Neue DPAs von AWS und Microsoft: Ist jetzt alles gut?

AWS und Microsoft haben in den letzten Wochen neue Verträge zur Datenverarbeitung veröffentlicht („data processing agreement/addendum", kurz „DPA"). Damit gelten für die Angebote dieser beiden großen Dienstleister jetzt insbesondere die neuen Standardvertragsklauseln. Sind damit alle „US-Probleme" gelöst? Ganz so einfach ist es nicht.

Worum geht es?

Für viele von Ihnen ist es inzwischen der tägliche Begleiter: Risikohinweise bei einem Datentransfer in die USA. Kaum ein größeres Reizthema begleitet die Datenschützer nun seit über einem Jahr. US-Dienstleister können kaum ohne Datenschutzrisiko genutzt werden, denn zumindest für Support-Dienstleistungen greifen fast alle von ihnen aus den USA heraus auf die Kundendaten zu. Und in den USA ist, so der EuGH im vergangenen Jahr, ein angemessenes Datenschutzniveau ohne eine – nicht absehbare – politische Lösung kaum mehr zu erreichen. Das ist eine Patt-Situation. Denn ohne US-Dienstleister kann kaum ein Unternehmen wirtschaften. EU-Lösungen sind in der gleichen Praktikabilität schlicht nicht flächendeckend verfügbar.

Was tun?

In der Praxis ist die Risikominimierung das zu erreichende Ziel. Grundlage für die Absicherung des Datenschutzniveaus (und damit der Einhaltung der DSGVO) sind in den meisten Fällen die sog. Standardvertragsklauseln (oder auch: Standarddatenschutzklauseln) der EU-Kommission. Diese mussten in den letzten Monaten dann jeweils umfangreich mit „zusätzlichen Maßnahmen" ergänzt werden, um den Anforderungen des EuGH möglichst gut zu entsprechen. Je nach genutztem US-Dienst können etwa Daten hochwirksam verschlüsselt oder so pseudonymisiert werden, dass der US-Dienstleister (und auch die US-Geheimdienste) diese keiner Person zuordnen können. Das ist aufwendig und nicht immer eine umsetzbare Lösung.

Im Juni hat die EU-Kommission neue Standardvertragsklauseln veröffentlicht („Standard Contractual Clauses“, kurz „SCC“). Viele von den nach der EuGH-Entscheidung im Sommer 2020 entwickelten „zusätzlichen Maßnahmen“ für einen besseren Datenschutz sind implementiert. Das betrifft z.B. Informations- und Abwehrpflichten, wenn Geheimdienste aus dem Drittstaat auf Daten zugreifen wollen. Enthalten sind jetzt auch Dokumentationspflichten, was das nationale Recht im Drittstaat überhaupt zulässt und erlaubt an Datenzugriffen.

Seit dem 27.09.2021 müssen für alle neuen Verträge mit Drittstaatentransfer diese neuen SCC 2021 verwendet werden. Altverträge können noch bis Dezember 2022 umgestellt werden.

Rechtssicher ist ein Drittstaatentransfer auch mit den neuen SCC 2021 nicht ohne weiteres. Die neuen Klauseln helfen aber ungemein, Rechtssicherheit zu erreichen.

Und was ist jetzt mit AWS und Microsoft?

Amazon Web Services Inc. („AWS“) und Microsoft haben in den letzten Tagen neue Datenschutzvereinbarungen veröffentlicht. Die DPA sind kein eigener Vertragstyp, sondern enthalten die Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO und Standardvertragsklauseln für den Drittstaatentransfer. Letztere sind notwendig, da beide Unternehmen i.d.R. zumindest aus den USA heraus im Support-Fall auf personenbezogene Daten zugreifen können. Ohne gesonderte Einstellung werden die in den Cloud-Diensten der beiden Anbieter abgelegten Daten auch außerhalb der EU und des EWR gespeichert. Die vertragliche Vereinbarung des DPA ist damit verpflichtend, um überhaupt datenschutzkonform agieren zu können.

Die augenfälligste Neuigkeit der beiden DPA: Es gelten jetzt die SCC 2021. Der frühe Umstieg war notwendig, da die SCC 2021 für alle jetzt neu abgeschlossenen Verträge zwingend ist.

Wann gelten die neuen DPA von AWS und Microsoft?

Neukunden, die erstmals Verträge mit AWS und Microsoft über Cloud-Dienstleistungen, also z.B. auch Microsoft 365 oder Office 365 abschließen, schließen damit auch die neuen DPA ab.

Für Bestandskunden behält sich AWS weitreichende Änderungsrechte vor. Regelmäßig genügt schon eine Information über neue Vertragsregelungen und die Weiternutzung durch den Kunden, damit AWS von einer Vertragsänderung ausgeht. Vertragsrechtlich gibt es durchaus Fragezeichen, ob dies möglich ist. Für die Vereinbarung des neuen DPA aber hilft dies, da sich die Rechtssicherheit für die Kunden erhöht, letztlich zu seinem Vorteil ist und soweit ersichtlich auch keine Mehrkosten hervorgerufen werden.

Microsoft regelt in seinen DPA, dass jeweils die beim erstmaligen Erwerb eines Produkts geltende Fassung vereinbart wird. Auch ist vorgesehen, dass bei Updates jeweils auch gleich die neue Vertragsfassung mit vereinbart wird, jedenfalls für die betroffenen Produktteile: Der Kunde stimmt dem nach den Microsoft-Vorstellungen also letztlich mit Installation zu. Um die SCC 2021 als Bestandskunde von Microsoft zu aktivieren, ist also eine derartige Änderung erforderlich, solange Microsoft nicht aktiv eine Vertragsänderung einleitet. Dies ist nach den Vertragsregelungen von Microsoft regelmäßig bei hoheitlichen Vorgaben ohne weiteres möglich. Für die SCC 2021 werden also vermutlich spätestens im Dezember 2022 auch Bestandskunden von Microsoft „aktiviert".

Und was gilt inhaltlich?

Inhaltlich halten beide Anbieter die Regelungen kurz: Die SCC 2021 werden nicht wiederholt, sondern es wird nur auf sie verwiesen. Microsoft sieht die Anwendung des Moduls „Auftragsverarbeiter zu Auftragsverarbeiter" vor, weil die Daten von der irischen Microsoft-Gesellschaft, die Auftragsverarbeiterin der Kunden ist, an einen Unterauftragnehmer in den USA übermittelt werden. AWS überlässt es dem Kunden, welches Modul gilt: Je nachdem, ob der Kunde selbst Auftragsverarbeiter oder Verantwortlicher ist, gilt das Modul „Auftragsverarbeiter zu Auftragsverarbeiter" oder aber „Verantwortlicher zu Auftragsverarbeiter", da AWS immer aus Auftragsverarbeiter auftritt.

Dem Leitgedanken der SCC 2021 entspricht dies nicht. Die Kommission sieht vor, dass diese Klauseln explizit vereinbart werden zwischen den Parteien. Ob das wirklich nötig ist, ist noch offen.

Allerdings besteht ein anderes Hindernis für diese Lösung: Die SCC 2021 verlangen etliche Dokumentationspflichten. Datenimporteure wie AWS und Microsoft müssen den Kunden unterstützen bei der Aufbereitung des nationalen Rechts der Drittstaaten und die Einhaltung der Klauseln dokumentieren. Das alles ist mit einem bloßen Verweis auf die SCC 2021 nicht getan. Der EuGH hat im vergangenen Jahr dieser Praxis ausdrücklich eine Absage erteilt. Die neuen DPA von AWS und Microsoft alleine genügen damit nicht, um den Anforderungen der SCC 2021 zu genügen. Ergänzend müssten die beiden Unternehmen mindestens Informationen bereitstellen über das nationale Recht in den Drittstaaten, in denen sie die Daten verarbeiten. Kunden müssten dies aus datenschutzrechtlicher Sicht verlangen. Vertragsrechtlich kann man sicher darüber streiten, ob die Angaben nicht proaktiv bereitgestellt werden müssen.

Was darüber hinaus die Regelungen für die Auftragsverarbeitung anbelangt, sind beide DPA denkbar kurz. Sie regeln die Pflichten von AWS und Microsoft bei der Auftragsverarbeitung weit unterhalb der Regelungsdichte, die die Kommission in ihrem neuen Muster für einen Vertrag nach Art. 28 DSGVO vorgelegt hat. Verpflichtend ist das neue Muster von der Kommission nicht. Ob aber die vage gehaltenen Pflichten von AWS und Microsoft ausreichen, wird in den nächsten Monaten weiter zu diskutieren sein. Zweifel daran bestanden schon bisher, bevor die Kommission ihr umfangreiches Muster veröffentlicht und damit auch international neue Standards gesetzt hat.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de