Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Postsendungen bitte an die Postanschrift des TLfDI, Postfach 900455, 99107 Erfurt!

Thüringer Landesbeauftragter für den Datenschutz und
die Informationsfreiheit (TLfDI), PF 900455, 99107 Erfurt

AZ: [redacted]

(Aktenzeichen bei Antwort angeben)

[redacted]

Ihre Nachricht vom : [redacted]
Ihr Zeichen :
Bearbeiter/in : [redacted]
Telefon : [redacted]
Erfurt, den : 19. Juni 2023

Anfrage zum Positionspapier Souveräne Clouds

Sehr geehrte [redacted],

in Ihrer Email [redacted] nehmen Sie Bezug auf das im Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) vom 11. Mai 2023 beschriebene Risiko, dem Anbietende sog. „Souveräner Clouds“ im Hinblick auf exterritoriale Einwirkungen, Zugriffe oder Offenlegungspflichten unterliegen (Ziffer 2.4) und fragen an, welche Maßnahmen in Betracht kommen, um zulässige Zugriffe auf personenbezogene Daten zu ermöglichen.

Die im Positionspapier beschriebenen Risiken beziehen sich auf zwei Szenarien: Zum einen auf die Übermittlung von personenbezogenen Daten in ein Drittland und zum anderen auf den Sonderfall (extraterritorialer) Zugriffsmöglichkeiten von Behörden eines Drittlandes auf personenbezogene Daten eines dem Anwendungsbereich der DS-GVO unterfallenden Unternehmens, was vor allem relevant ist, wenn die Muttergesellschaft des EWR-Unternehmens in einem Drittland ansässig ist.

Sollen personenbezogene Daten an Drittländer – also Empfänger in Staaten, die nicht der EU oder dem EWR angehören – übermittelt werden, bestimmt Art. 44 DS-GVO, dass dies nur zulässig ist, wenn der Verantwortliche und ggf. der Auftragsverarbeiter die Vorgaben der Datenschutz-Grundverordnung und insbesondere die in den Art. 45, 46 und 49 DS-GVO niedergelegten Bedingungen einhalten. Soweit ein angemessenes Schutzniveau beim Empfänger nicht durch einen Angemessenheitsbeschluss der europäischen Kommission nach Art. 45 Abs. 3 DS-GVO festgelegt wurde, darf ein Verantwortlicher bzw. Auftragsverarbeiter die Daten nur dann an ein Drittland übermitteln, wenn geeignete Garantien nach Art. 46 Abs. 1 DS-GVO vorliegen und den Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Dabei können die im Katalog geeigneter Kriterien enthaltenen Standardvertragsklauseln (Art. 46 Abs. 2 Buchst. c) DS-GVO) zwar grundsätzlich als Übermittlungsinstrument dienen. Allerdings hat der EuGH in seinem Grundsatzurteil vom 16. Juli 2020 („Schrems II"- C 311/18, RN 134) deutlich gemacht, dass der vorgesehene vertragliche Mechanismus auf der Eigenverantwortung der in der EU ansässigen Verantwortlichen beruht, die in jedem Einzelfall die Gleichwertigkeit des Schutzniveaus überprüfen und ggf. zusätzliche (ergänzende) Maßnahmen zu dessen Einhaltung ergreifen müssen. Dies gilt auch für Verantwortliche, die aus Drittländern angebotene Clouds nutzen wollen.

Weil also der Abschluss von Standarddatenschutzklauseln allein häufig nicht ausreicht, um den in Art. 46 Abs. 2 DS-GVO geregelten Erfordernis „geeigneter Garantien" zu genügen, hat der Europäische Datenschutzausschuss (EDSA) Empfehlungen zur praktischen Umsetzung der vom EuGH vorgegeben Prüfungen und Maßnahmen erlassen, die Sie unter https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf finden (EDSA-Empfehlungen 01/2020 v. 10.11.2020). Diese enthalten in Anlage 2 Beispiele für ergänzende technische, vertragliche und organisatorische Maßnahmen, wobei vor allem die beschriebenen technischen Maßnahmen, wie eine ausreichend gesicherte Verschlüsselung durch Anbietende zu ergreifen sind,

um einen – sofern überhaupt möglich - zulässigen Cloud-Betrieb sicherzustellen. Diese Bedingungen gelten auch für souveräne Clouds als Mindeststandards.

Auch im Fall (extraterritorialer) Zugriffsmöglichkeiten öffentlicher Stellen eines Drittlandes auf personenbezogene Daten, die im Anwendungsbereich der DS-GVO bzw. im EWR verarbeitet werden, besteht eine vergleichbare Gefährdungslage, mit der sich die Datenschutzkonferenz (DSK) in einem Beschluss vom 31. Januar 2023 auseinandergesetzt hat (https://datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf). Anders als im Fall der Übermittlung in Drittländer geht der Beschluss nicht von einem tatsächlich stattfindenden Datentransfer aus, sondern betrachtet das Risiko, dass Drittstaaten aufgrund des Unternehmens-Hauptsitzes im Drittland personenbezogene Daten aus dem globalen Firmenbereich erfragen können. Dabei wird zwar klargestellt, dass allein die abstrakte Gefahr, dass ein EWR-Unternehmen von seiner Muttergesellschaft oder einer öffentlichen Stelle angewiesen werden könnte, personenbezogene Daten in ein Drittland zu übermitteln, noch keinen Drittlandtransfer i. S. d. Art. 44 DS-GVO darstellt (Ziffer 1 des Beschlusses). Allerdings kann der Verantwortliche aufgrund der Rechtslage im Drittland verpflichtet sein, eine Einzelfallprüfung durchzuführen und sich zu vergewissern, dass hinreichende Garantien bestehen, um vertragliche Vereinbarungen auch tatsächlich einzuhalten, so dass es nicht zu Verarbeitungen kommt, die nach den Maßstäben der DS-GVO unzulässig sind (Ziffer 4 des Beschlusses). Analog dem ersten Szenario (tatsächlich stattfindender Drittlandstransfer) kann auch hier davon ausgegangen werden, dass allein vertragliche Zusicherungen als „geeignete Garantien“ nicht ausreichend sind. Es müssen weitere technische Maßnahmen getroffen werden. Können Stellen aufgrund technischer Maßnahmen z. B. durch Verschlüsselung gar nicht erst auf Daten aus dem globalen Firmenbereich zugreifen (immer dann, wenn die Stellen nicht im Besitz des nötigen Schlüsselmaterials sind), können diese Maßnahmen als hinreichende Garantien betrachtet werden, um auch das Zugriffsrisiko nach Ziffer 4 des Beschlusses einzudämmen. Deshalb sind die Maßnahmen der o. g. EDSA-Empfehlungen 01/2020 auch für die datenschutzrechtliche Bewertung eines Cloud-Angebots unter dem Gesichtspunkt des Risikos

eines Drittlandzugriffs relevant. Das Positionspapier greift unter Ziffer 2.4 den Gedanken des oben genannten DSK-Beschlusses lediglich kurz auf. Alternativ kann auch eine ausreichende tatsächliche und rechtliche Unabhängigkeit vom Mutterkonzern eine Option sein, hierzu sind dem TLfDI aber keine funktionierenden praktischen Beispiele bekannt.

Zusammenfassend kann für souveräne Clouds also gelten, dass der Anbieter entweder keine personenbezogenen Daten in ein Drittland übermittelt und kein Tochterunternehmen eines Drittlandkonzerns ist oder das Drittland einem Angemessenheitsbeschluss nach Art. 45 Abs. 3 DS-GVO unterfällt bzw. der Anbieter im Falle eines unsicheren Drittlands wirksame Maßnahmen nach den o.g. EDSA-Empfehlungen 01/2020 getroffen hat. Wie in dem in Rede stehenden Positionspapier der DSK ausgeführt, genügen allerdings rein vertragliche Maßnahmen nicht, um einen Drittlandtransfer personenbezogener Daten zu ermöglichen, auch wenn die Datenverarbeitung regelhaft in der EWR erfolgt. Der Vollständigkeit halber sei auch erwähnt, dass Nutzer auf den Verzicht solcher Maßnahmen, welche „geeignete Garantien“ umsetzen, nicht einwilligen können. Eine solche Einwilligung ist unwirksam und stellt damit auch keine Maßnahme dar, Ziffer 2.4 des DSK-Beschlusses zu souveränen Clouds umzusetzen (siehe https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf).

Für Rückfragen stehen wir gerne zur Verfügung. Soweit Sie jedoch weitergehende Fragen zu speziellen Cloud-Angeboten oder Verarbeitungsvorgängen haben, sollten Sie sich an die nach § 40 BDSG zuständige Aufsichtsbehörde wenden.

Mit freundlichen Grüßen
im Auftrag

[redacted]

Das Schreiben wurde im Entwurf gezeichnet und enthält rechtsgültig die entsprechende Namenswiedergabe.