Neue Regeln für den internationalen Datenverkehr

Grenzübertritt

Naida Šehić

Innerhalb der EU ist der Austausch personenbezogener Daten in der Regel unproblematisch. Bei Drittländern kann man ein „angemessenes Datenschutzniveau“ jedoch nicht automatisch voraussetzen. Was also tun?

Der globale Handel und die voranschreitende Digitalisierung und Vernetzung der Wirtschaft machen grenzüberschreitende Datenflüsse erforderlich. Um diesen Anforderungen gerecht zu werden, gilt im europäischen Binnenmarkt der Grundsatz des freien Datenverkehrs: Personenbezogene Daten dürfen und sollen ungehindert zwischen den Mitgliedstaaten der Europäischen Union fließen.

Wenn für die Verarbeitung personenbezogener Daten und damit für ihre Übermittlung eine Rechtsgrundlage besteht, dürfen diese innerhalb der EU ohne weitere Einschränkungen zwischen dem Datenexporteur und dem -importeur fließen, da in den Mitgliedstaaten ein angemessenes Datenschutzniveau gewährleistet ist. Sobald aber personenbezogene Daten in Länder außerhalb der EU übermittelt werden sollen, ist ein genauerer Blick in die Datenschutz-Grundverordnung (DSGVO) geboten.

Datenübermittlung nach Angemessenheitsbeschluss

Nach europäischem Datenschutzrecht besteht in Ländern außerhalb der EU kein angemessenes Datenschutzniveau. Die Rechtsordnungen dieser Länder können nach Auffassung der EU den Schutz personenbezogener Daten nicht ausreichend garantieren. Aus diesem Grund schränkt die DSGVO internationale Datenübermittlungen ein. Personenbezogene Daten dürfen nur dann in sogenannte Drittländer übermittelt werden, wenn in dem Empfangsstaat ein angemessenes Datenschutzniveau gewährleistet ist, der Datenimporteur ein solches durch geeignete Garantien herstellt oder die Datenübermittlung einer Ausnahmeregelung nach der DSGVO unterliegt.

Die Europäische Kommission kann mittels eines Beschlusses festlegen, dass ein bestimmtes Land, aber auch ein Wirtschaftszweig oder ein Gebiet außerhalb der EU ein hohes und demnach „angemessenes Datenschutzniveau“ gewährleistet.

Ist die Kommission von der Gleichwertigkeit des Datenschutzniveaus eines Landes überzeugt und erlässt sie einen Angemessenheitsbeschluss für dieses Land, unterliegt die Übermittlung personenbezogener Daten in das jeweilige Land keinen weiteren Einschränkungen. Derzeit ist die Liste der Staaten, für die die Kommission Angemessenheitsbeschlüsse erlassen hat, jedoch überschaubar: Andorra, Argentinien, Kanada (gilt

nur für private Stellen), Schweiz, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay. Zurzeit verhandelt die Kommission über Angemessenheitsbeschlüsse mit Japan und Südkorea. In einen Dialog zur „Angemessenheit ihres Datenschutzes“ wolle man ebenfalls mit Indien, Brasilien und Paraguay treten.

Wenn das Vereinigte Königreich am 29. März 2019 die EU verlässt, wird es aus datenschutzrechtlicher Sicht als Drittland gelten, sofern bis dahin keine Vereinbarungen zwischen der EU und Großbritannien erzielt werden können. Aus diesem Grund sollten deutsche Unternehmen bereits jetzt vertragliche Vorkehrungen mit Dienstleistern jenseits des Ärmelkanals treffen.

Für die USA besteht lediglich ein sektorspezifischer Angemessenheitsbeschluss der Kommission. Personenbezogene Daten dürfen ohne weitere Einschränkungen nur an US-Unternehmen übermittelt werden, die nach dem Programm „EU-U.S. Privacy Shield“ zertifiziert sind. Die Zertifizierung kann für Beschäftigtendaten (Human Resources; HR) sowie für alle übrigen Kategorien (Non-HR) erfolgen. Alle Unternehmen mit gültigen Privacy-Shield-Zertifizierungen sind auf der offiziellen Website des Programms öffentlich einsehbar (https://www.privacyshield.gov).

Neu nach der DSGVO ist das Erfordernis einer regelmäßigen Überprüfung der Angemessenheitsentscheidungen durch die Kommission spätestens alle vier Jahre, um ein kontinuierlich hohes Datenschutzniveau und die Einhaltung von Grundrechten im Drittland sicherzustellen.

Alternative Datenübermittlungsinstrumente

Liegt kein Angemessenheitsbeschluss der Europäischen Kommission für ein Drittland vor, können Unternehmen dennoch personenbezogene Daten dorthin übermitteln, wenn sie sich der alternativen Übermittlungsinstrumente nach der DSGVO bedienen (Abbildung). Diese Instrumente kompensieren das unzureichende Datenschutzniveau in einem Land, in dem der Datenimporteur selbst geeignete Garantien in Form von durchsetzbaren Rechten und wirksamen Rechtsbehelfen für die betroffenen Personen vorsieht. Im Folgenden sollen die wichtigsten alternativen Übermittlungsinstrumente nach der DSGVO skizziert werden.

Die sogenannten Standardvertragsklauseln erfreuen sich bei Unternehmen weiterhin großer Beliebtheit. Hierbei handelt es sich um durch die EU-Kommission vorgegebene Datenschutzverträge, die zwischen dem Datenexporteur und dem -importeur abgeschlossen werden können, um grenzüberschreitende Datenübermittlungen zu legitimieren. Die DSGVO spricht von „Standarddatenschutzklauseln“, dabei handelt es sich jedoch um dasselbe Instrument.

Es bestehen unterschiedliche Fassungen, je nachdem, ob die Datenübermittlung zwischen einem in der EU sitzenden Verantwortlichen und einem Verantwortlichen außerhalb der EU stattfindet oder ob es sich bei dem Datenempfänger im Drittland um einen Auftragsverarbeiter handelt (Controller to Controller und Controller to Processor). Die Standardvertragsklauseln sind auf der Website der Kommission abrufbar und müssen in einzelnen Punkten noch ausgefüllt werden (zum Beispiel Kategorien der zu übermittelnden Daten, Kreis der betroffenen Personen sowie technische und organisatorische Maßnahmen). Der vorgegebene Vertragstext darf jedoch nicht geändert werden, anderenfalls sind die Standarddatenschutzklauseln unwirksam.

Standardvertragsklauseln zunächst weiter gültig

Die derzeit verfügbaren Standardvertragsklauseln nehmen immer noch Bezug auf die bald obsolete EU-Datenschutzrichtlinie, was jedoch ihre Gültigkeit auch nach dem 25. Mai 2018 nicht beeinträchtigen sollte. Jedenfalls nicht, solange die Kommission keine DSGVO-konformen Standarddatenschutzklauseln erlassen hat. Die Kommission plant jedoch, auf die Bedürfnisse der Wirtschaft näher einzugehen und die Standarddatenschutzklauseln mit technischen und sektorspezifischen Klauseln zu ergänzen (beispielsweise für das Outsourcing von IT-Dienstleistungen oder die Verarbeitung sensibler Daten).

Standarddatenschutzklauseln bedürfen keiner weiteren Genehmigung durch die Aufsichtsbehörde. Sie können ausschließlich zwischen einem in der EU ansässigen Datenexporteur und einem außerhalb der EU sitzenden Datenimporteur wirksam abgeschlossen werden. Das Instrument eignet sich nicht zur Regelung von Datenübertragungen zwischen Unternehmen, die beide ihren Sitz in der EU haben. Eine Neuerung nach der DSGVO ist, dass auch Aufsichtsbehörden Standarddatenschutzklauseln erlassen dürfen, sofern diese vorab von der Europäischen Kommission genehmigt wurden.

Global agierende Unternehmen können auch selbst interne Regelungen für die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der Unternehmensgruppe festlegen und von der zuständigen Aufsichtsbehörde genehmigen lassen. Diese sogenannten Binding Corporate Rules (BCR) rechtfertigen zwar grenzüberschreitende Intercompany-Datentransfers, eignen sich jedoch nicht für die Legitimierung von Datenübermittlungen außerhalb der Unternehmensgruppe. Sie sind also vor allem für globale Konzerne sinnvoll. In Deutschland hat nur eine kleine Anzahl von Konzernen genehmigte Binding Corporate Rules erlassen.

DSGVO erlaubt branchenspezifische Kodizes

Durch die DSGVO soll auch ausdrücklich die Schaffung von sektorspezifischen Verhaltensregeln für den Datenschutz gefördert werden. Wirtschaftsverbände haben die Möglichkeit, datenschutzrechtliche Verhaltensregelungen für ihre Branchen auszuarbeiten. Ist ein solcher Verhaltenskodex (Code of Conduct) durch eine Aufsichtsbehörde offiziell genehmigt, können Unternehmen aus Drittländern, die sich diesem unterwerfen, auf Basis dieser Regelungen auch personenbezogene Daten aus der EU empfangen. Sie müssen allerdings rechtsverbindlich zusichern, die in den Verhaltensregelungen niedergelegten Pflichten zu erfüllen. Dieses alternative Instrument zur Übermittlung personenbezogener Daten an Drittländer ist eine Neuheit im Datenschutzrecht.

Unternehmen aus der EU sowie aus Nicht-EU-Ländern werden ab 25. Mai 2018 zudem die Möglichkeit haben, die Einhaltung der DSGVO mittels einer offiziell anerkannten Datenschutzzertifizierung nachzuweisen. Für die Auswahl und Akkreditierung der entsprechenden Zertifizierungsstellen sieht die DSGVO nun spezielle Regelungen vor. Die Kriterien für eine Zertifizierung sollen von den Aufsichtsbehörden auf Basis einschlägiger ISO-Normen entwickelt werden.

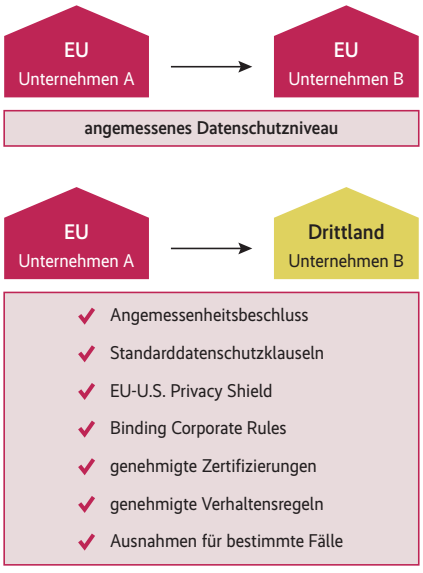
Diese Zertifizierungen können als Grundlage für grenzüberschreitende Datenübermittlungen dienen. Unternehmen aus der EU können dann personenbezogene Daten an zertifizierte Unternehmen außerhalb der EU übermitteln, sofern Letztere sich rechtsverbindlich und durchsetzbar dazu verpflichten, diese Da-

ten zu schützen. Diese Zertifizierungen müssen spätestens innerhalb von drei Jahren ab Ausstellung erneuert werden. In Deutschland führt die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden die Akkreditierung durch.

Keine Regeln ohne Ausnahme

Die DSGVO lässt, so wie auch schon das frühere Datenschutzrecht, Ausnahmen für die Übermittlung personenbezogener Daten an Unternehmen in Drittländern zu, für die weder ein Angemessenheitsbeschluss der Kommission besteht noch die oben genannten alternativen Instrumente zum Tragen kommen. Der Katalog der bestehenden Ausnahmen ist weit gefasst, deren Anwendung jedoch an enge Voraussetzungen geknüpft.

So dürfen beispielsweise personenbezogene Daten auf Basis einer Einwilligung des Betroffenen an Unternehmen außerhalb der EU übermittelt werden. Doch die Hürden für die zulässige Ausgestaltung einer solchen Einwilligung nach der DSGVO sind hoch – die betroffene Person muss diese ausdrücklich abgegeben haben und über die Risiken der beabsichtigten Datenübermittlung in das betreffende Drittland vorher informiert worden sein. Zudem muss die Einwilligung ausreichend bestimmt, das heißt, Art, Umfang und Zweck der Übermittlung müssen genau festgelegt sein.



Unternehmen aus Nicht-EU-Ländern stehen verschiedene Möglichkeiten offen, ein angemessenes Datenschutzniveau nachzuweisen.

Insbesondere bei grenzüberschreitenden Datenübermittlungen erweist es sich in der Praxis jedoch als schwierig, die geforderten Informationen gegenüber der betroffenen Person bereitzustellen. Denn oftmals ist für den Datenexporteur selbst nicht genau absehbar, welche weiteren Stellen neben dem festgelegten Empfänger Zugriff auf die personenbezogenen Daten im Zielland haben (könnten). Als weiteres Risiko kommt hinzu, dass die betroffene Person jederzeit das Recht hat, die erteilte Einwilligung zu widerrufen. Im Falle eines Widerrufs müsste auch die darauf gestützte grenzüberschreitende Datenübermittlung unterbleiben oder sich eines anderen Instruments bedienen.

Auch dürfen personenbezogene Daten zur Durchführung eines Vertrags mit der betroffenen Person oder in ihrem Interesse sowie zur Durchsetzung oder Verteidigung von Rechtsansprüchen an Stellen außerhalb der EU übermittelt werden. Die Datenübermittlung muss allerdings zur Erreichung der vorgenannten Zwecke tatsächlich erforderlich sein und darf nur gelegentlich und nicht wiederkehrend erfolgen.

„Gelegentlich" heißt nicht „ständig"

Dazu haben die europäischen Aufsichtsbehörden bereits klargestellt, dass Datenübermittlungen, die zwischen zwei Stellen systematisch und im Rahmen einer stabilen Geschäftsbeziehung erfolgen (etwa bei Bereitstellung einer Schnittstelle zu IT-Anwendungen), nicht als „gelegentlich" und „nicht wiederkehrend" qualifiziert werden können. Die Ausnahme kommt aber in Betracht, wenn beispielsweise im Rahmen einer Reisebuchung personenbezogene Daten des Reisenden an Hotels oder andere Reisedienstleister außerhalb der EU übermittelt werden.

Unter den Ausnahmen nach DSGVO sind auch die „zwingenden berechtigten Interessen" des Datenexporteurs hervorzuheben. Wenn die beabsichtigte Datenübermittlung nicht wiederkehrend ist, lediglich eine begrenzte Anzahl von Personen betrifft, der Datenexporteur ein zwingendes berechtigtes Interesse an der Übermittlung nachweisen kann und ihm kein anderes Instrument zur Übermittlung personenbezogener Daten an eine Stelle außerhalb der EU zur Verfügung steht, darf die Datenübermittlung in das jeweilige Drittland stattfinden.

Der Datenexporteur muss jedoch ernsthafte Versuche zur Heranziehung eines anderen Übermittlungsinstruments nachweisen können. Außerdem muss er die zuständige Aufsichtsbehörde und die betroffenen Personen über die Datenübermittlung informieren. Aus diesem Grund kommt diese Ausnahmeregelung nur in Einzelfällen und auch nur als letztes Mittel zur Rechtfertigung in Betracht.

Verstöße gegen die in der DSGVO niedergelegten Vorschriften bezüglich der Übermittlung personenbezogener Daten außerhalb der EU können mit einem Bußgeld von 20 Millionen Euro oder mit bis zu 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs belegt werden, es gilt der höhere Betrag. Die Aufsichtsbehörden sollen bei der Verhängung von Sanktionen unter anderem das Vorhandensein genehmigter Verhaltensregeln oder einer genehmigten Zertifizierung als mildernden Umstand berücksichtigen.

Ausblick

Im Vergleich zum bisherigen Datenschutzrecht sieht die DSGVO ein breiteres Spektrum von Instrumenten zur Rechtfertigung von Datenübermittlungen in Länder außerhalb der EU vor (siehe Abbildung). Neben altbewährten Instrumenten wie Angemessenheitsentscheidungen der Kommission, Standardvertragsklauseln oder Binding Corporate Rules führt die DSGVO auch neue Übermittlungsmechanismen wie etwa genehmigte Verhaltensregeln und Zertifizierungen ein. Es bleibt abzuwarten, ob diese neuen Mechanismen auch Erleichterungen für die Praxis bringen werden.

Zudem baut die DSGVO die Ausnahmeregelungen für Datenübermittlungen in bestimmten Einzelfällen aus und stellt durch die erhöhten Zulässigkeitsvoraussetzungen zugleich klar, dass diese Instrumente eine Ausnahme und nicht die Regel sein können. Unternehmen ist anzuraten, für sämtliche Übermittlungen personenbezogener Daten in Länder außerhalb der EU ein passendes Rechtfertigungsinstrument nach der DSGVO zu wählen und anzuwenden, da Verstöße in diesem Bereich mit empfindlichen Bußgeldern geahndet werden können. (ur@ix.de)

Naida Šehić

ist Juristin und Consultant bei der ISiCO Datenschutz GmbH sowie zertifizierte Datenschutzbeauftragte (TÜV Nord) und Mitglied der International Association of Privacy Professionals (IAPP).