Beschluss

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023

Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bewertet Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, die nach Artikel 28 Datenschutzgrundverordnung (DSGVO) im Auftrag im Europäischen Wirtschaftsraum (EWR) verarbeitet werden, datenschutzrechtlich wie folgt:

1. Die Gefahr allein, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln, genügt nicht, um eine Übermittlung in ein Drittland im Sinne des Artikels 44 fortfolgende DSGVO anzunehmen.[1,2]

2. Allerdings kann eine solche Gefahr dazu führen, dass solchen Rechtsvorschriften unterliegenden Auftragsverarbeitern die Zuverlässigkeit im Sinne von Artikel 28 Absatz 1 DSGVO fehlt, soweit nicht diese – oder auch der Verantwortliche – technische und/oder organisatorische Maßnahmen ergriffen haben, die hinreichend Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt, insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen

---

[1] Bericht der Arbeitsgruppe "Microsoft-Onlinedienste", Kapitel 3.2.3.4. b) iv., Randnummern 983 fortfolgende; Kapitel 3.2.3.5., Randnummern 1131 fortfolgende.

[2] Eine solche Gefahr kann aber Anhaltspunkt sein, um zu prüfen, ob eine Übermittlung in ein Drittland im Sinne des Artikels 44 fortfolgende DSGVO geplant ist, die beispielsweise Informationspflichten nach Artikel 13, 14 DSGVO auslöst.

angeht, im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht.[3]

3. Soweit das Risiko besteht, dass eine Norm oder Praxis, die nach EU-Recht unzulässige Verarbeitungen personenbezogener Daten verlangen kann, auch auf EWR-Tochtergesellschaften von Drittlands-Unternehmen anwendbar ist, genügt die Verarbeitung durch eine EWR-Tochtergesellschaft als Auftragsverarbeiter für sich genommen nicht, um eine Zuverlässigkeit im Sinne von Artikel 28 Absatz 1 DSGVO zu erreichen.[4] Soweit eine Norm oder Praxis eines Drittlands die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus dem EWR in ein Drittland durch eine als Auftragsverarbeiter tätige Stelle in dem EWR – zum Beispiel die EWR-Tochtergesellschaft eines Drittlands-Unternehmens – begründet, sind an die Sorgfalt der Zuverlässigkeitsprüfung im Sinne von Artikel 28 Absatz 1 DSGVO besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen.

4. Dies erfordert zunächst eine Bewertung sämtlicher Umstände des Einzelfalls, ob der Auftragsverarbeiter und/oder die von ihm verarbeiteten Daten unter diese drittstaatliche Norm oder Praxis fallen und wenn ja, ob der Auftragsverarbeiter dennoch hinreichend Garantien dafür bietet, dass es nicht zu Verarbeitungen kommt, die nach den Maßstäben der DSGVO beziehungsweise des anwendbaren mitgliedstaatlichen Rechts unzulässig sind.

   Dabei sind insbesondere die folgenden Punkte zu berücksichtigen:

   - das Ergebnis einer Prüfung hinsichtlich einer extraterritorialen Anwendbarkeit des Drittlands-Rechts und einer gegebenenfalls darüber hinausgehenden praktischen extraterritorialen Anwendung,

   - bei einer extraterritorialen Anwendbarkeit und/oder Anwendung: das Ergebnis einer Prüfung, ob das Recht oder die Praxis des Drittlands die Verpflichtungen aus dem Auftragsverarbeitungsvertrag beeinträchtigen könnten (in Anlehnung an die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses),

[3] Bericht der Arbeitsgruppe "Microsoft-Onlinedienste", Kapitel 3.2.3.5., Randnummern 1135 fortfolgende.
[4] Bericht der Arbeitsgruppe "Microsoft-Onlinedienste", Kapitel 3.2.3.4. b) v., Randnummern 1011 fortfolgende.

- das Risiko, dass die Drittlands-Muttergesellschaft eines EWR-Tochterunternehmens dieses anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln (Prüfung der Erkenntnisse zur Rechtslage/-praxis),
- ob der Auftragsverarbeitungsvertrag nach europäischen Maßstäben unzulässige Verarbeitungen auf der Grundlage von Drittlands-Recht erlaubt,
- etwaige Zusicherungen der Drittlands-Muttergesellschaft und des EWR-Unternehmens zum Umgang mit kollidierenden Anforderungen des Rechts eines Drittstaates und der Europäischen Union (EU),
- eine Bewertung der Rechtslage und -praxis des Drittlands, ob derartige Zusicherungen auch tatsächlich eingehalten werden können,
- eine Bewertung aller weiteren Aspekte, ob derartige Zusicherungen auch tatsächlich eingehalten werden,
- etwaige in der Vergangenheit festgestellte Datenschutzverstöße,
- die Schwere und Wahrscheinlichkeit einer Sanktionierung von Zuwiderhandlungen nach EU-Recht und dem Recht des Drittlands sowie
- der Ausschluss unzulässiger Übermittlungen durch geeignete technische und organisatorische Maßnahmen.

Bietet der Auftragsverarbeiter nach dieser Prüfung keine hinreichenden Garantien, sind die Risiken der europarechtswidrigen Datenverarbeitung durch technische und/oder organisatorische Maßnahmen auszugleichen, die genau diejenigen Defizite der Rechtslage oder -praxis des drittstaatlichen Rechts ausgleichen, die zu der mangelnden Zuverlässigkeit des Auftragsverarbeiters geführt haben.[5] Für die Frage, welche Maßstäbe an diese Maßnahmen zu stellen sind, können Verantwortliche die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses heranziehen, wobei jedoch zu beachten ist, dass diese Empfehlungen für den Kontext von Datenübermittlungen in Drittländer konzipiert

[5] Bericht der Arbeitsgruppe "Microsoft-Onlinedienste", Kapitel 3.2.3.4. b) v., Randnummern 1025 fortfolgende; Kapitel 3.2.3.5., Randnummern 1142 folgende.

worden sind,[6] sodass abweichende Bewertungen der Eignung bestimmter Maßnahmen nicht ausgeschlossen sind. Soweit eine Verarbeitung personenbezogener Daten im Auftrag den Zugriff des Auftragsverarbeiters auf Klardaten erfordert, ist in entsprechender Anwendung des Anwendungsfalls 6 des Anhangs 2 der Empfehlungen 01/2020 besonders kritisch zu prüfen, wie den Anforderungen des Artikels 28 Absatz 1 DSGVO ausreichend Rechnung getragen werden kann.[7]

5. Der Verantwortliche muss in der Lage sein, den Nachweis zu führen, dass ein Auftragsverarbeiter die Anforderungen aus Artikel 28 Absatz 1 und Erwägungsgrund 81 DSGVO an Fachwissen, Zuverlässigkeit und Ressourcen erfüllt.[8]

Die DSK wird sich auf der Grundlage dieses Beschlusses für eine weitere Behandlung dieser Fragestellung im Europäischen Datenschutzausschuss (EDSA) einsetzen.

[6] Bericht der Arbeitsgruppe "Microsoft-Onlinedienste", Kapitel 3.2.3.4. b) v., Randnummern 1042 fortfolgende; Kapitel 3.2.3.5., Randnummern 1146 fortfolgende.
[7] Bericht der Arbeitsgruppe "Microsoft-Onlinedienste", Kapitel 3.2.3.4. b) v., Randnummern 1053 fortfolgende; Kapitel 3.2.3.5., Randnummern 1149 fortfolgende.