

Kurzpapier Nr. 4

Datenübermittlung in Drittländer

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Die Datenschutz-Grundverordnung (DS-GVO) sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der Europäischen Union (EU)/des Europäischen Wirtschaftsraum (EWR) besondere Regelungen vor: Artikel 44 – 49. Länder außerhalb der EU/des EWR werden in der DS-GVO als "Dritt-länder" bezeichnet, in der Praxis wird auch der Begriff "Drittstaat" verwendet. Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob unabhängig von den in den Artikeln 45 fortfolgende geregelten spezifischen Anforderungen an Datenübermittlungen in Drittländer auch alle übrigen Anforderungen der DS-GVO (zum Beispiel Artikel 9 Absatz 3) an die in Rede stehende Datenverarbeitung eingehalten werden (1. Stufe). Steht nach diesem Prüfungsschritt einer Verarbeitung nichts entgegen, müssen gemäß Artikel 44 zusätzlich die spezifischen Anforderungen der Artikel 45 fortfolgende an die Übermittlung in Drittländer beachtet werden (2. Stufe; "2-Stufen-Prüfung"). Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Artikel 44 Satz 1 2. Halbsatz (siehe auch Erwägungsgrund 101).

Die DS-GVO sieht für Datentransfers in Drittländer folgende Möglichkeiten vor (für öffentliche Stellen gelten im Einzelfall ergänzende Regelungen):

- **Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Artikel 45 DS-GVO)**
- **Vorliegen geeigneter Garantien (Artikel 46 DS-GVO) oder**

- **Ausnahmen für bestimmte Fälle (Artikel 49 DS-GVO).**

1) Feststellung der Angemessenheit des Datenschutzniveaus im Drittstaat durch die Kommission (Artikel 45 DS-GVO)

Die Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in der DS-GVO gewährten Schutzniveau gleichwertig ist. Eine Datenübermittlung auf Grundlage eines solchen Angemessenheitsbeschlusses bedarf keiner weiteren Genehmigung durch die für den Verantwortlichen oder Auftragsverarbeiter zuständige nationale Aufsichtsbehörde.

Die DS-GVO sieht eine Fortgeltung der bereits erlassenen Angemessenheitsbeschlüsse vor (Artikel 46 Absatz 5 Satz 2).

Für den EU-US Privacy Shield hat die Kommission die Angemessenheit des Datenschutzniveaus festgestellt (C(2016) 4176 final).

2) Vorliegen geeigneter Garantien (Artikel 46 DS-GVO)

Eine Datenübermittlung in ein Drittland ist weiter zulässig, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien zur Gewährleistung eines angemessenen Schutzniveaus vorgesehen hat. Folgende Garantien kommen in Betracht:

a) Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Artikel 46 Absatz 2 Buchstabe b, Artikel 47)

Verbindliche interne Datenschutzvorschriften (BCR) wurden schon bisher in der Praxis verwendet und sind nun in der DS-GVO (anders als in der noch geltenden EU-Datenschutzrichtlinie 95/46/EG) ausdrücklich als Möglichkeit zur Erbringung "geeigneter Garantien" für Datenübermittlungen in Drittländer geregelt. Sie können vor allem bei international tätigen Konzernen mit internem Datenfluss (auch in Drittländer empfehlenswert sein. Dabei legt das Unternehmen Regelungen für den Umgang mit personenbezogenen Daten auch in Drittländern fest. Die BCR müssen einen Schutz bieten, der im Wesentlichen der DS-GVO entspricht. Der Mindestinhalt ist in Artikel 47 Absatz 2 festgelegt. Zudem müssen die BCR für alle betreffenden Mitglieder der Unternehmensgruppe rechtlich bindend sein und den betroffenen Personen durchsetzbare Rechte gewähren (Artikel 47 Absatz 1 Buchstabe a und b). Die Genehmigung der BCR erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde (Artikel 47 Absatz 1). Die konkreten Datenübermittlungen auf Grundlage der BCR werden dann nicht mehr einzeln genehmigt.

b) Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Artikel 46 Absatz 2 Buchstabe c und d)

Schließen der Datenexporteur und der Datenimporteur einen Vertrag unter Verwendung der Standarddatenschutzklauseln der Kommission, ist der darauf basierende Datentransfer ohne weitere Genehmigung durch die Aufsichtsbehörde zulässig (vorbehaltlich der weiteren Anforderungen nach

der DS-GVO). Auch den Aufsichtsbehörden ist es möglich, eigene Standarddatenschutzklauseln zu entwerfen. Diese bedürfen der Abstimmung im Kohärenzverfahren und sind anschließend von der Kommission förmlich zu genehmigen.

Die bereits bestehenden EU-Standardvertragsklauseln gelten gemäß Artikel 46 Absatz 5 Seite 2 ausdrücklich fort. Sofern die Standarddatenschutzklauseln in unveränderter Form verwendet werden, sind die Datenübermittlungen genehmigungsfrei. Dies gilt auch noch dann, wenn ihnen weitere Klauseln oder zusätzliche Garantien hinzugefügt werden, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Standarddatenschutzklauseln stehen und die Grundrechte und Grundfreiheiten der betroffenen Personen nicht beschneiden (Erwägungsgrund 109). Bei solchen Hinzufügungen sollten Unternehmen jedoch eine gewisse Vorsicht walten lassen, da im Falle eines inhaltlichen Widerspruchs zu den Standarddatenschutzklauseln die Übermittlung nicht mehr genehmigungsfrei ist.

c) Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Artikel 46 Absatz 2 Buchstabe e und f)

Neu hinzugekommen ist die Möglichkeit, Datenübermittlungen auf Grundlage von branchenspezifischen Verhaltensregeln gemäß Artikel 40 zu legitimieren, sofern diese mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters versehen sind und von der zuständigen Aufsichtsbehörde genehmigt worden sind.

Auch Zertifizierungen nach Artikel 42 können nun zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters als rechtliche Grundlage für einen Datentransfer in ein Drittland herangezogen werden, wenn die Zertifizierungsmechanismen zuvor genehmigt worden sind.

Die europäischen Aufsichtsbehörden werden in der Folgezeit die für eine praktische Anwendung dieser

Instrumente notwendigen weiteren Einzelheiten im Hinblick auf rechtliche Rahmenbedingungen und Verfahrensfragen erarbeiten.

d) Einzel ausgehandelte Vertragsklauseln (Artikel 46 Absatz 3)

Ebenso können einzeln ausgehandelte individuelle Vertragsklauseln eine Datenübermittlung in ein Drittland legitimieren, allerdings nur nach Genehmigung der Aufsichtsbehörde und Durchführung des Kohärenzverfahrens nach Artikel 63.

e) Rechte der betroffenen Personen

Gemäß Artikel 46 Absatz 1 am Ende ist es bei allen in Betracht kommenden geeigneten Garantien im Sinne von Artikel 46 zusätzlich erforderlich, den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe einzuräumen.

3) Ausnahmen für bestimmte Fälle (Artikel 49 DS-GVO)

Eine Datenübermittlung kann in einer Reihe besonderer, vom Gesetz explizit genannter und abschließender Fälle, auch zulässig sein, wenn weder ein Angemessenheitsbeschluss der Kommission noch geeignete Garantien vorliegen. Die hierfür von der DS-GVO definierten Ausnahmetatbestände sind gemäß ihrem Ausnahmecharakter eng auszulegen.

a) Einwilligung (Artikel 49 Absatz 1 Unterabsatz 1 Buchstabe a)

Eine wirksame Einwilligung der betroffenen Person in die Datenübermittlung in ein Drittland setzt zunächst eine ausdrückliche Einwilligung in die Weitergabe ihrer Daten für den konkreten Fall voraus. Weiter ist die betroffene Person vorher explizit über bestehende mögliche Risiken derartiger Datenübermittlungen aufzuklären, das heißt insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte gegebenenfalls nicht durchgesetzt werden können. Auch ist die betroffene Person darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann (Artikel 7 Absatz 3).

b) Erforderlichkeit zur Vertragserfüllung (Artikel 49 Absatz 1 Unterabsatz 1 Buchstabe b und c)

Eine Datenübermittlung in ein Drittland ist (vorbehaltlich der weiteren Anforderungen der DS-GVO) zulässig, wenn und soweit die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich ist. Wesentlich ist hier jeweils die strikte Erforderlichkeit gerade dieser Datenübermittlung zur Erfüllung des Vertragszwecks.

c) Wichtige Gründe des öffentlichen Interesses (Artikel 49 Absatz 1 Unterabsatz 1 Buchstabe d)

Die Übermittlung kann auch zulässig sein, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist. In Betracht kommen nur wichtige öffentliche Interessen, die im Recht der Europäischen Union oder des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sind (Artikel 49 Absatz 4). Wie aus Erwägungsgrund 112 hervorgeht, hatte der Gesetzgeber insoweit insbesondere Datentransfers im Rahmen der internationalen behördlichen Zusammenarbeit im Auge, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden.

d) Verfolgung von Rechtsansprüchen (Artikel 49 Absatz 1 Unterabsatz 1 Buchstabe e)

Auch die Verfolgung von Rechtsansprüchen kann eine Datenübermittlung legitimieren, wenn die Datenübermittlung hierzu erforderlich ist. In Erweiterung der bisherigen Regelung im Bundesdatenschutzgesetz (BDSG) kommt auch die Geltendmachung von Rechtsansprüchen in außergerichtlichen Verfahren in Betracht (Erwägungsgrund 111).

e) Schutz lebenswichtiger Interessen (Artikel 49 Absatz 1 Unterabsatz 1 Buchstabe f)

Ist die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage, ihre Einwilligung zu erteilen, darf die Datenübermittlung dennoch durchgeführt werden, soweit dies zum Schutz ihrer lebenswichtigen Interessen oder derjenigen anderer Personen erforderlich ist.

**f) Wahrung zwingender berechtigter Interessen
(Artikel 49 Absatz 1 Unterabsatz 2 Satz 1)**

Im Einzelfall kann eine Datenübermittlung in ein Drittland legitimiert sein, wenn ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung besteht, die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Anzahl von Personen betrifft und keine überwiegenden schutzwürdigen Interessen oder Rechte und Freiheiten der betroffenen Person entgegenstehen und der Verantwortliche durch geeignete Garantien den Schutz personenbezogener Daten gewährleistet. Voraussetzung für diese Übermittlungserlaubnis ist ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung, dem eine herausgehobene und besondere Bedeutung zukommt. Zudem muss die Übermittlung unbedingt erforderlich sein zur Verfolgung dieses berechtigten Interesses. Die Übermittlung darf sich nicht bereits auf einen der oben genannten Erlaubnistatbestände stützen lassen. Wird eine Übermittlung in ein Drittland auf Grundlage eines zwingenden berechtigten Interesses in einem absoluten Einzelfall durchgeführt, ist sowohl die Aufsichtsbehörde als auch die betroffene Person hierüber zu informieren (Artikel 49 Absatz 1 Unterabsatz 2 Satz 2 und 3).