Internationale Datentransfers in Drittstaaten – Rechtmäßigkeit unter Berücksichtigung der Einzelumstände der Übermittlungen

Draft-Konzept Stand Januar 2021

bitkom

Herausgeber:
Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin
Tel.: 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner:
Rebekka Weiß
T 030 27576-161
r.weiss@bitkom.org

Verantwortliches Bitkom-Gremium:
AK Datenschutz

Titelbild: © Fotograf – Stockagentur

bitkom

Inhaltsverzeichnis

bitkom

1 Einleitung

Die mit dem Urteil des Europäischen Gerichtshof („EuGH“) vom 16. Juli 2020, Az. C-311/18 („Schrems II-Urteil“) herbeigeführte Rechtslage hat lange Zeit für Ratlosigkeit und Unsicherheit innerhalb der Industrie zum Umgang mit internationalen Datentransfers geführt. Die Unsicherheit betrifft weniger den unmittelbar umsetzbaren Aspekt der Unwirksamkeit des Angemessenheitsbeschlusses zum Privacy Shield. Sie betrifft vielmehr die subtileren Konsequenzen für internationale Datentransfers generell. Denn nach Maßgabe des Urteils bestehen selbst im Falle der Verwendung von Standardvertragsklauseln im Sinne von Art. 46 Abs. 2 lit. d) DSGVO weitergehende Prüfanforderungen sowohl seitens der Unternehmen[1] als auch seitens der Aufsichtsbehörden[2] zur Frage der Notwendigkeit *zusätzlicher* Maßnahmen zugunsten des Schutzes der Rechte Freiheiten von Betroffenen bei Drittstaatentransfers. Zu den sich anschließenden Fragen zu den Auslösern für die Notwendigkeit zusätzlicher Maßnahmen sowie zu der Art der Maßnahmen selbst trifft der EuGH keine klaren Aussagen, sodass dieses Vakuum durch die Praxis zu füllen ist.

Das bestehende Vakuum ist aus Sicht der von BITKOM repräsentierten Mitgliedsunternehmen nicht akzeptabel, denn es fehlt an Rechts- und Planungssicherheit. Über alle Industriebereiche und unternehmensinterne Prozesse hinweg hat sich seit Jahren eine Praxis etabliert und im Vertrauen auf die bestehende Rechtlage auch verfestigt (hierzu unter B.). Diese Praxis sieht sich unter Umständen Veränderungen gegenüber, die als Folge einer undifferenzierten Umsetzung des Schrems II-Urteils disruptive Folgen haben können.[3]

Diese Bedenken haben in den vergangenen Monaten keinerlei Widerhall gefunden. Weder der Europäische Datenschutzausschuss noch die deutschen Aufsichtsbehörden haben hierzu bislang überzeugende Konzepte vorlegt. Das gilt sowohl für die unmittelbar nach Urteilsfällung herausgegebenen FAQs als auch für entsprechende Pressemitteilungen. Deshalb hat sich BITKOM seit August 2020 dieser Herausforderung im Rahmen einer Arbeitsgruppe angenommen und dabei das vorliegende Konzept (hierzu unter C.I.) entwickelt.

Dabei erläutert das Konzept auch die rechtlichen Grundlagen (hierzu unter C.II.). Diese Ausführungen sind umso relevanter, als die jüngsten Ausführungen des Europäischen Datenschutzausschusses auf den ersten Blick auf eine weniger flexible Interpretation der Rechtslage durch die Aufsichtsbehörden schließen lassen. Dementsprechend äußern sich auch deutschen Datenschutzaufsichtsbehörden zurückhaltend bzw. kritisch gegenüber dem von BITKOM favorisierten Ansatz.

2 Ausgangslage

Innerhalb der Mitgliedsunternehmen von BITKOM hat sich seit langem eine Praxis internationaler Datenflüsse etabliert. Internationale Datentransfers sind einer globalisierten Wirtschaft immanent. Unternehmen sämtlicher Größenordnungen und aller Sektoren und Industrien setzen etwa auf (digitale) Dienstleistungen, die mit internationaler Verfügbarkeit von Daten, auch und gerade in den USA verbunden sind. Der Fokus auf US-amerikanische Unternehmen ist dabei weder zufällig noch im Sinne eines Selbstzwecks beabsichtigt, sondern mangels Alternativen unumgänglich. Denn nur auf internationalen Märkten lassen sich leistungsfähige,

[1] Vgl. EuGH, Schrems II-Urteil, Rn. 132.
[2] Vgl. EuGH, Schrems II-Urteil, Rn. 146.
[3] Vgl. EuGH, Schrems II-Urteil, Rn. 135 Satz 1.

standardisierte und etablierte Lösungen oder Komponenten für solche Lösungen identifizieren. Diese Komponenten unterstützen bzw. ergänzen das Unternehmensportfolio der Verbands-Unternehmen im Rahmen der eigenen Wertschöpfungsketten oder auch nur zur Unterstützung interner Prozesse. Und nachdem die USA über Jahrzehnte hinweg strategischer Partner der deutschen und europäischen Wirtschaft war, haben sich insbesondere mit Unternehmen mit Sitz in den USA strategische Partnerschaften etabliert. Es kommt insofern nicht von ungefähr, dass etwa die Hälfte der Datenströme in Europa auf den Datenaustausch mit den USA zurückgeht.[4] Aber auch losgelöst von den USA als Zielland einer Datenübermittlung ist die Integration redaktioneller Inhalte, menschlichen Knowhows, technischer Komponenten sowie von prozeduraler Wertschöpfung vielschichtig und weitreichend:

- *Einbindung externer Inhalte:* Bestehende Prozesse und Ressourcen in Unternehmen werden lediglich ergänzt. Personenbezogene Daten spielen eine untergeordnete Rolle und sind allein Mittel zum Zweck der Verfügbarmachung. Entsprechende potenziell betroffene personenbezogene Daten gehen über organisationsbezogene Daten (digitale Identität innerhalb des Unternehmens, Kontaktdaten, Organisationszugehörigkeit, gewährte Rechte) kaum hinaus. *Beispiele: LinkedIn Learning; Einbindung von YouTube oder anderen Video-Playern auf der Unternehmens-Webseite.*

- *Einbindung technischer Komponenten:* Wenn und soweit erst die Einbindung der von Dritten (im Ausland) betriebenen technischen Komponenten und die damit potenziell verbundene Exposition personenbezogener Daten Unternehmensprozesse überhaupt erst ermöglicht, ist eine höhere Stufe der Integration erreicht. Damit geht ein entsprechender Verlust unmittelbarer Kontrolle einher. Die Relevanz für den Schutz personenbezogener Daten ist stark vom betroffenen Geschäftsprozess abhängig und kann dementsprechend stark ausgeprägt sein. Dennoch richtet sich in diesen Fällen die Auslagerung nicht auf die Arbeit mit personenbezogenen Daten, sondern allenfalls auf deren technische Verwaltung *Beispiele: Reiseplanungs- und Kostenabrechnungsapplikation, Daten- und Applikationshosting, Auslagerung von Infrastruktur und höheren Schichten der technischen Unternehmensarchitektur in die Cloud (IaaS, PaaS, Saas mit allen Abgrenzungsschwierigkeiten)*

- *(Teil-)Geschäftsprozess-Outsourcing:* Wo Prozesse ganz oder teilweise ausgelagert werden, wird insoweit zwar nicht die (rechtliche) Gesamtverantwortung, wohl aber ein entsprechendes Maß an operativer Verantwortung und damit Kontrolle externalisiert. Der damit verbundene Kontrollverlust umfasst gerade auch den Umgang mit personenbezogenen Daten auf der Ebene von Prozessen. Das gilt umso mehr, wenn und weil diese Prozesse auf Infrastruktur operationalisiert werden, die der rechtlich Verantwortliche nicht faktisch kontrollieren kann. Die so begründete Abhängigkeit und die Einwirkungsmöglichkeiten auf personenbezogene Daten und die Rechte und Freiheiten der Betroffenen legen das theoretisch höchste Risiko nahe und bedürfen sehr weitreichender Absicherung. *Beispiele: Auslagerung des Kundenservice, Auslagerung der Gehaltsabrechnung, Auslagerung des Reiseprozesses, Auslagerung von Logistik-Leistungen, Auslagerung des Betriebs der IT, 24/7 IT-Support, Server-Wartung.*

- *Datenübermittlung im Konzern:* Alle vorbenannten Facetten finden sich innerhalb von (internationalen) Konzernstrukturen auch von Unternehmen mit Sitz in Europa, insbesondere in Deutschland. Sie sind auf internationale Datenflüsse angewiesen, um interne technische Ressourcen in global skalierbarer Form verfügbar zu machen, einheitliche Prozesse zu unterhalten sowie Entwicklung, Betrieb und Wartung einer rationalen

[4] Vgl. *Weiß*, ZD 2020, 485.

Technologielandschaft abzusichern. Mit anderen Worten: Für international agierende Unternehmen mit Konzerngesellschaften oder Niederlassungen im Ausland sind internationale Datenflüsse Voraussetzung für ihre Existenz überhaupt. Über unternehmenseinheitliche Richtlinien und Verfahren sowie Kontroll- und Berichtssysteme lassen sich allerdings Risiken für personenbezogene Daten weit besser beherrschen als gegenüber Dritten. *Beispiele: Pooling von IT-Leistungen, Betrieb eines globalen Active Directory, Zentrale Personalverwaltung, Globales Intranet.*

3 Konzept einer am Übermittlungsrisiko orientierten Prüfung

3.1 Zusammenfassung

Das vorliegende Konzept erläutert die erforderliche Prüfsequenz einer Datenübermittlung und beschreibt auch die für diese Prüfung relevanten Komponenten inhaltlich. Im Wesentlichen identifiziert BITKOM dabei folgenden Komponenten:

- **Prüfung der Umstände de Datenübermittlung:** BITKOM hält es für erforderlich, zunächst die Charakteristik der Datenübermittlung unabhängig von dem betroffenen Drittland zu prüfen. Nach Maßgabe dieser Einzelumstände lassen sich nämlich Bedrohungen für die relevanten Schutzziele der DSGVO ableiten. Diese lassen sich anhand der Begründung des EuGH zum Schrems-II-Urteil auf die im Standard-Datenschutz-Modell[5] („SDM“) verankerten Gewährleistungsziele Transparenz, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit verdichten. Daraus lassen sich wiederum Risiken ableiten, die sich aus der Datenverarbeitung, genauer: aus der Datenübermittlung, als solcher ergeben. Denn mit einer Datenübermittlung geht die Aufgabe der faktischen Kontrolle über personenbezogene Daten einher. Der Umfang dieses Kontrollverlustes sowie die dadurch ausgelösten Bedrohungen für die Rechte und Freiheiten der Betroffenen bestehen aber nicht schlechthin, sondern in Abhängigkeit etwa von der technischen Ausprägung der Datenübermittlung und den betroffenen Daten selbst. Deshalb stehen die Ermittlung und Gewichtung dieser Einzelumstände am Startpunkt einer jeden Datenübermittlungsprüfung und fließen als Eingangsgröße in eine Gesamtprüfung ein.

- **Prüfung des Datenschutzniveaus im Drittland:** Nachdem der EuGH in seinem Urteil den Unternehmen […] eine Prüfung des Datenschutzniveaus im Drittland aufgegeben hat[6], hat BITKOM einen Katalog von Kriterien entwickelt, welche auf die relevanten Gewährleistungsziele des SDM zurückführbar sind und welche zwei privatrechtlich strukturierte Parteien im Rahmen der vertraglichen Gestaltung der Übermittlungsbeziehung nicht oder nur unvollständig adressieren können. In diesem Zusammenhang legt BITKOM Wert auf die Feststellung, dass in der Konstellation des Art. 46 DSGVO von Unternehmen nicht - und auch nicht ansatzweise - die Prüfungstiefe eines Angemessenheitsbeschlusses im Sinne von Art. 45 Abs. 2 DSVO erwartet werden kann. Denn einerseits ist dies die Aufgabe der Europäischen Kommission. Darüber hinaus ist das auch nicht erforderlich, weil mit dem Einsatz der Standardvertragsklauseln bereits ein Instrument Verwendung findet, welches gem. Art. 46 Abs. 2 lit. d) DSGVO aus normativen Gründen allein bereits ausreichen sollte, um das Datenschutzniveau zu gewährleisten. Insofern muss

[5] *Datenschutzkonferenz der unabhängien Datenschutzaufsichtsbehörden des Bundes und der Länder*, Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf Grundlage einheitlicher Gewährleistungsziele, Version. 2.0b vom 17. April 2020, abrufbar über https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/Standard-Datenschutzmodell.pdf;jsessionid=2BC564F660D1A026686B730CF3F54E50.1_cid344?__blob=publicationFile&v=2 (zuletzt abgerufen am 17.12.2020).
[6] Vgl. EugH, Schrems II-Urteil, Rn. 132.

sich die zusätzlich geforderte Prüftiefe in Grenzen halten und darf sich auch allein im Rahmen der vom EuGH problematisierten (massenhaften) behördlichen Zugriffe halten. Aus dieser Betrachtung heraus ist es unerlässlich die konkrete Verarbeitung und das damit einhergehender Risiko für die Betroffenen in die Gesamtbewertung einzubeziehen. Das insoweit evaluierte Datenschutzniveau wird in einem quantitativen oder qualitativen Wert zum Ausdruck gebracht und zu dem im ersten Prüfungsschritt identifizierten Übermittlungsrisiko in Beziehung gesetzt. Diese Beziehung gilt als hergestellt, wenn die im ersten Prüfungsschritt identifizierte Bedrohung für das Gewährleistungsziel nach SDM auf ein Defizit innerhalb der Regelungsprogramms des Ziellandes gerade im Hinblick auf dieses Gewährleistungsziel trifft.

- **Zusätzliche Maßnahmen**: Die Forderung nach zusätzlichen Maßnahmen ist leicht aufgestellt. Sinnvollerweise können solche Maßnahmen jedoch nur an konkrete Einzelumstände der Übermittlung anknüpfen, aus denen sich Bedrohungen für die Rechte und Freiheiten von Betroffenen[7] ergeben, wenn und soweit diese Umstände negativ auf identifizierte Bedrohungen für Gewährleistungsziele des SDM einzahlen. Korrekterweise ist der Anknüpfungspunkt nicht das Datenschutzniveau im Drittland, weil es nicht zur Disposition der Parteien steht. Zusätzliche, zwischen den Parteien zu vereinbarende Maßnahmen können prozeduraler, organisatorischer oder technischer Art sein und potenziell auf alle Aspekte des Übermittlungsrisikos wirken. Nicht in allen Szenarien müssen immer zusätzliche Maßnahmen erforderlich sein, ebenso wenig können in allen Fällen durch zusätzlichen Maßnahmen die Risiken für die Rechte und Freiheiten der Betroffenen ausreichend mitigiert werden.

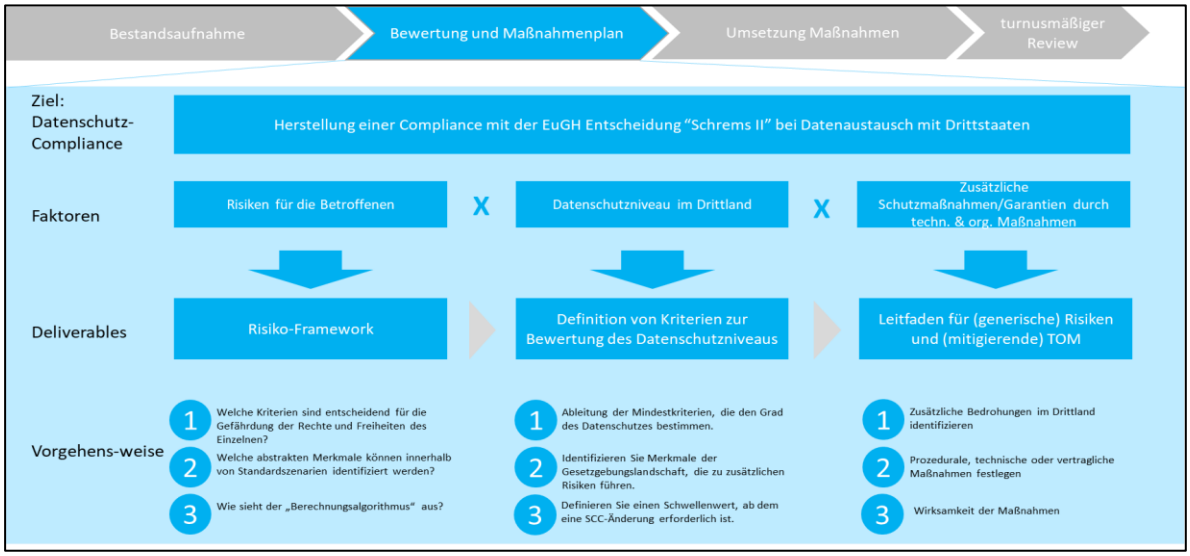

Abbildung 1: Risiko-Management-Prozess Datenübermittlung

[7] Vgl. auch Conseil d’Etat, Urt. v. 13.10.2020, Az. 444937, Rn. 11-14 (deutsche Übersetzung abrufbar unter https://datenrecht.ch/wp-content/uploads/444937-CNLL-et-autres-DE.pdf, zuletzt abgerufen am 15.12.2020), weshalb der Schwerpunkt der Prüfung eben nicht das Datenschutzniveau im Drittland ist, sondern die damit ggf. verbundenen oder vertieften Bedrohungen für Rechte und Freiheiten der Betroffenen.

- **Gesamtergebnis Datenübermittlungsrisiko:** Als Ergebnis der Prüfung steht das im Rahmen der Datenübermittlung geringstmögliche Risiko aus der Sicht des Betroffenen. Wenn und solange dieses „Netto- Risiko“ diesseits einer Akzeptanzschwelle liegt, kann die Datenübermittlung durchgeführt werden. BITKOM ist sich bewusst, dass es auch und gerade nach Maßgabe einer solchen Prüfung Datenverarbeitungen geben kann, die nicht oder nicht in der ursprünglich geplanten Form stattfinden können.

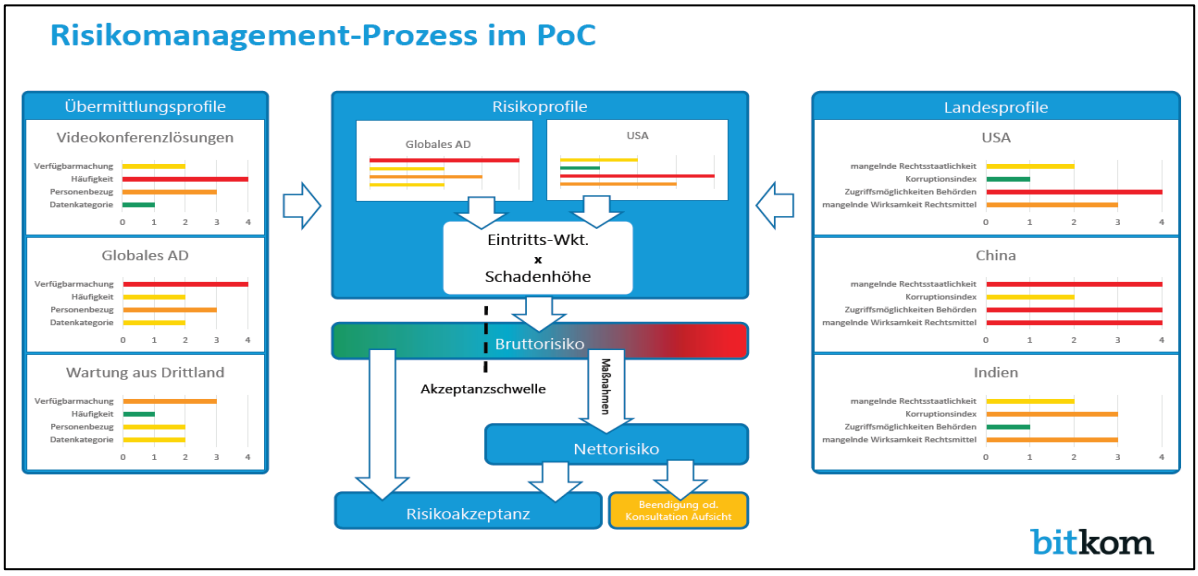

Abbildung 2: Komponenten des Datenübermittlungsrisikos

3.2 Rechtliche Würdigung

Selbstverständlich sind die durch das Schrems-II-Urteil formulierten Anforderungen zum Schutze der Rechte und Freiheiten des Betroffenen umzusetzen. Dieser Herausforderung stellt sich BITKOM mit dem hier vertretenen Konzept. Während in der öffentlichen Diskussion, auch von Seiten der Aufsichtsbehörden, allein das betroffene Drittland der Maßstab für die Notwendigkeit zusätzlicher Maßnahmen bis hin zur Änderung von Datenverarbeitungen zu sein scheint, setzt sich BITKOM für eine stärkere Fokussierung auf die individuellen Einzelaspekte der Datenverarbeitung ein (vgl. oben unter C.I.) und stützt die Berücksichtigung dieser Übermittlungsparameter neben dem Datenschutzniveau im Drittland auf nachfolgende rechtliche Gesichtspunkte:

- Zunächst muss in Rechnung gestellt werden, dass der hier vertretene Ansatz in Szenarien des Art. 46 DSGVO einschlägig ist, wo es an einem Angemessenheitsbeschluss der EU-Kommission nach Art. 45 Abs. 3 DSGVO gerade fehlt. Es kann daher unmöglich von Unternehmen erwartet werden, tiefste rechtliche und tatsächliche Ermittlungen anzustellen, die dann ggf. bei verschiedenen Unternehmen auch noch unterschiedlich ausfallen. Sofern Unternehmen darüber hinaus auf Standardvertragsklauseln in ihrer jeweils aktuellen Fassung setzen, ist zudem ein ganz wesentlicher Teil der Übermittlungsgrundlage gegeben. Je höher demgegenüber die Anforderungen an zusätzliche Maßnahmen sind, desto eher liegt darin ein Wertungswiderspruch zu Art. 46 Abs. 2 DSGVO, der ja gerade ausreichende vertragliche Garantien beinhaltet und ausreichen lässt. Insoweit BITKOM vor

diesem Hintergrund mehr Flexibilität bei der Bestimmung der Notwendigkeit weitergehender Maßnahmen einfordert, ist dies weit entfernt von einer Absage an das Datenschutzniveau der DSGVO.

- Der Wortlaut der DSGVO selbst lässt keinen Zweifel daran, dass die Entscheidung der Rechtmäßigkeit der Datenübermittlung in Drittstaaten gerade nach Maßgabe der für die Datenübermittlung relevanten Umstände des Einzelfalls zu treffen ist.

  - Der durch Art. 24 Abs. 1 S. 1, 32 Abs. 1, 2 sowie Art 35 sowie Art. 5 Abs. 1 DSGVO eingeführte Ansatz zur Berücksichtigung von Risiken für die Rechte und Freiheiten der Betroffenen erfordert die Ermittlung konkreter Umstände des Einzelfalls zur Ableitung von entsprechenden Bedrohungen. Zu diesen Umständen zählen u.a. grundsätzlich die Datenkategorien, die Zwecke, Mengengerüste, bestehende Schutzmaßnahmen, etc.[8] Mögen auch nicht alle Aspekte für das spezifisch mit der Tatsache der Übermittlung verbundene Risiko relevant sein, verdeutlicht dies doch die Vielzahl der Variablen, die einer Prüfung zugrunde zu legen sind.

  - Nach EG 108 ist die Verarbeitung (und damit die sie prägenden Einzelaspekte) für den angemessenen Schutz in den Mittelpunkt zu stellen und nicht (lediglich) die Drittlandproblematik. Zudem verdeutlicht EG 108, dass der Schutz *angemessen* sein muss, d.h. er gilt nicht absolut.[9]

  - Nachdem Art. 44 Abs. 1 1. HS DSGVO neben den spezifischen Normen de 5. Kapitels der DSGVO auch auf die übrigen Normen der DSGVO verweist, gelten Art. 24, 32, 35 und 5 DSGVO selbstverständlich auch im Bereich der Datenübermittlung. Eine Verkürzung der Betrachtung der Datenübermittlung auf das Element des Drittlands ist demgegenüber nicht ersichtlich.

  - Art. 46 DSGVO nimmt Bezug auf „geeignete“ Garantien, sofern es an einem Angemessenheitsbeschluss fehlt. Das Kriterium der „Geeignet“ ist der Wertung und damit der Anwendung im Einzelfall zugänglich. Maßstab der Geeignetheit ist der Schutz der betroffenen Person.[10] Um den Schutzbedarf für die betroffene Person im Kontext einer internationalen Datenübermittlung zu bestimmen und ggf. angemessene Maßnahmen abzuleiten, Art. 5 Abs. 1 lit. f) DSGVO, muss das für die Betroffenen bestehende Risiko zunächst ermittelt werden. Andernfalls kann über deren Wirksamkeit keinerlei valide Aussage getroffen werden. Insofern muss die Beurteilung einer Datenübermittlung ins Drittland nach Art. 44 ff. DSGVO ebenfalls das Konzept der Berücksichtigung der Einzelaspekte einer Datenübermittlung zugrunde legen.

- Nach Maßgabe der vorliegenden Entwurfsfassung vom 13.11.2020 zur Implementierung neuer Standard-Datenschutzklauseln der Europäischen Kommission sieht es auch die Europäische Kommission als erforderlich an, dass Datenimporteur und Datenexporteur die *Einzelumstände* einer Datenübermittlung in Betracht ziehen, um das erforderliche Datenschutzniveau im Drittland zu gewährleisten. So verweist das Dokument in EG 20 aber auch in den Standardvertragsklauseln selbst unter Klausel 2 (b) (i) in einem nicht abschließenden Katalog auf die Notwendigkeit der Prüfung von Parametern wie etwa der Datenkategorien oder der Kategorien von Empfängern. Eine solche Einzelfallprüfung ist aber nur sinnvoll, wenn und soweit sie einen Einfluss auf zusätzliche Maßnahmen

[8] Vgl. EG 75 DSGVO.
[9] Vgl. zur Relevanz des EG 108 auch EuGH, Schrems II-Urteil, Rn. 95, 131.
[10] Vgl. EG 108 S. 1 DSGVO.

hat. Davon ist jedenfalls dann auszugehen, wenn die Ausprägung solcher Variablen Schadenshöhe oder die Eintrittswahrscheinlichkeit eines Risikos bestimmen.

- Auch nach Äußerungen des Europäische Datenschutzausschuss („EDSA“) kommt es nicht allgemein oder gar allein auf das Datenschutzniveau im Drittland an, sondern es ist nach Maßgabe der Einzelheiten der Datenübermittlung zu differenzieren.

  - So stellt der EDSA etwa auf die Rollen der an der Datenübermittlung Beteiligten ab und diskutiert erforderliche technische Maßnahmen in Abhängigkeit zur Anwendbarkeit spezifischer, Zugriff einräumender Rechtsakte, etwa Section 702 FISA. Nur wenn und soweit der jeweilige Importeur oder weitere Empfänger in den USA überhaupt in dessen Anwendungsbereich fallen, kommt der EDSA zu dem Schluss, dass ein behördlicher Zugriff durch technische Maßnahmen vollständig ausgeschlossen oder wirkungslos gemacht werden müsse.[11] Insofern muss die Eigenschaft des Empfängers als ein Parameter (von mehreren) Eingang in die Prüfung finden können.

  - Sogar für den Fall der Anwendbarkeit bestimmter Rechtsnormen, die den Zugriff ermöglichen, fragt der EDSA nach dem jeweiligen Risiko, insbesondere nach der (konkreten) Wahrscheinlichkeit eines behördlichen Zugriffs. Damit ist bereits auf der Ebene anwendbarer Rechtsnormen keine pauschale Betrachtung ausreichend, sondern der Weg zu einer differenzierten Prüfung eröffnet.[12]

  - Außerdem verweist der der EDSA darauf, dass zusätzliche Maßnahmen zum Datenschutz und zur Datensicherheit risikobasiert zu treffen sind: So verweist er in Bezug auf die Anwendung spezifischer Sicherheitsanforderungen auf Risiken, die für *übermittelte Kategorien personenbezogener Daten* bestehen.[13] Die Notwendigkeit der Prüfung eben dieser Details steht auch für BITKOM im Vordergrund.

  - Schließlich ziehen sich Hinweise auf die Berücksichtigung der konkreten Umstände der einzelnen Übermittlung durch die gesamte Stellungnahme des EDSA.[14] Insofern kann man nur schlussfolgern, dass es sich insoweit um ein die Stellungnahme tragendes Konzept handelt.

- Auch die in Art. 7 und 8 EU GRCh geschützten Rechte auf Privatsphäre und Datenschutz stehen eiern differenzierenden Betrachtung nicht entgegen. Denn beide gelten nicht schlechthin und uneingeschränkt. Vielmehr unterliegen sie grundrechtsimmanenten bzw. gesetzlichen Schranken, welche eine genauere Betrachtung der Einzelumstände der Datenübermittlung zulassen und auch erfordern:

  - Das Recht auf Privatsphäre endet an der Grenze ihres Schutzbereichs. Insoweit hat das Bundesverfassungsgericht in seiner Entscheidung zu heimlichen Tonbandaufnahmen[15] nach Maßgabe der von ihm entwickelten *Sphärentheorie* zum Recht auf informationelle Selbstbestimmung nach verschiedenen Graden der persönlichen Betroffenheit differenziert, namentlich nach Intim-, Privat- und Sozialsphäre.[16] Es gelten insoweit differenzierende Rechtfertigungsbedürfnisse bzw. Duldungspflichten. Nachdem Art. 7 EU GRCh sogar

[11] EDSA, Empfehlung 1/2020, Rn. 44.
[12] EDSA, Empfehlung 1/2020, Rn. 135.
[13] EDSA, Empfehlung 1/2020, Rn. 135.
[14] EDSA, Empfehlung 1/2020, Rn. 77. 93, 97, 122.
[15] BVerfGE 34, 238 ff.
[16] Vgl. BVerfGE 34, 238 (245).

ausdrücklich die Privatsphäre, die Wohnung, das Familienleben und die (private) Kommunikation als Schutzgüter nennt, ist die Sphärentheorie gewissermaßen schon auf Ebene des Grundrechts verankert. Auf der Grundlage von Art. 7 EU GRCh besteht demnach außerhalb seines ausdrücklichen Schutzbereichs kein bzw. ein geringer Schutzbedarf. Demnach muss der Kontext der personenbezogenen Daten zunächst ermittelt und (vor dem Hintergrund von Art. 7 EU GRCh) gewichtet werden. Das hat mit dem Drittland zunächst gar nichts zu tun.

- Das Recht auf Schutz personenbezogener Datenschutz aus Art. 8 EU GRCh gewährleistet das Institut des Datenschutzes als Gegenstand sekundärrechtlicher Rechtssetzung auf EU-Ebene.[17] Sein Schutzbereich ist demnach nicht abschließend bestimmt, sondern das Recht verweist insoweit auf die es ausgestaltenden Regelungen, Art. 8 Abs. 2 EU GRCh. Diese Regelungen erfüllen das in Art. 8 EU GRCh genannte Recht mit Leben und bringen es mit anderen Grundfreiheiten in Einklang.[18] Insofern ist die Ermittlung eines etwa bestehenden Schutzbedarfs für personenbezogene Daten unter Berücksichtigung der Einzelumstände ihrer Übermittlung keine Frage des Konflikts mit Art. 8 EU GRCh, sondern ist allein am Maßstab der DSGVO zu messen.[19]

- Schließlich legt auch der EuGH selbst nach dem Schrems II-Urteil eine individuelle Prüfung des Einzelfalls nahe[20].

  - So sollen Aufsichtsbehörden auch im Angesicht von vereinbarten Standardvertragsklauseln Datenübermittlungen im Einzelfall „im Lichte aller Umstände der Übermittlung“ prüfen, ob „der nach dem Unionsrecht erforderliche Schutz“ gewährleistet werden kann[21] und solche Übermittlungen ggf. unter Anwendung von Art. 58 Abs. 2 lit. f) DSGVO aussetzen oder verbieten. Bemerkenswert ist das vor allem deshalb, weil der EuGH – in Ergänzung zum Wortlaut des Art. 58 Abs. 2 lit. f) DSGVO – ausdrücklich alle Umstände der Übermittlung für relevant hält.[22]

  - Den gleichen Prüfungsmaßstab wie für Aufsichtsbehörden erlegt der EUGH auch den Unternehmen selbst auf.[23]

  - Zusammenfassen lässt sich festhalten, dass auch nach Auffassung des EuGH die Variablen der Verarbeitung bzw. Übermittlung zu prüfen und zu gewichten sind, um den sich hieraus und vor dem Hintergrund der Situation im Drittland zusätzlich ergebenden Schutzbedarf zu ermitteln und hieran anknüpfende zusätzliche Maßnahmen abzuleiten.

Nach allem ist eine differenzierte Betrachtung der (Übermittlungs-)Umstände im Einzelfall nicht nur gestattet und sinnvoll, sondern auch geboten. Die Berücksichtigung der individuellen Parameter der Datenübermittlung ist ein wesentlicher Bestandteil des von BITKOM vorgeschlagenen Risikobehandlungsprozesses für (internationale) Datenübermittlungen.

[17] *Buchholtz/Stenzel*, in: Gierschmann u.a., DSGVO Komm., Art. 1 Rn. 32.
[18] Vgl. EG 4 S. 2 DSGVO.
[19] Und die DSGVO gewährt keinen absoluten, sondern lediglich angemssenen Schutz im Lichte der Verarbeitung, EG 108.
[20] Vgl. insoweit auch auch oben Fn. 5.
[21] EuGH, Schrems II-Urteil, Rn. 146.
[22] Vgl. EuGH, Schrems II-Urteil, Rn. 146.
[23] EuGH, Schrems II-Urteil, Rn. 132.

3.3 Modellierung der Risiko-Bewertung

Phase 1 – Risikoermittlung

1. Benennung eines Lebenssachverhalts (Szenario)
2. Identifikation eines Risikos in dem Szenario (Referenz: Datenschutzgrundsätze)
3. Benennung einer Risiko-Quelle (Wiederkehrend/standardisierbar für Zwecke dieses Konzepts)
4. Beschreibung einer Bedrohung (Wiederkehrend/standardisierbar für Zwecke dieses Konzepts)

Phase 2 - Schadensermittlung

1. Beschreibung potenzieller tatsächlicher Schäden
2. Zuordnung von Schadenskategorien (standardisierbar nach Maßgabe von EG 75 DSGVO)
3. Benennung der Eintrittswahrscheinlichkeit (nach Maßgabe von ISO/IEC 29134 standardisierbar)
4. Bezifferung einer Schadenshöhe (standardisierbar nach Maßgabe BITKOM Leitfaden Bitkom-Leitfaden, „Risk Assessment & Datenschutz-Folgenabschätzung“, S. 50 ff.)

Phase 3 - Risikobewertung

1. Verrechnung von Schadenshöhe und Eintrittswahrscheinlichkeit („reine“ Rechenarbeit)
2. Abbildung des Risikos auf einer Heat-Map zur Ermittlung der Risiko-Toleranz (entspricht der Akzeptanzschwelle; ggf. mit Aufsichtsbehörden abzustimmen)

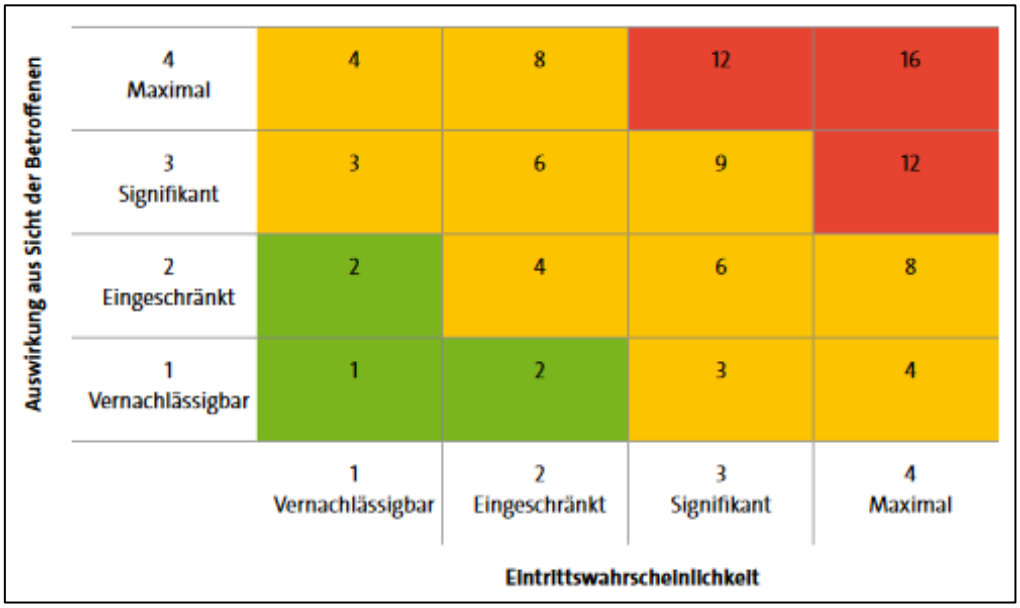

Abbildung 3: Visualisierung des Übermittlungsrisikos

3.4 Modellierung der Datenschutzniveaus im Drittland

Die Betrachtung des Datenschutzniveaus im Drittland muss sich immer in einem für das Unternehmen vertretbaren und leistbaren Rahmen bewegen. Die Anforderungen an eine solche Prüfung darf auch nicht zu Wettbewerbsverzerrungen zwischen großen Unternehmen mit eigener Rechtsabteilung und kleinen und mittelständischen Unternehmen führen, die nicht über die notwendigen Mittel für eine tiefgehende Prüfung verfügen. Daher ist es umso wichtiger, dass eine Bewertung nach klaren Kriterien erfolgt und zu einem Landes-Risiko-Profil zusammengestellt werden. Für jedes Land werden dabei sowohl Bedrohungen, die sich aus behördlichen Zugriffen auf Daten für den Betroffenen ergeben können (bspw. Diskriminierung, Einreiseverbote, politische Verfolgung) betrachtet, als auch Eintrittswahrscheinlichkeiten aufgrund der gesetzlich vorgesehenen Hürden für Zugriffe auf solche Daten.

3.5 Auswahl und Steuerung von zusätzlichen Maßnahmen

Die Auswahl von Maßnahmen zur Mitigation der ermittelten Risiken stellt im Weiteren eine wichtige Grundlage für die Zulässigkeit der Übermittlung im Endergebnis dar. Liegt basierend auf den Rahmenbedingungen der Übermittlung („Übermittlungsprofil“ und „Landesprofil“) das Risiko („Brutto-Risiko“) über der Risikoakzeptanzschwelle, gilt eine Übermittlung in das Drittland ohne zusätzliche Schutzmaßnahmen als nicht vertretbar und kann somit von den Aufsichtsbehörden untersagt werden.

Etwa identifizierte und durch die Rechtslage im Drittland gegebenenfalls verstärkte Bedrohungen für Gewährleistungsziele nach SDM steuern erforderliche zusätzliche Maßnahmen, die im Ergebnis zugunsten der Rechte und Freiheiten der Betroffenen wirken. Bei der Auswahl der Maßnahmen sollte bereits darauf geachtet werden, dass die jeweilige Maßnahme auch auf Aspekte der Eintrittswahrscheinlichkeit oder des Schadenspotentials aus der Perspektive des Betroffenen wirkt und insoweit das Risiko positiv verändert. Unter Berücksichtigung der entsprechenden Maßnahmen („Risikobehandlung“) muss das Risiko erneut bewertet werden („Netto-Risiko“). Nur wenn das Netto-Risiko unter der Risiko-Akzeptanzschwelle liegt und damit voraussichtlich nicht zu einem inakzeptablen Risiko für die Rechte und Freiheiten natürlicher Personen führt, kann von einem angemessenen Schutzniveau bei der Datenübermittlung in das Drittland ausgegangen werden. Insofern ist darauf hinzuweisen, dass – anders als im Unternehmensrisiko-Management – eine Risikoakzeptanz jenseits der Akzeptanzschwelle ausgeschlossen ist. Die Akzeptanzschwelle muss sich dabei nach den allgemeinen Maßstäben im Datenschutz richten und darf objektiv gesehen unter dem Niveau eines hohen Risikos liegen.

Der Datenexporteur sollte auf eine angemessene und nachvollziehbare Dokumentation der getroffenen Annahmen und Entscheidungen achten, um den Anforderungen an die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO gerecht zu werden.

4 Ausblick

4.1 Datenschutz-Schutzprofile als Referenz-Profile

Zunächst treffen die nach Maßgabe des unter C.III. bis C.V. beschriebenen Prozesses individuell erstellten Datenschutz-Schutzprofile eine Aussage über das jeweils zugrunde liegende Szenario. Sie können aber über den konkret beschriebenen Sachverhalt hinaus als Referenz für die Bewertung anderer Sachverhalte dienen. Damit wird durch die Erstellung einzelner Datenschutz-Schutzprofile bereits ein gewisses Maß an Skalierbarkeit erreicht. Die Skalierbarkeit ist desto höher, je mehr Datenschutz-Schutzprofile erstellt werden. Denn nachdem immer entscheidend sein wird, ob andere Sachverhalte im Hinblick auf ihre datenschutzrechtliche Relevanz durch dieselbe Ausprägung der datenschutzrechtlich relevanten Variablen gekennzeichnet sind, entsteht mit einer größeren Zahl von Datenschutz-Schutzprofilen eine exponentiell wachsende Zahl an Referenz-Konstellationen.

4.2 Schutzprofile vs. Parametrisierung

Das weitergehende Ziel der Aktivitäten von BITKOM im Zusammenhang mit internationalen Datenübermittlungen ist die Entwicklung eines technischen Verfahrens zur standardisierten und automatisierten Prüfung von Datenübermittlungen („das Produkt“). Denn die Integrationstiefe von technischen Komponenten und Services Dritter in den Geschäftsprozessen der Mitgliedsunternehmen bedingt neben dem Standardisierungserfordernis auch das Kriterium eines schnellen und auch für Nicht-Juristen oder Datenschutzexperten umsetzbaren Prüf-Protokolls. Das Produkt soll Unternehmen auf der Grundlage des hier dokumentierten Vorgehens zu rechtlich vertretbaren Prüfergebnissen sowie Handlungsanweisungen führen. Gemeinsam mit der entsprechend weiterzuführenden Dokumentation für das Produkt sowie den bei individuellen Prüfungen entstehenden Datensätzen kommen die Unternehmen zudem ihren Rechenschaftspflichten aus Art. 5 Abs. 2 DSGVO nach.

Der von BITKOM eingeschlagene Weg basiert auf der Erkenntnis, dass die für das Übermittlungsrisiko relevanten Variablen aber auch deren Ausprägungen nicht unendlich umfangreich bzw. verschieden sind. Deshalb lässt sich die Prüfung auch weitgehend von konkreten, einem Datenschutz-Schutzprofil zugrundeliegenden Szenarien entkoppeln. Stattdessen kann die Prüfung vollständig parametrisiert erfolgen. Dabei werden alle Einzelkomponenten in Variablen abgebildet, die wiederum durch eine Anzahl vordefinierter Werte ausgeprägt sein können. Die Variablen werden (nach ggf. unterschiedlicher Gewichtung) miteinander technisch verknüpft, wo logische Abhängigkeiten bestehen. Das gilt für die Elemente des Übermittlungsrisikos ebenso wie für die in Betracht kommenden zusätzlichen Maßnahmen. *Beispiele: Verknüpfung von Datenübermittlungsparametern, um Aussagen über Schadenshöhe oder Eintrittswahrscheinlichkeiten zu treffen, Verknüpfung von Maßnahmen mit einem Werte oder mehreren Werten einer oder mehrerer Übermittlungsvariablen, um die 1:n-Beziehung zwischen Maßnahmen und Risikovariablen zu fixieren.*

BITKOM ist sich der Herausforderung bewusst, dass die Parameter nicht nur initial vollständig sein müssen, um die Risiken ausreichend und umfassend abzubilden. Vielmehr ist es auch erforderlich, die jeweiligen Einträge im Hinblick auf jeweilige die aktuelle Sach- und Rechtslage aktuell zu halten. Zudem müssen die Komponenten des Prüfschemas flexibel und anpassbar sein. BITKOM ist von der Notwendigkeit und Sinnhaftigkeit einer solchen Herangehensweise überzeugt und treibt diese Entwicklung deshalb weiter voran.

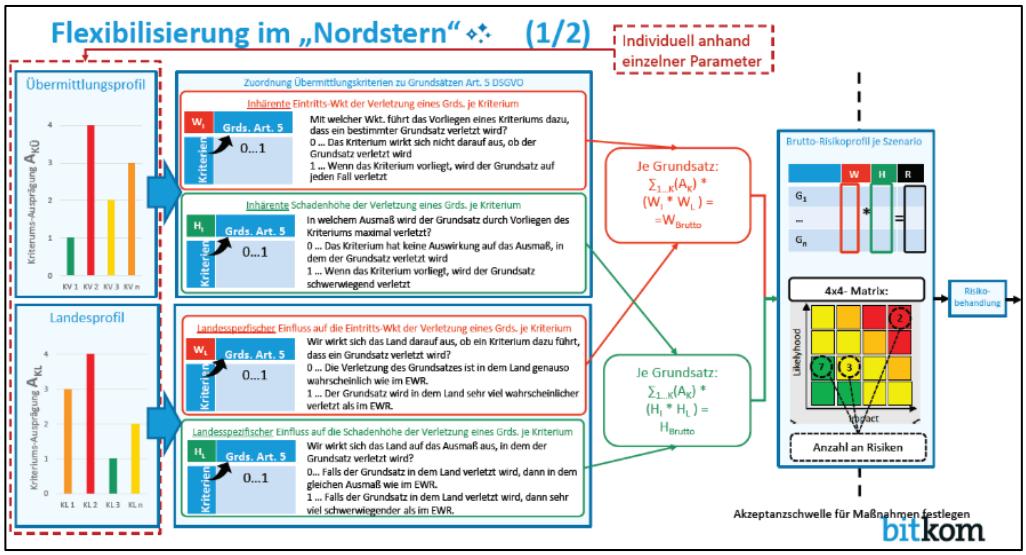

Abbildung 4: Parametrisierung von Übermittlungs- und Drittlandkomponente

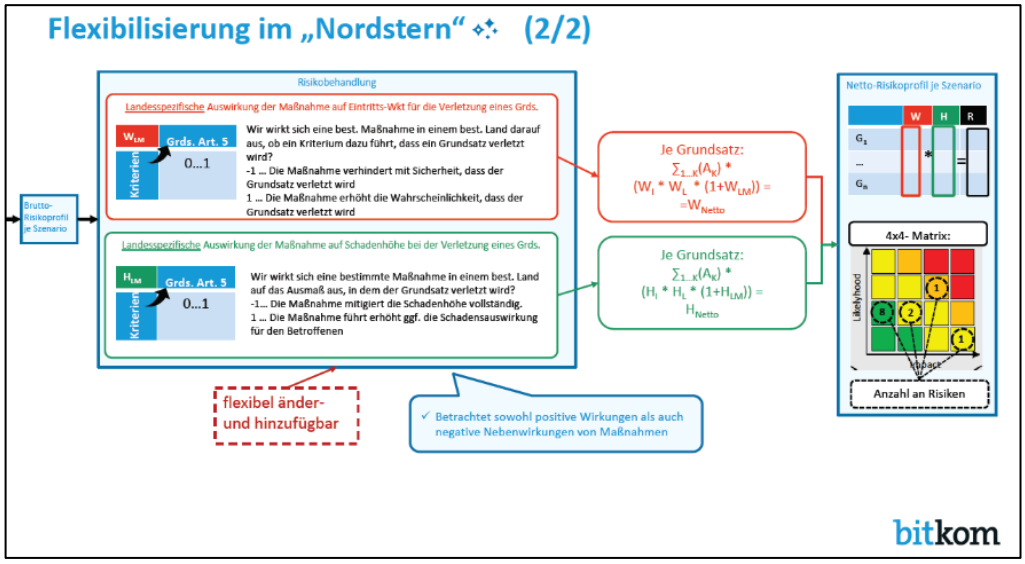

Abbildung 5: Überführung in „klassische“ Komponenten der Risikobewertung