Neues zum Drittstaatentransfer

Wann dürfen US-Dienstleister datenschutzkonform genutzt werden? Was gilt es zu beachten, um das Datenschutzrisiko beim Transfer von Daten in Länder außerhalb des EWR zu minimieren? Seit der EuGH-Entscheidung in Sachen Schrems II sind diese Fragen ein (leidiger) Dauerbrenner. Vor wenigen Tagen hat der Europäische Datenschutzausschuss neue Leitlinien hierzu erlassen. Wir haben das Wichtigste daraus für Sie zusammengefasst

Die Leitlinien 05/2021 des Europäischen Datenschutzausschusses (EDSA), die am 18.11.2021 angenommen wurden, befassen sich mit dem „Zusammenspiel zwischen der Anwendung von Artikel 3 und den Bestimmungen über internationale Übermittlungen gemäß Kapitel V der DSGVO". Ein sperriger Titel für eine höchst praxisrelevante Thematik:

Wann ist überhaupt von einem „Drittstaatentransfer" von Daten auszugehen? Ist dies nur dann der Fall, wenn personenbezogene Daten physisch auf Servern in Ländern außerhalb des Europäischen Wirtschaftsraums (EWR) gespeichert werden? Oder reichen bereits Support-Zugriffe etwa aus den USA heraus, wie dies jedenfalls auf 3. Ebene bei Microsoft, AWS und vielen mehr der Regelfall ist? Ist womöglich bereits dann von einem Drittstaatentransfer im Sinne der DSGVO auszugehen, wenn Daten auf Servern im EWR gespeichert sind, diese Daten aber z.B. von US-Unternehmen oder ihren EU-Töchtern kontrolliert werden (dann gibt es u.U. Zugriffsrechte der US-Behörden unter dem CLOUD ACT)?

Diese in der Praxis hoch relevanten und umstrittenen Fragen diskutiert der EDSA in seinen Leitlinien. Diese sind nicht verbindlich – weder für nationale Datenschutzaufsichtsbehörden noch für Unternehmen. Sie geben aber wertvolle Anhaltspunkte, wie hoch das Risiko eines aufsichtsbehördlichen Einschreitens ist und mindern so die bestehenden Rechtsunsicherheiten.

Kriterien für das Vorliegen eines Drittstaatentransfers

Der EDSA definiert drei Kriterien, bei deren kumulativem Vorliegen von einem Drittstaatentransfer von Daten auszugehen ist. In diesem Fall müssen die Vorgaben der Art. 44 ff. DSGVO eingehalten werden:

1. Ein Unternehmen verarbeitet personenbezogene Daten im Anwendungsbereich der DSGVO.

2. Dieses Unternehmen macht die personenbezogenen Daten einem anderen Unternehmen zugänglich, durch Übermittlung oder auf andere Weise.

3. Das andere Unternehmen befindet sich in einem Drittland oder ist eine internationale Organisation.

Diese Kriterien sind denkbar weit: Anders als der Begriff „Drittstaatentransfer" vermuten lässt, müssen Daten nicht notwendigerweise in ein Drittland geschickt werden. Es reicht vielmehr, wenn die Daten auf Servern im EWR gespeichert bleiben und ein Unternehmen aus dem Drittland diese dort „ansehen" kann. Diese Position wird nicht nur vom EDSA, sondern, soweit ersichtlich, auch von der überwiegenden Literatur so vertreten.

Für die Praxis bedeutet das, dass alle der folgenden Optionen einen „Drittstaatentransfer" im Sinne der DSGVO darstellen und damit für jede der folgenden Situationen angemessene Garantien für die Absicherung der Datenverarbeitung im Drittland vorgesehen werden müssen:

- **Versand** in Drittländer
- **Supportzugriffe** aus Drittländern
- **Behördenzugriffe** aus Drittländern

All das gilt auch dann, wenn nur der Auftragnehmer in der EU ansässig ist und hier – z.B. als IT-Dienstleister oder Tochterunternehmen eines US-Konzerns – personenbezogene Daten im Auftrag verarbeitet. Für den „Rückversand" der personenbezogenen Daten vom **Auftragnehmer** an den Verantwortlichen gelten die Anforderungen der Art. 44 ff. DSGVO.

Ein abzusichernder Drittstaatentransfer liegt natürlich nur dann vor, wenn Daten übertragen werden, nicht, wenn dies nur theoretisch denkbar ist. Bei Supportzugriffen sollte aber regelmäßig schon vorab

und nicht erst im Supportfall eine Absicherung für den Drittstaatentransfer geschaffen werden: Wenn Hilfe benötigt wird, bleibt regelmäßig keine Zeit mehr, um die entsprechenden Absicherungen zu schaffen. Bei Behördenzugriffen aus Drittländern kann dies anders sein, je nach nationalem Recht und – jedenfalls bei Akzeptanz eines risikobasierten Ansatzes, wie dieser aus den neuen Standardvertragsklauseln ersichtlich ist – der Antwort auf die Frage, ob auch praktisch mit solchen Zugriffen zu rechnen ist.

Ein Drittstaatentransfer liegt nicht vor, wenn EU-Bürger ihre Daten direkt an ein Unternehmen übermitteln, das nicht dem Anwendungsbereich der DSGVO unterliegt, beispielsweise bei einer **direkten Bestellung** von Kleidung bei einem Unternehmen in Singapur, welches zwar eine Website in englischer Sprache unterhält, aber weder eine Niederlassung in der EU hat noch seine Kollektion gezielt EU-Bürgern anbietet.

Nicht erfasst sind nach einem Beispiel des EDSA auch **Remote-Work-Zugriffe**: Wenn der Arbeitnehmer eines deutschen Unternehmens auf einer Dienstreise aus Indien heraus auf den Unternehmensserver zugreift und personenbezogene Daten verarbeitet, ist dies kein Datentransfer nach Indien und die Vorgaben der Art. 44 ff. DSGVO müssen nicht eingehalten werden.

Folgen des Vorliegens eines Drittstaatentransfers

Werden Daten in Drittstaaten übertragen, muss der Datentransfer durch angemessene Garantien abgesichert werden. Angemessene Garantien können etwa ein Angemessenheitsbeschluss der EU-Kommission sein (z.B. für UK oder Kanada), die Vereinbarung der (neuen) Standardvertragsklauseln mit Prüfung der Rechtslage im Zielstaat und etwaigen zusätzlichen Maßnahmen. Bei unternehmensinternen Transfers können auch Binding Corporate Rules die Datenflüsse absichern.

Grundvoraussetzung für eine DSGVO-konforme Datenverarbeitung ist indes stets, die Verarbeitungsprozesse im Unternehmen zu kennen. Dies gilt auch und gerade für Drittstaatentransfers. Dokumentiert werden können die Transfers etwa im Kontext der Verarbeitungsverzeichnisse. Die Datenschutzaufsichtsbehörden erwarten dies spätestens seit dem EuGH-Schrems II-Urteil im Sommer 2020. In der Bundesrepublik wird seit Juni 2021 eine von mehreren Landes-

datenschutzbehörden abgestimmte Schwerpunktprüfung der Drittstaatentransfers ausgewählter Unternehmen durchgeführt. Wir berichteten hierzu in unserem Newsletter vom Juni 2021.

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