Bitkom Konzept zur Erhaltung der internationalen Datentransfers

Bitkom hat am 22.12.2020 zu dem Entwurf der EDSA-Empfehlungen zur Implementierung des Schrems II-Urteils des EuGH (Recommendations 01/2020) Stellung genommen. Darin hat Bitkom u.a. ein eigenes Vorgehensmodell präsentiert, das eine maßvolle und zugleich rechtskonforme Umsetzung des Urteils ermöglicht. Im Nachgang hat Bitkom u.a. mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit konstruktive Gespräche geführt und um Feedback gebeten. In diesem Zusammenhang sind vor allem die praktische Notwendigkeit der Flexibilität einerseits sowie die rechtsdogmatische Herausforderungen andererseits diskutiert worden. Als Ergebnis dieser Gespräche möchte Bitkom seine bisherigen Ausführungen ergänzen und mit dem hierdurch vorgelegten Konzept vertieft zu dem Bedürfnis nach einer differenzierenden Umsetzung des Schrems-II-Urteils sowie zu den entsprechenden rechtlichen Anknüpfungspunkten Stellung nehmen. Bitkom verbindet damit die Erwartung, dass der BfDI diese Erwägungen nachvollziehen und in die Erörterungen auf EDSA-Ebene einbringen kann. Die endgültige Version der EDSA-Empfehlungen sollte den Unternehmen sodann Raum für eine differenzierende Umsetzung der rechtlichen Anforderungen und damit Rechtssicherheit geben.

I. Bedürfnis nach Differenzierung

Bitkom hat innerhalb der Mitgliedschaft eine Reihe von Übermittlungsszenarien identifiziert, für die dringend eine abgestufte Umsetzung des Schrems-II-Urteils erforderlich ist. Denn andernfalls stehen der Aufwand für zusätzliche Maßnahmen bis hin zur kompletten Umgestaltung oder gar Einstellung ganzer Geschäftsprozesse bzw. Lieferantenbeziehungen in keinem Verhältnis zur tatsächlichen Bedrohung für das Recht auf informationelle Selbstbestimmung der Betroffenen. Dieses Missverhältnis kann sich aus technischen Übermittlungskonstellationen ebenso wie aus den ggf. übermittelten Daten oder einer Kombination solcher Aspekte ergeben, und es wäre weder durch das Urteil Schrems II noch durch die DSGVO gerechtfertigt. Dies vorweggeschickt, hält Bitkom in diesen Fällen eine Prüfung der Einzelumstände einer Datenübermittlung bzw. des Datenschutzniveaus im jeweiligen Drittland keinesfalls für verzichtbar. Wir gelangen aber zu der Auffassung, dass in solchen Fällen kompensierende Maßnahmen oder gar prozessuale Änderungen nicht bis zum Stadium der Unmöglichkeit von behördlichen Datenzugriffen implementiert werden müssen. Dies ergibt sich bereits aus Art. 52 der Charta der Grundrechte der Europäischen Union, wonach Übermittlungen auf Grundlage von Art. 46 DS-GVO-Instrumenten (z. B. EU Standardvertragsklauseln oder Binding Corporate Rules) nur zulässig sind, wenn Datenzugriffe durch drittstaatliche Behörden nur in einem Umfang stattfinden können, der auch nach EU-Recht zulässig wäre. Zugriffe sind hiernach nur bzw. dann zulässig,

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

wenn eine ausreichend klare *gesetzliche Grundlage* gegeben ist sowie im Rahmen von *Erforderlichkeit und Verhältnismäßigkeit. Weitere Voraussetzung ist, dass d*en betroffenen Personen ausreichende Rechtsbehelfe gegen solche Zugriffe zur Verfügung stehen (vgl. Art. 47 EU Grundrechtecharta; in der Regel ist gerichtlicher Rechtsschutz nötig). Das bedeutet somit, dass von Verantwortlichen nicht grundsätzlich gefordert werden kann, dafür Sorge zu tragen, dass behördliche Zugriffe absolut ausgeschlossen sind, weil sie dies eben auch nach EU-Recht nicht sind. Es kommt auch hier auf den Vergleichsmaßstab und ein entsprechend dem EU Recht vergleichbares Schutzniveau an.

Einen solchen Ausschluss behördlicher Zugriffe zu verlangen, hieße im Übrigen auch, ein Schutzniveau im Drittland vorauszusetzen, das auch bei Verarbeitung in Deutschland nicht gegeben wäre; auch hier unterliegen verarbeitete Daten, auch personenbezogene Daten, der Beschlagnahme sowie weiteren Maßnahmen der Gefahrenabwehr, der Strafverfolgung, sowie G10-Maßnahmen. Darüber hinaus wäre eine Argumentation, die auf einen grundsätzlichen Ausschluss etwaiger grenzüberschreitender Beschlagnahmemaßnahmen zielte, schon deswegen verfehlt, weil entsprechende Maßnahmen in Deutschland seit der mit Wirkung vom 01.01.2008 eingefügten Regelung § 110 Abs. 3 StPO gesetzlich verankert sind. Es dürfte nicht zu rechtfertigen sein, von anderen Ländern, gleich, ob sie Drittländer sind oder nicht, ein Schutzniveau für personenbezogene Daten zu fordern, das das jeweilige Ursprungsland selbst nicht gewährleistet. Anhaltspunkte dafür, dass dies verlangt werden könnte, sind auch Schrems II nicht zu entnehmen.

Insoweit vertritt Bitkom daher die Position, dass es in der unternehmerischen Praxis keine in jeglicher Hinsicht absolut sichere Lösung gibt, sondern „nur“ eine beanstandungsfreie Lösung unter Berücksichtigung der Rechte und Freiheiten betroffener Personen das Ziel sein kann. Folgt man dieser Position, werden das Recht auf informationelle Selbstbestimmung betroffener Personen und die ebenso in der Charta der Grundrechte der EU anerkannte unternehmerische Freiheit (Art. 16 EU Grundrechtecharta), auf die sich die Mitgliedsunternehmen von Bitkom berufen - in Einklang gebracht.

Darüber hinaus kann ein ausreichendes Maß an Schutz betroffener Personen auch dadurch erreicht werden, dass die objektive Wahrscheinlichkeit des Eintritts von Bedrohungsszenarien für das Recht auf informationelle Selbstbestimmung des Betroffenen bei der Evaluation von geeigneten, zusätzlichen Maßnahmen bzw. Garantien in relevanter Weise gewichtet wird. Dabei setzen wir den Abschluss beispielsweise von EU-Standarddatenschutzklauseln in der jeweils aktuellen Fassung oder Binding Corporate Rules stets voraus.

Szenarien, bei denen eine entsprechende Flexibilität aus Sicht der Praxis erforderlich ist, sind etwa die nachfolgend beschriebenen:

- **Konzernweites Active Directory;** es handelt sich hier um einen Fall besonderer Relevanz, da das Active Directory, das hier beispielhaft für alle vergleichbaren Steuerungsinstrumente steht, als zentrales System der Zugriffs- und Zugangskontrolle sowie der Rechtesteuerung in IT-Systemen zum Einsatz kommt. In diesem Falle sind ausschließlich Informationen betroffen, die der Organisation zuzuordnen sind. Auch wenn die Namen der Mitarbeiter, ihre Funktion und ihre Zuordnung bzw. Erreichbarkeit innerhalb der Organisation Teil dieser Daten sind, hat die Organisation selbst ein hohes Vertraulichkeitsinteresse, welches im Drittland gegebenenfalls enttäuscht werden könnte. Stellt man dem das Bedürfnis nach globaler Vernetzung, Erreichbarkeit und Zugangsmöglichkeit zu Netzwerken – zumal in Zeiten globaler Integration von Wertschöpfungs- und Unterstützungsprozessen – gegenüber, wird deutlich, dass die disruptive Auswirkung einer Untersagung oder auch nur vollständiger Verschlüsselung dieser Daten ohne Rücksicht auf den Betriebszustand zu jedem Zeitpunkt weder intendiert sein wird noch praktikabel realisierbar ist. Positiv zu betonen sind auch die technischen und

organisatorischen Kontrollmöglichkeiten innerhalb eines Konzerns, die das Risiko für die betroffenen Personen und letztlich auch in Bezug auf staatliche Zugriffe noch einmal reduzieren.

- **Active Directory-as-a-Service;** in diesem Falle sind ausschließlich Informationen betroffen, die der Organisation zuzuordnen sind und die im entscheidenden Umfang auch noch verschlüsselt sind. Auch wenn etwa dienstliche Account-Informationen und verknüpfte Rechte auf Objekte als Teil dieser Daten einen Personenbezug haben werden, hat doch in erster Linie die Organisation selbst ein Vertraulichkeitsinteresse, welches im Drittland gegebenenfalls enttäuscht werden könnte und weniger die Mitarbeiter selbst. Zudem erscheint kein Szenario realistischer Weise vorstellbar, in welchem Behörden nach eben diesen Daten "fragen" bzw. sich Zugang zu gerade diesen Daten verschaffen wollen und es zu Nachteilen für Betroffene kommt. Vielmehr stellt sich das Active Directory-as-a-Service gerade bei kleinen und mittleren Unternehmen oft als gegenüber unstrukturierten Lösungen auch unter dem Gesichtspunkt des Schutzes informationstechnischer Systeme oft als überlegen dar, da es zentrale Infrastrukturkomponenten in die Hand vertrauenswürdiger Anbieter legt und dem Unternehmen damit Werkzeuge an die Hand gibt, die in eigener Infrastruktur fehlen würden.
- **Wartung, Support und Service (Remote-Zugriff); die Aufgabe ist hierbei die Systemkonfiguration, Systemwartung und Fehleranalyse. Ein Zugriff auf personenbezogene Nutzdaten ist unabhängig vom Ort der Verarbeitung durch technische und organisatorische Maßnahmen vor Zugriffen Dritter zu schützen.** Daher erscheint das gesamte durch das Schrems-II-Urteil adressierte Szenario für die Bedrohung von Gewährleistungszielen ganz unabhängig von den relevanten Daten nicht realistisch. Denn hier können meist keine personenbezogenen Daten beim Empfänger im Drittland verarbeitet werden, allenfalls temporär im Rahmen eines Supportfalles. Bei einer Wartung sind die personenbezogenen Daten selbst nicht Ziel der Verarbeitung Richtig ist in dem Falle allerdings, dass die geschilderte Sicherheit der Verarbeitung auch tatsächlich durch Maßnahmen gestützt sein muss, was bereits eine Anforderung im Rahmen der durch den Dienstleister nach Art. 28 (1) i.V.m 32 DSGVO zu ergreifenden technischen und organisatorischen Maßnahmen (TOMs) und unabhängig von einer Drittlandsübermittlung ist. Im eigenen Interesse werden Unternehmen gerade in diesem Anwendungsfall besonders sorgfältig vorgehen, um die Gefahr von Angriffen auf ihre IT-Infrastruktur nach Möglichkeit auszuschließen.
- **Globales Intranet;** in diesem Falle sind - in bei weitem größten Umfang - Informationen betroffen, die der Organisation zuzuordnen sind. Auch wenn Namen der Mitarbeiter, ihre Stellung und Erreichbarkeit in der Organisation Teil dieser Daten sind, hat doch in erster Linie die Organisation selbst ein hohes Vertraulichkeitsinteresse, welches im Drittland gegebenenfalls enttäuscht werden könnte. Es geht hier nicht um Daten im privaten Kontext, deren ev. Offenbarung einen Mitarbeiter in seiner Privatsphäre beeinträchtigen. Zudem muss die global tätige Organisation ohnehin schon Maßnahmen zum Schutz der Vertraulichkeit der Informationen treffen. Eine zusätzliche Bedrohung für betroffene Personen durch ein Datenschutz-Defizit im Drittland und Zugriffe durch Behörden sehen wir daher nicht. Auch wenn teilweise die Ansicht vertreten wird, subjektive Aspekte dürften bei einer Beurteilung nicht berücksichtigt werden, greift zumindest das Argument hinsichtlich Art. 52 der Charta der Grundrechte der EU (s.o.). Staatliche Zugriffe müssen vom Umfang her nicht gänzlich ausgeschlossen werden; dies zu verlangen, käme im Ergebnis einem Tätigkeitsverbot für die betroffenen Dienstleister gleich, da es verlangen würde, dass sie sich in ihrer Rechtsordnung gesetzlich verankerten Maßnahmen widersetzen. Es erscheint kaum vorstellbar, beispielsweise von einem Dienstleister in Deutschland zu verlangen, einen Beschlagnahmebeschluss nicht zu befolgen oder sich einer Durchsuchungsmaßnahme zu widersetzen, wenn diese rechtmäßig erfolgen, und gleichwohl wird dies in der Öffentlichkeit von Dienstleistern

im Drittland immer wieder verlangt. Der Kunde eines Dienstleisters wäre auch schlecht beraten, wollte er sich wissentlich auf eine Geschäftsbeziehung mit einem Dienstleister einlassen, der die gesetzlichen Anforderungen seines Landes missachtet. Stellt man dem das Bedürfnis nach globaler Vernetzung, Zusammenarbeit und Austausch – zumal in Zeiten virtueller Teams und Matrixorganisationen - gegenüber, wird deutlich, dass die disruptive Auswirkung einer aufsichtsbehördlichen Nutzungsuntersagung oder auch nur vollständiger Verschlüsselung dieser Daten zu jedem Zeitpunkt weder intendiert sein kann, noch durch Schrems II verlangt wird, noch realisierbar bzw. praktisch sinnvoll ist (insbesondere mit Blick auf bestimmte Ausprägungen der Verschlüsselung und der Schlüsselverwaltung).

- **Globales Adressbuch;** in diesem Falle sind in bei weitem größten Umfang Informationen betroffen, die der Organisation zuzuordnen sind. Auch wenn Namen der Mitarbeiter, ihre Rolle und Erreichbarkeit in der Organisation Gegenstand dieser Daten sind, hat doch in erster Linie die Organisation selbst ein Vertraulichkeitsinteresse, welches im Drittland gegebenenfalls enttäuscht werden könnte, s. o. bereits die entsprechenden Ausführungen zu Globales Intranet. Zudem muss jede Organisation ohnehin schon Maßnahmen zum Schutz der Vertraulichkeit der Informationen treffen. Eine zusätzliche Bedrohung für betroffene Personen durch ein niedrigeres Datenschutz-Niveau im Drittland und Zugriffe durch Behörden sehen wir daher nicht. Auch wenn teilweise die Ansicht vertreten wird, subjektive Aspekte dürften bei einer Beurteilung nicht berücksichtigt werden, greift zumindest das Argument hinsichtlich Art. 52 der Charta der Grundrechte der EU (s.o.). Staatliche Zugriffe müssen vom Umfang her nicht gänzlich ausgeschlossen werden. Stellt man dem das Bedürfnis nach globaler Vernetzung, Zusammenarbeit und Austausch – zumal in Zeiten virtueller Teams und Matrixorganisationen - gegenüber, wird deutlich, dass die disruptive Auswirkung einer aufsichtsbehördlichen Nutzungsuntersagung oder auch nur vollständiger Verschlüsselung dieser Daten zu jedem Zeitpunkt weder intendiert sein kann noch realisierbar bzw. praktisch sinnvoll ist (insbesondere mit Blick auf bestimmte Ausprägungen der Verschlüsselung und der Schlüsselverwaltung).
- **Newsletter-Tools;** in diesem Falle beschränken sich übermittelte Daten auf (dienstliche) E-Mail-Adressen sowie ggf. Vor- und Nachnamen sowie die zu übermittelnden Inhalte. Diese sind bei Newslettern auf Grund ihrer Zielrichtung an eine Vielzahl von Empfängern generisch gestaltet. Mit welcher Motivation sich Behörden Zugriff zu diesen Daten verschaffen wollen sollten, ist unklar. Daher sehen wir auch hier faktisch keine relevanten Bedrohungen für die Rechte und Freiheiten der Betroffenen bei einer Verarbeitung von Klardaten im Drittland. Ergänzende Maßnahmen werden dadurch nicht ausgeschlossen und können im Einzelfall auch angezeigt sein, es bedarf jedoch immer einer Betrachtung der Erforderlichkeit und Geeignetheit. Auch wenn teilweise die Ansicht vertreten wird, subjektive Aspekte dürften bei einer Beurteilung nicht berücksichtigt werden, greift zumindest das Argument hinsichtlich Art. 52 der Charta der Grundrechte der EU (s.o.). Staatliche Zugriffe müssen vom Umfang her nicht gänzlich ausgeschlossen werden.
- **Business Lern-Plattformen;** in diesem Falle sind in bei weitem größten Umfang Informationen betroffen, die eine enge Anbindung an die Organisation haben. Auch wenn (pseudonyme) Account-Informationen und andere Informationen den Mitarbeiter betreffen, beschränkt sich doch deren Relevanz auf den Kontext der Organisation und der Rolle des Mitarbeiters in dieser. Insofern hat auch hier in erster Linie die Organisation selbst ein Vertraulichkeitsinteresse, welches im Drittland gegebenenfalls enttäuscht werden könnte und weniger die Mitarbeiter*innen. Daher muss und wird die Organisation ohnehin schon Maßnahmen zum Schutz der Vertraulichkeit der Informationen treffen. Eine zusätzliche Bedrohung durch ein niedrigeres Datenschutz-Niveau

im Drittland und Zugriffe durch Behörden sehen wir daher nicht. Auch wenn teilweise die Ansicht vertreten wird, subjektive Aspekte dürften bei einer Beurteilung nicht berücksichtigt werden, greift zumindest das Argument hinsichtlich Art. 52 der Charta der Grundrechte der EU (s.o.). Staatliche Zugriffe müssen vom Umfang her nicht gänzlich ausgeschlossen werden. Stellt man dem die Relevanz von Lernmaterial in diversen Sprachen und mit unterschiedlichstem Inhalt gegenüber, erscheinen Untersagungen oder allzu strikte technische Anforderungen beispielsweise an Verschlüsselung dieser Daten nicht notwendig zum Schutze der Betroffenen.

- **Online-Kollaborations-Werkzeuge;** in diesem Falle sind Informationen betroffen, die eine enge Anbindung an die Organisation haben. Auch wenn – häufig pseudonyme - Account-Informationen die Mitarbeiter betreffen, beschränkt sich deren Relevanz auf den Kontext der Organisation. Insofern hat auch hier in erster Linie die Organisation selbst ein Vertraulichkeitsinteresse, welches im Drittland gegebenenfalls enttäuscht werden könnte. Daher muss und wird die Organisation ohnehin schon Maßnahmen zum Schutz der Vertraulichkeit der Informationen treffen. Eine zusätzliche Bedrohung für betroffene Personen durch ein niedrigeres Datenschutz-Niveau im Drittland und Zugriffe durch Behörden sehen wir daher nicht. Auch wenn teilweise die Ansicht vertreten wird, subjektive Aspekte dürften bei einer Beurteilung nicht berücksichtigt werden, greift zumindest das Argument hinsichtlich Art. 52 der Charta der Grundrechte der EU (s.o.). Staatliche Zugriffe müssen vom Umfang her nicht gänzlich ausgeschlossen werden. Stellt man -gerade dieser Tage in der anhaltenden Corona-Pandemie – diesen Erwägungen das Bedürfnis nach Überwindung von Entfernungen im Rahmen virtueller Zusammenarbeit gegenüber, erscheinen Untersagungen oder über den Stand der Technik hinausgehende Anforderungen an die Verschlüsselung dieser Daten nicht notwendig zum Schutze der Betroffenen oder gar kontraproduktiv, da sich mögliche Betriebsrisiken und somit Einschränkungen bei der Betriebssicherheit, Verfügbarkeit und Integrität der Daten ergeben können.
- **Software-as-a-Service Lösungen;** Eine Organisation wird ohnehin Maßnahmen zum Schutz der Vertraulichkeit der personenbezogenen Daten umsetzen. Hierbei ist sowohl die Zugriffskontrolle beim Verantwortlichen als auch die Zugriffskontrolle beim Dienstleister klar geregelt und überwacht. Zudem wird diese durch zusätzliche Maßnahmen, wie z.b. Verschlüsselung sensibler Felder oder der zugrundeliegenden Datenbank sowie Pseudonymisierung und Datenminimierung flankiert. Eine zusätzliche Bedrohung durch ein Datenschutz-Defizit im Drittland und Zugriffe durch Behörden sehen wir daher auch hier nicht. Vielmehr sollte auch eine Abwägung gegen mögliche Betriebsrisiken und somit Einschränkungen bei den Gewährleistungszielen Verfügbarkeit und Integrität der personenbezogenen Daten durchgeführt werden.

II. Rechtliche Verortung der Differenzierung

1. „Geeignetheit“ als Korrektiv

Anknüpfungspunkt für eine nach den konkreten Umständen des Einzelfalls differenzierende Ableitung von zusätzlichen Maßnahmen ist der Begriff der „Geeignetheit“ von Garantien i.S.v. Art. 46 Abs. 1 DSGVO. Damit sind zunächst die Erkenntnis und das Bekenntnis verbunden, dass eine Datenübermittlungskonstellation – so wenig sie aus der Sicht des Betroffenen eine Bedrohung darstellen mag – nicht per se aus der Prüfung des Art. 46 Abs. 1 DSGVO ausgesondert werden kann und soll. Gleichzeitig setzt die Prüfung der Geeignetheit einer Garantie denknotwendig voraus, dass eine Datenübermittlung in ein Drittland vorliegt, in dem das Datenschutzniveau (ggfs. „noch“) nicht nach Art. 45 Abs. 3 als angemessen eingestuft ist und damit potentiell ein „Mangel an Datenschutz“ (vgl. EG 108 S. 1

DSGVO) besteht. Nur dann ist mit EG 108 zu prüfen, welche Bedrohungslage im konkreten Fall besteht, welche Garantien geeignet sind und ob überhaupt ein Defizit im Datenschutzniveau besteht, das durch potenzielle – vertragliche, technische oder organisatorische – Maßnahmen in Ausgleich gebracht werden muss und kann. Eine solche am Einzelfall orientierte Prüfung der Geeignetheit kann nur am Ende erfolgen und stellt danach ein Korrektiv und kein Vorab-Kriterium dar. Dies trägt auch der Ansicht des EuGH Rechnung, der im Schrems II-Urteil auf eine Betrachtung der Umstände des Einzelfalles abstellt. Dabei ist auch zu berücksichtigen, dass das Fehlen einer Einstufung nach Art. 45 Abs. 3 DSGVO keineswegs bedeutet oder auch nur indiziert, dass das Schutzniveau nicht objektiv angemessen wäre; vielmehr hat in der Regel noch gar kein Prüfverfahren stattgefunden.

2. Beurteilungsspielraum des Verantwortlichen

Dem Verantwortlichen ist gem. Art. 44, 45 Abs. 1 3, 46 Abs. 1 und EG 108 S. 1 DSGVO im Hinblick auf die „geeigneten Garantien" zur Erreichung eines angemessenen (Daten-)Schutzniveaus Flexibilität dabei einzuräumen, ob eine an sich abstrakt geeignete (vertragliche, organisatorische, oder technische) Maßnahme auch tatsächlich implementiert werden muss. Denn der Begriff der Geeignetheit eröffnet einen an der Bedrohungslage für den Betroffenen im Einzelfall orientierten und vom Verantwortlichen auszufüllenden Beurteilungsspielraum. Dieser Beurteilungsspielraum knüpft nicht nur an das im Drittland bestehende Datenschutzniveau an, sondern nimmt auch das tatsächliche Schutzbedürfnis des Betroffenen in den Blick.

a) Nach Maßgabe von Art. 44 DSGVO sind sowohl Kapitel V als auch die sonstigen Bestimmungen der DSGVO im Falle der Übermittlung personenbezogener Daten in einen Drittstaat der Maßstab für die Rechtmäßigkeit der Verarbeitung. Gemäß Art. 45 Abs. 1 DSGVO ist im Zielland ein „angemessenes" Datenschutzniveau erforderlich. Daraus folgt zweierlei: (1) Es muss kein identisches Datenschutzniveau erreicht werden; insbesondere kann nicht ein Datenschutzniveau verlangt werden, das über das des Ursprungslandes hinausgeht. (2) Was insoweit zur Angemessenheit führt, ist nach den in Art. 45 Abs. 2 DSGVO beschriebenen Kriterien zu bemessen. Auf der Grundlage dieser Kriterien fasst die Europäische Kommission einen Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO.

Art. 46 Abs. 1 DSGVO nimmt demgegenüber ein Szenario in den Blick, in welchem eine Entscheidung nach Art. 45 Abs. 3 DSGVO nicht vorliegt. In einem solchen Falle liegt kein abstrakt-generelles, normatives Kriterium vor, an dessen Vorliegen ein angemessenes Datenschutzniveau geknüpft werden könnte. Dann muss und kann auf „geeignete Garantien" zurückgegriffen werden, die der Verantwortliche [...] implementieren muss.

b) Wenn und soweit der Verantwortliche Standarddatenschutzklauseln verwendet, dürfen die Anforderungen an diese Garantien aus normativen Gründen nicht überspannt werden. Das folgt zunächst aus der Wertung des Art. 46 Abs. 2 DSGVO, wonach bei Vorliegen einer der in Art. 46 Abs. 2 DSGVO genannten Varianten der Rechtsanwender ohne besondere Genehmigung einer Aufsichtsbehörde davon ausgehen können muss, dass ein angemessenes Datenschutzniveau gewährleistet ist. Das trifft gem. Art. 46 Abs. 2 lit. c) DSGVO insbesondere dann zu, wenn die nach Art. 93 Abs. 2 DSGVO von der Europäischen Kommission erlassenen Standarddatenschutzklauseln verwendet werden.

c) Zu beachten ist außerdem, dass Art. 46 Abs. 1 DSGVO eine konkrete Datenübermittlungssituation im Blick hat, d.h. sich die Garantien in der konkreten Übermittlungskonstellation bewähren müssen. Das ergibt sich daraus, dass „der" Verantwortliche bzw. Auftragsverarbeiter in den Blick genommen wird und nicht etwa das Drittland oder (Kategorien von) Datenempfänger(n) oder aber Verantwortliche/Auftragsverarbeiter allgemein. Die Geeignetheit von Maßnahmen kann also nicht schlechthin bestimmt werden, sondern ist im Lichte der konkreten Übermittlungssituation – individuell - zu evaluieren.

d) Innerhalb einer solchen individuellen Prüfung sind Maßnahmen „geeignet“, wenn und soweit sie den damit verfolgten Zweck fördern. Im Hinblick auf den konkreten Zweck von geeigneten Garantien führt EG 108 aus, dass *der Verantwortliche oder der Auftragsverarbeiter einen Ausgleich zwischen den in einem Drittland bestehenden Mangel an Datenschutz und den Schutz der betroffenen Person* schaffen soll. Maßgeblich für die Frage, was „geeignet“ ist, ist danach die Frage, ob und inwieweit die betroffene Person infolge eines Mangels des Datenschutzes im Drittland konkret schutzbedürftig ist. Damit entfallen Konstellationen, in denen es an der Kausalität zwischen dem Schutzbedürfnis/einer Bedrohungslage für den Betroffenen einerseits und dem mangelnden Datenschutzniveau im Drittland andererseits fehlt. Es entfallen auch Konstellationen, in denen es selbst angesichts eines mangelnden Datenschutzniveaus im Drittland und daraus folgenden, abstrakten Bedrohungen an einem Schutzbedürfnis fehlt, weil sich vernünftiger Weise keine Szenarien identifizieren lassen, in welchen die Bedrohungen sich auch tatsächlich zulasten des Betroffenen niederschlagen.

So, wie es Situationen gibt, in denen die in den Standarddatenschutzklauseln enthaltenen Regelungen möglicherweise kein ausreichendes Mittel darstellen, um in der Praxis den effektiven Schutz der in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten, gibt es andererseits – und das hat auch der EuGH eingeräumt (vgl. aaO Rn. 126) - Situationen, in denen das angemessene Datenschutzniveau durchaus allein auf der Grundlage der Standarddatenschutzklauseln garantiert werden kann. Es bleibt somit festzuhalten, dass zusätzlich zu Standarddatenschutzklauseln geeignete Maßnahmen nicht in jedem Fall ergriffen werden müssen, mithin auch Fälle gegeben sind, in denen diese gar nicht erforderlich sind. Dabei kann es sich bei einer etwa erforderlichen zusätzlichen Maßnahme auch um kompensierende und nicht ausschließlich schadenspräventive Maßnahmen handeln (z.B. Schadensersatzregelungen, Zusicherung von Rechtsvertretung im Drittland, Beteiligung an etwaigen Rechtsmittelverfahren), sofern sich diese als geeignet darstellen, ein Defizit an Datenschutz im Drittland auszugleichen. Die Entscheidung zwischen schadenspräventiven, kompensierenden und keinen zusätzlichen Maßnahmen muss aber an den Einzelfall und dabei an ein Kriterium anknüpfen, das die konkrete Übermittlungskonstellation in den Blick nimmt. Diese Rolle kann die Bedrohungsanalyse einnehmen.

3. Kein Widerspruch zur EuGH-Entscheidung

Eine am Einzelfall orientierte und die individuelle Bedrohungslage berücksichtigende Auslegung des Begriffs der Geeignetheit aus Art. 46 Abs. 1 DSGVO steht auch nicht im Widerspruch zur Schrems-II-Entscheidung des EuGHs. Denn auch nach Aussage des Gerichts ist es zunächst einmal Sache des Verantwortlichen [...], die entsprechenden Garantien/Maßnahmen festzulegen, (EuGH, Schrems II, Rn. 131). Zudem legt auch der EuGH insoweit einen relativen Maßstab zur Bestimmung zusätzlicher Maßnahmen/Garantien an, indem er auf die Lage im Drittland (EuGH, Schrems II, Rn. 133) und den Einzelfall (EuGH, Schrems II, Rn. 134) abstellt. Die „Lage“ und der Einzelfall werden bestimmt durch rechtliche und die tatsächlichen Gegebenheiten – etwa durch die Rechtsanwendung in der Praxis, die das erforderliche Schutzniveau beeinflussen. In diesem Rahmen überlässt es der EuGH dem Verantwortlichen, die entsprechenden Maßnahmen/Garantien festzulegen, wenngleich diese der Nachprüfung durch die Aufsichtsbehörden unterliegen werden (EuGH, Schrems II, Rn. 135).

III. Konsequenzen hieraus für den BITKOM

BITKOM würde es begrüßen, wenn der EDSA die vorstehenden Darlegungen aufgreifen und in eine neue Version der Empfehlungen einfließen lassen würde. Denn nur dann, wenn die Verantwortlichen in der Lage sind, den Prüfungsrahmen, der objektiv zutreffend ist, im Einzelfall bestimmen zu können, und in dem für pauschalisierende

Ausschlüsse kein Raum bleibt, können sie zutreffend und beanstandungsfrei feststellen, ob eine bestimmte Übermittlung aufgrund der Umstände im Einzelfall zulässig ist.