Neue Regeln für den Datentransfer in Drittstaaten

© mitay20 - stock.adobe.com

Datenschutz. Spätestens seit Einführung der EU-Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 sollte für jedes Unternehmen klar sein, dass bei der Übermittlung personenbezogener Daten in Länder außerhalb des Europäischen Wirtschaftsraums (sog. Drittstaaten) Vorsicht geboten ist. Die Rechtsanwälte Georg Huber und Fabian Bösch von der Kanzlei Greiter, Pegger, Kofler & Partner infomieren in diesem Zusammenhang über die neuen Standarddatenschutzklauseln der EU.

Nach der DSGVO muss bei einer Datenübermittlung in Drittstaaten neben den allgemeinen Voraussetzungen der Datenverarbeitung zusätzlich zumindest eine der folgenden Voraussetzungen vorliegen:

- Angemessenheitsbeschluss der EU-Kommission
- Konzerninterne Binding Corporate Rules
- Standarddatenschutzklauseln
- Genehmigte branchenweite Verhaltensregeln
- Individuell genehmigte Verträge
- Einzelfallausnahmen für bestimmte (limitierte) Verarbeitungsvorgänge (Einwilligungen, Notwendigkeit für Vertragserfüllung etc.)

Die weit überwiegende Anzahl der Übermittlungen in Drittstaaten basiert entweder auf einem Angemessenheitsbeschluss oder auf den Standarddatenschutzklauseln.

Angemessenheitsbeschluss und andere Ausnahmen

Angemessenheitsbeschlüsse für Drittländer erlässt die EU-Kommission dann, wenn im betroffenen Land ein gleich hohes Datenschutzniveau wie in der EU herrscht.

Derzeit gibt es einige wenige Angemessenheitsbeschlüsse, unter anderem für Argentinien, Kanada, Israel, Japan, Neuseeland, Schweiz und jüngst auch für das Vereinigte Königreich. Für die USA wurde der frühere Angemessenheitsbeschluss, das sogenannte „Privacy Shield“, mit dem Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 für ungültig erklärt.

Bei Datenübermittlungen in andere Staaten

wird in der Regel der Abschluss von Standarddatenschutzklauseln („SCC“ – „Standard Contract Clauses“), also eines Datenschutzvertrages mit dem jeweiligen Datenempfänger, erforderlich sein.

Zu den häufigsten Datenempfängern gehören Internetgiganten und Cloudanbieter wie Microsoft Office 365, Amazon Web Services (AWS), Google Analytics, Salesforce, SAP, Facebook, aber auch MailChimp. Datentransfers in Drittländer betreffen daher nicht nur große Konzerne, sondern auch viele KMU. Auch KMU müssen daher sicherstellen, dass SCC vereinbart wurden.

Neue Standarddatenschutzklauseln

Mit Beschluss vom 4. Juni 2021 hat die EU-Kommission neue, an die DSGVO angepasste Versionen der SCC geschaffen.

Die neuen SCC enthalten vier verschiedene Module (statt bisher nur zwei Varianten), je eine für die Übermittlung

- von Verantwortlichem zu Verantwortlichem,
- von Verantwortlichem zu Auftragsverarbeiter,
- von Auftragsverarbeiter zu (Sub-)Auftragsverarbeiter und
- von Auftragsverarbeiter zu Verantwortlichem.

Die wichtigsten Neuerungen der neuen Standardvertragsklauseln sind laut EU-Kommission:

- Aktualisierung im Einklang mit der DSGVO;
- Abdeckung einer breiten Palette von Transferszenarien anstelle separater Klauseln;
- mehr Flexibilität bei komplexen Verarbeitungsketten dank eines „modularen Ansatzes“ und der Möglichkeit, dass sich mehr als zwei Parteien anschließen und die Klauseln nutzen können;
- ein Werkzeug für die Einhaltung des Schrems-II-Urteils;
- Beispiele möglicher „zusätzlicher Maßnahmen“ wie Verschlüsselung, die Unternehmen erforderlichenfalls ergreifen können.

Außerdem enthalten die neuen SCC auch schon die Regelungen für einen Auftragsverarbeitervertrag, sodass hierfür – anders als bisher – keine gesonderte Vereinbarung mehr benötigt wird.

Die alte Version der SCC sollte künftig nicht mehr verwendet werden. Außerdem müssen alle schon bisher abgeschlossenen (alten) SCC bis spätestens 27.12.2022 durch die neuen SCC ersetzt werden, da diese dann von den Datenschutz Behörden nicht mehr als ausreichend anerkannt werden und Bußgelder drohen. Hier besteht also in den nächsten Monaten dringender Handlungsbedarf.

Bei Verwendung der neuen SCC sollte genau darauf geachtet werden, dass die jeweils richtige Va-riante der vier Module verwendet wird. Der Datenexporteur muss also vorab genau klären, wie die Rollenverteilung zwischen ihm und dem Datenempfänger ausgestaltet ist (Wer ist Verantwortlicher? Wer ist (Sub-)Auftragsverarbeiter?).

Es ist denkbar, dass in einem Unternehmen verschiedene Varianten der SCC abgeschlossen werden müssen, eben je nachdem, wer der Empfänger der Daten ist und welche Rollenverteilung vorliegt. Mit jedem einzelnen Datenempfänger sind SCC abzuschließen.

Anders als Angemessenheitsbeschlüsse bieten die SCC aber keinen absoluten Schutz, sondern sehen immer auch eine Pflicht des Übermittlers und des Empfängers vor, einen allfälligen Mangel des Datenschutzniveaus im Empfängerland zu prüfen und gegebenenfalls in geeigneter Weise auszugleichen. Das ist insbesondere für Länder wie China, aber auch die USA schwierig.

Insbesondere muss sichergestellt werden, dass die Daten vor Eingriffen durch staatliche Überwachungsprogramme (z. B. Geheimdienste wie die amerikanische NSA) geschützt sind und dass den Betroffenen geeignete Mittel zur Verfügung stehen, sich gegen unverhältnismäßige staatliche Eingriffe zu wehren. Oftmals führt dies dazu, dass eine Übermittlung in Drittländer nur mit umfassenden technischen Sicherheitsmaßnahmen, insbesondere einer Verschlüsselung der Daten, zulässig sein wird.

Zu beachten ist darüber hinaus, dass eine Drittlandübertragung auch dann vorliegen kann, wenn zwar der Datenempfänger innerhalb des EWR ist, aber Personen aus Drittländern Zugriff auf die Daten haben. Das könnte typischerweise der Fall sein, wenn US-Unternehmen Cloudservices in Europa anbieten, aber aufgrund ihrer nationalen Gesetze, z. B. dem US Cloud Act, gezwungen sein könnten, Daten aus der europäischen Cloud an die US-Behörden herauszugeben.

Handlungsempfehlungen

1. Für jede Datenübermittlung in einen Drittstaat ist zu prüfen, ob eine hinreichende Grundlage für die Übermittlung nach der DSGVO vorliegt.
2. Ist das nicht der Fall, sollten unverzüglich die neuen Standarddatenschutzklauseln mit dem jeweiligen Empfänger abgeschlossen werden und gleichzeitig geprüft werden, ob hinreichende Garantien im Empfängerland für den Schutz der Daten bestehen.
3. Gibt es keine solchen Garantien sind technische Vorkehrungen, wie etwa eine Verschlüsselung zu prüfen. Allenfalls ist auch zu prüfen, ob nicht etwa auch ein Dienstleister aus dem EWR herangezogen werden könnte (z.B. für den Email-Versand).
4. Auf systematische Datenübermittlungen in die USA sollte aufgrund der derzeit unsicheren Lage so weit wie möglich verzichtet werden.
5. Alle bereits abgeschlossenen (alten) Standarddatenschutzklauseln müssen durch die neue Version der SCC ersetzt werden. Hierzu sollte man rechtzeitig an die jeweiligen Vertragspartner herantreten. ▲

Zu den Autoren:

RA Dr. Georg Huber, LL.M., CIPP/E
ist Rechtsanwalt bei Greiter Pegger Kofler & Partner in Innsbruck. Er hat unter anderem an der University of Chicago studiert und ist als Anwalt in Österreich und in New York zugelassen.
Mag. Fabian Bösch, B.A. ist Rechtsanwalt und Partner in der Kanzlei Greiter Pegger Kofler & Partner (www.lawfirm.at). Seine Tätigkeitsschwerpunkte liegen im Arbeits- und Datenschutzrecht sowie in den Bereichen Digitalisierung, IP- und IT-Recht. Er ist außerdem auch zertifizierter Datenschutzbeauftragter (TÜV).