Stellungnahme

EDSA Empfehlungen 01/2020 “on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”

Please note: An English version of this position paper will be provided soon

Bundesverband der Deutschen Industrie e.V.

EU-Transparenzregisternummer: 1771817758-48

Stand: 16.12.2020

Executive Summary

Der BDI bedankt sich für die Gelegenheit, zu den Empfehlungen zu ergänzenden Maßnahmen zu Übertragungsinstrumenten für internationale Datentransfers 01/2020 Stellung nehmen zu können. Mit dem EuGH-Urteil vom 16.07.2020 (Rechtssache C-311/18, Schrems II) wurde die Verantwortung für die Sicherstellung eines angemessenen Datenschutzniveaus für die Verarbeitung personenbezogener Daten in Drittstaaten einseitig auf die für die Datenverarbeitung Verantwortlichen in der EU verlagert, ohne diesen jedoch zugleich das nötige Instrumentarium für die Bewältigung dieser Mammutaufgabe zur Verfügung zu stellen. Obgleich der BDI es zuvörderst als **Aufgabe des Unionsgesetzgebers** betrachtet, die **Datenübermittlung in Drittstaaten abstrakt-generell auf Basis der DSGVO zu ermöglichen**, wurden von der deutschen Industrie mit Blick auf die EuGH-Entscheidung dringend praktikable und ausgewogene Handreichungen und Leitlinien seitens der Datenschutzaufsicht und der EU-Kommission erwartet, um diese in die Lage zu versetzen, auch künftig die in einer globalisierten und digitalisierten Wirtschaft unverzichtbaren Datenübertragungen in Länder außerhalb der EU praxisgerecht datenschutzkonform zu gestalten.

Diesen Erwartungen werden die Empfehlungen 01/2020 in der jetzigen Fassung nach Einschätzung des BDI jedoch nicht gerecht. Die Schritt-für-Schritt-Vorgaben zum Vorgehen der Datenexporteure zur Erfüllung ihrer datenschutzrechtlichen Rechenschaftspflicht zeichnen sich durch einen dogmatischen Ansatz aus, der den in der DSGVO **verankerten risikobasierten Ansatz nur unzureichend berücksichtigt** und für viele Unternehmen in der Praxis nicht leistbar sein wird. Zugleich verkennt die von dem EDSA vorgenommene Gewichtung der möglichen zusätzlichen Maßnahmen mit einem klaren Schwerpunkt auf technische Maßnahmen, an die überdies unangemessen hohe Anforderungen gestellt werden, die Möglichkeiten und Erfordernisse der Praxis und erweist sich ebenfalls als unverhältnismäßig. Die aufgeführten Use Cases werden der Komplexität der praktischen Sachverhalte nicht gerecht und würden in ihrer Pauschalität zu völlig unangemessenen Ergebnissen führen.

Die Empfehlungen in der vorliegenden Form würden den vom EuGH belassenen geringen Handlungsspielraum beim Datentransfer in Drittstaaten auf Basis von Standarddatenschutzklauseln zusätzlich unverhältnismäßig beschränken. Im Ergebnis würde hierdurch ein Großteil des Datentransfers, nicht nur in die Vereinigten Staaten, sondern auch in viele andere Drittstaaten ohne Angemessenheitsbeschluss faktisch unmöglich werden – mit

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband
BUSINESSEUROPE

Hausanschrift
Breite Straße 29
10178 Berlin

Postanschrift
11053 Berlin

Ansprechpartner
Ines Nitsche
T: +493020281711
F: +493020282711

E-Mail:
I.Nitsche@bdi.eu

Internet
www.bdi.eu

gravierenden negativen Auswirkungen für den internationalen Daten- und Wirtschaftsverkehr.

Der **BDI fordert daher eine Anpassung der Empfehlungen** derart, dass sie den Datenexporteuren unter ausgewogener Berücksichtigung der verfassungs- und datenschutzrechtlichen Grundsätze in der Praxis umsetzbare Hinweise für den Einsatz der Übertragungsinstrumente und ggf. zusätzlich erforderlicher Maßnahmen an die Hand geben, **mit dem ausdrücklichen Ziel, diese in ihrem Bestreben zu unterstützen, den in einer globalisierten Wirtschaft erforderlichen Datentransfer in Drittstaaten aufrecht zu erhalten und rechtssicher zu gestalten**.

1. Risikobasierten Ansatz und Verhältnismäßigkeit beachten

Die vom EDSA in seinen Empfehlungen angestellten Erwägungen und Hinweise konzentrieren sich einseitig auf die Rechte der von der Datenverarbeitung Betroffenen und berücksichtigen in den vorgegebenen Prüfungsschritten und Use Cases nicht ausreichend die in der Datenschutzgrundverordnung (DSGVO) verankerten Grundsätze der Verhältnismäßigkeit und des risikobasierten Ansatzes, die auch dem EuGH-Urteil vom 16.07.2020 (Rechtssache C-311/18, Schrems II) zugrunde liegen. So betont Erwägungsgrund (EG) 4 der DSGVO, dass „*das Recht auf Schutz der personenbezogenen Daten […] kein uneingeschränktes Recht [ist]; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden*“.[1] Durch die den EDSA-Empfehlungen zugrundeliegende unausgewogene Betrachtungsweise würden auch solche **Datenübermittlungen in Drittländer beschränkt**, die unter angemessener Abwägung aller Umstände im Einzelfall **kein konkretes Risiko für den Datenschutz des Betroffenen** mit sich brächten. Dies hätte massive negative Auswirkungen auf alle Bereiche der Industrie, angefangen von alltäglicher Kommunikation mit Mitarbeitern außerhalb der EU über notwendige Handelstransaktionen mit Unternehmen und Einrichtungen in Drittstaaten bis hin zu der Aufrechterhaltung der Sicherheit von IT-Netzwerken und der internationalen Zusammenarbeit bei der Gesundheitsforschung zur Bekämpfung der Corona-Pandemie.

a) Angemessene Berücksichtigung der Umstände bei Sachverhaltsermittlung und Prüfung der Rechtslage

Der vom EDSA vorgegebene Prozess für die Ermittlung des relevanten Sachverhalts ist nicht an den Gegebenheiten und Möglichkeiten der Praxis orientiert und daher mit unangemessenen Belastungen für die Unternehmen, insbesondere KMU, verbunden. So wird beispielsweise das Verständnis von Datentransfer erweitert auf etwaige Weiterleitungen von Auftragsverarbeitern im Drittland zu deren Subdienstleistern in einem anderen Drittland (vgl. Absätze 10, 31 und 31). Außerdem sollen Zusatzmaßnahmen bereits dann erforderlich sein, wenn Daten zwar in ein Drittland mit Angemessenheitsbeschluss übertragen werden, aber hierfür durch ein Drittland ohne angemessenes Schutzniveau durchgeleitet werden (vgl. Use Case 3). Die Ermittlung der gesamten Kette von Unterverarbeitern und des genauen „Wegs“ der

[1] Vgl. auch EuGH-Urteil C-311/18 („Schrems II“) v. 16.07.2020, Rnr. 172.

Daten wird – abhängig von der Komplexität der jeweiligen Lieferkette – vor allem für KMU in der Praxis kaum durchführbar sein und übersteigt in dieser Pauschalität die Grenze der Verhältnismäßigkeit.

Es sollte daher **klargestellt werden**, dass die Sachverhaltsprüfung auf die Datenübertragung an den Datenimporteur sowie an von diesem ggf. beauftragten Subdienstleister, der Daten im Drittland verarbeitet, begrenzt ist. Jedenfalls sollten die Anforderungen an die Ermittlung des Sachverhalts unter Berücksichtigung aller Umstände explizit stets **auf das Maß des Zumutbaren im Einzelfall beschränkt** werden. Zudem sollte eine Klarstellung erfolgen, dass vom Anwendungsbereich der Empfehlungen Datenübermittlungen an Importeure mit Sitz außerhalb der Union ausgenommen sind, soweit die DSGVO gemäß Artikel 3 Absätze 2 und 3 unmittelbar auf sie anwendbar ist.

Überdies wird die **geforderte detaillierte Prüfung des Datenschutzniveaus des jeweiligen Drittlands** unter Verweis auf die ebenfalls jüngst veröffentlichten restriktiven Empfehlungen 2/2020 zu grundlegenden Garantien[2] von mittelständischen Unternehmen in der Praxis **kaum leistbar** sein und selbst internationale Konzerne vor große Herausforderungen stellen. Auch insoweit sollte daher zumindest klargestellt werden, dass der **Umfang der Analyse stets auf das Maß des Zumutbaren im Einzelfall** beschränkt ist. Um die Datenexporteure in ihrer Evaluierung zu unterstützen und eine homogene Bewertungsgrundlage zu bieten, sollten überdies **einheitliche relevante Informationen zu den Überwachungsgesetzen und der diesbezüglichen Rechtslage in bestimmten Drittländern aufbereitet** und veröffentlicht werden. Die pauschalen Hinweise auf mögliche Informationsquellen in Annex 3 derer sich der Datenexporteur mit Unterstützung des Importeurs bedienen kann, sind hierfür nicht ausreichend.

Soweit gleichwohl eine genaue Risikobewertung von den Datenexporteuren verlangt wird, sollten diese hierbei auch **sämtliche Umstände des Datentransfers** im Einzelfall berücksichtigen können, **um zu angemessenen Ergebnissen** zu gelangen. Hierzu gehört jedoch nicht nur die objektive Rechtslage im jeweiligen Drittland, wie vom EDSA in den Empfehlungen nahegelegt (vgl. insb. Absatz 42), sondern **auch die Wahrscheinlichkeit eines**

[2] Während die EU-Kommission in den jüngst veröffentlichten SCC für den Drittstaatentransfer auf Artikel 23 DSGVO als Prüfungsmaßstab verweist (vgl. Absatz 19 des Durchführungsbeschlusses zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer).

Datenzugriffs im konkreten Einzelfall. Die auf Basis objektiver Kriterien (insb. des Umfangs der erledigten Zugangsersuchen von Behörden) ermittelte Wahrscheinlichkeit eines Datenzugriffs bzw. eines entsprechenden Antrags seitens der Behörde im Drittland im konkreten Einzelfall ist eine Schlüsselkomponente bei der Risikobewertung in der unternehmerischen Praxis. Das tatsächliche Risiko, einem solchen Datenzugangsantrag ausgesetzt zu sein, variiert nämlich erheblich abhängig vom Geschäftsmodell des Datenexporteurs und -importeurs und der Datenkategorie (Geschäftsdaten/private Informationen).

Die Berücksichtigung der Eintrittswahrscheinlichkeit für Risikoprüfungen ist der DSGVO immanent (vgl. u. a. Artikel 24 und 25 DSGVO). Dementsprechend betont auch der EuGH in seiner Entscheidung an mehreren Stellen, dass die **Prüfung und Bewertung stets im Lichte aller Umstände** des konkreten Datentransfers zu erfolgen hat.[3] Auch die EU-Kommission scheint das EuGH-Urteil in diesem Sinne auszulegen, denn in ihrem jüngst veröffentlichten Entwurf für modernisierte Standardvertragsklauseln stellt sie klar, dass bei der Prüfung insbesondere die besonderen Umstände der Übermittlung zu berücksichtigen sind, wie beispielsweise einschlägige praktische Erfahrungen des Datenimporteurs dahingehend, ob in der Vergangenheit Datenzugangsanträge der Behörden für die jeweilige Datenart gestellt wurden oder nicht ("*To that end, they should in particular take into account the specific circumstances of the transfer ([…] and any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred) […]"*).[4]

Die Beschränkung der Datenübermittlung in Drittländer auch in Fällen, in denen die Prüfung im konkreten Kontext kein relevantes Risiko für die personenbezogenen Daten der betroffenen Person ergibt, wäre unverhältnismäßig und nicht im Einklang mit den Vorgaben des EuGH-Urteils und der DSGVO.

Daher sollte in **Absatz 33 der Empfehlungen klargestellt werden**, dass auch die Wahrscheinlichkeit des Zugriffs von Behörden im konkreten Fall ergänzend zu den weiteren Kriterien zu berücksichtigen ist. Die kategorische

---

[3] Vgl. z. B. EuGH „Schrems II" Absätze 112, 121, 146.

[4] Vgl. Absatz 20 des Durchführungsbeschlusses zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer.

Ausnahme von vermeintlich subjektiven Kriterien für die Risikobewertung in **Absatz 42** sollte demgegenüber **gestrichen** werden.

b) Angemessene Gewichtung und Auswahl zusätzlicher Maßnahmen

Auch die Ausführungen zur Auswahl und Gewichtung der Kategorien zusätzlicher Maßnahmen lässt hinreichende Erwägungen zu risikobasiertem Ansatz und Verhältnismäßigkeitsgrundsatz vermissen.

So legen die Empfehlungen nahe, dass vertragliche und organisatorische Maßnahmen grundsätzlich nicht allein oder in Kombination zur Herstellung eines angemessenen Datenschutzniveaus im Einzelfall ausreichten, sondern regelmäßig nur ergänzend zu technischen Maßnahmen zur Anwendung kommen können (vgl. z. B. Absatz 48). Diese pauschale Aussage steht in Widerspruch zum Grundsatz, dass auch die Auswahl der ggf. erforderlichen zusätzlichen Maßnahmen im Einzelfall unter Berücksichtigung aller Umstände zu erfolgen hat. Für **technische und organisatorische Maßnahmen** bestimmen **Artikel 24 und 25 DSGVO explizit**, dass der Einsatz unter *„Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“* zu erfolgen hat. Entsprechendes ist im Kommissionsentwurf für neue Standardvertragsklauseln vorgesehen mit dem Zusatz, dass technische Maßnahmen in Betracht gezogen werden sollen, wenn sie die Erfüllung des Verarbeitungszwecks nicht verhindern.[5]

Die jeweiligen Umstände eines Datentransfers werden jedoch regelmäßig von derart vielen Faktoren bestimmt, dass sich eine pauschale Bewertung einzelner Kategorien von Maßnahmen als ausreichend oder unzureichend, losgelöst vom konkreten Fall, verbietet.

Auch wenn die Behörden eines Drittlands naturgemäß nicht an die vertraglichen Absprachen zwischen Datenexporteur und Datenimporteur gebunden sind, so ist jedoch beispielsweise eine Verpflichtung des Datenimporteurs, eine Behördenanfrage zurückzuweisen und entsprechende Informationspflichten gegenüber dem Datenexporteur von großer Bedeutung, um

[5] Vgl. Entwurf Durchführungsführungsbeschluss zu Standardvertragsklauseln für den Datentransfer in Drittländer, Annex, Abschnitt 2, Klausel 1, Module 1 bis 4 jeweils zum Unterpunkt „Sicherheit der Verarbeitung“.

festzustellen, ob ein Zugriffsversuch überhaupt stattfindet. Zusammen mit organisatorischen Maßnahmen kann in geeigneten Fällen auch auf diese Weise ein angemessenes Datenschutzniveau sichergestellt werden.

In Absatz 48 sollte daher klargestellt werden, dass auch vertragliche und organisatorische Maßnahmen allein oder in Kombination ausreichen können, wenn eine angemessene Risikobewertung im Einzelfall kein relevantes Risiko für den Datenschutz der Betroffenen ergibt.

Überdies sollten auch d**ie Kriterien für die Auswahl eines oder mehrerer zusätzlicher Maßnahmen** (vgl. **Absatz 49**) im Lichte der DSGVO und des in ihr verankerten Verhältnismäßigkeitsgrundsatzes **um weitere Faktoren**, wie z. B. dem Zweck der Datenverarbeitung oder der Wahrscheinlichkeit des Datenzugriffs im konkreten Fall seitens einer öffentlichen Stelle im Drittland, **ergänzt** werden. Andernfalls besteht die Gefahr, dass als Ergebnis des gebotenen Abwägungsprozesses unangemessene Vorkehrungen seitens der Unternehmen ergriffen werden müssten, an denen die beabsichtigte Übertragung und Verarbeitung in der Praxis häufig scheitern würde.

Die durch eine unzureichende Abwägung drohende Schieflage für die im Einzelfall zu ergreifenden Maßnahmen wird bereits durch die in Annex 2 aufgeführten Beispiele für zusätzliche Maßnahmen deutlich, die noch nicht einmal die bisher in Absatz 49 aufgeführten Faktoren, wie z. B. die Art der zu verarbeitenden Daten, ausreichend berücksichtigen. Die **pauschale Anforderung, auf allen Stufen der Datenverarbeitung eine umfassende Verschlüsselung vorzusehen**, ignoriert darüber hinaus, dass in der Praxis die **bezweckten und notwendigen Datenverarbeitungen** durch den Empfänger **häufig gerade die unverschlüsselte Verarbeitung der Daten erfordern** (z. B. für den konzerninternen Austausch von Personal- und Mitarbeiterdaten oder Kundendateien). Diese würden durch die geforderte Datenverschlüsselung **verhindert** werden, weshalb diese Maßnahme in diesen Fällen keine geeignete Lösung darstellt. Überdies werden manche Unternehmen, insbesondere KMU, nicht über die Werkzeuge bzw. Mittel verfügen, um eine starke Verschlüsselung anzuwenden.

Außerdem hätte das strikte Verbot der Datenentschlüsselung auf allen Verarbeitungsstufen **gravierende Implikationen für die IT-Sicherheit**. Für bestimmte Technologien, wie die Inspektion von Datenpaketen zur Bekämpfung von Malware und DDOS-Attacken, ist die Entschlüsselung der Datenpakete notwendig. Bei einem Verbot dieser Maßnahme hätten viele Unternehmen künftig Probleme ein hohes IT-Sicherheitsniveau zu erhalten.

Um tatsächlich einen praktischen Nutzen für die Unternehmen bei der Umsetzung der datenschutzrechtlichen Anforderungen an den Drittstaatentransfer zu bieten und als Orientierung für eine umfassende Risikobewertung im Einzelfall dienen zu können, sollten die **Beispiele flexibel und differenziert ausgestaltet werden.**

2. Use Cases praxistauglich und flexibel gestalten

Wie bereits oben ausgeführt, erweisen sich die im Annex 2 der Empfehlungen exemplarisch aufgeführten **Use Cases** als **unausgewogen** und in der Praxis nicht bzw. nur mit unangemessenem Aufwand umsetzbar. In Use Case 6 und 7 stellt der EDSA lediglich pauschal klar, dass er keine technischen Lösungen für Fälle des Transfers unverschlüsselter Daten an Datenimporteure sieht, die mit diesen Daten Rechenoperationen durchführen und auch nicht für Fälle des Fernzugriffs auf unverschlüsselte Daten für Geschäftszwecke. **Sonstige Lösungsansätze,** etwa in Form von vertraglichen und/oder organisatorischen Maßnahmen unter Einbeziehung einer konkreten Risikobewertung auf der Grundlage aller relevanten Umstände des Einzelfalls, **lassen diese Anwendungsfälle vermissen**. Dabei betreffen jedoch beide holzschnittartig dargestellten Fallgruppen in der Praxis eine Vielzahl äußerst relevanter Datenverarbeitungen, wie z. B. die Nutzung von Cloud-/SaaS-Providern oder auch den konzerninternen Austausch von Personal- und Mitarbeiterdaten im **Tagesgeschäft,** die völlig unterschiedliche Risikopotenziale bergen können. Use Case 6 und 7 implizieren im Zusammenhang mit den übrigen Ausführungen zu in Frage kommenden Schutzmaßnahmen jedoch, dass es für sämtliche unter diese weit gefassten Kategorien fallenden Sachverhalte keine geeigneten zusätzlichen Maßnahmen gäbe, womit den Unternehmen pauschal sämtlicher Handlungsspielraum für den Erhalt aller unter diese Use Cases fallenden Datenverarbeitungen genommen würde – mit gravierenden negativen Folgen für den internationalen Daten- und Wirtschaftsverkehr.

Vor diesem Hintergrund und eingedenk obiger Ausführungen, sollten die aufgeführten **Anwendungsfälle einer kritischen Prüfung unterzogen und derart flexibel gestaltet** werden, dass sie der Komplexität der unterschiedlichen Szenarien in der Praxis und den damit einhergehenden unterschiedlichen Risikopotenzialen gerecht werden können. In der vorliegenden Form erweisen sich die Use Cases als unverhältnismäßig und für die Unternehmen nicht hilfreich.

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 40 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Ansprechpartner

Ines Nitsche
Abt. Recht, Wettbewerb und Verbraucherpolitik
Telefon: +49 30 2028-0
i.nitsche@bdi.eu

BDI Dokumentennummer: D 1295