EU-Mitteilung

DATENÜBERMITTLUNG IN DRITTLÄNDER

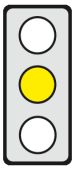
cep**Analyse** Nr. 25/2017

Centrum für Europäische Politik

KERNPUNKTE

Ziel der Mitteilung: Personenbezogene Daten sollen bei gleichzeitig hohem Datenschutzniveau leichter in Drittländer übermittelt werden können, um so den gegenseitigen Handel zu fördern und internationale Kriminalität wirksam zu bekämpfen.

Betroffene: EU-Bürger und Unternehmen, die Daten aus der EU transferieren oder erhalten, Behörden.



Pro: (1) Die geplante Erleichterung der Datenübermittlung in Drittländer senkt die Kosten, die Unternehmen tragen müssen, wenn sie Daten aus der EU übermitteln wollen.

(2) Nur eine tatsächliche Angleichung der Datenschutzniveaus in Drittländern an das Niveau der EU ermöglicht einen wirklich hohen Datenschutz. Es ist daher sachgerecht, dass die Kommission sich für hohe Datenschutzniveaus in Drittländern einsetzen will.

Contra: (1) Die dem Angemessenheitsbeschluss immanente Vorstellung, dass Drittländer ein „angemessenes" Schutzniveau aufweisen können, ist derzeit wenig realistisch.

(2) Standarddatenschutzklauseln und verbindliche interne Datenschutzvorschriften binden nur die beteiligten Unternehmen. Sie können daher weder Datenzugriffe durch Geheimdienste im Drittland verhindern noch das Fehlen wirksamer Rechtsbehelfe kompensieren.

INHALT

Titel

Mitteilung COM(2017) 7 vom 10. Januar 2017: **Austausch und Schutz personenbezogener Daten in einer globalisierten Welt**

Kurzdarstellung

- **Hintergrund und Ziele**
  - Ab Mai 2018 regeln die allgemeine Datenschutzgrundverordnung [DSGVO, (EU) 2016/679; s. cep**Analyse**] und die Polizei-Richtlinie [(EU) 2016/680] – letztere für den Bereich der Strafverfolgung –, wie Wirtschaft und Behörden personenbezogene Daten in der EU verarbeiten dürfen (s. cep**Studie** zum EU-Datenschutzrecht). Sie regeln auch, unter welchen Voraussetzungen diese Daten in Drittländer übermittelt werden dürfen, und sehen dafür bekannte und neue Übermittlungsinstrumente vor (S. 3–6).
  - Der globale Handel und das steigende Bedürfnis nach Schutz der Privatsphäre führen weltweit zum vermehrten Erlass von Datenschutzvorschriften. Zugleich wird die Datenübermittlung in Drittländer für EU-Unternehmen und Behörden im Zuge der Digitalisierung immer wichtiger (S. 2 und 8).
  - Uneinheitliche Datenschutzniveaus und unterschiedliche Datenschutzrechtssysteme in EU und Drittländern stellen jedoch Hindernisse für die internationale Datenübermittlung dar (S. 2 und 13).
  - Die Kommission will die „hohen Datenschutzstandards" der EU weltweit propagieren und sich für eine größere Angleichung der Datenschutzrechtssysteme von Drittländern an diese Standards einsetzen. Ziel ist es, eine Datenübermittlung in Drittländer bei gleichzeitig hohem Datenschutzniveau zu ermöglichen oder zu erleichtern, um (S. 2–4)
    - den freien Handel zu fördern und
    - grenzüberschreitende Kriminalität und andere Verstöße wirksamer zu bekämpfen.
  - Hierzu will die Kommission
    - die „Übermittlungsinstrumente" der DSGVO – Rechtsgrundlagen für die Datenübermittlung in Drittländer – verstärkt nutzen (S. 6–13); dazu zählen
      - der „Angemessenheitsbeschluss", mit dem die Kommission das Datenschutzniveau eines Drittlandes für „angemessen" erklärt,
      - „alternative Instrumente", die die Datenübermittlung auch ohne Angemessenheitsbeschluss erlauben.
    - auf internationaler Ebene für hohe Datenschutzstandards werben (S. 2–3 und 13–15) und die Zusammenarbeit zwischen den Datenschutzbehörden in der EU und den zuständigen Behörden von Drittländern verbessern (S. 14 und 15) sowie
    - den Austausch personenbezogener Daten zwischen Strafverfolgungsbehörden erleichtern, um die Zusammenarbeit bei der Strafverfolgung innerhalb der EU und mit Drittländern zu verbessern (S. 15–18).

- **„Angemessenheitsbeschlüsse"**
  - Angemessenheitsbeschlüsse sind Beschlüsse, mit denen die Kommission nach umfassender Bewertung des Datenschutzrechtssystems eines Drittlandes feststellt, dass dessen Datenschutzniveau demjenigen der EU „der Sache nach gleichwertig" und damit „angemessen" ist (Art. 45 Abs. 1, 3 DSGVO, S. 4 und 7).
  - Sie ermöglichen eine freie Datenübermittlung ins Drittland, ohne dass der Übermittler eine Genehmigung einholen oder für zusätzliche Garantien sorgen muss (S. 7).

Autoren: Dr. Anja Hoffmann, LL.M. Eur. und Bastian Sattelberger | hoffmann@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-107 | www.cep.eu

– Sie können auf bestimmte geografische Gebiete oder Wirtschaftszweige im Drittland beschränkt werden (S. 5).
– Die Kommission will mit ausgewählten Drittländern in einen Dialog zur „Angemessenheit" ihres Datenschutzniveaus treten. Die Auswahl will sie nach Kriterien wie dem Umfang der Handelsbeziehungen und der Datenübermittlungen der EU mit dem Land treffen (S. 9 und 11).
– Zu diesen Ländern gehören (S. 9 und 11)
  - wichtige asiatische Handelspartner wie Japan, Korea und ggf. Indien,
  - lateinamerikanische Länder, insbesondere Mercosur-Länder wie Brasilien oder Paraguay sowie
  - an die EU angrenzende und sonstige Länder, die Interesse bekunden.
– Die Kommission will für die ausgewählten Länder – landesweit oder beschränkt auf bestimmte Gebiete oder Sektoren – Angemessenheitsbeschlüsse treffen (S. 9 und 11).
– Sie will diese Länder bei der Einführung „solider" Datenschutzvorschriften unterstützen und eine Angleichung ihrer Vorschriften an den EU-Standard anstreben (S. 11).
– Die Kommission will bestehende Angemessenheitsbeschlüsse – insbesondere den sog. EU-US-Datenschutzschild mit den USA (s. cep**Studie** zum Privacy Shield) – überwachen und regelmäßig überprüfen, um eventuellen Änderungen des Schutzniveaus im Drittland Rechnung tragen zu können (S. 10–11).

► **„Alternative Instrumente" zur Datenübermittlung**
– Liegt kein Angemessenheitsbeschluss für ein Drittland vor, können Übermittler das unzureichende Datenschutzniveau durch „geeignete Garantien" kompensieren, indem sie die in der DSGVO aufgeführten „alternative Übermittlungsinstrumente" nutzen, um Daten legal in das Drittland zu übermitteln (S. 5). Alternative Übermittlungsinstrumente sind u.a.:
  - „Standarddatenschutzklauseln": Das sind Klauseln in Verträgen zwischen in der EU aktiven Unternehmen und Partnern in Drittländern. Sie werden von der Kommission erlassen oder genehmigt (Art. 46 Abs. 2 lit. c, d DSGVO).
  - „Verbindliche interne Datenschutzvorschriften" (Binding Corporate Rules – BCR): Das sind unternehmenseigene Datenschutzregeln für Datentransfers in Drittländer, die von Aufsichtsbehörden genehmigt werden müssen. Sie erlauben Übermittlungen innerhalb multinationaler Konzerne und ab Inkrafttreten der DSGVO auch innerhalb „einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben", wie einem Joint Venture oder einer Arbeitsgemeinschaft (Arge). (Art. 47 Abs. 1 DSGVO, S. 5)
  - „Genehmigte Verhaltensregeln" und „Zertifizierungsverfahren": Unternehmen in Drittländern können – von einer zuständigen europäischen Aufsichtsbehörde genehmigte – Verhaltensregeln zum Datenschutz anwenden oder sich ihren Datenschutzstandard zertifizieren lassen. Gegenüber dem Datenübermittler in der EU verpflichten sie sich mit rechtlichen – z.B. vertraglichen – Zusagen zur Einhaltung der entsprechenden Anforderungen (Art. 40–42 DSGVO, S. 6).
– Die Kommission will u.a. mit der Industrie, Behörden und internationalen Organisationen zusammenarbeiten, um die alternativen Übermittlungsinstrumente an die Anforderungen einzelner Industriezweige, Geschäftsmodelle und Wirtschaftsteilnehmer anzupassen und so ihre Nutzung zu fördern (S. 5, 11–13).
– Zur Förderung von Standarddatenschutzklauseln schlägt sie insbesondere vor (S. 11–13),
  - neue Klauseln zu erlassen, prioritär für Verträge zwischen Auftragsverarbeitern – das sind Stellen, die Daten im Auftrag eines datenschutzrechtlich Verantwortlichen verarbeiten, – oder
  - geltende Klauseln u.a. durch technische oder geschäftsmodellspezifische Garantien zu ergänzen, die
    - auf die Anforderungen eines bestimmten Sektors zugeschnitten sind, z.B. spezifische Garantien für die Übermittlung sensibler Gesundheitsdaten enthalten, oder
    - sich auf spezifische Verarbeitungsvorgänge beziehen, die in bestimmten Drittländern häufig genutzt werden, z.B. Outsourcing von Dienstleistungen, die für EU-Unternehmen durchgeführt werden.
– Hinsichtlich anderer alternativer Instrumente regt die Kommission an (S. 11 und 12),
  - „sektorale" BCR zu entwickeln für Unternehmensgruppen mit gemeinsamer Wirtschaftstätigkeit, z.B. für die Reisebranche, sowie für Datenübermittlungen zwischen Auftragsverarbeitern;
  - Anforderungen und technische EU-Standards für Zertifizierungsverfahren festzulegen;
  - die Konvergenz zwischen BCR und vergleichbaren Unternehmensrichtlinien („Cross Border Privacy Rules") der Asiatisch-Pazifischen Wirtschaftskooperation (APEC) zu fördern, um Unternehmen den Wechsel zwischen beiden Systemen zu erleichtern.

► **Internationale Zusammenarbeit beim Datenschutz**
– Die Kommission will hohe Datenschutzstandards global fördern, indem sie (S. 13, 15)
  - „multilaterale Foren" wie den G20-Gipfel 2017 oder die Vereinten Nationen nutzt, um „eine weltweite Kultur der Achtung der Datenschutzrechte zu fördern",
  - die „rasche Verabschiedung der modernisierten Fassung" der Europäischen Datenschutzkonvention [SEV Nr. 108] sowie den Beitritt der EU zu dieser unterstützt und bei Drittländern für deren Beitritt wirbt. Diese Konvention ist ein völkerrechtlicher Vertrag, dem bislang 50 Länder beigetreten sind. Anknüpfend an die EU-Datenschutzgrundsätze stellt sie bindende Regeln für den Datenschutz und die internationale Datenübermittlung auf und strebt ein einheitlich hohes Schutzniveau bei ihren Vertragsstaaten an.
– Die Kommission will die behördliche Zusammenarbeit mit Drittländern verbessern, um die wirksame Durchsetzung von Datenschutzvorschriften zu erleichtern. Sie erwägt insbesondere (S. 14–15),
  - mit wichtigen Drittländern Rahmenübereinkommen – u.a. zur gegenseitigen Amtshilfe – zu schließen,
  - auf Basis von Art. 50 DSGVO „Mechanismen für die internationale Zusammenarbeit" zu entwickeln.

- **Internationale Zusammenarbeit bei der Strafverfolgung**
  - Auch im Bereich der Strafverfolgung und sonstigen Rechtsdurchsetzung will die Kommission die Zusammenarbeit mit Drittländern verbessern, um den Datenaustausch bei hohem Schutzniveau zu erleichtern.
  - Insbesondere kündigt die Kommission eine Prüfung der Möglichkeiten an (S. 15–18),
    - für „qualifizierte" Drittländer Angemessenheitsbeschlüsse nach Art. 36 Abs. 3 der Polizei-Richtlinie [(EU) 2016/680] zu erlassen sowie
    - mit Drittländern Datenschutz-Rahmenabkommen nach Vorbild des Abkommens zwischen der EU und den USA („Umbrella Agreement") auszuhandeln, um den Datenaustausch bei der Strafverfolgung und zur Durchsetzung staatlicher Maßnahmen im Bereich Wettbewerb/Verbraucherschutz zu verbessern.
  - Ferner will die Kommission (S. 16–18)
    - den datenschutzkonformen Austausch „elektronischer Beweismittel" – das sind z.B. elektronische Spuren eines Täters wie IP-Adressen – erleichtern und so die Strafverfolgung im „Cyberraum" verbessern;
    - die Datenschutzregeln bestehender Kooperationsabkommen zwischen Europol und „Dritten" – etwa den Strafverfolgungsbehörden in Drittstaaten – überprüfen;
    - beim Austausch von Fluggastdatensätzen (PNR, s. cep**Analyse**) mit Drittstaaten „einheitliche Standards und einen besonderen Grundrechtsschutz" anwenden und ggf. eine Modellvereinbarung erarbeiten.

Politischer Kontext

In ihrem Arbeitsprogramm 2017 [COM(2016) 710] kündigte die Kommission bereits die Prüfung neuer Angemessenheitsbeschlüsse für ein „hohes Schutzniveau im Datenaustausch" mit Drittländern an (S. 14).

Politische Einflussmöglichkeiten

Generaldirektionen: GD Justiz und Verbraucher (federführend)

BEWERTUNG

Ökonomische Folgenabschätzung

Die von der Kommission **geplante Erleichterung der Datenübermittlung in Drittländer senkt** tendenziell den Aufwand und damit **die Kosten, die** europäische wie außereuropäische **Unternehmen** häufig **tragen müssen, wenn sie Daten** rechtskonform **aus der EU** in Drittländer **übermitteln wollen.** Diese Kosten bestehen etwa in den notwendigen Vertragsabschlüssen mit Standarddatenschutzklauseln oder der aufwendigen unternehmensinternen Implementierung von BCR zur Datenübermittlung in ein Drittland (vgl. cep**Studie** zum Privacy Shield) beim Fehlen eines entsprechenden Angemessenheitsbeschlusses.
Die Instrumente der DSGVO – mit der die Kommission die Erleichterung hauptsächlich erreichen will – sind grundsätzlich zweckmäßig. Allerdings ist bei ihrer Anwendung Vorsicht geboten:
Durch den vermehrten Einsatz von Angemessenheitsbeschlüssen ist Unternehmen zwar häufiger eine Datenübermittlung ins Drittland ohne weitere Genehmigungen oder Garantien möglich. In der Folge werden betroffene Unternehmen entlastet und genießen Rechtssicherheit. Angemessenheitsbeschlüsse können aber ihre Rechtfertigung verlieren, wenn zuvor unbekannte, schwerwiegende Datenschutzdefizite im Drittland offenbar werden oder neu entstehen. Dies kann im Grenzfall dazu führen, dass der Europäische Gerichtshof (EuGH) sie für ungültig, da rechtswidrig erklärt. Dies geschah bei dem ehemaligen Angemessenheitsbeschluss für die USA („Safe Harbour"), nachdem umfassende Zugriffe auf die Daten europäischer Bürger durch amerikanische Geheimdienste bekannt worden waren [vgl. Schrems-Urteil (C-362/14), cep**Studie** zum Privacy Shield]. Betroffene Unternehmen sehen sich in einem solchen Fall erheblicher Rechtsunsicherheit gegenüber und müssen ggf. sehr kurzfristig auf alternative Rechtsgrundlagen ausweichen. Die von der Kommission vorgesehene Überwachung und regelmäßige Prüfung der bestehenden Angemessenheitsbeschlüsse ist daher unverzichtbar. Nur so kann ein Absinken des Datenschutzniveaus in Drittländern frühzeitig erkannt, diesem eventuell gegengesteuert und so ein hohes Datenschutzniveau durchgesetzt werden.
Dass die Kommission sich bei der Auswahl der Drittländer, mit denen sie Angemessenheitsbeschlüsse fassen will, an wirtschaftlichen oder politischen Überlegungen – etwa dem Umfang der Handelsbeziehungen mit einem Drittland – orientieren will, erhöht tendenziell den Nutzen der Beschlüsse. Das Datenschutzniveau darf durch solche Überlegungen und den damit einhergehenden Druck aber nicht untergraben werden.
Eine Anpassung der alternativen Instrumente zur Datenübermittlung an einzelne Industriezweige, Geschäftsmodelle und Wirtschaftsteilnehmer erweitert zwar ihren Anwendungsbereich und erleichtert ihre Implementierung und Verwendung für Unternehmen.
Die alternativen Instrumente allein können aber in der Regel keinen ausreichenden Datenschutz in Drittländern garantieren, da sie nur die beteiligten Unternehmen, nicht dagegen die Staaten binden (s.a. juristische Bewertung)**.** Ihr Einsatz ist folglich für Unternehmen durchaus risikobehaftet, da sie in der EU für im Drittland begangene Datenschutzverstöße haften können. In Ermangelung von Alternativen sollte die Kommission die Instrumente daher zwar fördern, aber darauf hinwirken, dass ihre Schutzlücken durch zusätzliche Anforderungen – etwa eine Pflicht zur Verschlüsselung der Daten – geschlossen werden.
Letztlich ermöglicht – abseits aller Instrumente – **nur eine tatsächliche Angleichung der Datenschutzniveaus in Drittländern an das Niveau der EU einen wirklich hohen Datenschutz** und somit eine stabile Erleichterung bei der Übermittlung von Daten. **Es ist daher sachgerecht, dass die Kommission sich** in Foren –

wie dem G-20-Gipfel – **für hohe Datenschutzniveaus in Drittländern einsetzen** sowie für die EU-Datenschutzkonvention werben **will.**

Juristische Bewertung

Kompetenz

Unproblematisch.

Subsidiarität

Angemessenheitsbeschlüsse und Beschlüsse, durch die die Kommission Standarddatenschutzklauseln erlässt oder genehmigt, sind Durchführungsrechtsakte, die sich im Rahmen der EU-Verträge halten und im Ausschussverfahren erlassen werden müssen (Art 45 Abs. 3, 46 Abs. 2, 93 DSGVO). Soweit die EU für den Abschluss internationaler Rahmenabkommen ausschließlich zuständig ist, ist das Subsidiaritätsprinzip nicht anwendbar.

Sonstige Vereinbarkeit mit EU-Recht

Die DSGVO ermöglicht flexiblere Lösungen für Datenübermittlungen in der Wirtschaft oder zwischen Behörden als die bisherige Datenschutzrichtlinie 95/46/EG. Sie stellt an diese aber auch hohe Anforderungen, deren tatsächliche Erfüllbarkeit in der Praxis fraglich ist.

Die dem Angemessenheitsbeschluss immanente Vorstellung, dass Drittländer in allen notwendigen Belangen **ein „angemessenes" Schutzniveau aufweisen können, ist** – auch angesichts genauerer Vorgaben durch den EuGH – **derzeit** in der Praxis **wenig realistisch.** Genau dies ist aber Voraussetzung für einen Angemessenheitsbeschluss. Welche „Verbiegungen" nötig sind, zeigt der „Privacy Shield"-Beschluss der Kommission für die USA. Hinzu kommt, dass wegen der anstehenden Erhöhung des Schutzniveaus in der EU durch die DSGVO im Prinzip alle bestehenden Angemessenheitsbeschlüsse überprüft werden müssen. Die Kommission sollte auch diesen Überprüfungen klar Priorität einräumen.

Alternative Übermittlungsinstrumente wie Standarddatenschutzklauseln und BCR müssen nicht nur „geeignete Garantien" bieten. Darüber hinaus müssen die Betroffenen im Drittland „durchsetzbare Rechte und wirksame Rechtsbehelfe" haben (Art. 46 Abs. 1 DSGVO). Der Europäische Gerichtshof (EuGH) hat insoweit im Schrems-Urteil (C-362/14) gefordert, dass sich Betroffene im Drittland nicht nur gegen Grundrechtseingriffe durch staatliche Maßnahmen wehren, sondern dort auch ihre Rechte auf Zugang zu sowie Berichtigung oder Löschung von Daten durchsetzen können müssen.

Der EuGH hat zudem weitere Voraussetzungen für Angemessenheitsbeschlüsse aufgestellt, die auf alternative Übermittlungsinstrumente wie Standarddatenschutzklauseln und BCR übertragbar sind (vgl. cep**Studie** zum Privacy Shield). So muss es u.a. wirksame Mechanismen zur Überwachung und Kontrolle der Einhaltung der Datenschutzregeln geben. Eingriffe in das Grundrecht auf Schutz personenbezogener Daten – etwa durch Behördenzugriffe – müssen sich auf das „absolut Notwendige" beschränken. Insbesondere letzteres ist in der Praxis nicht nur politisch schwer durchsetzbar, sondern lässt sich auch nicht durch vertragliche **Standarddatenschutzklauseln oder BCR** regeln. Denn diese **binden nur die beteiligten Unternehmen**, nicht aber das Drittland selbst bzw. dessen Behörden. **Sie können daher weder** anlass- und grenzenlose **Datenzugriffe durch Geheimdienste im Drittland verhindern noch das Fehlen wirksamer** gerichtlicher **Rechtsbehelfe kompensieren.**

Eine Einschätzung der EU-Datenschutzbehörden zu der Frage, inwieweit Standarddatenschutzklauseln und BCR im Lichte der EuGH-Rechtsprechung überhaupt weiter verwendet werden dürfen, steht noch aus. Bis zu einer Entscheidung des EuGH ist die Zukunft dieser Instrumente ungewiss. Der EuGH wird in einem beim irischen High Court anhängigen Verfahren (Az. 2016/4809P) möglicherweise bald Gelegenheit erhalten, zur Verwendbarkeit der Klauseln für Datentransfers in die USA Stellung zu nehmen. Es ist nicht unrealistisch, dass er auch an den Klauseln Kritik üben wird.

Datenschutzrechtliche Defizite im Drittland können aber ggf. dadurch verringert werden, dass die EU in internationalen Abkommen mit Drittländern auch die notwendigen Datenschutzgarantien – z.B. eine Beschränkung staatlicher Zugriffe oder effektive Kontrollen und Rechtsmittel – verbindlich vereinbart, anstatt insoweit – wie beim „Privacy Shield" – auf vage Zusagen ausländischer Regierungen zu vertrauen. Problematisch ist, dass internationale Abkommen völkerrechtlich über das EU-Recht hinaus Wirkung entfalten und – anders als Angemessenheitsbeschlüsse – vom EuGH als solche nicht für ungültig erklärt werden können.

Auswirkungen auf das deutsche Recht

Abhängig von der konkreten Ausgestaltung.

Zusammenfassung der Bewertung

Die geplante Erleichterung der Datenübermittlung in Drittländer senkt die Kosten, die Unternehmen tragen müssen, wenn sie Daten aus der EU übermitteln wollen. Die dem Angemessenheitsbeschluss immanente Vorstellung, dass Drittländer ein „angemessenes" Schutzniveau aufweisen können, ist derzeit aber wenig realistisch. Standarddatenschutzklauseln und BCR binden nur die beteiligten Unternehmen. Sie können daher weder Datenzugriffe durch Geheimdienste im Drittland verhindern noch das Fehlen wirksamer Rechtsbehelfe kompensieren. Letztlich ermöglicht nur eine tatsächliche Angleichung der Datenschutzniveaus in Drittländern an das Niveau der EU einen wirklich hohen Datenschutz. Es ist daher sachgerecht, dass die Kommission sich für hohe Datenschutzniveaus in Drittländern einsetzen will.