***Entwurf* Anlage 2 zu Art. 44** **Art. 44 DSGVO**

Empfehlungen (engl. „*recommendations*“) 01/020 des **Europäischen Datenschutzausschusses** vom 10. November 2020 zu den **Anforderungen der Aufsichtsbehörden an die Datenübermittlung in Drittländer** (also nach außerhalb der EU) **und an internationale Organisationen**

Der **Europäische Gerichtshof** (EuGH) hat in seinem Urteil vom 6. Oktober 2015, C-362/14 die Unwirksamkeit der Safe-Harbor-Regelung („Schrems I“) und im Urteil vom vom 16. Juli 2020 (C-311/18 = NJW 2020, 2613 = DuD 2020, 685 = MMR 2020, 597) die Unwirksamkeit der Privacy-Shield-Vereinbarung („Schrems II“) festgestellt. Die so genannten Standardvertragsklauseln (dazu RdNrn. 37 bis 44 zu Art. 46 DSGVO) hätten zwar weiterhin Gültigkeit, es seien jedoch **zusätzliche Maßnahmen** im Hinblick auf die Übermittlung von personenbezogenen Daten in Drittstaaten notwendig.

Anknüpfend an die **Notwendigkeit** dieser **zusätzlichen Maßnahmen** hat der **Europäischen Datenschutzausschuss** am 10. November 2020 **Empfehlunge**n (engl. „*recommendations*“ 01/2020) in Englisch auf fast 40 Seiten vorgelegt.

Diese umfangreichen ***Recommendations* gliedern sich in**

- eine Zusammenfassung (engl. „*executive summary*“),
- eine Darstellung der Verantwortlichkeit beim Datentransfer (Ziff. 1 bis 68),
- einem kurzen Anhang 1 mit Begriffsdefinitionen,
- einem fast 20-seitigen Anhang 2 mit Beispielen für zusätzliche Maßnahmen (Ziff. 69 bis 137) sowie
- einem kurzen Hinweis auf mögliche Informationsquellen zur Bewertung von Situationen im Drittland (Ziff. 138).

Nachfolgend werden in deutsch sowie kurz und knapp daraus die **Zusammenfassung** der Empfehlungen (**A.**) **und** die in **Anhang 2** genannten Ausführungen und Beispiele für zusätzliche Maßnahmen (**B**.) jeweils in einem Überblick dargestellt*.

A. Zusammenfassung und Vorgehensweise des EDSA

Der **Europäische Datenschutzausschuss** (EDSA) stellt zunächst grundsätzlich festgestellt, dass der Datenschutz auch bei einer Übermittlung in Drittländer gewährleistet sein muss, damit es nicht zur Aushöhlung und Verwässerung des in Europa zugesicherten Schutzniveaus kommt. **Verantwortlich sind die Datenexporteure**. Sie müssen prüfen, ob und gegebenenfalls welche zusätzlichen Maßnahmen einzusetzen sind. Um die

Datenexporteure zu unterstützen, hat der EDSA diese Empfehlungen abgegeben und geht dabei zunächst in 6 Schritten vor:

In einem **1. Schritt** müssen sich Datenexporteure Kenntnis über ihre Übermittlungen verschaffen, insbesondere wohin genau die Daten übermittelt werden.

Der **2. Schritt** besteht in einer Prüfung, ob ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt. Ist dies der Fall, so ist Grundsatz nichts zu veranlassen, in Einzelfällen können indessen zusätzliche Maßnahmen notwendig werden. Liegt kein Angemessenheitsbeschluss vor, so sind die Übermittlungswerkzeuge nach Art. 46 zu prüfen.

In einem **3. Schritt** muss geprüft werden, ob es etwas im Recht oder der Praxis des Drittlandes gibt, das sich negativ auf die Wirksamkeit der Übermittlungswerkzeuge auswirkt. Dies umfasst insbesondere eine Beurteilung des Rechts des Drittlandes und dort im Wesentlichen die Frage des Datenzugriffs durch öffentliche Stellen oder Behörden. *(Anmerkung der Herausgeber des Kommentars BMH: Bereits dieser Schritt dürfte die meisten kleineren und mittleren Unternehmen bzw. öffentliche Stellen überfordern.)*

In einem **4. Schritt** sind solche zusätzlichen Maßnahmen festzulegen und umzusetzen, die notwendig sind damit die übermittelten Daten in Drittland ein dem EU vergleichbares Niveau erreichen. Dazu enthalten die Empfehlungen des EDSA im **Anhang 2** eine nicht abschließende Liste von Beispielen zusätzlicher Maßnahmen (siehe B.).

Als **5. Schritt** sind formale Verfahrensschritte einzuleiten, damit die Zusatzmaßnahmen greifen und umgesetzt werden.

Der **6. und letzte Schritt** erfordert, dass in angemessenen zeitlichen Abständen eine Neubewertung im Hinblick auf der Schutzniveau der in ein Drittland übermittelten Daten vorgenommen wird.

B. Beispiele für zusätzliche Maßnahmen im Anhang 2

Die in der **Anhang 2** enthaltenen in den Ziffern 69 bis 137 zusätzlichen (nicht abschließenden) Maßnahmen erfassen

- **technische Maßnahmen** (engl. *technical measures*), Ziff. 72 bis 91 (nachfolgend **B.I**),
- **zusätzliche vertragliche Maßnahmen** (engl. *additional contractual measures*), einschließlich von Transparenzanforderungen und stehen unter dem Gebot, eine ordnungsgemäße Dokumentation (vgl. Art. 5 Abs. 2 DSGVO), Ziff. 92 bis 121 (**B.II**) und
- **organisatorische Maßnahmen** (engl. *organisational measures*), Ziff. 122 bis 137 (**B.III**).

Der EDSA stellt zunächst Szenarien dar, für die sich **wirksame** Maßnahmen finden lassen, weil damit öffentliche Behörden in Drittländern vom Zugang zu personenbezogenen Daten ausgeschlossen werden. Denn ein Zugang zu Daten soll nach Ziff. 74 den Behörden nur dann gewährt werden, wenn ein solcher Zugang in einer demokratischen Gesellschaft als erforderlich und verhältnismäßig erachtet wird (engl. *necessary and proportionate in a democratic society*). Dieses Kriterium zieht sich durch das ganze Papier des EDSA (vgl. z.B. die Anwendungsfälle 6 und 7).

B.I Wirksame technische Maßnahmen

Die Möglichkeit, durch wirksame **technische Maßnahmen** zur Zulässigkeit zu kommen, erläutert der EDAS beispielhaft den ersten fünf von insgesamt sieben **Anwendungsfällen**:

Anwendungsfall 1 (Ziff. 79)
Datenspeicherung zum Zweck des Backups oder zu anderen Zwecken, die keinen Zugriff auf Daten im Klartext benötigen:
Die **Nutzung eines Hosting-Dienstleisters** durch einen Datenexporteur beispielsweise zum Zwecke des Back-ups, ist zulässig, wenn vor der Übertragung eine starke Verschlüsselung (engl. *strong encryption*) erfolgt und der Verschlüsselungsalgorithmus dem Stand der Technik (engl. *state-of-the-art*; vgl. Art. 32 DSGVO) entspricht und der Schlüssel ausschließlich der Kontrolle des Datenexporteurs unterliegt.

Anwendungsfall 2 (Ziff. 80 bis 83)
Übermittlung von pseudonymisierten Daten:
Dies betrifft die Vorgänge, bei denen ein Datenexporteur die **Daten zuerst pseudonymisiert** und dann in ein Drittland übermittelt (z.B. zur Analyse zu wissenschaftlichen Zwecken) übermittelt. Wenn nur und ausschließlich der Datenexporteur und weder der Datenimporteur noch die Behörden im Drittland diese pseudonymisierten Daten einer identifizierten oder identifizierbaren natürlichen Person zuordnen können, soll ein solcher Datentransfer in ein Drittland zulässig sein.

Anwendungsfall 3 (Ziff. 84)
Verschlüsselte Daten, die Drittländer nur durchqueren:
Sollen personenbezogene Daten ein **unsicheres Drittland nur durchqueren**, um in ein sicheres Drittland zu gelangen, so muss eine dem aktuellen Stand der Technik entsprechende Transportverschlüsselung eingesetzt werden. Diese muss den Schutz vor Angriffen insbesondere der dortigen öffentlichen Behörden des Drittlandes bieten, womit nach dem EDSA gegebenenfalls auch eine Ende-zu-Ende-Verschlüsselung notwendig werden kann.

Anwendungsfall 4 (Ziff. 85)
Geschützte Empfänger:
Damit werden Fälle erfasst, bei denen die Übermittlung an einen solchen **Datenimporteur** erfolgt, der **in seinem Drittland besonders geschützt** ist (z.B. weil es sich um einen Berufsgeheimnisträger wie Arzt oder Anwalt handelt). Hier soll ein Transportverschlüsselung eine wirksame Maßnahme sein, wobei gleichzeitig für diesen Fall festgestellt wird, dass die Daten durch eine sichere Ende-zu-Ende-Verschlüsselung geschützt sein müssen und ausschließlich der im Drittland besonders geschützte Datenimporteur den Entschlüsselungsschlüssel hat.

Anwendungsfall 5 (Ziff. 86)
Geteilte oder Mehrparteien-Datenverarbeitung:
Dies soll den Fall erfassen, dass der **Datenexporteur seine Daten aufteilt**, an mehrere Auftragsverarbeiter verschickt und diese dann nach Verarbeitung ihrer Ergebnisse diese wieder an den Datenexporteur zurücksenden. Diese Aufteilung muss aber so erfolgen, dass bei allen beteiligten Auftragsverarbeitern praktisch nur pseudonymisierte Daten vorliegen. Auch darf bei einer Zusammenarbeit aller Auftragsdatenverarbeitung kein Personenbezug entstehen und dies auch nicht durch die dortigen öffentlichen Behörden möglich sein.

In den beiden letzten Anwendungsfällen (Nr. 6 und 7) wird erläutert, dass es **keine wirksamen technischen Maßnahmen** gibt **und deshalb zusätzliche vertragliche Maßnahmen** notwendig sind:

Anwendungsfall 6 (Ziff. 88)
Übermittlung an Cloud-Dienstleister oder sonstige Auftragsverarbeiter, der den Zugang zu den Daten im Klartext benötigt:
Dies betrifft die in der Praxis häufigen Fälle, in denen ein Datenexporteur die **Dienste eines Cloud-Dienstleisters oder sonstigen Auftragsverarbeiters nutzt**. Hier liegen nach dem EDSA keine wirksamen technischen Maßnahmen vor, wenn der Cloud-Dienstleister den Zugang zu den Daten im Klartext braucht und den dortigen öffentlichen Behörden der Zugang zu diesen Daten in einer Art und Weise möglich ist, die über das in einer demokratischen Gesellschaft für erforderlich und verhältnismäßig erachtete Maß hinausgehen. Die Situation kann auch nicht durch eine Transportverschlüsselung oder Data-at-rest-Verschlüsselung (also Verschlüsselung der gespeicherten Daten) durch den Datenimporteur geheilt werden.
(Anmerkung der Herausgeber: Dies dürfte ein klassischer Fall der Praxis sein. Wird z.B. im Rahmen von Office 365 die Microsoft Cloud genutzt, so bestehen aufgrund der vom EuGH als übermäßig angesehen staatlichen Eingriffsbefugnisse der US-Behörden keine wirksamen technischen Maßnahmen, die eine Datenübermittlung rechtfertigen).

Anwendungsfall 7 (Ziff. 90)

Fernzugriff auf Daten für Geschäftszwecke:

Hiervon soll der Beispielsfall umfasst sein, dass eine Unternehmensgruppe Daten an ein Unternehmen ihrer Gruppe in einem Drittland übermittelt, weil dort beispielsweise Personaldienstleistungen erbracht werden oder weil aus diesem Drittland heraus in der EU ansässige Kunden des Datenexporteurs telefonisch oder elektronisch kontaktiert werden sollen. Sofern der Datenimporteur die Daten für eigene Zwecke ohne erforderlichen Anlass nutzen kann und die Behörden dieses Drittlandes einen Zugang zu den Daten haben, die über das in einer demokratischen Gesellschaft für erforderlich und verhältnismäßig erachtete Maß hinausgehen, gibt es nach Auffassung des EDSA keine wirksame technische Maßnahme, die eine Verletzung von Betroffenenrechten verhindern kann.

B.II Zusätzliche vertragliche Maßnahmen

Nach Auffassung des EDSA sind in den Fällen, in denen **keine wirksamen technischen Maßnahmen möglich** sind, **zusätzliche vertragliche Maßnahmen** zu prüfen. Allerdings stellt der EDSA auch immer wieder fest, dass damit nicht die gesetzlichen Rechte und die staatlichen Zugriffsmöglichkeiten öffentliche Behörden verhindert werden können (z.B. in Ziff. 95). Für die Praxis ergibt sich daraus die Verpflichtung für Datenexporteure, zu versuchen, die **Datenimporteure** zu folgendem **durch Vertrag zu verpflichten** (Ziff. 100 und 101):

- Die gesetzlichen Vorschriften aufzulisten, welche die staatlichen Zugriffe erlauben.
- Informationen und Statistiken vorzulegen, die derartige Zugriffsmöglichkeiten erläutern und Angaben zu allen konkreten Zugangsanfragen in einen bestimmten Zeitraum zu machen.
- Angaben zu Maßnahmen zu machen, wie der Datenimporteur versucht, den Zugang und Zugriff staatliche Stellen zu verhindern.
- Darzulegen, ob und in welchem Umfang öffentliche Behörden einem Datenimporteur verbieten, die entsprechenden Informationen an den Datenexporteur weiterzugeben.

In allen Fällen und Situationen besteht die Pflicht zur Transparenz und Dokumentation (vgl. auch Art. 5 Abs. 2 DSGVO).

Der EDSA macht darauf aufbauend **Vorschläge für Klauseln in den Verträgen** zwischen Datenexporteur und Datenimporteur (Ziff. 102 bis 111). So ist nach dem EDSA zu vereinbaren, dass ein Importeur verpflichtet ist, jede Anordnung zur Offenlegung von Daten durch Behörden zu überprüfen und entsprechende Anordnungen anzufechten (Ziff. 112).

(Anmerkung der Herausgeber: In der Praxis hat diese Forderung bereits zu einer Änderung der Vertragsmuster von Microsoft geführt, nämlich das Angebot zusätzlicher Schutzmaßnahmen zu den Standardvertragsklauseln.)

Allerdings wird für die Wirksamkeit und damit im Endeffekt für die Zulässigkeit als weitere Voraussetzung gefordert, dass in dem entsprechenden Drittland bis zur Entscheidung eines dortigen Gerichts eine Aussetzung der Anordnung, also ein einstweiliger Rechtsschutz, ebenso möglich sein muss, wie die Information an den Exporteur über die staatlichen Maßnahmen.

Vorgeschlagen und erörtert werden schließlich auch Klauseln zur Information von betroffenen Personen über Anfragen oder Anordnungen öffentlicher Behörden des Drittlandes. Schließlich könnte auch in einem Vertrag zwischen Datenexporteur und Datenimporteur eine Verpflichtung enthalten sein, betroffene Personen bei der Ausübung ihrer Rechte im Drittland auf gerichtlichem Wege zu unterstützen (Ziff. 120).

B.III Organisatorische Regelungen als zusätzliche Maßnahme

Neben technischen Maßnahmen und vertraglichen Regelungen listet EDSA **organisatorische Regelungen** auf, mit denen der Schutz personenbezogenen Daten im gesamten Verarbeitungszyklus aufrechterhalten werden soll (Ziff. 122 bis 137). Dazu können sowohl beim Datenexporteur als auch beim Datenimporteur gehören:

- Interne Richtlinien (zum Datenschutz und zur Datensicherheit) mit klarer Aufgabenzuweisung,
- Meldekanälen und Standardbetriebsabläufen in den Fällen behördlicher Anfragen,
- die Schulung des Personals und regelmäßige Audits sowie
- die Einbeziehung des Datenschutzbeauftragten.

In allen Fällen soll die Dokumentation zwecks Transparenz und Rechenschaft geregelt werden.