TIM WYBITUL / LUKAS STRÖBEL / MARIAN RUEß

Übermittlung personenbezogener Daten in Drittländer

Überblick und Checkliste für die Prüfung nach der DS-GVO

Datentransfer
Grenzüberschreitende Datenverarbeitung
Standarddatenschutzklauseln
BCRs

■ Die grenzüberschreitende Übermittlung von Daten ohne vorherige rechtliche Prüfung, ist bereits jetzt nach dem noch bis zum 24.5.2018 geltenden BDSG erheblichen Risiken ausgesetzt. Die Einführung der EU-Datenschutzgrundverordnung (DS-GVO) sowie des gleichzeitig in Kraft tretenden neuen BDSG (BDSG 2018) stellt Praktiker vor neue Herausforderungen. Die DS-GVO vereinfacht zwar den Datenaustausch innerhalb der EU, indem sie einheitliche Mindestschutzanforderungen aufstellt. Für Datenübermittlungen in Drittländer stellen sich dagegen wichtige Fragen. Der folgende Beitrag beschreibt die ab dem 18.5.2018 geltenden Voraussetzungen für eine solche Datenübermittlung in Drittländer. Zudem zeigt er Lösungsansätze auf und gibt pragmatische Handlungsempfehlungen. Der Beitrag enthält auch Checklisten für die Prüfung der Zulässigkeit der Übermittlung personenbezogener Daten in Drittländer nach der DS-GVO.
Lesedauer: 26 Minuten

■ The cross-border transfer of data without prior legal review is already exposed to substantial risks based on the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), which is still valid until 24 May 2018. The introduction of the EU General Data Protection Regulation (GDPR/DS-GVO), as well as the new BDSG (BDSG 2018), which will then come into effect at the same time, presents new challenges for practitioners. Indeed, the GDPR simplifies the transfer of data within the EU by establishing a uniform minimum protection requirement. However, important questions arise for data transfers into third countries. The following article describes the requirements valid as of 18 May 2018 for such a data transfer into third countries. Furthermore, it depicts approaches to a solution and provides pragmatic guidance. The article also contains checklists to review the permissibility of the transfer of personal data into third countries pursuant to the GDPR.

I. Einleitung

Die grenzüberschreitende Übermittlung und sonstige Verarbeitung[1] personenbezogener Daten[2] ist in der heutigen technisierten Arbeitswelt unerlässlich. Datentransfers sind für den internationalen Handel und die internationale Zusammenarbeit zwischen Unternehmen entscheidend.[3] Um solche Datenübermittlungen in Staaten außerhalb der EU (sog. Drittländer)[4] rechtmäßig zu gestalten, müssen Unternehmen auch künftig rechtliche Anforderungen umsetzen. Der vorliegende Überblick gibt praktische Hilfestellungen zur Rechtslage nach der ab dem 25.5.2018 europaweit unmittelbar geltenden EU-Datenschutzgrundverordnung (DS-GVO). Er stellt die datenschutzrechtliche Zulässigkeit und die Voraussetzungen der Übermittlung von personenbezogenen Daten in Drittländer dar.

II. Anwendungsbereich der DS-GVO

Der folgende Abschnitt beschreibt in knapper und auf die Unternehmenspraxis zugeschnittener Form, welche Datenübermittlungen in den Anwendungsbereich der DS-GVO fallen.

1. Sachlicher Anwendungsbereich der DS-GVO

Die Verordnung[5] gilt in sachlicher Hinsicht für die automatisierte Verarbeitung[6] personenbezogener Daten.[7] Hierbei ist es unerheblich, ob die Verarbeitung vollständig oder nur teilweise automatisiert stattfindet.[8] Zudem findet die Verordnung auf die nicht-automatisierte Verarbeitung von personenbezogenen Daten Anwendung, die bereits in einer Datei gespeichert sind oder noch gespeichert werden sollen.[9] Die Anwendung der DS-GVO auf die nicht-automatisierte Verarbeitung personenbezogener Daten kann etwa Notizen oder Informationen aus Beobachtungen betreffen. Auch wenn solche Daten erst später automatisiert verarbeitet werden sollen, gilt die DS-GVO bereits ab der Erhebung der Daten.

2. Räumlicher Anwendungsbereich

In räumlicher Hinsicht ist die DS-GVO anwendbar, wenn eine Datenverarbeitung i.R.d. Tätigkeit einer Niederlassung des Verantwortlichen[10] oder des Auftragsverarbeiters[11] in der EU erfolgt (sog. Niederlassungsprinzip).[12] Die DS-GVO kann über die EU hinaus auch extraterritorial gelten, wenn ausländische Verantwortliche oder Auftragsverarbeiter personenbezogene Da-

1 Vgl. Art. 4 Nr. 23 DS-GVO.
2 Vgl. Art. 4 Nr. 1 DS-GVO.
3 Vgl. Erwägungsgrund 101 Satz 1 DS-GVO.
4 Die EWR-Staaten (Island, Lichtenstein und Norwegen) gehören entgegen verbreiteter Ansicht zunächst auch zu den Drittländern i.S.d. DS-GVO. Dies würde sich erst ändern, sofern sie die Anwendung der DS-GVO verbindlich beschließen sollten; vgl. *Pauly*, in: Paal/Pauly, DS-GVO, 1. Aufl. 2017, Vorb. Art. 44 Rdnr. 3; im Verhältnis zu Altverträgen vgl. *Franck*, ZD 2017, 509 – in diesem Heft.
5 Soweit in diesem Überblick von „Verordnung" die Rede ist, ist damit die DS-GVO gemeint.
6 Vgl. Art. 4 Nr. 2 DS-GVO.
7 Vgl. Art. 2 Abs. 1 DS-GVO.
8 Vgl. Erwägungsgrund 15 DS-GVO.
9 Vgl. Art. 2 Abs. 1 DS-GVO a.E. Zu den Ausnahmen vom weiten Anwendungsbereich vgl. *Wybitul*, Hdb. DSGVO, 1. Aufl. 2017, Einl. Rdnr. 23. Für den Beschäftigtendatenschutz soll gem. § 26 Abs. 7 BDSG 2018 der Anwendungsbereich auch auf Datenverarbeitungen ausgedehnt werden, bei denen die Daten nicht in einem Dateisystem gespeichert werden oder gespeichert werden sollen. Somit sind künftig voraussichtlich auch Interviews mit Mitarbeitern i.R.v. internen Untersuchungen vom Beschäftigtendatenschutz erfasst; vgl. zum neuen Beschäftigtendatenschutz *Wybitul*, NZA 2017, 413 ff.
10 Verantwortlicher ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet; vgl. Art. 4 Nr. 7 DS-GVO. Der Verantwortliche ist primärer Normadressat der DS-GVO.
11 Auftragsverarbeiter ist, wer personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, vgl. Art. 4 Nr. 8 DS-GVO.
12 Vgl. Art. 3 Abs. 1 DS-GVO.

ten von in der EU ansässigen Personen verarbeiten (sog. Marktortprinzip).[13] Dies setzt voraus, dass diese Unternehmen betroffenen Personen in der Union Waren oder Dienstleistungen anbieten oder das Verhalten betroffener Personen in der EU beobachten. Das mit der DS-GVO eingeführte Marktortprinzip stellt die Praxis künftig vor neue Herausforderungen. Denn die hohen Anforderungen der DS-GVO können künftig auch für Unternehmen ohne eigene Niederlassung in der EU gelten.[14]

III. Voraussetzungen einer Übermittlung personenbezogener Daten an Empfänger in Drittländern

Um festzustellen, ob eine Übermittlung personenbezogener Daten an Empfänger[15] in Drittländern außerhalb der EU nach der DS-GVO zulässig ist, müssen Unternehmen eine zweistufige Zulässigkeitsprüfung vornehmen.[16]

Auf der ersten Stufe dieser Prüfung muss der Verantwortliche (also das Unternehmen) sicherstellen, dass die geplante Übermittlung grundsätzlich den allgemeinen materiell-rechtlichen Anforderungen der DS-GVO entspricht.[17] Erst wenn diese Voraussetzungen erfüllt sind, prüft der Verantwortliche in einer zweiten Stufe die besonderen Voraussetzungen für die Übermittlung von personenbezogenen Daten in Drittländer.[18]

1. Erste Prüfungsstufe: Übermittlung an einen Dritten

Art. 6 Abs. 1 Satz 1 DS-GVO sieht zunächst ein sog. grundsätzliches Verbot mit Erlaubnisvorbehalt vor.[19] Von diesem Verbot ist zunächst jede Verarbeitung (und damit auch jede Übermittlung)[20] personenbezogener Daten betroffen.[21] Übermittelt ein Unternehmen personenbezogene Daten an Dritte, muss es sich daher zunächst auf einen der Rechtfertigungstatbestände der DS-GVO berufen können. Neben der Einwilligung[22] der betroffenen Person gibt es etwa in den Art. 6 und 9 DS-GVO weitere Erlaubnistatbestände. Diese Erlaubnistatbestände sehen grundsätzlich eine Interessenabwägung vor.[23] Dabei muss der Verantwortliche die von ihm mit der Verarbeitung verfolgten Zwecke mit den berechtigten Interessen der betroffenen Person abwägen.[24]

Darüber hinaus können andere Rechtsvorschriften die Übermittlung oder sonstige Verarbeitung personenbezogener Daten rechtfertigen, etwa nach Art. 88 DS-GVO i.V.m. § 26 BDSG 2018[25] bei der Verarbeitung personenbezogener Daten im Beschäftigungskontext.[26] Als eine solche Rechtsgrundlage kommt z.B. auch eine Betriebsvereinbarung in Betracht.[27] Wie bei jeder Datenverarbeitung muss der Verantwortliche auch bei Datenübermittlungen an Empfänger in Drittländern zunächst im Einzelfall prüfen, ob die Übermittlung auf einer ersten Stufe grundsätzlich von einem Erlaubnistatbestand gedeckt ist.[28]

Checkliste: Übermittlung personenbezogener Daten an einen Dritten – Prüfungsstufe 1

1. Anwendbarkeit der DS-GVO
2. Übermittlung personenbezogener Daten an einen Dritten
   - Einwilligung
   - Gesetzlicher Erlaubnistatbestand
   - Sonstiger Erlaubnistatbestand (z.B. Betriebsvereinbarung)

Die Checkliste stellt kurz dar, welche Anforderungen Verantwortliche auf der Stufe 1 zur datenschutzrechtlichen Rechtmäßigkeit der Übermittlung personenbezogener Daten an einen Dritten prüfen müssen.

2. Zweite Prüfungsstufe: Spezifische Anforderungen für die Übermittlung in Drittländer

Sind die beschriebenen allgemeinen datenschutzrechtlichen Voraussetzungen (s.u. III.1.) für eine Datenverarbeitung erfüllt, prüft der Verantwortliche auf der zweiten Stufe die spezifischen Anforderungen für die Übermittlung personenbezogener Daten in Drittländer.[29] Diese spezifischen Anforderungen ergeben sich aus den Art. 44 ff. DS-GVO.

Grundsätzlich dürfen personenbezogene Daten nur dann an Empfänger bzw. Verantwortliche in Drittländern übermittelt werden, wenn das Daten übermittelnde Unternehmen dabei sämtliche Vorgaben des 5. Kapitels der DS-GVO einhält.[30] Diese Vorgaben dienen insbesondere dazu, die Interessen der von der Datenübermittlung betroffenen Personen zu schützen.[31]

Art. 45 DS-GVO regelt die Grundsätze zur grenzüberschreitenden Datenübermittlung auf der Grundlage eines sog. Angemessenheitsbeschlusses der *EU-Kommission*.[32] Die Voraussetzungen eines solchen Angemessenheitsbeschlusses werden nachstehend näher dargestellt. Eine weitere Möglichkeit zur zulässigen grenzüberschreitenden Datenübermittlung bietet Art. 46 DS-GVO, der die Datenübermittlung vorbehaltlich geeigneter Garantien regelt. Art. 47 DS-GVO führt weitere Einzelheiten zu diesen geeigneten Garantien, die verbindlichen internen Datenschutzvorschriften (sog. Binding Corporate Rules – BCRs), näher aus.

a) Angemessenheitsbeschluss der EU-Kommission

Die grenzüberschreitende Übermittlung von Daten an Empfänger in Drittländern kann insbesondere dann zulässig sein, wenn die *EU-Kommission* i.R.e. entsprechenden Beschlusses festge-

13 Vgl. Art. 3 Abs. 2 DS-GVO.
14 S.a. *Albrecht*, CR 2016, 88, 90.
15 Vgl. zur Definition des Begriffs „Empfänger" Art. 4 Nr. 9 DS-GVO.
16 Vgl. *Preuß*, Die Kontrolle von E-mails und sonstigen elektronischen Dokumenten im Rahmen unternehmensinterner Ermittlungen, 2016, S. 464; *Deutlmoser/Filip*, ZD-Beil. 6/2012, 1, 6.
17 Dies umfasst auch die Pflicht, dass die Verarbeitung nach den Grundsätzen der DS-GVO aus Art. 5 DS-GVO stattzufinden hat, vgl. *Ambrock/Karg,* ZD 2017, 154, 155 f.
18 Vgl. dazu *Auer-Reinsdorff/Conrad*, Hdb. IT- und Datenschutzrecht, 2. Aufl. 2016, § 35 Rdnr. 35, 94.
19 Vgl. auch das in Art. 5 Abs. 1 lit. a DS-GVO geregelte Rechtmäßigkeitsprinzip der Verordnung; ebenso *Buchner/Petri*, in: Kühling/Buchner, DS-GVO, 1. Aufl. 2017, Art. 6 Rdnr. 11 ff.
20 Vgl. Art. 4 Nr. 2 DS-GVO.
21 Auch unter der Geltung der DS-GVO gibt es kein ausdrücklich normiertes sog. „Konzernprivileg". Zwar wird in Erwägungsgrund 48 DS-GVO ausgeführt, dass „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Unternehmen sind, ein berechtigtes Interesse an der Datenübermittlung haben können". Allerdings bleiben lt. Erwägungsgrund 48 DS-GVO die Grundprinzipien unberührt, sodass insb. ein Erlaubnistatbestand erfüllt sein muss; vgl. m.w.Nw. *Kort,* ZD 2016, 555, 558 sowie *Lachenmann,* DSRITB 2016, 535, 536, der von einem „kleinen Konzernprivileg" spricht.
22 Vgl. Art. 4 Nr. 11, 6 Abs. 1 lit. a DS-GVO.
23 Dies hat auch der *EuGH* kürzlich in Bezug auf den ähnlich lautenden Art. 7 lit. f DS-RL festgestellt, vgl. *EuGH* ZD 2017, 24 m. Anm. *Kühling/Klar* = MMR 2016, 842 m. Anm. *Moos/Rothkegel*.
24 Vgl. *Pötters/Rauer*, in: Wybitul (o. Fußn. 9), Art. 6 Rdnr. 47.
25 Vgl. BGBl. Nr. 44 v. 5.7.2017, Teil I., S. 2159 ff.
26 Vgl. zum neuen Beschäftigtendatenschutz nach § 26 BDSG 2018 und Art. 88 DS-GVO *Wybitul*, NZA 2017, 413 ff. sowie *Pötters/Wybitul/Böhm*, in: Wybitul (o. Fußn. 9), Art. 88.
27 Vgl. *Loof/Schefold,* ZD 2016, 107, 109; *Sörup/Marquardt*, ArbRAktuell 2016, 103, 105.
28 Vgl. zu den Erlaubnistatbeständen der DS-GVO *Schuppert/Pflüger*, in: Wybitul (o. Fußn. 9), Art. 44 Rdnr. 1 ff.
29 *Schröder*, in: Kühling/Buchner (o. Fußn. 19), Art. 44 Rdnr. 20; *Pauly* (o. Fußn. 4), Art. 44. Rdnr. 2.
30 Vgl. Art. 44 DS-GVO.
31 Vgl. Art. 44 Satz 2 DS-GVO und Erwägungsgrund 101 Satz 3 DS-GVO.
32 Vgl. zu den Anforderungen des Angemessenheitsbeschlusses *Molnár-Gábor/Kaffenberger,* ZD 2017, 18, 19.

stellt hat, dass das betreffende Drittland[33] über ein angemessenes Schutzniveau verfügt.[34] In einer solchen Fallkonstellation gelten letztlich die gleichen Vorgaben wie bei einer Datenübermittlung innerhalb der EU.[35] Die bereits von der *EU-Kommission* gefassten Angemessenheitsbeschlüsse verlieren mit der Geltung der DS-GVO auch nicht ihre Gültigkeit. Denn Art. 45 Abs. 9 DS-GVO legt fest, dass bereits von der *EU-Kommission* verabschiedete Angemessenheitsbeschlüsse auf Grundlage von Art. 25 Abs. 6 DS-RL[36] künftig bis auf weiteres fortgelten.[37]

Einer dieser Angemessenheitsbeschlüsse ist das sog. Privacy Shield für die USA. Dieser ist seit dem 12.6.2016 als Nachfolgeregelung zum Safe Harbor-Abkommen in Kraft.[38] Unternehmen dürfen sich nur dann nach dem Privacy Shield zertifizieren lassen,[39] wenn sie die in dem Abkommen näher ausgeführten verbindlichen Prinzipien umsetzen und befolgen. Über die Einhaltung der vereinbarten Prinzipien wacht das US-Handelsministerium (*Federal Trade Commission – FTC*) gemeinsam mit der *EU-Kommission*, indem es die Unternehmen zur Errichtung eines effektiven Systems der Selbstkontrolle oder aber alternativ zu regelmäßigen externen Audits verpflichtet.[40] Es geht also i.E. beim Privacy Shield um das tatsächliche Einhalten verbindlicher rechtlicher Vorgaben und nicht lediglich um die bloße Zertifizierung bei der *FTC*. Für Übermittlungen an nach dem Privacy Shield zertifizierte Unternehmen gilt das Datenschutzniveau grundsätzlich als angemessen i.S.v. Art. 45 DS-GVO.[41] Neben den allgemeinen Voraussetzungen für die Übermittlung personenbezogener Daten an Dritte[42] müssen übermittelnde Unternehmen in solchen Fällen keine sonstigen Schutzmaßnahmen umsetzen.

b) Standarddatenschutzklauseln (SCCs)

Art. 46 Abs. 1 DS-GVO erlaubt es Unternehmen, vorbehaltlich geeigneter Garantien personenbezogene Daten an Verantwortliche zu übermitteln, für die kein Angemessenheitsbeschluss gilt. Nach dieser Vorschrift kann das Unternehmen durch den Abschluss von EU-Standarddatenschutzklauseln (da ehemals Standardvertragsklauseln/EU Standard Contractual Clauses – im Folgenden: SCCs) mit der empfangenden Stelle solche geeigneten Garantien schaffen und ein angemessenes Datenschutzniveau sicherstellen.[43] Auch hier geht es nicht nur darum, einen entsprechenden Vertrag zwischen Datenübermittler und Datenempfänger zu schließen. Vielmehr ist entscheidend, dass der Datenempfänger die Verpflichtungen aus den SCCs auch tatsächlich umsetzt.

Bereits unter der noch geltenden DS-RL hat die *EU-Kommission* gem. Art. 26 Abs. 4 DS-RL drei verschiedene Varianten von SCCs erlassen.[44] Diese SCCs bleiben auch nach dem 25.5.2018 zunächst in Kraft. Erst wenn die *Kommission* sie durch einen erneuten Beschluss ändern, ersetzen oder aufheben sollte,[45] verlieren diese Vertragsvorlagen ihre Wirkung als geeignete Garantien.[46]

Verpflichtet sich der Datenempfänger im Drittland zur Einhaltung der in den SCCs festgelegten Datenschutzstandards, so gilt für ihn grundsätzlich ein angemessenes Datenschutzniveau. Jedoch ist es nicht ausreichend, wenn der Empfänger lediglich die SCCs unterschreibt. Entscheidend ist letztlich, dass er die Verpflichtungen aus den SCCs auch tatsächlich umsetzt.

Der standardisierte Text der SCCs ermöglicht es Unternehmen, die Datenübermittlung in ein Drittland durch einen unkomplizierten Vertragsschluss relativ kurzfristig zulässig zu gestalten.[47] Praktische Probleme bereitet vielen Unternehmen die hierbei vorgeschriebene notwendige detaillierte Beschreibung der Übermittlung im Anhang zu den SCCs. Gerade deutsche Aufsichtsbehörden verlangen hier unter Berufung auf das Transparenzprinzip genaue Angaben.[48] Um diesen Anforderungen gerecht zu werden, sollten Unternehmen rechtzeitig alle von dem Datentransfer betroffenen internen Funktionen bzw. Abteilungen beteiligen.

Auch der Datenempfänger im Drittland verpflichtet sich mit Abschluss der SCCs zu einer ganzen Reihe datenschutzrechtlicher Pflichten. Dies umfasst etwa das Verbot, die empfangenen Daten an Stellen in einem Drittland weiterzugeben, die nicht über ein angemessenes Datenschutzniveau verfügen (sog. Onward-Transfer).[49] I.E. verpflichtet der Empfänger sich, EU-Datenschutzstandards einzuhalten. Die zuständige Aufsichtsbehörde kann die Einhaltung der Verpflichtungen auch beim Datenempfänger im Drittland prüfen.[50] Ggf. kann die Behörde die Datenübermittlung verbieten[51] oder auch Geldbußen[52] verhängen.[53]

Seit dem Safe Harbor-Urteil des *EuGH*[54] stellen manche Datenschützer auch SCCs als geeignete Sicherheit für Datenübermitt-

---

33 Angemessenheitsbeschlüsse der *EU-Kommission* müssen nicht automatisch das gesamte Drittland umfassen. Die *EU-Kommission* kann die Angemessenheit des Datenschutzniveaus auch nur für ein bestimmtes Gebiet oder einen oder mehrere spezifische Sektoren in dem Drittland feststellen. Ein Beispiel hierfür ist Kanada. Mit B. v. 4.1.2002 (2002/2/EG) legte die *Kommission* fest, dass das Datenschutzniveau in Kanada im Anwendungsbereich des Personal Information Protection and Electronic Documents Act (PIPEDA) als angemessen gilt. Der PIPEDA ist kanadisches Bundesrecht. Jedoch besteht im kanadischen Datenschutzrecht eine konkurrierende Gesetzgebungskompetenz. Erlassen die Provinzen datenschutzrechtliche Gesetze, gehen diese dem Bundesrecht vor. Je nach Sitz der datenempfangenden Stelle in Kanada kann also möglicherweise nicht auf den Angemessenheitsbeschluss zurückgegriffen werden.

34 Vgl. Art. 45 Abs. 1 DS-GVO.

35 Vgl. zu diesen Anforderungen III.1.

36 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-RL).

37 Eine aktuelle Liste der Staaten, für die Angemessenheitsbeschlüsse der *EU-Kommission* existieren, ist abrufbar unter: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm. Darunter finden sich etwa Andorra, Neuseeland, die Schweiz und Uruguay.

38 Das Safe Harbor-Abkommen wurde vom *EuGH* für unwirksam erklärt, *EuGH* ZD 2015, 549 m. Anm. *Spies*.

39 Eine Liste der zertifizierten Unternehmen findet sich auf der Internetseite des *US-Handelsministeriums*, abrufbar unter: https://www.privacyshield.gov/list. Derzeit umfasst die Liste rd. 2.500 teilnehmende Unternehmen, darunter z.B. auch Konzerne wie *Facebook* oder *Amazon*.

40 *EU-Kommission*, B. v. 12.7.2016 – C/2016/4176, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.DEU, Paragraf 26 Satz 5.

41 Das durch das Privacy Shield tatsächlich gewährte Schutzniveau wird von vielen Stimmen in Politik und Fachliteratur angezweifelt. So hat der *Ausschuss des Europäischen Parlaments für „Bürgerliche Freiheiten, Justiz und Inneres" (LIBE)* Ende März 2017 eine kritische Resolution zum Privacy Shield verabschiedet. Darin kritisieren die EU-Parlamentarier u.a. Schwierigkeiten bei der Rechtsdurchsetzung für EU-Bürger sowie die behauptete Massenüberwachung durch die *US-Regierung*. Entsprechend forderte der *Ausschuss* die *EU-Kommission* zu einer offiziellen Überprüfung des Datenschutzniveaus unter dem Privacy Shield auf; vgl. zum aktuellen Diskussionsstand *Philipp*, EuZW 2017, 324 ff.

42 Vgl. zur Definition von „Dritter" Art. 4 Nr. 10 DS-GVO.

43 Art. 46 Abs. 2 lit. c DS-GVO.

44 Ein Set für die Datenübermittlung eines Verantwortlichen an einen Auftragsverarbeiter (2010/87/EU) sowie zwei leicht abgewandelte Sets für die Datenübermittlung zwischen zwei Verantwortlichen (2001/497/EG / 2004/915/EG).

45 Standarddatenschutzklauseln erlässt die *EU-Kommission* gem. Art. 46 Abs. 2 lit. c, 93 Abs. 2 DS-GVO.

46 Art. 46 Abs. 5 Satz 2 DS-GVO.

47 Zu Änderungen am Text der Klauseln vgl. *Lange/Filip,* in: BeckOK DatenSR, DS-GVO, Art. 46 Rdnr. 28.

48 Vgl. *Lange/Filip* (o. Fußn. 49), Rdnr. 31.

49 (EU-)controller to (Non-EU/EEA-)controller – Decision 2001/497/EC: Set I Clause 5 (b), Appendix 2 No. 6, Appendix 3 No. 3; (EU-)controller to (Non-EU/EEA-)controller – Decision 2004/915//EC: Set II Clause Clause 2 (i).

50 Vgl. Art. 57 Abs. 1 lit. a und h DS-GVO; vgl. auch *Lang,* in: Moos, Datennutzungs- und Datenschutzverträge, 1. Aufl. 2014, Teil 5 I Rdnr. 11.

51 Vgl. Art. 58 Abs. 2 lit. f DS-GVO.

52 Art. 58 Abs. 2 lit. i i.V.m. 83 Abs. 5 lit. c DS-GVO.

53 Vgl. zu der Kontrolle durch die Aufsichtsbehörde auch Art. 4 Abs. 1 lit. b und c der Entscheidung 2001/497/EG hinsichtlich Standardvertragsklauseln.

54 *EuGH* ZD 2015, 549 m. Anm. *Spies*; vgl. *Schröder*, in: Schröder, Datenschutzrecht, 2. Aufl. 2016, 7. Kap. II. (2.); zur Beschwerde von Max Schrems *Jensen*, ZD-Aktuell 2016, 05204.

lungen in Drittländer in Frage.[55] Diese Kritiker argumentieren u.a., die Angemessenheitsentscheidungen der *Kommission* zu SCCs könnten nicht mehr gültig sein, da das Ausmaß der Massenüberwachung durch die USA erst nach Verabschiedung der SCCs bekannt wurde. Aktuell ist vor dem *High Court of Irland* ein entsprechendes Verfahren anhängig. Dieses Gerichtsverfahren strebte die irische Datenschutzaufsichtsbehörde mit dem Ziel an, die Frage der Zulässigkeit von SCCs vom *EuGH* entscheiden zu lassen.[56] Bis der *EuGH* zu dieser Frage entscheidet, wird voraussichtlich jedoch noch einige Zeit vergehen. Zumindest bis dahin bleiben die Beschlüsse der *Kommission* zu den SCCs jedenfalls gültig.[57] SCCs sind somit für Unternehmen mittelfristig noch ein rechtssicherer und unkomplizierter Weg, um Datenübermittlungen in Drittländer abzusichern. Zudem lassen sich viele der berechtigten Kritikpunkte an dem Safe Harbor-Abkommen nicht ohne weiteres auf die Angemessenheitsentscheidung zu SCCs übertragen.

c) Verbindliche interne Datenschutzvorschriften (BCRs)

Grenzüberschreitende Übermittlungen innerhalb von Unternehmen oder Unternehmensgruppen[58] kann das Unternehmen auf der zweiten Stufe auch durch BCRs rechtfertigen.[59] Die zuständige[60] Aufsichtsbehörde kann solche BCRs genehmigen.[61] Bei der Einführung und Umsetzung von BCRs unterliegt das Unternehmen aber umfassenden Vorgaben. Art. 47 DS-GVO enthält hierzu einen umfassenden Anforderungskatalog. Dieser setzt im Wesentlichen die Anforderungen um, die die *Art. 29-Datenschutzgruppe* seit Einführung der ersten BCRs Ende der 90er-Jahre veröffentlicht hat.[62]

Sobald BCRs eingeführt und genehmigt sind, bieten sie gerade internationalen Konzernen eine sehr gute Möglichkeit, den internen Datentransfer auf der zweiten Stufe sicher und unkompliziert zu gestalten. Jedoch sollten sich Unternehmen darauf einstellen, dass auch nach der DS-GVO das Genehmigungsverfahren für BCRs zeitaufwändig und komplex bleibt.[63] Gerade für Unternehmen mit hohen globalen Datenschutzstandards bieten BCRs allerdings ein hohes Maß an Rechtssicherheit und Flexibilität.

d) Genehmigte Verhaltensregeln (CoC)

Ein bereits vor der DS-GVO bekanntes Mittel[64] zur Legitimierung von Übermittlungen personenbezogener Daten in Drittländer sind genehmigte Verhaltensregeln (sog. Codes of Conduct – CoC).[65] Verbände und Vereinigungen, welche datenverarbeitende Stellen repräsentieren, können solche Leitlinien konzipieren und aufstellen.[66] Solche CoC sollen dann die Bestimmungen der DS-GVO präzisieren.[67] Damit CoC Datenübermittlungen rechtfertigen können, müssen sie rechtsverbindliche und durchsetzbare Verpflichtungen zur Anwendung geeigneter Garantien durch Verantwortliche oder Auftragsverarbeiter im Drittland enthalten.[68] Insbesondere müssen sie Rechtsschutzmöglichkeiten der betroffenen Personen sicherstellen. Der Daten übermittelnde Verantwortliche muss auch den Datenempfänger an die Einhaltung der CoC binden. Dies kann er insbesondere mittels vertraglicher oder sonstiger Pflichten umsetzen.[69]

Ob ein Unternehmen CoC als Instrument zur Legitimation grenzüberschreitender Datenübermittlungen einsetzen kann, hängt von den jeweiligen Verbänden und Vereinigungen ab. Für diese ist das Genehmigungsverfahren auch nach der DS-GVO relativ aufwändig und kompliziert. Zudem bleibt auch dem Verantwortlichen angesichts notwendiger zusätzlicher Absicherungen ein nicht unerheblicher Restaufwand.[70] Allerdings kann es für viele international operierende Unternehmen sehr ratsam sein, sich zeitnah mit den sie vertretenden Verbänden bzw. Vereinigungen abzustimmen, um so möglichst bald zu rechtssicheren und belastbaren Lösungen zu gelangen.

e) Zertifizierung

Als weitere Möglichkeit der Legitimierung einer Datenübermittlung in Drittländer auf der zweiten Stufe können Verantwortliche Stellen oder Auftragsverarbeiter in Drittländern auch gem. Art. 42 DS-GVO bestimmte Verarbeitungsvorgänge zertifizieren lassen.[71] Eine solche Zertifizierung bescheinigt dem Datenempfänger, dass er i.R.e. bestimmten Datenverarbeitungssvorgangs personenbezogene Daten grundsätzlich in Einklang mit der DS-GVO verarbeitet.[72] Zertifizierungen können sowohl die zuständige Aufsichtsbehörde[73] als auch eine gem. Art. 43 DS-GVO akkreditierte Zertifizierungsstelle ausstellen.

Zur Legitimation einer Datenübermittlung auf der zweiten Stufe müssen die Parteien zusätzlich zur Zertifizierung der Verarbeitung rechtsverbindliche und durchsetzbare Verpflichtungen zur Wahrung der Betroffenenrechte schließen.[74] Der Vorteil für Unternehmen durch eine Zertifizierung ist ein deutlich höheres Maß an Sicherheit als z.B. bei einer bloßen vertraglichen Verpflichtung. Bei der Datenübermittlung i.R.e. zertifizierten Verarbeitung dürften Sanktionen in Bezug auf die Grenzüberschreitung weitgehend ausgeschlossen sein.

3. Einwilligung sämtlicher betroffener Personen

Wenn die betroffene Person wirksam in die Datenübermittlung in das Drittland einwilligt, können Unternehmen personenbezogene Daten auch dann in Drittländer übermitteln, wenn die Übermittlung die sonstigen Voraussetzungen der Art. 45-47 DS-GVO nicht erfüllt.[75] In diesem Fall benötigt das Unternehmen zur Rechtfertigung der Übermittlung auf zweiter Stufe kei-

55 So z.B. das *Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD)*, das in einem Positionspapier v. 14.10.2015 zum Safe Harbor-Urteil feststellt, dass in konsequenter Anwendung der Vorgaben des *EuGH* eine Datenübermittlung auf Basis von SCCs nicht mehr zulässig sei.

56 Vgl. zum aktuellen Stand dieses Verfahrens die PM des *Irish Data Protection Commissioner*, abrufbar unter: https://www.dataprotection.ie/docs/16-03-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm.

57 So auch die *Art. 29-Datenschutzgruppe* in einer Stellungnahme v. 16.10.2015 zum Safe Harbor-Urteil; darin gehen die Datenschutzbehörden davon aus, dass die SCCs zunächst weiter verwendet werden können.

58 Dies betrifft auch Gruppen von Unternehmen (sog. Binnentransfers); vgl. zur Definition Art. 4 Nr. 19 DS-GVO.

59 Vgl. auch Erwägungsgrund 110 DS-GVO.

60 Die zuständige federführende Aufsichtsbehörde bestimmt sich dabei gem. Art. 56 Abs. 1 DS-GVO nach dem Sitz der Hauptniederlassung bzw. der einzigen Niederlassung des Verantwortlichen.

61 Art. 47 Abs. 1 DS-GVO.

62 Vgl. *Klug*, in: Gola, DS-GVO, 1. Aufl. 2017, Art. 47 Rdnr. 6, mit einer Aufzählung der einschlägigen Working Paper der *Art. 29-Datenschutzgruppe*.

63 Vgl. *Schröder* (o. Fußn. 29), Art. 47 Rdnr. 4; *Lange/Filip* (o. Fußn. 47), Art. 47 Rdnr. 14 ff.

64 Vgl. Art. 27 DS-RL, § 38a BDSG. Diese der Regelung in der DS-GVO ähnlichen Verhaltensregeln erlangten in Deutschland kaum praktische Bedeutung. Dies lag vermutlich daran, dass in der alten Ausgestaltung die durch Verhaltensregeln erlangte Rechtssicherheit im Vergleich mit dem notwendigen Abstimmungsaufwand eher gering war; vgl. *Wolff*, ZD 2017, 151 f.

65 Vgl. Art. 46 Abs. 2 lit. e DS-GVO.

66 Art. 40 DS-GVO.

67 Art. 40 Abs. 2 DS-GVO.

68 Vgl. *Klug* (o. Fußn. 62), Art. 46 Rdnr. 12; *Lange/Filip* (o. Fußn. 47), Art. 46 Rdnr. 52.

69 Art. 40 Abs. 3 DS-GVO.

70 *Wolff*, ZD 2017, 151, 154; *Ambrock/Karg*, ZD 2017, 154, 157.

71 Vgl. Art. 46 Abs. 2 lit. f DS-GVO.

72 Zu den genauen Voraussetzungen vgl. *Lange/Filip* (o. Fußn. 47), Art. 46 Rdnr. 52; *Pauly* (o. Fußn. 4), Art. 46 Rdnr. 33.

73 Damit schafft die DS-GVO für die Aufsichtsbehörde eine Doppelrolle als Zertifizierungsstelle und gleichzeitig als Aufsichtsbehörde. Gerade bei kostenpflichtigen Zertifizierungen birgt dies einen Interessenkonflikt. Angesichts der Tatsache, dass akkreditierte Zertifizierungsstellen gem. Art. 43 Abs. 2 lit. e DS-GVO nachweisen müssen, in keinem Interessenskonflikt zu stehen, ist dies erstaunlich; vgl. hierzu *Lepperhoff*, in: Gola (o. Fußn. 62), Art. 42 Rdnr. 8.

74 Vgl. Art. 46 Abs. 2 lit. f DS-GVO.

75 Art. 49 Abs. 1 Unterabs. 1 lit. a DS-GVO.

ne zusätzlichen Garantien. Die DS-GVO stellt jedoch hohe Anforderungen an eine solche Einwilligungserklärung.[76] Eine wirksame Einwilligung muss danach freiwillig, informiert sowie ausdrücklich und konkret sein.[77]

a) Freiwilligkeit

Die betroffene Person muss die Einwilligung zunächst freiwillig erteilen.[78] D.h., die Einwilligung muss auf ihrer freien Entscheidung beruhen.[79] Für eine solche freie Entscheidung muss die betroffene Person eine echte Wahlfreiheit haben.[80]

Die betroffene Person hat regelmäßig dann keine echte Wahlfreiheit, wenn die Gewährung von Leistungen von einer Einwilligung in solche Datenverarbeitungen abhängig gemacht wird, die nicht dem eigentlichen Geschäft dienen.[81] Die Regelung bedeutet zwar kein vollständiges „Koppelungsverbot".[82] Jedoch geht sie weiter als der bisherige § 28 Abs. 3a BDSG, der ein Koppelungsverbot lediglich in Monopolsituationen festlegt.[83] In der Praxis wird die Regelung das Geschäftsmodell „Dienstleistung gegen Daten" wohl erheblich erschweren.[84] Ggf. werden Unternehmen künftig ihre Dienste in unterschiedlichem Umfang und zu unterschiedlichen Kosten einmal mit Einwilligung und einmal ohne Einwilligung anbieten.[85]

Die Freiwilligkeit von Einwilligungserklärungen im Arbeitsverhältnis war bereits unter dem bisherigen BDSG heftig umstritten. Manche Aufsichtsbehörden und Stimmen in der Literatur bewerteten eine Einwilligung im Arbeitsverhältnis generell als unfreiwillig,[86] während das *BAG* auch im Arbeitsverhältnis zu Recht grundsätzlich die Möglichkeit einer freiwilligen Einwilligung durch den Arbeitnehmer anerkannte.[87]

Nach der DS-GVO ist eine Einwilligung auch im Arbeitsverhältnis grundsätzlich möglich.[88] Ein generelles Verbot ohne die Möglichkeit der Abwägung im Einzelfall wäre eine ungerechte Schlechterstellung von Arbeitnehmern. Entsprechend sieht auch § 26 Abs. 2 BDSG 2018 die Möglichkeit einer Einwilligung im Arbeitsverhältnis ausdrücklich vor, auch wenn die bestehende Abhängigkeit des Arbeitnehmers ausdrücklich anerkannt wird.[89] Insbesondere kann danach auch im Arbeitsverhältnis Freiwilligkeit vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder aber, wenn Arbeitgeber und Arbeitnehmer gleichgelagerte Interessen haben.[90]

b) Informiertheit

Die betroffene Person muss alle für ihre Einwilligung relevanten Umstände kennen, um in eine Datenverarbeitung einwilligen zu können.[91] Möchte der Verantwortliche eine Datenübermittlung in Drittländer auf die Einwilligung stützen, muss er alle hiervon betroffenen Personen über alle relevanten Umstände der Datenübermittlung informieren. Es ist zweckmäßig, insbesondere auch darüber zu unterrichten, dass die Datenschutzbestimmungen in dem entsprechenden Drittland ggf. ein deutlich geringeres Datenschutzniveau bieten als in der EU.[92]

Der Verantwortliche muss den betroffenen Personen die notwendigen Informationen in zumutbarer und auch für Nichtjuristen einfach verständlicher Sprache mitteilen.[93] Wird diese Erklärung jedoch zu umfangreich, ist der betroffenen Person die Prüfung dieser Einwilligungserklärung ggf. nicht mehr zumutbar.[94] Dieser Spagat ist eine der besonders großen Herausforderungen an Unternehmen durch die DS-GVO. Daher sollten die Aufsichtsbehörden und Gerichte hier letztlich keine überzogenen Maßstäbe anlegen.

c) Ausdrückliche und konkrete Willensbekundung

Die betroffene Person muss ihren Willen i.R.e. Einwilligung klar und konkret zum Ausdruck bringen. Jedoch sieht die DS-GVO keine bestimmte Form für Einwilligungserklärungen vor. Entsprechend kann die betroffene Person die Einwilligungserklärung auch mündlich erteilen. Auch konkludente (also durch schlüssiges Verhalten abgegebene) Erklärungen kommen in Betracht.[95] Allerdings schränkt Erwägungsgrund 32 DS-GVO die Möglichkeit zur Erteilung solcher konkludenter Einwilligungen ein. Dieser Erwägungsgrund stellt klar, dass jedenfalls Stillschweigen, Untätigkeit oder bereits vorausgefüllte Kästchen (sog. Opt-out) nicht den Anforderungen an eine Einwilligung entsprechen.[96] In der Praxis ergeben sich aus den Dokumentationspflichten des Verantwortlichen jedenfalls faktische Anforderungen an die Form von Einwilligungen. Verantwortliche Unternehmen müssen grundsätzlich nachweisen können, dass sie Daten entsprechend den Vorgaben der DS-GVO verarbeiten.[97] Hierfür müssen sie rechtssicher nachweisen können, dass relevante Einwilligungen in wirksamer Form erteilt worden sind. Das kann der Verantwortliche bei mündlich oder konkludent erteilten Einwilligungen regelmäßig nicht leisten.

---

76 Diese Anforderungen entsprechen den Anforderungen an Einwilligungen gem. Art. 4 Nr. 11 und Art. 7 DS-GVO, vgl. *Wendehorst/Graf v. Westphalen*, NJW 2016, 3745.

77 Vgl. *Pauly* (o. Fußn. 4), Art. 49 Rdnr. 5 ff.; *Lange/Filip* (o. Fußn. 47), Art. 49 Rdnr. 4 ff. Besonderheiten zu Einwilligungen von Minderjährigen regelt Art. 8 DS-GVO, ausf. *Ernst,* ZD 2017, 110, 111. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten muss der Verantwortliche weitere Voraussetzungen beachten, Art. 9 Abs. 2 lit. a DS-GVO.

78 Art. 4 Nr. 11 DS-GVO.

79 *Ernst*, in: Paal/Pauly (o. Fußn. 4), Art. 4 Rdnr. 69 ff.

80 *Fladung/Pötters,* in: Wybitul (o. Fußn. 9), Art. 7 Rdnr. 13 ff.; *Ernst,* ZD 2017, 110, 112. Die Forderung nach einer sog. differenzierten Einwilligung, vgl. *Ambrock/Karg*, ZD 2017, 154, 158, d.h. dass der Verantwortliche für jede Stufe der Datenübermittlung in ein Drittland eine gesonderte Einwilligung einzuholen hat, ist wegen des klaren Wortlauts von Erwägungsgrund 43 DS-GVO („zu verschiedenen Verarbeitungsvorgängen") abzulehnen. Die Datenübermittlung in ein Drittland ist ein zusammenhängender Verarbeitungsvorgang, auch wenn dessen Rechtmäßigkeit abgestuft geprüft wird.

81 Vgl. Art. 7 Abs. 4 DS-GVO. Erwägungsgrund 43 DS-GVO präzisiert diese Regelung weiter. Danach ist eine Einwilligung nicht freiwillig erteilt, wenn ein „klares Ungleichgewicht" zwischen der betroffenen Person und dem Verantwortlichen besteht.

82 Ob die Regelung in der DS-GVO faktisch ein Koppelungsverbot darstellt, ist eine letztlich unerhebliche Definitionsfrage. Während *Dammann,* ZD 2016, 307, 311 ein „verkapptes Koppelungsverbot" erkennt, bezweifelt dies *Frenzel*, in: Paal/Pauly (o. Fußn. 4), Art. 7 Rdnr. 21.

83 *Gierschmann*, ZD 2016, 51, 54.

84 *Wybitul* (o. Fußn. 9), Einl., Rdnr. 292; a.A. *Frenzel* (o. Fußn. 82), Rdnr. 21. Danach sei die Preisgabe der Daten in solchen Geschäftsmodellen Bestandteil des Vertrags, da damit die Leistung an sich bezahlt würde.

85 *Gierschmann,* ZD 2016, 51, 54.

86 Vgl. z.B. *Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit*, 22. TB, S. 95; 18. TB, S. 197; *Schmidt,* JZ 1974, 247.

87 *BAG* ZD 2015, 330 m. Anm. *Wybitul*.

88 *Wybitul/Pötters,* RDV 2016, 10, 12 f.; *Kort,* ZD 2016, 555, 556 f.; zum Streitstand nach der alten Rechtslage *Wybitul/Böhm*, BB 2015, 2101 ff.

89 S. hierzu und zum neuen Arbeitsrecht nach Art. 88 DS-GVO und § 26 BDSG 2018 allg. *Wybitul*, NZA 2017, 413 ff.

90 Vgl. *Wybitul*, NZA 2017, 413, 416 f.

91 Zudem muss er über seine Rechte und Pflichten informiert werden. I.R.d. Einwilligungserklärung umfasst das gem. Art. 7 Abs. 3 DS-GVO das jederzeitige Recht zum Widerruf. Sollte der Verantwortliche planen, die Datenübermittlung ggf. auch auf einen gesetzlichen Erlaubnistatbestand zu stützen, sollte die betroffene Person vor Abgabe einer Einwilligungserklärung hierüber informiert werden. Ansonsten setzt sich der Verantwortliche dem Vorwurf aus, bei der betroffenen Person treuwidrig den Eindruck erweckt zu haben, er könne über die Verwendung seiner Daten frei disponieren.

92 Vgl. hierzu noch zur DS-RL WP 12 (26) und WP 114 (14).

93 Vgl. *Wendehorst/Graf v. Westphalen,* NJW 2016, 3745 ff.

94 Das folgt aus dem Transparenzgebot des Art. 5 Abs. 1 lit. a DS-GVO; vgl. *Ernst,* ZD 2017, 110, 113.

95 Vgl. *Buchner/Kühling*, in: Kühling/Buchner (o. Fußn. 19), Art. 7 Rdnr. 38.

96 Vgl. *Ernst,* ZD 2017, 110, 113.

97 Vgl. Art. 5 Abs. 2 sowie Art. 24 Abs. 1 DS-GVO, sog. Verantwortlichkeitsprinzip.

4. Sonstige Ausnahmen

Neben der Möglichkeit zur Einwilligung in die Datenübermittlung enthält Art. 49 Abs. 1 DS-GVO auch eine Aufzählung weiterer Ausnahmetatbestände, die eine Datenübermittlung in ein Drittland ohne Vorliegen der Voraussetzungen der Art. 45-47 DS-GVO ermöglichen.

a) Vertragserfüllung

Ein solcher Ausnahmetatbestand kann vorliegen, wenn die Übermittlung zur Erfüllung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person erforderlich ist.[98] Könnte der Verantwortliche das Ziel des Vertrags jedoch auch ohne die entsprechende Datenübermittlung erreichen oder genügt die Übersendung anonymisierter Daten, so soll er die Übermittlung nach der bisherigen Auffassung der Datenschutzaufsichtsbehörden nicht auf diesen Tatbestand stützen können.[99] Auch wenn der Verantwortliche den Vertrag nicht mit der betroffenen Person, sondern lediglich in ihrem Interesse geschlossen hat,[100] kann der Tatbestand erfüllt sein.[101]

b) Wichtige Gründe des öffentlichen Interesses

Die Übermittlung in Drittländer kann ausnahmsweise auch dann ohne weitere Voraussetzungen rechtmäßig sein, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist.[102] Erwägungsgrund 112 DS-GVO führt als Beispiele für solche wichtigen Gründe etwa das öffentliche Interesse am Datenaustausch zwischen Wettbewerbs-, Steuer- und Zollbehörden auf. Für die Unternehmenspraxis ist dieser Ausnahmetatbestand wohl weniger relevant.

c) Geltendmachung von Rechtsansprüchen

Eine weitere praktisch wichtige Ausnahme gilt, wenn die Übermittlung personenbezogener Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.[103]

Erforderlich ist eine solche Datenübermittlung nur dann, wenn sie in direktem Zusammenhang mit dem entsprechenden Verfahren steht.[104] Durch das Merkmal der Erforderlichkeit wird der Grundsatz auf Datenminimierung[105] zu einem entscheidenden Faktor. Der Verantwortliche sollte daher immer im Einzelfall prüfen, ob z.B. auch eine anonymisierte oder pseudonymisierte Übermittlung der Daten zur Geltendmachung, Ausübung oder Verteidigung der Rechtsansprüche ausreicht. Eine Übersendung der Klardaten kann dann ggf. nicht erforderlich bzw. zulässig sein.

Anders als die vergleichbare Regelung im BDSG schränkt die DS-GVO den Tatbestand nicht auf Verfahren „vor Gericht" ein. Die genaue Definition dieser Einschränkung hatte bei Datenübermittlungen nach dem BDSG regelmäßig für Diskussionsstoff gesorgt.[106] Letzte Zweifel beseitigt nach der DS-GVO nun Erwägungsgrund 111, der ausdrücklich auch außergerichtliche Verfahren und Verfahren auf dem Verwaltungsweg mit in den Ausnahmetatbestand einbezieht. Damit sind z.B. Datenübermittlungen i.R.v. Pre-Trial Discovery-Verfahren[107] und Auskunftsverlangen des *US Departement of Justice (DoJ)* vom Anwendungsbereich dieses Ausnahmetatbestands umfasst.[108]

d) Lebenswichtige Interessen/öffentliche Register

Der Ausnahmetatbestand zum Schutz lebenswichtiger Interessen[109] dient der Übertragung medizinischer Daten.[110] Ebenso wie der Ausnahmetatbestand der Übermittlung aus einem öffentlichen Register[111] handelt es sich dabei um eine Spezialregelung mit einem in der allgemeinen Unternehmenspraxis wohl eher überschaubaren Anwendungsbereich.

e) Wahrung zwingender berechtigter Interessen des Verantwortlichen

Anders als das bislang geltende BDSG sieht die DS-GVO auch Übermittlungen zur Verwirklichung berechtigter Interessen des Verantwortlichen vor. An eine solche Übermittlung nach Art. 49 Abs. 1 Unterabs. 2 DS-GVO sind aber hohe Anforderungen geknüpft. Die Regelung ist ein Auffangtatbestand. Sie gilt nur für Übermittlungen, für die die anderen Ausnahmetatbestände nicht einschlägig sind. Die Regelung betrifft somit Datenübermittlungen in Drittländer, die nicht bereits nach Art. 45, 46 DS-GVO rechtmäßig sind.

Übermittlungen auf der Grundlage von Art. 49 Abs. 1 Unterabs. 2 DS-GVO sind nur unter engen Voraussetzungen zulässig. Erforderlich ist hierfür, dass die Übermittlung nicht wiederholt erfolgt, es nur eine begrenzte Zahl an betroffenen Personen gibt, die Übermittlung für die Wahrung zwingender berechtigter Interessen des Verantwortlichen erforderlich ist, die Rechte und Freiheiten der betroffenen Personen nicht überwiegen und der Verantwortliche geeignete Garantien vorgesehen hat. Zusätzlich muss der Verantwortliche die zuständige Datenschutzaufsichtsbehörde von der Übermittlung in Kenntnis setzen.

Durch die hohen Anforderungen und umfangreichen Offenlegungspflichten ist die Ausnahmeregelung in der Praxis allenfalls in begrenzten Einzelfällen zu empfehlen. Die flächendeckende Übermittlung personenbezogener Daten wird sich durch diese Vorschrift eher nicht rechtfertigen lassen.

5. Zusammenfassung zur zweiten Prüfungstufe bei grenzüberschreitenden Datenübermittlungen

Unternehmen können die spezifischen Anforderungen an die Zulässigkeit einer Datenübermittlung nach Art. 44 ff. DS-GVO auf unterschiedliche Arten erfüllen.

Entweder übermitteln Unternehmen die personenbezogenen Daten an Empfänger mit angemessenem Datenschutzniveau. Ein angemessenes Datenschutzniveau kann das Unternehmen auf verschiedene Weise gem. Art. 45 und 47 DS-GVO sicherstellen, nämlich insbesondere auf der Grundlage von SCCs, BCRs, genehmigten Verhaltensregeln und Zertifizierungen. Welche der verschiedenen Varianten für eine konkrete Datenübermittlung je-

98 Art. 49 Abs. 1 Unterabs. 1 lit. b DS-GVO.

99 Z.B. legte die *Art. 29-Datenschutzgruppe* dieses Erfordernis bzgl. der DS-RL so aus, dass die Übermittlung von Fluggastdatensätzen von Fluggesellschaften an US-Behörden nicht für die Erfüllung des Vertrags zwischen der Fluggesellschaft und dem Passagier notwendig sei. Dass die Fluggesellschaft bei Nichtübersenden der Daten ggf. die Landerechte entzogen bekommen könnte, sei für die Einschätzung nicht relevant; s. ausf. hierzu *Art. 29-Datenschutzgruppe*, WP 66 – Stellungnahme 6/2002 zur Übermittlung von Informationen aus Passagierlisten und anderer Daten von Fluggesellschaften an die Vereinigten Staaten.

100 Das betrifft z.B. Verträge zu Gunsten Dritter nach § 328 BGB.

101 Art. 49 Abs. 1 Unterabs. 1 lit. c DS-GVO.

102 Art. 49 Abs. 1 Unterabs. 1 lit. d DS-GVO.

103 Art. 49 Abs. 1 Unterabs. 1 lit. e DS-GVO.

104 Zur bisherigen Rechtslage *Simitis,* in: Simitis, BDSG, 8. Aufl. 2014, § 4c Rdnr. 21.

105 Art. 5 Abs. 1 lit. c DS-GVO.

106 Insb. geht es dabei um die Frage, ob der Ausnahmetatbestand auch Verfahren im Vorfeld von Gerichtsverfahren umfasst. Nach hier vertretener Auffassung war richtigerweise bereits nach BDSG und DS-RL der Begriff weit auszulegen. Das ergibt sich einerseits aus dem Vergleich mit den anderen Sprachfassungen der DS-RL und andererseits aus einer teleologischen Auslegung. Sinn und Zweck der Ausnahmevorschrift war es bereits nach dem BDSG, der verantwortlichen Stelle die Verteidigung eigener Rechte zu ermöglichen. Dabei kann es keinen Unterschied machen, ob dies i.R.e. Gerichtsverhandlung geschieht oder im Vorfeld einer solchen Gerichtsverhandlung.

107 Dabei handelt es sich um ein dem eigentlichen Hauptverfahren vorgelagertes Erkenntnisverfahren zur Erlangen von Beweismitteln, das u.a. in den USA besteht. Neben eidlichen Zeugenvernehmungen (Depositions) und dem schriftlichen Austausch von gegenseitig zu beantwortenden Fragen steht vor allem die Auswertung großer, von der Gegenseite zur Verfügung gestellter Datenmengen im Vordergrund.

108 Ausf. zur Weitergabe von personenbezogenen Daten von EU-Unternehmen an US-Behörden s. *Metz/Spittka*, ZD 2017, 361 ff.

109 Art. 49 Abs. 1 Unterabs. 1 lit. f DS-GVO.

110 *Ambrock/Karg*, ZD 2017, 154, 159.

111 Art. 49 Abs. 1 Unterabs. 1 lit. g DS-GVO.

weils am besten geeignet ist, sollte das Unternehmen auf der Grundlage des jeweiligen Sachverhalts im Einzelfall entscheiden.

Besteht bei der datenimportierenden Stelle kein angemessenes Datenschutzniveau, kann der Verantwortliche die Datenübermittlung ggf. auf einen der Ausnahmetatbestände des Art. 49 DS-GVO stützen. Hier sollte der Verantwortliche im jeweiligen Einzelfall vor der Übermittlung genau prüfen, ob einer der Ausnahmetatbestände einschlägig und auch praktikabel ist.

Checkliste: Spezifische Anforderungen für die Übermittlung personenbezogener Daten in Drittländer – Prüfungsstufe 2

- Besteht ein Angemessenheitsbeschluss?
- EU-Standarddatenschutzklauseln (SCCs)
- Verbindliche interne Datenschutzvorschriften (BCRs)
- Genehmigte Verhaltensregeln (CoC)
- Zertifizierung des Datenimporteurs
- Einwilligung aller betroffenen Personen
- Übermittlung zur Vertragserfüllung
- Übermittlung zur Wahrung des öffentlichen Interesses
- Übermittlung zur Geltendmachung von Rechtsansprüchen
- Übermittlung zur Wahrung lebenswichtiger Interessen
- Übermittlung aus einem öffentlichen Register
- Übermittlung zur Wahrung berechtigter Interessen

Die Checkliste stellt dar, welche Fragen sich Verantwortliche stellen sollten und welche Optionen sie haben, um die spezifischen Anforderungen der DS-GVO für die Übermittlung personenbezogener Daten in Drittländer zu erfüllen.

IV. Fazit und Handlungsempfehlungen

Die Änderungen der DS-GVO in Bezug auf die Rechtfertigung von Datenübermittlungen in Drittländer erscheinen im Vergleich zu anderen Neuerungen der Verordnung eher überschaubar. Bei genauerem Hinsehen gibt es jedoch auch in Bezug auf grenzüberschreitende Datenübermittlungen aus der EU durchaus geänderte Anforderungen durch die DS-GVO. Vor allem drohen bei Fehlern deutlich schärfere Sanktionen. Insbesondere Bußgelder und Schadensersatzansprüche dürften in der Höhe drastisch steigen.

Daher sind Unternehmen gut beraten, im Zuge der unumgänglichen Umsetzungsprojekte zur Implementierung der DS-GVO auch zu prüfen, ob sie ihr Datenschutzkonzept und ihre entsprechenden Strukturen bei der transnationalen Datenübermittlung anpassen sollten. Unternehmen sollten die baldige Geltung der DS-GVO zum Anlass nehmen, ein rechtssicheres Datenübermittlungskonzept im Konzern oder an Dritte zu entwickeln. Gerade für multinational operierende Unternehmen oder Konzerne werden daher rechtssichere Regelungen und Strukturen bei der grenzüberschreitenden Datenübermittlung ein wesentlicher Baustein von Projekten zur Implementierung der DS-GVO sein.

Tim Wybitul
ist Rechtsanwalt, Fachanwalt für Arbeitsrecht und Partner der Kanzlei Hogan Lovells International LLP in Frankfurt/M. sowie Mitherausgeber der ZD.

Dr. Lukas Ströbel
ist Rechtsanwalt bei Hogan Lovells International LLP in Frankfurt/M.

Marian Dennis Rueß
ist Rechtsreferendar im Bezirk des OLG Frankfurt/M.