.

Mitunter ist die betreffende Rechtsvorschrift oder das betreffende bilaterale Abkommen bereits in Kraft getreten. Möglicherweise enthält sie/es jedoch nicht das für die Einhaltung von Artikel 9 geeignete Regelwerk oder nur eine sehr allgemeine Bestimmung, die (selbst wenn sie einige positive Elemente enthält) für eine rechtmäßige Übermittlung nicht ausreicht.[52]

In solchen Fällen ist es üblich, in einer Standardklausel auf Vertraulichkeit und den Schutz personenbezogener Daten hinzuweisen; dies gilt insbesondere für bestimmte Arten bilateraler Abkommen, beispielsweise im Bereich der Zollzusammenarbeit. Diese Klauseln enthalten im Allgemeinen eine Erklärung dahin gehend, dass personenbezogene Daten nur dann ausgetauscht werden dürfen, wenn sich der Empfänger dazu verpflichtet, die Daten auf eine Weise zu schützen, die der der exportierenden Partei zumindest gleichwertig ist.

„Gleichwertigkeit“ ist im Wesentlichen das Ergebnis von Harmonisierung, ebenso wie bei den einzelstaatlichen Datenschutzrechtsvorschriften nach der Umsetzung der Richtlinie. Der Grundsatz der „Angemessenheit“ setzt zwar keinen Harmonisierungsbedarf voraus, doch verlangt er, wie unter Punkt 4.2 beschrieben, die Einhaltung der Kerngrundsätze. Es kann außerdem nicht davon ausgegangen werden, dass das (im Abkommen festgelegte) „gleichwertige“ Schutzniveau in der Praxis tatsächlich gewährleistet ist.

Dies bedeutet, dass die „Gleichwertigkeits“klausel in diesen bilateralen Abkommen an sich noch nicht die Einhaltung von Artikel 9 gewährleistet. Der für die Verarbeitung Verantwortliche sollte in diesen Fällen ergänzende Maßnahmen zur Gewährleistung der Einhaltung von Artikel 9 beschließen, bevor die Übermittlung oder Reihe von Übermittlungen stattfindet.

[52] Siehe z. B. Artikel 17 des Abkommens zwischen der Europäischen Gemeinschaft und der Republik Indien über Zusammenarbeit und gegenseitige Amtshilfe im Zollbereich (ABl. L 304 vom 30.9.2004, S. 25), abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22004A0930(01)&rid=8

9. Aufsicht und Durchsetzung

Wie im Strategiepapier des EDSB „Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001“[53] („Strategiepapier zur Einhaltung der Verordnung“) beschrieben, steht dem EDSB eine Reihe von Aufsichts- und Durchsetzungsinstrumenten zur Verfügung, mit deren Hilfe er seine Aufgabe der Überwachung der Einhaltung der Verordnung wahrnehmen kann. Diese Instrumente können in den in Artikel 9 geschilderten Situationen je nach Art der Verarbeitungstätigkeit (und vor allem des Risikoniveaus) eingesetzt werden.

- Aufsichtsinstrumente

- Vorabkontrollen

In manchen Fällen mag die Art der bei Übermittlungen erfolgenden Verarbeitungsvorgänge unter die in Artikel 27 Absatz 2 der Verordnung niedergelegten Kriterien fallen. Dann müsste der für die Verarbeitung Verantwortliche beim EDSB eine Meldung zur Vorabkontrolle einreichen, in der er alle relevanten Aspekte der Verarbeitung darstellt.

In diesen Fällen kann eine Vorabkontrolle unabhängig davon erforderlich sein, ob der Empfänger als angemessen eingestuft wurde oder nicht. Geht es bei den Verarbeitungen beispielsweise um Gesundheitsdaten, die an ein als angemessen eingestuftes Land (z. B. die Schweiz) übermittelt werden sollen, muss die Verarbeitung auf jeden Fall zur Vorabkontrolle gemeldet werden.

Bei anderer Gelegenheit hat es der EDSB aufgrund der zugrunde liegenden Verarbeitung möglicherweise sowohl mit einer Konsultation (wie unter Punkt 6.3 beschrieben) als auch mit einer Vorabkontrolle zu tun.

Die Einreichung einer Meldung zur Vorabkontrolle kann auch mit Blick auf Artikel 27 Absatz 1 der Verordnung erforderlich sein, wenn die Verarbeitungen möglicherweise besondere Risiken für die Rechte und Freiheiten der betroffenen Person beinhalten. Dies könnte in bestimmten spezifischen Situationen, die noch in einer Leitlinie zu definieren wären, aufgrund der Komplexität und Sensibilität der Daten beispielsweise auf Informationen zutreffen, die durch Cloud Computing-Dienste verarbeitet werden.[54] In diesem Zusammenhang werden Kundendaten häufig an Server von Cloud-Anbietern und an Datenzentren in verschiedenen Teilen der Welt übermittelt. Da es keinen stabilen Standort für die Daten gibt, könnte es sein, dass der EDSB zu überprüfen hat, ob etwaige angemessene Garantien tatsächlich im Einklang mit Artikel 9 stehen, und dabei alle möglicherweise an dem Cloud-Umfeld beteiligten Empfänger abzudecken hat. Dies ist allerdings auch von den Bedingungen abhängig,

[53] Strategiepapier „Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001“, angenommen am 13. Dezember 2010. abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_DE.pdf

[54] Vgl.: Stellungnahme des Europäischen Datenschutzbeauftragten vom 16. November 2012 zur Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_DE.pdf

die ganz allgemein mit Anbietern von Cloud Computing-Diensten zu vereinbaren sind. Derzeit bestehen daher keine weiteren Anforderungen bezüglich einer Vorabkontrolle.

- Konsultationen, Beschwerden, Inspektionen

Dem EDSB stehen noch weitere Aufsichtsinstrumente zur Verfügung, mit denen die Einhaltung der Vorschriften gewährleistet werden kann, darunter z. B., wie bereits erwähnt, Konsultationen. Die Konsultationsstrategie findet in vollem Umfang Anwendung auf Übermittlungen gemäß Artikel 9.

Eine betroffene Person, die sich durch die Übermittlungen beeinträchtigt fühlt, kann gemäß Artikel 32 und 33 der Verordnung Beschwerde einlegen, wenn ihrer Auffassung nach ihre Datenschutzrechte verletzt wurden.

Desgleichen kann der EDSB Inspektionen beschließen, bei denen er die Einhaltung von Artikel 9 der Verordnung kontrolliert oder im Zusammenhang mit Beschwerden Beweismittel erhebt.

- Durchsetzungsinstrumente

Die Durchsetzungsbefugnisse des EDSB sind in Artikel 47 der Verordnung geregelt und werden in dem Strategiepapier zur Einhaltung der Verordnung ausführlich erörtert. In der Regel entscheidet der EDSB mit Blick auf die angestrebten Ergebnisse über das wirksamste Vorgehen. Bei Übermittlungen gemäß Artikel 9 ist der EDSB befugt,

* bei einem behaupteten Verstoß gegen die Verordnung den für die Verarbeitung Verantwortlichen mit der Angelegenheit zu befassen und gegebenenfalls Vorschläge zur Behebung dieses Verstoßes zu machen;

* den für die Verarbeitung Verantwortlichen zu ermahnen und zu verwarnen;

* die Verarbeitung vorübergehend oder endgültig zu verbieten;

* das betroffene Organ oder die betreffende Einrichtung der Gemeinschaft und, falls erforderlich, das Europäische Parlament, den Rat und die Kommission mit der Angelegenheit zu befassen;

* unter den im Vertrag vorgesehenen Bedingungen den Gerichtshof der Europäischen Gemeinschaften anzurufen;

* beim Gerichtshof der Europäischen Gemeinschaften anhängigen Verfahren beizutreten.

Diese Befugnisse werden unter Berücksichtigung der spezifischen Gegebenheiten in der Rechtsordnung des Empfängers oder dessen Verarbeitungspraxis wahrgenommen, die den Schutz der natürlichen Person gefährden könnten (siehe Punkt 6.2.1 zur Befugnis des EDSB, Datenübermittlungen zu verbieten oder auszusetzen).

ANHANG 1

Artikel 9 der Verordnung (EG) Nr. 45/2001

Übermittlung personenbezogener Daten an Empfänger, die nicht Organe oder Einrichtungen der Gemeinschaft sind und die nicht der Richtlinie 95/46/EG unterworfen sind

(1) Personenbezogene Daten werden an Empfänger, die nicht Organe oder Einrichtungen der Gemeinschaft sind und die nicht den aufgrund der Richtlinie 95/46/EG erlassenen Rechtsvorschriften unterliegen, nur übermittelt, wenn ein angemessenes Schutzniveau in dem Land des Empfängers oder innerhalb der empfangenden internationalen Organisation gewährleistet ist und diese Übermittlung ausschließlich die Wahrnehmung von Aufgaben ermöglichen soll, die in die Zuständigkeit des für die Verarbeitung Verantwortlichen fallen.
(2) Die Angemessenheit des von dem betreffenden Drittland oder der betreffenden internationalen Organisation gebotenen Schutzniveaus ist anhand aller Umstände einer Datenübermittlung oder einer Reihe von Datenübermittlungen zu beurteilen. Besonders zu berücksichtigen sind dabei die Art der Daten, der Zweck und die Dauer des geplanten Verarbeitungsvorgangs oder der geplanten Verarbeitungsvorgänge, das Drittland oder die internationale Organisation der Endbestimmung, die in dem betreffenden Drittland oder der betreffenden internationalen Organisation geltenden allgemeinen und sektoriellen Rechtsvorschriften sowie die in diesem Land oder in dieser internationalen Organisation geltenden Standesregeln und Sicherheitsmaßnahmen.
(3) Die Organe und Einrichtungen der Gemeinschaft unterrichten die Kommission und den Europäischen Datenschutzbeauftragten über die Fälle, in denen das betreffende Drittland oder die betreffende internationale Organisation ihres Erachtens kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.
(4) Die Kommission unterrichtet die Mitgliedstaaten über die in Absatz 3 genannten Fälle.
(5) Die Kommission stellt gemäß Artikel 25 Absätze 4 und 6 der Richtlinie 95/46/EG fest, ob ein Drittland oder eine internationale Organisation ein angemessenes Schutzniveau gewährleistet oder nicht, und die Organe und Einrichtungen der Gemeinschaft treffen die erforderlichen Maßnahmen, um den Entscheidungen der Kommission nachzukommen.
(6) Abweichend von den Absätzen 1 und 2 kann das Organ oder die Einrichtung der Gemeinschaft personenbezogene Daten übermitteln, sofern
a) die betroffene Person ohne jeden Zweifel ihre Einwilligung zu der geplanten Übermittlung gegeben hat, oder
b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist, oder
c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person zwischen dem für die Verarbeitung Verantwortlichen und einem Dritten geschlossen wird, oder
d) die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, oder
e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist, oder
f) die Übermittlung aus einem Register erfolgt , das gemäß dem Gemeinschaftsrecht zur Unterrichtung der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die im Gemeinschaftsrecht für die Einsichtnahme festgelegten Voraussetzungen im Einzelfall gegeben sind.
(7) Unbeschadet des Absatzes 6 kann der Europäische Datenschutzbeauftragte eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten nach einem Drittland oder an eine internationale Organisation genehmigen, die kein angemessenes Schutzniveau im Sinne der Absätze 1 und 2 gewährleisten, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.
(8) Die Organe und Einrichtungen der Gemeinschaft unterrichten den Europäischen Datenschutzbeauftragten über alle Kategorien von Fällen, in denen sie die Absätze 6 und 7 angewandt haben.

ANHANG 2

Checkliste zur Vorbereitung einer Übermittlung

Für die Verarbeitung Verantwortliche sollten ihre Datenschutzbeauftragten von Anfang an einbeziehen und sie um ihren Rat und um Hinweise bezüglich der Einhaltung der Vorschriften bitten. Die folgenden Maßnahmen und rechtlichen Überprüfungen sollten durchgeführt werden, bevor eine oder mehrere internationale Übermittlung/-en stattfindet/stattfinden.

1) Ist in dem Land des Empfängers oder innerhalb der empfangenden internationalen Organisation ein angemessenes Schutzniveau gewährleistet?

Überprüfen Sie die Liste der Angemessenheitsentscheidungen der Kommission: Andorra, Argentinien, Kanada (privater Sektor), Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, US Safe Harbour (bestimmte Tätigkeiten des privaten Sektors) und Uruguay.

A: **Ja** – die Übermittlung kann stattfinden, sofern die anderen Vorschriften der Verordnung (EG) Nr. 45/2001 eingehalten werden.

A: **Nein oder nicht sicher** – weiter mit Frage 2.

Hinzuziehung des EDSB: Unterrichtung, Konsultation oder Genehmigung des EDSB nicht erforderlich.

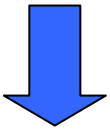
2) Gibt es andere Gründe für die Annahme, dass von dem Empfänger im Drittland oder der internationalen Organisation ein angemessenes Schutzniveau geboten wird?

Der für die Verarbeitung Verantwortliche hat zu überprüfen, ob für die konkreten Übermittlungen ein angemessenes Schutzniveau besteht. Diese Überprüfung sollte auf die konkreten Zweckbestimmungen und Empfänger im Drittland oder der internationalen Organisation der Endbestimmung beschränkt sein.

A: **Ja** – die Übermittlung kann stattfinden, sofern die Beurteilung der Angemessenheit sorgfältig dokumentiert wird und die anderen Vorschriften der Verordnung (EG) Nr. 45/2001 eingehalten werden.

A: **Nein** – weiter mit Frage 3.

Hinzuziehung des EDSB: Genehmigung des EDSB nicht erforderlich. Unter bestimmten Voraussetzungen könnten wir konsultiert werden (schlagen Sie in der Leitlinie des EDSB zu Konsultationen im Bereich Aufsicht und Durchsetzung nach).



3) Gilt eine Ausnahmeregelung?

Ist die Übermittlung *nicht* wiederholt, massiv oder strukturell und trifft einer der folgenden Umstände zu?

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung zu der geplanten Übermittlung gegeben oder
b) die Übermittlungen sind für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erforderlich oder
c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person zwischen dem für die Verarbeitung Verantwortlichen und einem Dritten geschlossen wird, oder
d) die Übermittlung ist für die Wahrung eines wichtigen öffentlichen Interesses oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben oder
e) die Übermittlung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich oder
f) die Übermittlung erfolgt aus einem Register, das zur Unterrichtung der Öffentlichkeit bestimmt ist.

A: **Ja** – die Übermittlung kann stattfinden, sofern sie nicht wiederholt, massiv oder strukturell ist. Ferner sollte eine der Bedingungen in Artikel 9 Absatz 6 der Verordnung (EG) Nr. 45/2001 erfüllt sein und alle anderen Bestimmungen der Verordnung eingehalten werden.

A: **Nein** – weiter mit Frage 4.

Vorherige Einbeziehung des EDSB: Genehmigung des EDSB nicht erforderlich. Unter bestimmten Voraussetzungen könnten wir konsultiert werden (schlagen Sie in der Leitlinie des EDSB zu Konsultationen im Bereich Aufsicht und Durchsetzung nach).

4) Kann der für die Verarbeitung Verantwortliche „angemessene Garantien“ bieten?

Unter „angemessenen Garantien“ versteht man Datenschutzgarantien, die ad hoc geschaffen werden und die es in der Rechtsordnung oder Praxis des Empfängers am Bestimmungsort noch nicht gibt. Zweck dieser Garantien ist es, in Fällen, in denen keine Ausnahmen greifen, Schutz dort zu gewähren, wo er im Bestimmungsland der Daten oder bei der empfangenden internationalen Organisation nicht besteht.

A: **Ja** – die Übermittlung kann stattfinden, sofern die anderen Vorschriften der Verordnung (EG) Nr. 45/2001 eingehalten werden.

A: **Nein** – die Übermittlung darf nicht stattfinden.

Hinzuziehung des EDSB: Bei der Entscheidung über eine Hinzuziehung des EDSB sind drei Optionen denkbar:

- Eine vorherige Genehmigung oder Konsultation ist nicht erforderlich, wenn Standardvertragsklauseln zum Einsatz kommen.

- Eine vorherige Genehmigung ist nicht erforderlich, doch könnte eine Konsultation erforderlich sein (schlagen Sie in der Leitlinie des EDSB zu Konsultationen im Bereich Aufsicht und Durchsetzung nach), wenn beispielsweise ein spezifisches verbindliches Instrument (im Gegensatz zu Standardvertragsklauseln) für den Einsatz entweder im privatrechtlichen der im öffentlich-rechtlichen Bereich von dem Organ oder der Einrichtung der EU entwickelt wird.

- Eine vorherige Genehmigung ist erforderlich in Ausnahmefällen, in denen sich die Übermittlungen auf spezifische Garantien stützen und nicht in einem rechtsverbindlichen Instrument geregelt sind.

Der EDSB kann auch entscheiden, dass in anderen zur Konsultation eingereichten Fällen je nach dem Risikoniveau der Übertragung eine Genehmigung erforderlich ist.

Ist eine vorherige Genehmigung erforderlich, sollten beim EDSB eine gründliche Analyse der „Angemessenheit“ sowie die Entwürfe des/der entsprechenden Instruments/Instrumente eingereicht werden.

5) Überprüfen Sie, ob die zugrunde liegende Verarbeitungstätigkeit vorabkontrollpflichtig ist und reichen Sie gegebenenfalls die entsprechende Meldung beim EDSB ein.

ANHANG 3

Liste der beim EDSB im Zusammenhang mit Artikel 9 eingereichten Anträge auf Genehmigung (Artikel 9 Absatz 7), Konsultationen durch Behörden (Artikel 28 Absatz 1 und Artikel 46 Buchstabe d) sowie ausgewählte Konsultationen des Gesetzgebers (Artikel 28 Absatz 2)

Anträge auf Genehmigung (Artikel 9 Absatz 7)

- Entscheidung des EDSB vom 13. Februar 2014 über die gemäß Artikel 9 Absatz 7 der Verordnung (EG) Nr. 45/2001 von OLAF über die Investigative Data Consultation Platform vorgenommenen Übermittlungen personenbezogener Daten, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_EN.pdf; Anhang – Entwurf eines Abkommens über die Verwaltungszusammenarbeit zwischen dem „Europäischen Amt für Betrugsbekämpfung“ (OLAF) und [Partner], abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_Annex_EN.pdf

Konsultationen durch Behörden (Artikel 28 Absatz 1 und Artikel 46 Buchstabe d)

- Antwort vom 16. Juli 2012 auf eine Konsultation bezüglich der überarbeiteten Muster für die Datenschutzvertragsklauseln für Vereinbarungen über die Verwaltungszusammenarbeit, die mit Drittlandsbehörden oder internationalen Organisationen abgeschlossen werden (Fall 2012-0086), abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-07-16Model%20Data%20Protection%20Clauses_OLAF_D-1051_EN.pdf
- Antwort vom 3. April 2012 auf eine Konsultation bezüglich der überarbeiteten Muster von OLAF für die Datenschutzvertragsklauseln für Vereinbarungen über die Verwaltungszusammenarbeit, die mit Drittlandsbehörden oder internationalen Organisationen abgeschlossen werden (Fall 2012-0086), abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-04-03%20Model%20Data%20Protection%20Clauses_OLAF_D-746_EN.pdf
- Antwort vom 4. Oktober 2010 an den Datenschutzbeauftragten der Europäischen Agentur für Flugsicherheit zum Thema internationale Übermittlungen, abrufbar unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-10-04_Letter_DPO_EASA_EN.pdf
- Antwort vom 21. Dezember 2010 auf eine Konsultation betreffend die Übermittlung personenbezogener Daten von externen Experten der EFSA durch die EFSA an American Express Corporate Travel SA (AMEX) (Fall 2009-390), abrufbar unter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2010/10-12-21_EFSA_AMEX_DE.pdf

- Antwort vom 2. Juli 2009 auf eine Konsultation bezüglich der Übermittlung personenbezogener Daten an Drittländer: „Angemessenheit" von Unterzeichnern des Übereinkommens Nr. 108 des Europarats, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

- Antwort vom 6. Mai 2009 auf eine Konsultation bezüglich der Behandlung von Übermittlungen personenbezogener Daten durch OLAF, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-05-06_OLAF_transfers_EN.pdf

Ausgewählte Konsultationen durch den Gesetzgeber (Artikel 28 Absatz 2)

- Stellungnahme vom 14. März 2014 zum Entwurf eines Beschlusses des Rates über den Standpunkt der Europäischen Union im Gemischten Ausschuss EU-China für Zusammenarbeit im Zollbereich in Bezug auf die gegenseitige Anerkennung des Programms für zugelassene Wirtschaftsbeteiligte der Europäischen Union und des Programms „Measures on Classified Management of Enterprises" der Volksrepublik China, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-14_EU-China_Customs_DE.pdf

- Stellungnahme vom 20. Februar 2014 zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA" und zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Über die Funktionsweise der Safe-Harbour-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen", abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_DE.pdf

- Stellungnahme vom 9. Februar 2012 zum Vorschlag für einen Beschluss des Rates über den Standpunkt der EU im Gemischten Ausschuss EU-USA für Zusammenarbeit im Zollbereich in Bezug auf die gegenseitige Anerkennung des Programms für zugelassene Wirtschaftsbeteiligte der Europäischen Union und des Programms „Customs-Trade Partnership Against Terrorism" der Vereinigten Staaten von Amerika, ABl. C 160/01 vom 6.6.2012, S. 1, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-09_EU_US_Joint_Customs_DE.pdf

- Stellungnahme vom 12. März 2010 zum Vorschlag für einen Beschluss des Rates über den Standpunkt der EU im Gemischten Ausschuss EU-Japan für Zusammenarbeit im Zollbereich in Bezug auf die gegenseitige Anerkennung der Programme für zugelassene Wirtschaftsbeteiligte in der Europäischen Union und in Japan, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-12_EU-Japan_DE.pdf