Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Arbeitskreis „Datenschutz International“

Whitepaper zu den Drittlandtransfers in der EU-Datenschutz-Grundverordnung

Mitglieder des Arbeitskreises:
Harald Eul,
Harald Eul Consulting
Maik Goehrke
Deutsche Bahn/Schenker
Paul Gürtler,
Targobank
Dr. Jörg Hladjk,
Jones Day
Gabriela Krader,
Deutsche Post DHL
Jörn Kriegel,
IKB
Andreas Leonhardt,
Öhringen
Dr. Joachim Rieß,
Daimler
Steffen Weiß,
GDD

22.07.2016

I. Einleitung

Die EU-Datenschutz-Grundverordnung (DS-GVO) knüpft, wie bereits die EU-Datenschutzrichtlinie 95/46/EG, **besondere Bedingungen** an die Übermittlung personenbezogener Daten in ein sog. **„Drittland“** außerhalb des Europäischen Wirtschaftsraums und legt diese Bedingungen in Kapitel V fest. Neben den Drittländern führt die DS-GVO die Kategorie der „internationalen Organisationen“ ein, wobei solche durch mindestens zwei Staaten oder andere Völkerrechtssubjekte auf Dauer hinsichtlich der Erfüllung überstaatlicher Aufgaben gebildet werden und damit nicht mit internationalen Unternehmensgruppen beispielsweise des Privatrechts gleichzusetzen sind.[1] Ziel der Vorgaben des Kapitel V ist es, das durch die DS-GVO gewährleistete Schutzniveau nicht zu untergraben. Dies gilt auch für die **Weiterübermittlung** von personenbezogenen Daten durch das jeweilige Drittland oder die internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation (vgl. Art. 44 Satz 1 2. Hs.).

Hinsichtlich der Prüfabfolge im Falle eines „Drittlandbezugs“ kann auf die etablierte **2-Stufen-Prüfung** zurückgegriffen werden, wobei zunächst nach der Zulässigkeit der Datenverarbeitung insgesamt zu fragen ist (**1. Stufe**), hierzu zählen alle Vorgaben der DS-GVO zum Datenumgang, und sodann die Anforderungen des Kapitel V geprüft werden (**2. Stufe**). Betroffene sind hinsichtlich eines beabsichtigten Datentransfers in ein Drittland zu informieren. Die Information hat die Angabe eines gültigen oder fehlenden Angemessenheitsbeschlusses der Kommission oder anderer geeigneter und angemessener Garantien nach den Art. 46, 47 oder 49 Abs. 1 zu beinhalten. Bei Verwendung anderer angemessener Garantien ist auf die Möglichkeit des Erhalts einer Kopie dieser Garantien hinzuweisen bzw. hat ein Hinweis zu erfolgen, wo diese verfügbar sind (vgl. Art. 13 Abs. 1 Buchst. f.).

II. Management Summary

Durch die DS-GVO erfolgt kein Paradigmenwechsel im Bereich der Drittlandtransfers. Bereits in der EU-Datenschutzrichtlinie vorhandene oder durch die aufsichtsbehördliche Praxis entwickelte Instrumente werden **bestätigt** und in ihren Vorgaben teilweise **erweitert** (vgl. Angemessenheitsbeschlüsse) bzw. gesetzlich **konkretisiert** (vgl. verbindliche interne Datenschutzvorschriften). Nach Anwendung der DS-GVO ab dem 25.05.2018 sollte das Hauptaugenmerk für datenverarbeitende Stellen zunächst auf die **Gültigkeit bestehender Beschlüsse bzw. Garantien** gelegt werden. Hierbei sind ändernde Beschlüsse der Kommission oder Beschwerden von Betroffenen ebenso relevant, wie Stellungnahmen bzw. Handlungen von Aufsichtsbehörden oder gar Entscheidungen des EuGH.

Datenverarbeiter können sich die **neuen Ausprägungen der Drittlandtransfers** zunutze machen, so insbesondere die verbindlichen internen Datenschutzvorschriften, die europa-

[1] Beispiele für internationale Organisationen, vgl. http://www.bmwi.de/DE/Themen/Digitale-Welt/Internationale-Dimension/internationale-organisationen.html.

weit auf gesetzliche Grundlage gestellt werden und nunmehr auch für Gruppen von Unternehmen mit gemeinsam ausgeübter Wirtschaftstätigkeit gelten sollen.

Hinsichtlich der Folgen eines Datenexports in ein Land oder an eine internationale Organisation ohne angemessenes Schutzniveau und ohne Garantien zu Gunsten der Betroffenen werden Datenverarbeiter mit **erhöhten Risiken** konfrontiert: Ein Verstoß gegen die Vorgaben des Kapitel V wird mit einem Bußgeld bis zu 20.000.000 EUR oder im Fall eines Unternehmens mit bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres geahndet, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 5).

III. Angemessenheitsbeschluss der EU-Kommission

Besteht für die internationale Organisation oder das Drittland ein Angemessenheitsbeschluss der EU-Kommission[2], soll das durch die DS-GVO etablierte Schutzniveau auch beim Empfänger gewahrt sein (Art. 45 Abs. 1), wobei die DS-GVO nunmehr von einem „der Sache nach gleichwertigen Schutzniveau ausgeht“ (vgl. ErwG 104). Neben Ländern können nunmehr auch **Gebiete** oder ein bzw. mehrere spezifische **Sektoren** von einem Angemessenheitsbeschluss profitieren. Datenexporte an Empfänger im Geltungsbereich eines Angemessenheitsbeschlusses bedürfen keiner Genehmigung der zuständigen Aufsicht (Art. 45 Abs. 1 Satz 2).

Bei der Prüfung der Angemessenheit des Schutzniveaus gibt die DS-GVO der Kommission Parameter vor, an die sie sich zu halten hat (vgl. Art. 45 Abs. 2), so auch die Prüfung von Zugriffsberechtigungen von Behörden auf personenbezogene Daten. Ferner soll die Kommission ihre getroffenen Beschlüsse mindestens **alle vier Jahre** überprüfen, was bis dato nur bei Anhaltspunkten für eine Verletzung von Datenschutzvorschriften oder einem Schaden für den Betroffenen vorgesehen war. Ferner obliegen der Kommission fortlaufende Überwachungspflichten für das jeweilige Drittland bzw. die internationale Organisation (Art. 45 Abs. 4).

Sollte die Kommission eine Angemessenheitsentscheidung widerrufen, ändern oder aussetzen, können Datenverarbeiter weitehrhin auf **alternative Garantien** zur Gewährleistung eines angemessenen Schutzniveaus zurückgreifen (Art. 45 Abs. 7). Ebenso wie Drittländer mit einem angemessenen Schutzniveau werden nunmehr auch solche im Amtsblatt der Europäischen Union sowie auf der Webseite der Kommission veröffentlicht, die über kein solches Niveau mehr verfügen. Bestehende Angemessenheitsbeschlüsse **bleiben in Kraft**, bis sie durch die Kommission geändert, ersetzt oder aufgehoben werden oder gar durch eine Entscheidung des Europäischen Gerichtshofs für ungültig erklärt werden.[3] Das

---

[2] Eine Aufstellung der Angemessenheitsbeschlüsse findet sich unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

[3] So z.B. der Angemessenheitsbeschluss zu Safe Harbor, vgl. EuGH, Urteil vom 06.10.2015 - C-362/14.

EU-U.S. Privacy Shield[4] wird nach seiner Verabschiedung durch die Kommission auch in der DS-GVO über Art. 45 Berücksichtigung finden können.

IV. Verbindliche interne Datenschutzvorschriften

Während die EU-Datenschutzrichtlinie die verbindlichen internen Datenschutzvorschriften („Binding Corporate Rules“, (BCRs)) noch nicht explizit adressiert, sondern diese vielmehr auf Basis aufsichtsbehördlicher Praktiken sowie Stellungnahmen der Artikel 29-Datenschutzgruppe entwickelt wurden, formuliert die DS-GVO über Art. 47 konkrete Anforderungen an BCRs. Demnach soll es **Mitgliedern einer Unternehmensgruppe** aber auch einer **Gruppe von Unternehmen** möglich sein, mittels durch die zuständige Aufsicht im **Kohärenzverfahren** genehmigter interner Datenschutzvorschriften personenbezogene Daten an Empfänger in Drittländer zu übermitteln. Die nunmehr gesetzliche Berücksichtigung von BCRs verhilft nunmehr zu deren Gültigkeit auch in den Mitgliedstaaten, in denen die BCRs derzeit keine anerkannte Garantie für den Drittlandtransfer darstellen.[5]

Profitieren können von solchen Regeln einerseits **Mitglieder einer Unternehmensgruppe**, folglich nicht Dienstleister außerhalb der Unternehmensgruppe bzw. deren Unterauftragnehmer. Neben den BCRs für verantwortliche Stellen sind auch solche für **Auftragsverarbeiter** von Art. 47 umfasst (vgl. Begriffsdefinition in Art. 4 Abs. 20). Andererseits soll es in der DS-GVO auch rechtlich unabhängigen Unternehmen möglich sein, das Schutzniveau über interne Datenschutzvorschriften herzustellen, wenn eine **gemeinsame Wirtschaftstätigkeit** ausgeübt wird, was bei Geschäftspartnern bereits der Fall sein könnte.

Hinsichtlich ihrer Inhalte formuliert die DS-GVO **Mindestanforderungen**, (vgl. Art. 47 Abs. 1 und 2), die teilweise auf den bereits durch die Artikel 29-Datenschutzgruppe über entsprechende Arbeitspapiere entwickelten Anforderungen basieren.[6] Mit Anwendung der DS-GVO wird sich eine Unternehmensgruppe oder eine Gruppe von Unternehmen aus verschiedenen Quellen bei der Gestaltung von BCRs bedienen müssen: Zum einen die Vorgaben des Art. 47 der DS-GVO, sodann die Anforderungen der Artikel 29-Datenschutzgruppe, die als Zusammenschluss der genehmigenden Aufsichtsbehörden bereits eigene Anforderungen erarbeitet hat, sowie mögliche Konkretisierungen durch die EU-Kommission zu **Format und Verfahren für den Informationsaustausch** über BCRs zwischen Verantwortlichem, Auftragsverarbeitern und Aufsichtsbehörden mittels sog. Durchführungsrechtsakte (vgl. Art. 47 Abs. 3).

Bezüglich des Kohärenzverfahrens ist noch unklar, ob alle 28 Aufsichtsbehörden der EU-Mitgliedstaaten ihre Anmerkungen zu den jeweiligen BCRs geben werden oder ob eine gegenseitige Anerkennung wie nach heutigem Stand möglich ist. Das bisher etablierte Verfahren der Aufsicht in Gestalt der gegenseitigen Anerkennung („Mutual Recognition“) bzw.

---

[4] Vgl. Whitepaper des Arbeitskreises zu den Datenexporten in die USA, https://www.gdd.de/aktuelles/startseite/whitepaper-zu-den-datenexporten-in-die-usa sowie http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

[5] So derzeit in Portugal.

[6] Vgl. WP 153, WP 154, WP 155, WP 195, WP 204.

dem der Kooperation[7] findet keine Anwendung mehr. Vorteilhaft am neuen Model der Kohärenz ist, dass ein Unternehmen die Datenschutzvorschriften nur noch mit einer Aufsichtsbehörde koordinieren muss, anstatt wie bisher mit einer federführenden Behörde und zwei co-prüfenden Behörden. Darüber hinaus wird die in Teilen der Mitgliedstaaten **vorhandene Genehmigungspflicht für Einzelübermittlungen**[8] im Rahmen der BCRs entfallen, da die DS-GVO entsprechende Benachrichtigungs- bzw. Genehmigungspflichten nicht mehr vorsieht. Folglich können Daten nach erfolgreicher Beendigung des Kohärenzverfahrens unmittelbar fließen.

Bestehende und genehmigte BCRs erhalten ihre Gültigkeit, bis sie von einer Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden (Art. 46 Abs. 5).

V. Vertragliche Garantien

Standarddatenschutzklauseln[9] werden weiterhin als geeignete Garantien für die Datenübermittlung in ein Drittland oder an eine internationale Organisation anerkannt und durch die EU-Kommission über das Ausschußverfahren erlassen (vgl. Art. 46 Abs. 2). Eine besondere **Genehmigungspflicht** für den Einsatz der Standarddatenschutzklauseln besteht nicht, wodurch die bisherige uneinheitliche Rechtslage auf nationaler Ebene mit bestehenden Genehmigungs- bzw. Vorlagepflichten[10] harmonisiert wird.

Neben der Kommission können auch Aufsichtsbehörden Standarddatenschutzklauseln annehmen und durch das Ausschußverfahren durch die Kommission genehmigen lassen (Art. 46 Abs. 2 lit. d). Auch Verantwortliche oder Auftragsverarbeiter können eigene Vertragsklauseln für den Drittlandtransfer entwickeln und durch die zuständige Aufsicht genehmigen lassen (Art. 46 Abs. 3 lit. a). Ähnliche Initiativen bestehen bereits im derzeitigen Rechtsrahmen.[11] Die bestehenden EU-Standardvertragsklauseln[12] behalten weiterhin ihre Gültigkeit, bis sie durch Beschluss der Kommission geändert, ersetzt oder aufgehoben werden oder durch ein Urteil des EuGH für ungültig erklärt werden.[13] Im öffentlichen Be-

---

7 Für die Aufsichtsbehörden, die nicht am Anerkennungsverfahren teilnehmen.

8 http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.

9 Nach derzeitiger Begrifflichkeit „EU-Standardvertragsklauseln“.

10 EU Commission, Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries, abrufbar unter http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf.

11 Vgl. Microsoft, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf oder Amazon AWS, https://blogs.aws.amazon.com/security/post/Tx3QAALRNBIK9K1/Customer-Update-AWS-and-EU-Safe-Harbor.

12 Controller-to-Controller (Entscheidung 2001/497/EG, "Set I." bzw. 2004/915/EG, Set II.; Controller-to-Processor (Entscheidung 2010/87/EU).

13 Vgl. jüngste Vorlageentscheidung des Irish Data Protection Commissioners, https://www.dataprotection.ie/docs/25-05-2016-Statement-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-and-Referral-to-the-CJEU/1570.htm.

reich können von der Aufsicht genehmigte **Verwaltungsvereinbarungen** Datentransfers an Stellen außerhalb der EU legitimieren (Art. 46 Abs. 3).

VI. Zertifizierung und Verhaltensregeln

Ein angemessenes Schutzniveau im Drittland oder bei der internationalen Organisation soll auch durch genehmigte **Verhaltensregeln** gem. Art. 40 oder genehmigte **Zertifizierungsverfahren** nach Art. 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters im Drittland zur Anwendung der geeigneten Garantien, einschließlich der Rechte der Betroffenen (vgl. Art. 46 Abs. 2 lit. e und f), hergestellt werden können. Verhaltensregeln können grundsätzlich durch Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, ausgearbeitet und der zuständigen Aufsicht vorgelegt werden.

Stellen, die Zertifizierungsverfahren betreiben, müssen durch eine nationale Akkreditierungsstelle akkreditiert werden, bevor ihre Verfahren besiegelte Zusicherungen nach der DS-GVO geben können. Bezüglich der Art der im jeweiligen Verfahren verwendeten Garantien für den Drittlandtransfer schweigt sich die DS-GVO aus, so dass in einer Gesamtschau durch eine Akkreditierungsstelle bzw. eine Aufsicht zu beurteilen ist, ob die getroffenen vertraglichen oder sonstigen verbindlichen Maßnahmen als ausreichend zu erachten sind.

VII. Ausnahmen vom angemessenen Schutzniveau

Auch die DS-GVO enthält **Ausnahmen** vom grundsätzlich geforderten angemessenen Schutzniveau beim Datenempfänger außerhalb des Europäischen Wirtschaftsraums. Diese Ausnahmen entsprechen im Wesentlichen denen des Art. 26 Abs. 1 der EU-Datenschutzrichtlinie, der über § 4c Einzug in das Bundesdatenschutzgesetz (BDSG) gehalten hat. Hinweise zu Datenübermittlungen auf Basis von Art. 26 Abs. 1 der EU-Datenschutzrichtlinie finden sich auf europäischer Ebene in Arbeitsunterlagen bzw. Stellungnahmen der Artikel 29-Datenchutzgruppe[14], die auf Grund des ähnlichen Gesetzeswortlauts in weiten Teilen auch bei Anwendung der DS-GVO herangezogen werden können.

Änderungen ergeben sich bei der **Einwilligung** (Art. 49 Abs. 1 lit. a), die nunmehr **ausdrücklich** erteilt werden muss und über bestehende mögliche Risiken für Datenübermittlungen ohne begleitende Schutzmaßnahmen des Kapitel V zu unterrichten hat.

Der Export personenbezogener Daten zu **Prozesszwecken in die USA** wird durch die DS-GVO nur noch eingeschränkt möglich sein. Art. 48 verlangt, dass jeglicher Datenfluss in ein Drittland, der auf dem Urteil eines Gerichts oder einer anderen Entscheidung einer Verwaltungsbehörde im Drittland basiert, nur dann anerkannt und vollstreckbar werden soll, wenn ihm eine **internationale Übereinkunft**, so beispielsweise ein Rechtshilfeabkommen, zwischen dem ersuchenden Drittland und der Europäischen Union oder einem

[14] WP 114; WP 12 S. 26 ff.

Mitgliedstaat, zu Grunde liegt. Verfahren, die in Ländern wie den USA als **„Pre-Trial Discovery of Documents“** bezeichnet werden, erfüllen derzeit nicht die Vorgaben des Art. 48 DS-GVO, da sie nicht durch ein Rechtshilfeabkommen mit der Bundesrepublik Deutschland begleitet werden.[15]

Für den Fall, dass keine der Ausnahmen für die Datenübermittlung greift, kein Angemessenheitsbeschluss der Kommission vorliegt und keine Garantien des Art. 46 Abs. 2 zu Gunsten des Betroffenen geschaffen werden können, ermöglicht Art. 49 Abs. 1 eine **einmalige Datenübermittlung** in ein Drittland oder eine internationale Organisation ohne angemessenes Schutzniveau, vorausgesetzt diese betrifft nur eine **begrenzte Zahl von betroffenen Personen**, ist zur Wahrung der **zwingenden berechtigten Interessen** des Verantwortlichen erforderlich, die den Interessen oder Rechten und Freiheiten des Betroffenen **überwiegen** und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf Grundlage der Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Welche Garantien als angemessen zu erachten sind, spezifiziert die DS-GVO nicht. Diese können grundsätzlich vertraglicher, aber auch technisch-organisatorischer Natur sein.

In welchem Umfang diese Ausnahme für Datenverarbeiter nutzbar ist, ist offen. Sie sollte jedenfalls nur für **außergewöhnliche Umstände** gelten, in denen ein Datenexport in ein Drittland realisiert werden muss. Hierbei ist im Sinne der **Rechenschaftspflicht** des Art. 5 Abs. 2 darauf zu achten, dass die geforderten berechtigten Interessen und realisierten Garantien ausreichend **dokumentiert** sind. Ferner sind die zuständige Aufsichtsbehörde und der Betroffene von der Übermittlung in Kenntnis zu setzen, wobei dem Betroffenen - neben den Informationspflichten des Art. 13 - die verfolgten zwingenden berechtigten Interessen zu kommunizieren sind.

Bonn, 22. Juli 2016

[15] Deutlmoser/Filip, ZD-Beilage 6/2012, 11.