Stellungnahme des EDSA nach Artikel 64 DSGVO

Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben

Angenommen am 7. Oktober 2024

Zusammenfassung

Die dänische Aufsichtsbehörde ersuchte den EDSA um eine Stellungnahme zu Angelegenheiten mit allgemeiner Geltung gemäß Artikel 64 Absatz 2 DSGVO. Die Stellungnahme trägt zu einer harmonisierten Auslegung bestimmter Aspekte von Artikel 28 DSGVO – gegebenenfalls in Verbindung mit Kapitel V DSGVO – durch die nationalen Aufsichtsbehörden bei. Die Stellungnahme befasst sich insbesondere mit Fragen zur Auslegung bestimmter Pflichten Verantwortlicher, die Auftragsverarbeiter und Unterauftragsverarbeiter nutzen. Diese ergeben sich vor allem aus Artikel 28 DSGVO sowie aus dem Wortlaut von Auftragsverarbeitungsvereinbarungen. Die Fragen betreffen sowohl die Verarbeitung personenbezogener Daten im EWR als auch die Verarbeitung nach einer Übermittlung in ein Drittland.

Der Ausschuss kommt in dieser Stellungnahme zu dem Schluss, dass die Verantwortlichen die Informationen über die Identität (d. h. Name, Anschrift, Ansprechpartner(in)) aller Auftragsverarbeiter, Unterauftragsverarbeiter usw. jederzeit zur Verfügung haben sollten, damit sie ihren Verpflichtungen gemäß Artikel 28 DSGVO unabhängig von dem mit der Verarbeitungstätigkeit verbundenen Risiko bestmöglich nachkommen können. Zu diesem Zweck sollte der Auftragsverarbeiter dem Verantwortlichen all diese Informationen proaktiv zur Verfügung stellen und sie stets auf dem neuesten Stand halten.

Gemäß Artikel 28 Absatz 1 DSGVO sind Verantwortliche verpflichtet, nur Auftragsverarbeiter in Anspruch zu nehmen, die „hinreichend Garantien“ dafür bieten, dass „geeignete“ Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Der EDSA ist in seiner Stellungnahme der Auffassung, dass die Aufsichtsbehörden bei der Bewertung der Einhaltung dieser Verpflichtung und des Grundsatzes der Rechenschaftspflicht (Artikel 24 Absatz 1 DSGVO) durch die Verantwortlichen berücksichtigen sollten, dass die Inanspruchnahme von Auftragsverarbeitern nicht zu einer Senkung des Schutzniveaus für die Rechte der betroffenen Personen führen sollte. Die *Verpflichtung* des Verantwortlichen zu überprüfen, ob die (Unter-)Auftragsverarbeiter „hinreichend Garantien“ für die Durchführung der vom Verantwortlichen festgelegten geeigneten Maßnahmen bieten, sollte unabhängig von dem Risiko für die Rechte und Freiheiten der betroffenen Personen gelten. Der *Umfang* dieser Überprüfung wird jedoch in der Praxis je nach Art dieser technischen und organisatorischen Maßnahmen variieren und kann je nach Höhe des Risikos strenger oder umfangreicher sein.

Der EDSA führt in der Stellungnahme weiter aus, dass der ursprüngliche Auftragsverarbeiter zwar sicherstellen sollte, dass er Unterauftragsverarbeiter vorschlägt, die hinreichende Garantien bieten, dass jedoch die endgültige Entscheidung über die Beauftragung eines bestimmten Unterauftragsverarbeiters und die damit verbundene Verantwortung, auch in Bezug auf die Überprüfung der Garantien, beim Verantwortlichen verbleibt. Die Aufsichtsbehörden sollten bewerten, inwiefern der Verantwortliche nachweisen kann, dass die Überprüfung der Angemessenheit der von seinen (Unter-)Auftragsverarbeitern gebotenen Garantien zur Zufriedenheit des Verantwortlichen erfolgt ist. Der Verantwortliche kann sich auf die von seinem Auftragsverarbeiter erhaltenen Informationen verlassen und bei Bedarf darauf aufbauen (z. B. wenn sie unvollständig oder ungenau erscheinen oder Fragen aufwerfen). Insbesondere sollte der Verantwortliche bei

Verarbeitungsvorgängen, die ein hohes Risiko für die Rechte und Freiheiten betroffener Personen darstellen, seine Überprüfung insbesondere hinsichtlich der bereitgestellten Informationen vertiefen. In diesem Zusammenhang ist der EDSA der Ansicht, dass der Verantwortliche gemäß der DSGVO nicht verpflichtet ist, die Unterauftragsverarbeitungsvereinbarungen systematisch anzufordern, um zu prüfen, inwiefern die im ursprünglichen Vertrag vorgesehenen Datenschutzverpflichtungen in der Verarbeitungskette weitergereicht wurden. Der Verantwortliche sollte von Fall zu Fall prüfen, ob eine Kopie solcher Vereinbarungen anzufordern oder zu überprüfen ist, damit er die Einhaltung seiner Rechenschaftspflicht nachweisen kann.

Erfolgt die Übermittlung personenbezogener Daten außerhalb des EWR zwischen zwei (Unter-)Auftragsverarbeitern gemäß den Weisungen des Verantwortlichen, so unterliegt der Verantwortliche auch den Pflichten nach Artikel 28 Absatz 1 DSGVO in Bezug auf „hinreichende Garantien", neben den Pflichten nach Artikel 44, um sicherzustellen, dass das durch die DSGVO garantierte Schutzniveau nicht durch die Übermittlung personenbezogener Daten untergraben wird. Der Auftragsverarbeiter/Exporteur sollte die einschlägige Dokumentation im Einklang mit der Rechtsprechung und den Erläuterungen in den Empfehlungen 01/2020 des EDSA erstellen. Der Verantwortliche sollte diese Dokumentation prüfen und der zuständigen Aufsichtsbehörde vorlegen können. Der Verantwortliche kann sich auf die vom Auftragsverarbeiter/Exporteur erhaltenen Dokumentationen oder Informationen stützen und bei Bedarf darauf aufbauen. Der Umfang und die Ausgestaltung der Pflicht des Verantwortlichen, diese Dokumentation zu prüfen, können davon abhängen, auf welcher Grundlage die Übermittlung erfolgt und ob es sich um eine Erst- oder eine Weiterübermittlung handelt.

Der EDSA befasst sich in der Stellungnahme auch mit einer Frage zur Formulierung von Auftragsverarbeitungsvereinbarungen. Ein grundlegendes Element in diesem Zusammenhang ist die Verpflichtung des Auftragsverarbeiters, personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, „*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, [zur Verarbeitung] verpflichtet ist*" (Artikel 28 Absatz 3 Buchstabe a DSGVO). Darin spiegelt sich der Grundsatz wider, dass Verträge das Gesetz nicht außer Kraft setzen können. Angesichts der Vertragsfreiheit, welche es den Parteien überlässt, ihre Auftragsverarbeitungsvereinbarung innerhalb der Grenzen von Artikel 28 Absatz 3 DSGVO an die jeweiligen Gegebenheiten anzupassen, ist der EDSA der Auffassung, dass die Aufnahme der Formulierung „*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*" (wörtlich übernommen oder sehr ähnlich formuliert) dringend zu empfehlen, aber nicht verpflichtend ist.

Was Varianten wie „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*" angeht, ist der EDSA der Ansicht, dass dies von der Vertragsfreiheit umfasst ist und an sich nicht gegen Artikel 28 Absatz 3 Buchstabe a DSGVO verstößt. Gleichzeitig weist der EDSA in seiner Stellungnahme auf eine Reihe von Problemen hin, da eine solche Klausel den Auftragsverarbeiter nicht von der Einhaltung seiner Verpflichtungen gemäß der DSGVO entbindet.

Für personenbezogene Daten, die außerhalb des EWR übermittelt werden, hält es der EDSA für unwahrscheinlich, dass die Formulierung „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*" für sich genommen ausreicht,

um die Anforderungen von Artikel 28 Absatz 3 Buchstabe a DSGVO in Verbindung mit Kapitel V zu erfüllen. Wie aus den Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer und den Empfehlungen zu verbindlichen internen Datenschutzvorschriften („binding corporate rules" – „BCR") des Verantwortlichen („Empfehlungen für BCR für Verantwortliche") hervorgeht, hindert Artikel 28 Absatz 3 Buchstabe a DSGVO nicht grundsätzlich daran, in den Vertrag Bestimmungen aufzunehmen, die sich auf die Anforderungen des Rechts eines Drittlandes an die Verarbeitung der übermittelten personenbezogenen Daten beziehen. Wie auch in diesen Dokumenten sollte jedoch unterschieden werden zwischen den Rechtsvorschriften des Drittlandes, die das von der DSGVO garantierte Schutzniveau untergraben würden, und solchen, die dies nicht tun. Schließlich erinnert der EDSA daran, dass die Möglichkeit, dass das Recht eines Drittlandes die Einhaltung der DSGVO behindert, von den Parteien vor Abschluss des Vertrags (zwischen dem Verantwortlichen und dem Auftragsverarbeiter oder zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter) berücksichtigt werden sollte.

Wenn der Auftragsverarbeiter personenbezogene Daten innerhalb des EWR verarbeitet, kann er sich unter bestimmten Umständen dennoch dem Recht eines Drittlandes gegenübersehen. Der EDSA unterstreicht, dass die Aufnahme eines Wortlauts in den Vertrag, der so ähnlich lautet wie „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*", den Auftragsverarbeiter nicht von seinen Verpflichtungen gemäß der DSGVO entbindet.

Schließlich ist der EDSA der Auffassung, dass die Verpflichtung des Auftragsverarbeiters, nur auf Grundlage dokumentierter Weisungen zu verarbeiten, die Nutzung der Formulierung „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*" (wörtlich übernommen oder sehr ähnlich formuliert) nicht als dokumentierte Weisung des Verantwortlichen verstanden werden kann.

Inhalt

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 63 und Artikel 64 Absatz 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO, im Folgenden „DSGVO"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 11 und Artikel 22 seiner Geschäftsordnung –

in Erwägung nachstehender Gründe:

(1) Die wesentliche Aufgabe des Europäischen Datenschutzausschusses (im Folgenden der „Ausschuss" oder der „EDSA") besteht darin, die kohärente Anwendung der DSGVO im gesamten Europäischen Wirtschaftsraum („EWR") sicherzustellen. Nach Artikel 64 Absatz 2 der DSGVO können jede Aufsichtsbehörde, der Vorsitz des Ausschusses oder die Kommission beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem EWR-Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten. Diese Stellungnahme dient der Prüfung einer Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat.

(2) Die Stellungnahme des Ausschusses wird gemäß Artikel 64 Absatz 3 der DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSA binnen acht Wochen ab dem ersten Arbeitstag nach dem Beschluss des Vorsitzes und der zuständigen Aufsichtsbehörden über die Vollständigkeit des Dossiers angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden.

HAT FOLGENDE STELLUNGNAHME ERLASSEN:

1 EINLEITUNG

1.1 Zusammenfassung des Sachverhalts

1. Am 5. Juli 2024 ersuchte die dänische Aufsichtsbehörde (im Folgenden „DK-AB") den Europäischen Datenschutzausschuss (im Folgenden „EDSA" oder „Ausschuss") um eine Stellungnahme zu den Rechenschaftspflichten der Verantwortlichen in Bezug auf die Verarbeitungskette und die Beziehung zwischen den Verantwortlichen und ihren (Unter-)Auftragsverarbeitern (im Folgenden das „Ersuchen").

[1] Soweit in dieser Stellungnahme auf „Mitgliedstaaten" Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten" zu verstehen. Soweit in dieser Stellungnahme auf die „Union" Bezug genommen wird, ist dies als Bezugnahme auf den „EWR" zu verstehen.

2. Die dänische Aufsichtsbehörde erklärte das Dossier am 8. Juli 2024 für vollständig. Der Vorsitzende des Ausschusses erklärte das Dossier am 9. Juli 2024 für vollständig. Am selben Tag wurde das Dossier vom Sekretariat des EDSA verbreitet. Angesichts der Komplexität der Angelegenheit beschloss der Vorsitz, die gesetzliche Frist im Einklang mit Artikel 64 Absatz 3 der DSGVO und Artikel 10 Absatz 4 der Geschäftsordnung zu verlängern.

3. Die DK-AB verweist in ihrem Ersuchen auch auf den vom EDSA im Januar 2023 angenommenen Bericht über die Ergebnisse seiner ersten koordinierten Durchsetzungsmaßnahme[2] innerhalb des Rahmens für die koordinierte Durchsetzung („Coordinated Enforcement Framework (CEF)“)[3]. Im Mittelpunkt dieser koordinierten Maßnahme stand die Nutzung von cloudbasierten Diensten durch öffentliche Stellen. In dem Bericht des EDSA wiesen die an der koordinierten Maßnahme teilnehmenden Aufsichtsbehörden auf acht ermittelte Herausforderungen hin, die konkret mit der Nutzung von cloudbasierten Diensten durch öffentliche Stellen verbunden sind. Zudem legten sie eine Liste von Punkten vor, die die einschlägigen Interessenträger bei der Beurteilung von Cloud-Diensten und der Zusammenarbeit mit Cloud-Anbietern berücksichtigen sollten.[4] Während in den meisten dieser Punkte der Umfang der durch die DSGVO auferlegten Verpflichtungen sowohl für die Verantwortlichen als auch für die Auftragsverarbeiter klar ist, bleibt der genaue Umfang bestimmter Verpflichtungen im Rahmen der DSGVO nach Auffassung der DK-AB unklar[5].

Die dänische Aufsichtsbehörde (DK-AB) stellte die folgenden Fragen:

4. Frage 1.1: Folgende Fragen werden vor dem Hintergrund von Artikel 5 Absatz 2 und Artikel 24 Absatz 1 DSGVO gestellt und beziehen sich auf Situationen, in denen ein Auftragsverarbeiter mit der Verarbeitung im Auftrag des Verantwortlichen beauftragt wird, um die Einhaltung der Bestimmungen u. a. von Artikel 28 Absatz 1 und Artikel 28 Absatz 2 zu dokumentieren (einschließlich der Vorlage von Unterlagen bei der Aufsichtsbehörde bei Kontrollen):

    a. Muss der Verantwortliche alle Unterauftragsverarbeiter des Auftragsverarbeiters, deren Unterauftragsverarbeiter usw. entlang der gesamten Verarbeitungskette kennen oder nur die erste Stufe von Unterauftragsverarbeitern, die vom Auftragsverarbeiter beauftragt werden?

    b. Inwieweit und mit welcher Detailtiefe muss der Verantwortliche Folgendes überprüfen und dokumentieren:

        i. die Hinlänglichkeit der von den Auftragsverarbeitern, deren Unterauftragsverarbeitern usw. gebotenen Garantien,
        ii. den Inhalt der Verträge zwischen dem ursprünglichen Auftragsverarbeiter und den weiteren Auftragsverarbeitern, um festzustellen, ob den weiteren Auftragsverarbeitern gemäß Artikel 28 Absatz 4 DSGVO dieselben Verpflichtungen auferlegt wurden, und
        iii. ob die Auftragsverarbeiter, deren Unterauftragsverarbeiter usw. die Anforderungen des Verantwortlichen gemäß Artikel 28 Absatz 1 erfüllen?

[2] Bericht über die koordinierte Durchsetzungsmaßnahme 2022: Nutzung von cloudbasierten Diensten durch öffentliche Stellen (2022 Coordinated Enforcement Action – Use of cloud-based services by the public sector“), 17. Januar 2023 (im Folgenden „CEF-Bericht über Cloud-Dienste“).

[3] Der Rahmen für die koordinierte Durchsetzung (CEF) wurde vom EDSA im Oktober 2020 eingerichtet, um die Durchsetzung und die Zusammenarbeit zwischen den Aufsichtsbehörden zu rationalisieren. Siehe Dokument des EDSA über den Rahmen für eine koordinierte Durchsetzung der Verordnung 2016/679, angenommen am 20. Oktober 2020, Version 1.1.

[4] CEF-Bericht über Cloud-Dienste, S. 10-20.

[5] Ersuchen, S. 1.

5. Frage 1.2: Bei Übermittlungen oder Weiterleitungen von einem (Unter-)Auftragsverarbeiter an einen anderen (Unter-)Auftragsverarbeiter gemäß den Weisungen des Verantwortlichen: Inwieweit muss der Verantwortliche im Rahmen seiner Verpflichtung nach Artikel 28 Absatz 1 DSGVO in Verbindung mit Artikel 44 DSGVO die Dokumentation von (Unter-)Auftragsverarbeitern bewerten und nachweisen können, dass das Schutzniveau für personenbezogene Daten durch die (Weiter-)Übermittlungen nicht untergraben wird?

6. Frage 1.3: Variiert der Umfang der Verpflichtungen nach Artikel 28 Absätze 1 und 2 DSGVO in Verbindung mit Artikel 5 Absatz 2 und Artikel 24 DSGVO und in Verbindung mit den Antworten auf die Fragen 1.1 und 1.2 je nach dem mit der Verarbeitungstätigkeit verbundenen Risiko? Wenn ja: Welchen Umfang haben diese Verpflichtungen bei Verarbeitungstätigkeiten mit geringem Risiko und welchen Umfang haben sie bei Verarbeitungstätigkeiten mit hohem Risiko?

7. Frage 2: Muss ein Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht eines Mitgliedstaats gemäß Artikel 28 Absatz 3 DSGVO die in Artikel 28 Absatz 3 Buchstabe a vorgesehene Ausnahme „*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*“ (wörtlich übernommen oder sehr ähnlich formuliert) enthalten, um mit der DSGVO in Einklang zu stehen?

8. Frage 2a: Wenn Frage 2 verneint wird, ist es für sich genommen ein Verstoß gegen Artikel 28 Absatz 3 Buchstabe a DSGVO, wenn ein Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht eines Mitgliedstaats die Ausnahme nach Artikel 28 Absatz 3 Buchstabe a DSGVO auf das Recht von Drittländern im Allgemeinen ausweitet (z. B. „sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist“)?

9. Frage 2b: Wenn Frage 2a verneint wird, sollte eine solche erweiterte Ausnahme stattdessen als dokumentierte Weisung des Verantwortlichen im Sinne von Artikel 28 Absatz 3 Buchstabe a DSGVO verstanden werden?

1.2 Zulässigkeit des Ersuchens um Stellungnahme nach Artikel 64 Absatz 2 DSGVO

10. Gemäß Artikel 64 Absatz 2 der DSGVO kann insbesondere jede Aufsichtsbehörde beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten.

11. Die ersten von der dänischen Aufsichtsbehörde (DK-AB) vorgelegten Fragen beziehen sich auf die Rechenschaftspflicht der Verantwortlichen gemäß Artikel 28 DSGVO (Fragen 1.1, 1.2 und 1.3), während sich die letzte Frage auf den konkreten Inhalt des Vertrags oder Rechtsinstruments zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Buchstabe a DSGVO bezieht (Frage 2).

12. Der Ausschuss ist der Ansicht, dass diese Fragen mit der Auslegung der DSGVO zusammenhängen, insbesondere im Hinblick auf die Beziehung zwischen den Verantwortlichen und deren (Unter-)Auftragsverarbeitern sowie hinsichtlich der Auslegung von Artikel 5 Absatz 2, Artikel 24 und Artikel 28 DSGVO. Das Ersuchen bezieht sich zum einen auf die Rechenschaftspflicht der Verantwortlichen und den Umfang der Dokumentation, die die Aufsichtsbehörden von den Verantwortlichen erwarten sollten, die (Unter-)Auftragsverarbeiter mit der Durchführung von Verarbeitungstätigkeiten in ihrem Namen beauftragen, und zum anderen auf den Inhalt der Verträge oder der Rechtsinstrumente zwischen dem Verantwortlichen und dem Auftragsverarbeiter. Daher betrifft dieses Ersuchen eine „*Angelegenheit mit allgemeiner Geltung*“ im Sinne von Artikel 64 Absatz 2 DSGVO.

13. Darüber hinaus ist der Ausschuss der Auffassung, dass das Ersuchen der DK-AB im Einklang mit Artikel 10 Absatz 3 der Geschäftsordnung des EDSA begründet ist, da die DK-AB Argumente für die Notwendigkeit einer einheitlichen Auslegung der im Ersuchen behandelten Fragen angeführt hat.

14. Gemäß Artikel 64 Absatz 3 DSGVO gibt der EDSA keine Stellungnahme ab, wenn er bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat[6]. Der EDSA hat die Fragen, die sich aus dem Ersuchen der DK-AB ergeben, noch nicht beantwortet. Darüber hinaus bieten die verfügbaren EDSA-Leitlinien, insbesondere die EDSA-Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter"[7] (im Folgenden „EDSA-Leitlinien 07/2020"), zwar einige Anhaltspunkte für den Umfang der Rechenschaftspflicht des Verantwortlichen gemäß Artikel 28 DSGVO, doch gehen sie nicht vollständig auf alle im Ersuchen aufgeworfenen Fragen ein[8]. Konkret geht beispielsweise die zu Artikel 28 Absatz 3 Buchstabe a DSGVO verfügbare Leitlinie nicht speziell auf die im Ersuchen der DK-AB enthaltene Frage ein, ob der Wortlaut *„sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist"* in Verträge oder Rechtsinstrumente zwischen Verantwortlichen und Auftragsverarbeitern aufzunehmen ist.

15. Aus diesen Gründen ist der Ausschuss der Auffassung, dass der Antrag der DK-AB zulässig ist und dass die Fragen, die sich aus dem Ersuchen der dänischen Aufsichtsbehörde ergeben, in einer gemäß Artikel 64 Absatz 2 DSGVO angenommenen Stellungnahme zu beleuchten sind.

2 BEGRÜNDETHEIT DES ERSUCHENS

2.1 Zur Auslegung von Artikel 28 Absatz 1, Artikel 28 Absatz 2 und Artikel 28 Absatz 4 DSGVO in Verbindung mit Artikel 5 Absatz 2 und Artikel 24 Absatz 1 (Fragen 1.1 und 1.3)

16. Dieser Abschnitt befasst sich mit den Fragen 1.1 und 1.3, die dem Ausschuss vorgelegt wurden und die im obigen Abschnitt „Zulässigkeit des Ersuchens" wiedergegeben sind.

17. Artikel 28 DSGVO regelt die Beziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter und erlegt den Verantwortlichen und den Auftragsverarbeitern direkte Verpflichtungen auf. Einleitend sei darauf hingewiesen, dass der Begriff „Auftragsverarbeiter" in Artikel 4 Nr. 8 DSGVO allgemein definiert ist und sowohl den ursprünglichen Auftragsverarbeiter, der direkt von dem Verantwortlichen beauftragt wird, als auch den Auftragsverarbeiter des Auftragsverarbeiters und so weiter entlang der Verarbeitungskette umfasst.

18. Der EDSA unterstreicht, dass die Bewertung der Rolle der Parteien (und ob sie als alleinige oder gemeinsam Verantwortliche oder als Auftragsverarbeiter handeln) nicht in den Anwendungsbereich des Ersuchens fällt. Der EDSA erinnert daran, dass es in erster Linie den Parteien obliegt, ihre tatsächliche Rolle in Abhängigkeit von den faktischen Gegebenheiten oder Umständen des Falles zu

[6] Artikel 64 Absatz 3 der DSGVO und Artikel 10 Absatz 4 der Geschäftsordnung des EDSA.
[7] Leitlinien 07/2020 des EDSA zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Version 2.1, angenommen am 7. Juli 2021.
[8] Siehe insbesondere die EDSA-Leitlinien 07/2020, Abschnitt 1.1 „Auswahl des Auftragsverarbeiters" auf Seite 36, Unterabschnitt 1.3.4 *„Der Auftragsverarbeiter muss die in Artikel 28 Absätze 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhalten (Artikel 28 Absatz 3 Buchstabe d DSGVO)"* auf Seite 44, Abschnitt 1.6 „Unterauftragsverarbeiter" auf Seite 49.

beurteilen[9], unbeschadet der Zuständigkeit der Aufsichtsbehörde zu prüfen, ob ihre Einschätzung zutrifft.

19. In Anbetracht der obigen Fragen konzentriert sich diese Stellungnahme ausschließlich auf den Anwendungsbereich und den Umfang der Verpflichtungen des Verantwortlichen gemäß Artikel 28 Absatz 1 DSGVO, zu überprüfen, ob die (Unter-)Auftragsverarbeiter „hinreichende Garantien" gemäß Artikel 28 Absatz 2 bieten, sowie auf die damit verbundene Rechenschaftspflicht des Verantwortlichen gemäß Artikel 5 Absatz 2 und Artikel 24 Absatz 1 DSGVO[10].

20. Darüber hinaus stellt der Ausschuss fest, dass sich die vorstehenden Fragen nicht auf die Haftung des Verantwortlichen gegenüber betroffenen Personen für die in seinem Auftrag durchgeführten Verarbeitungstätigkeiten beziehen, z. B. in Bezug auf das Recht betroffener Personen auf Schadenersatz gemäß Artikel 82 der DSGVO. Dieser Abschnitt konzentriert sich daher darauf, den Aufsichtsbehörden Erläuterungen zur Auslegung von Artikel 28 Absatz 1 und Artikel 28 Absatz 2 DSGVO in Verbindung mit Artikel 5 Absatz 2 und Artikel 24 DSGVO in Bezug auf bestimmte Verpflichtungen an die Hand zu geben, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben. Für die Beantwortung dieser Fragen wird der Ausschuss eine Bewertung durchführen, die sich auf Situationen konzentriert, in denen keine Übermittlung personenbezogener Daten in Länder außerhalb des EWR erfolgt. Im Gegensatz dazu werden im Abschnitt zu Frage 1.2 Situationen bewertet, in denen es zu Übermittlungen in der Verarbeitungskette kommt.

2.1.1 Identifizierung der Akteure entlang der Verarbeitungskette

21. Zu der Frage, ob der Verantwortliche im Wesentlichen alle Unterauftragsverarbeiter des Auftragsverarbeiters, deren Unterauftragsverarbeiter usw. in der gesamten Verarbeitungskette kennen sollte oder nur die erste Ebene der vom Auftragsverarbeiter beauftragten Unterauftragsverarbeiter, erinnert der EDSA zunächst an Folgendes: *„Obwohl die [Verarbeitungs-]Kette recht lang sein mag, behält der Verantwortliche seine zentrale Rolle bei der Bestimmung des Zwecks und der Mittel der Verarbeitung"*[11].

22. Der EDSA versteht die Begriffe „kennen" [eng. „identify"] und „Informationen über die Identität" im Kontext der Beantwortung der Frage dahingehend, dass sie sich auf den Namen, die Anschrift, die Kontaktperson (Name, Position, Kontaktdaten) des Auftragsverarbeiters und die Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Zuständigkeiten, falls mehrere Unterauftragsverarbeiter genehmigt wurden) beziehen.[12]

---

[9] EDSA-Leitlinien 07/2020, Absatz 12.

[10] Diese Frage ist getrennt von allen anderen Verpflichtungen des Verantwortlichen (oder der [Unter-]Auftragsverarbeiter), die Einhaltung der DSGVO zu gewährleisten, z. B. die Einhaltung des Grundsatzes der Rechtmäßigkeit, von Art. 32 oder Kapitel V der DSGVO. Der Verantwortliche kann dennoch für eine Verarbeitung in seiner Funktion als Verantwortlicher verantwortlich sein, die nicht im Einklang mit diesen DSGVO-Bestimmungen steht, selbst wenn er die Verpflichtungen zur Überprüfung seiner (Unter-)Auftragsverarbeiter gemäß Art. 28 Absatz 1 der DSGVO erfüllt hat. Diese Stellungnahme befasst sich nicht mit der Pflicht des Verantwortlichen, andere DSGVO-Bestimmungen als Artikel 24 Absatz 1, Artikel 28 Absatz 1 und Artikel 28 Absatz 2 DSGVO einzuhalten.

[11] EDSA-Leitlinien 07/2020, Absatz 152.

[12] Dies entspricht den Informationen, die für die Identifizierung von Auftragsverarbeitern gemäß Anhang IV der Standardvertragsklauseln der Europäischen Kommission zwischen Verantwortlichen und Auftragsverarbeitern (Durchführungsbeschluss 2021/915 der Kommission vom 4. Juni 2021) und Anhang III der Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer (Durchführungsbeschluss 2021/914 der Kommission vom 4. Juni 2021) erforderlich sind.

23. Hinsichtlich der Auswahl der Auftragsverarbeiter sollten die Verantwortlichen in der Lage sein, die Zwecke und Mittel der Verarbeitung gemäß Artikel 4 Nr. 7 DSGVO selbst festzulegen. In dieser Hinsicht wird die Festlegung der Empfänger (einschließlich der Auftragsverarbeiter) als ein „wesentliches Mittel" der Verarbeitung betrachtet, über das der Verantwortliche entscheidet[13].

24. Zu diesem Zweck ist für die Beauftragung von **weiteren Auftragsverarbeitern** durch den ursprünglichen Auftragsverarbeiter die vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen gemäß Artikel 28 Absatz 2 DSGVO erforderlich. Die EDSA-Leitlinien 07/2020 stellen klar, dass die Pflichten gemäß Artikel 28 Absatz 2 DSGVO „*ausgelöst werden, wenn ein (Unter-)Auftragsverarbeiter beabsichtigt, einen weiteren Akteur in Anspruch zu nehmen, womit ein weiteres Glied in die Kette eingefügt wird, indem ihm Tätigkeiten übertragen werden, die die Verarbeitung personenbezogener Daten erfordern*".[14]

25. Beschließt der Verantwortliche zum Zeitpunkt der Vertragsunterzeichnung bestimmte Unterauftragsverarbeiter zu akzeptieren, so sollte eine Liste der zugelassenen Unterauftragsverarbeiter in den Vertrag oder einen Anhang zum Vertrag aufgenommen werden. Die Liste sollte dann entsprechend der allgemeinen oder gesonderten Genehmigung des Verantwortlichen auf dem neuesten Stand gehalten werden.[15]

26. Hinsichtlich der Beauftragung von Unterauftragsverarbeitern sieht die DSGVO die Möglichkeit einer allgemeinen oder gesonderten Genehmigung vor. **Im Falle einer gesonderten Genehmigung** sollte der Verantwortliche schriftlich festlegen, welcher Unterauftragsverarbeiter für welchen konkreten Verarbeitungsvorgang und welchen Zeitraum zugelassen ist[16]. Wird der Antrag des Auftragsverarbeiters auf eine gesonderte Genehmigung nicht innerhalb der gesetzten Frist beantwortet, sollte er als abgelehnt betrachtet werden[17].

27. **Im Falle einer allgemeinen Genehmigung** sollte der Auftragsverarbeiter dem Verantwortlichen die Möglichkeit geben, zum Zeitpunkt der Unterzeichnung der allgemeinen Genehmigung eine Liste der Unterauftragsverarbeiter zu genehmigen, und ihm die Möglichkeit geben – einschließlich einer ausreichenden Frist –, gegen spätere Änderungen der Unterauftragsverarbeiter Einspruch zu erheben.[18] Die Ausschuss erinnert daran, dass es dem ursprünglichen **Auftragsverarbeiter** obliegen

---

[13] EDSA-Leitlinien 07/2020, Absatz 40.

[14] In den EDSA-Leitlinien 07/2020 heißt es in Absatz 151: „*Datenverarbeitungstätigkeiten werden häufig von einer großen Zahl von Akteuren durchgeführt, und die Ketten der Unterauftragsvergabe werden immer komplexer. Mit der DSGVO werden besondere Pflichten eingeführt, die ausgelöst werden, wenn ein (Unter-)Auftragsverarbeiter beabsichtigt, einen weiteren Akteur in Anspruch zu nehmen, womit ein weiteres Glied in die Kette eingefügt wird, indem ihm Tätigkeiten übertragen werden, die die Verarbeitung personenbezogener Daten erfordern. Die Prüfung der Frage, ob der Diensteanbieter als Unterauftragsverarbeiter auftritt, sollte im Einklang mit den obigen Ausführungen zum Begriff des Auftragsverarbeiters durchgeführt werden*".

[15] EDSA-Leitlinien 07/2020, Absatz 154.

[16] EDSA-Leitlinien 07/2020, Absätze 153 und 155. Gemäß Klausel 7.7 Option 1 der Standardvertragsklauseln der Europäischen Kommission zwischen Verantwortlichen und Auftragsverarbeitern ist die Liste der gesondert vom Verantwortlichen genehmigten Unterauftragsverarbeiter in Anhang IV zu finden, der stets auf dem neuesten Stand zu halten ist.

[17] EDSA-Leitlinien 07/2020, Absatz 155.

[18] Siehe auch EDSA-Leitlinien 7/2020, Absatz 156. „*Alternativ kann der Verantwortliche seine allgemeine Genehmigung zur Inanspruchnahme von Unterauftragsverarbeitern erteilen (im Vertrag, einschließlich einer Liste mit diesen Unterauftragsverarbeitern in einem Anhang) (...)*". Von Bedeutung ist in diesem Zusammenhang auch die Stellungnahme 14/2019 des EDSA zu dem von der dänischen Aufsichtsbehörde vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO). Gemäß Klausel 7.7 Option 2 der Standardvertragsklauseln der Europäischen Kommission zwischen Verantwortlichen und Auftragsverarbeitern

sollte, dem Verantwortlichen **proaktiv bestimmte Informationen zur Verfügung zu stelle**n, und dass *„die Pflicht des Auftragsverarbeiters, den Verantwortlichen über jede Änderung bei den Unterauftragsverarbeitern zu informieren, impliziert, dass der Auftragsverarbeiter solche Änderungen gegenüber dem Verantwortlichen **aktiv** anzeigt oder kennzeichnet*“.[19]

28. Dies bedeutet, dass die Informationen zur Identifizierung aller Unterauftragsverarbeiter des Auftragsverarbeiters für den Verantwortlichen leicht zugänglich sein sollten. Die Identifizierung dieser Akteure ist besonders wichtig, damit der Verantwortliche in der Lage ist, die Kontrolle über seine Verarbeitungstätigkeiten auszuüben, für die er verantwortlich ist, und im Falle eines Verstoßes gegen die DSGVO zur Rechenschaft gezogen werden kann.

29. Der Auftragsverarbeiter sollte daher alle Informationen darüber bereitstellen, wie die Verarbeitungstätigkeit im Auftrag des Verantwortlichen durchgeführt wird, einschließlich Informationen über den eingesetzten Unterauftragsverarbeiter[20] und eine Beschreibung der Verarbeitung, mit der der Unterauftragsverarbeiter betraut ist[21].

30. Weitere rechtliche Gründe rechtfertigen es, dass der Verantwortliche sämtliche Auftragsverarbeiter und Unterauftragsverarbeiter kennen muss. Auftragsverarbeiter, denen Daten offengelegt oder übermittelt werden, gelten als „Empfänger“[22].

    - Um die Transparenzanforderungen gemäß Artikel 13 Absatz 1 Buchstabe e und Artikel 14 Absatz 1 Buchstabe e DSGVO zu erfüllen, sollten die Verantwortlichen die betroffenen Personen über die Datenempfänger oder Kategorien von Datenempfängern informieren und dabei so spezifisch und konkret wie möglich sein[23]. In den Verzeichnissen von Verarbeitungstätigkeiten müssen auch Angaben zu den

besitzt der Auftragsverarbeiter die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind, und unterrichtet den Verantwortlichen im Voraus schriftlich über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern.

[19] EDSA-Leitlinien 07/2020, Absatz 128 (Hervorhebung hinzugefügt). Siehe auch Fußnote 14.

[20] EDSA-Leitlinien 7/2020, Absatz 143.

[21] Siehe z. B. Anhang IV der Standardvertragsklauseln der Europäischen Kommission zwischen Verantwortlichen und Auftragsverarbeitern und Anhang II der Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer.

[22] Art. 4 Nr. 9 DSGVO; WP29-Leitlinien zur Transparenz im Rahmen der Verordnung (EU) 2016/679 („Guidelines on transparency under Regulation 2016/679“), angenommen am 29. November 2017, zuletzt überarbeitet und angenommen am 11. April 2018, WP260 rev.01, gebilligt vom EDSA (im Folgenden „WP29-Transparenzleitlinien“), S. 37.

[23] WP29-Transparenzleitlinien, S. 37 ([aus dem Englischen übersetzt] *„Im Einklang mit dem Grundsatz von Treu und Glauben müssen die Verantwortlichen möglichst zweckdienliche Informationen zu den Empfängern für die betroffenen Personen bereitstellen. In der Praxis werden dies gemeinhin die benannten Empfänger sein, damit die betroffenen Personen genau wissen, wer im Besitz ihrer personenbezogenen Daten ist. Entscheiden sich die Verantwortlichen für die Angabe der Kategorien von Empfängern, sollten diese Informationen unter Angabe der Empfängerart (d. h. der von diesen durchgeführten Aktivitäten), der Industrie, des Sektors und Teilsektors sowie des Standorts der Empfänger so genau wie möglich ausfallen.*“); EDSA-Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1, angenommen am 28. März 2023, (im Folgenden „EDSA-Leitlinien 01/2022 (Auskunftsrecht)“), Absatz 117 („*bereits nach Artikel 13 und 14 DSGVO [sollten] die Angaben zu den Empfängern oder den Kategorien von Empfängern im Sinne der Transparenz und Fairness so konkret wie möglich sein [...].*“); siehe EuGH, Urteil vom 12. Januar 2023, *RW gegen Österreichische Post AG*, Rn. 25; Schlussanträge des GA zu EuGH C-154/21, Rn. 36 („*[Artikel 13 und 14 der DSGVO legen die Pflicht des Verantwortlichen fest], der betroffenen Person Informationen über die Kategorien von Empfängern oder die konkreten Empfänger von sie betreffenden personenbezogenen Daten bereitzustellen, wenn diese Daten bei der betroffenen Person oder nicht bei der betroffenen Person erhoben werden*“).

„Kategorien von Empfängern“ enthalten sein (Artikel 30 Absatz 1 Buchstabe d DSGVO).

- Artikel 15 DSGVO sieht unter anderem das Recht auf Auskunft über die Empfänger oder Kategorien von Empfängern vor, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden[24]. Der Gerichtshof hat klargestellt, dass diese Bestimmung für den Verantwortlichen die Verpflichtung beinhaltet, der betroffenen Person die tatsächliche Identität der Empfänger mitzuteilen[25]. Abgesehen von Fällen, in denen der Verantwortliche der betroffenen Person nur die Kategorien von Empfängern nennen kann, sollte es dem Verantwortlichen grundsätzlich immer möglich sein, die Namen der Empfänger zu erfragen und den betroffenen Personen die erforderlichen Informationen unverzüglich zu übermitteln.

- Artikel 19 DSGVO sieht vor, dass der Verantwortliche allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mitteilt, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der EuGH stellte klar, dass Artikel 19 Satz 2 der betroffenen Person ausdrücklich das Recht einräumt, über die konkreten Empfänger unterrichtet zu werden[26].

31. Auch wenn dies in diesen Bestimmungen nicht ausdrücklich vorgesehen ist, ist der Ausschuss der Ansicht, dass die Verantwortlichen für die Zwecke von Artikel 28 Absätze 1 und 2 DSGVO die Informationen über die Identität aller Auftragsverarbeiter, Unterauftragsverarbeiter usw. jederzeit zur Verfügung haben sollten[27], damit sie ihren Verpflichtungen gemäß den oben genannten Bestimmungen bestmöglich nachkommen können. Eine solche Verfügbarkeit ist auch notwendig, damit die Verantwortlichen alle Informationen erheben und bewerten können, die zur Erfüllung der Anforderungen der DSGVO erforderlich sind, u. a. damit sie Auskunftsersuchen gemäß Artikel 15 DSGVO unverzüglich beantworten und umgehend auf Verletzungen des Schutzes personenbezogener Daten reagieren können, die entlang der Verarbeitungskette auftreten. Dies gilt unabhängig von dem mit der Verarbeitungstätigkeit verbundenen Risiko.

---

[24] Artikel 15 Absatz 1 Buchstabe c DSGVO. EDSA-Leitlinien 01/2022 (Auskunftsrecht), Absätze 116-117.

[25] EuGH, Urteil vom 12. Januar 2023, *RW gegen Österreichische Post AG*, C-154/21, Rn. 51: „*Nach alledem ist auf die Vorlagefrage zu antworten, dass Art. 15 Abs. 1 Buchst. c DSGVO dahin auszulegen ist, dass das in dieser Bestimmung vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten bedingt, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen, es sei denn, dass es nicht möglich ist, die Empfänger zu identifizieren, oder dass der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sind; in diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen.*“.
Der Gerichtshof erkannte an, dass die betroffene Person alternativ entscheiden kann, „*nur Informationen über die Kategorien von Empfängern anzufordern.*“. Urteil des EuGH vom 12. Januar 2023, *RW gegen Österreichische Post AG*, C-154/21, Rn. 43.
EDSA-Leitlinien 01/2022 (Auskunftsrecht), Absatz 117.

[26] Urteil des EuGH vom 12. Januar 2023, *RW gegen Österreichische Post AG*, C-154/21, Rn. 41.

[27] Diese Informationen sind erforderlich, damit der Verantwortliche seine Pflichten auch dann erfüllen kann, wenn die Verarbeitungskette unterbrochen ist, weil ein (Unter-)Auftragsverarbeiter nicht erreichbar, unkooperativ oder zahlungsunfähig ist und ein anderer (Unter-)Auftragsverarbeiter kontaktiert werden muss.

32. Zu diesem Zweck sollte der Auftragsverarbeiter[28] dem Verantwortlichen proaktiv alle Informationen zur Identität aller Auftragsverarbeiter, Unterauftragsverarbeiter usw., die im Auftrag des Verantwortlichen verarbeitend tätig sind, zur Verfügung stellen und diese Informationen über alle beteiligten Unterauftragsverarbeiter jederzeit auf dem neuesten Stand halten. Der Verantwortliche und der Auftragsverarbeiter können in den Vertrag weitere Einzelheiten darüber aufnehmen, wie und in welchem Format der Auftragsverarbeiter diese Informationen bereitstellen soll, da der Verantwortliche möglicherweise ein bestimmtes Format vorgibt, damit er die Informationen leichter abrufen und verwalten kann.

2.1.2 Überprüfung und Dokumentation der Hinlänglichkeit der von allen Auftragsverarbeitern in der Verarbeitungskette gebotenen Garantien durch den Verantwortlichen

33. Die Fragen 1.1.b.i, 1.1.b.iii und 1.3 sollen klären, in welchem Umfang und in welcher Ausführlichkeit der Verantwortliche die Hinlänglichkeit der von allen Auftragsverarbeitern in der Verarbeitungskette bereitgestellten Garantien überprüfen und dokumentieren sollte und inwiefern die Verpflichtungen nach Artikel 28 Absatz 1 und Artikel 28 Absatz 2 DSGVO in Verbindung mit Artikel 5 Absatz 2 und Artikel 24 DSGVO je nach dem mit der Verarbeitungstätigkeit verbundenen Risiko variieren. In Bezug auf diese Fragen hebt der Ausschuss Folgendes hervor:

34. In Artikel 5 Absatz 2 DSGVO ist der Grundsatz der Rechenschaftspflicht verankert, indem der Verantwortliche für die Einhaltung der Datenschutzgrundsätze nach Artikel 5 Absatz 1 DSGVO verantwortlich gemacht wird und in der Lage sein muss, die Einhaltung dieser Grundsätze nachzuweisen. Artikel 5 Absatz 2 DSGVO gilt für alle in Artikel 5 Absatz 1 DSGVO aufgeführten allgemeinen Grundsätze.

35. Artikel 24 Absatz 1 DSGVO enthält die Verpflichtung des Verantwortlichen nachzuweisen, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. Eine der Pflichten, auf die der Grundsatz der Rechenschaftspflicht Anwendung findet, wird jedoch weiterentwickelt: die Umsetzung „geeigneter technischer und organisatorischer Maßnahmen“[29]. Gemäß Artikel 24 Absatz 1 DSGVO ist der Begriff „Risiko“[30] für die Anwendung dieser Bestimmung relevant, da es sich dabei um eines der Kriterien

[28] Zur Einhaltung von Artikel 28 Absatz 2 DSGVO, damit der Verantwortliche über die Hinzuziehung von Unterauftragsverarbeitern entscheiden kann und zur Einhaltung von Artikel 28 Absatz 1 DSGVO, damit der Verantwortliche prüfen kann, ob die (Unter-)Auftragsverarbeiter hinreichende Garantien für die Umsetzung der technischen und organisatorischen Maßnahmen bieten.

[29] Urteil vom 25. Januar 2024, *BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, Rn. 36: „*Art. 24 DSGVO sieht eine allgemeine Verpflichtung des für die Verarbeitung personenbezogener Daten Verantwortlichen vor, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Verarbeitung im Einklang mit der DSGVO erfolgt, und den Nachweis dafür erbringen zu können*“.

[30] In Erwägungsgrund 75 der DSGVO sind einige Beispiele für Risiken aufgeführt: „*wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann*“; Erwägungsgrund 76 legt Folgendes fest: „*Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt*.“ Wie der EuGH zusammengefasst hat, hängen „*[n]ach dem 76. Erwägungsgrund der DSGVO […] außerdem Eintrittswahrscheinlichkeit und Schwere des Risikos von den Besonderheiten der betreffenden Verarbeitung ab und sollte dieses Risiko anhand einer objektiven Bewertung beurteilt werden*.“ (EuGH, Urteil vom 14. Dezember 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, Rn. 36).

handelt, die der Verantwortliche bei der Bewertung der Angemessenheit solcher Maßnahmen berücksichtigen muss[31]. Dort heißt es außerdem, dass diese Maßnahmen erforderlichenfalls überprüft und aktualisiert werden müssen.

36. Wie der EuGH festgestellt hat, *„erlegen Art. 5 Abs. 2 und Art. 24 DSGVO den für die Verarbeitung personenbezogener Daten Verantwortlichen eine allgemeine Rechenschaftspflicht sowie Compliance-Pflichten auf. Insbesondere verpflichten diese Bestimmungen die Verantwortlichen, zur Wahrung des Rechts auf Datenschutz geeignete Maßnahmen zu ergreifen, um etwaigen Verstößen gegen die Vorschriften der DSGVO vorzubeugen." [32].*

37. Der Grundsatz der Rechenschaftspflicht richtet sich an den Verantwortlichen, auch wenn dieser Auftragsverarbeiter oder Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten in seinem Namen betraut hat.

38. Gemäß Artikel 28 Absatz 1 DSGVO darf ein Verantwortlicher, der einen Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten in seinem Namen beauftragt, nur mit einem Auftragsverarbeiter arbeiten, der „*hinreichend Garantien dafür biete[t], dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen*" der DSGVO „*erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet*"[33]. Wie in den EDSA-Leitlinien 07/2020 dargelegt, findet sich der Grundsatz der Rechenschaftspflicht auch in Artikel 28 DSGVO wieder[34].

39. In diesem Zusammenhang weist der EDSA darauf hin, dass die Aufsichtsbehörden bei der Bewertung der Einhaltung von Artikel 24 Absatz 1 und Artikel 28 Absatz 1 DSGVO berücksichtigen sollten, dass **die Beauftragung von Auftragsverarbeitern das Schutzniveau für die Rechte der betroffenen Personen** im Vergleich zu einer Verarbeitung unmittelbar durch den Verantwortlichen nicht mindern sollte. Dies bezieht sich auf die Beauftragung des ursprünglichen Auftragsverarbeiters, aber auch auf die Beauftragung weiterer Auftragsverarbeiter entlang der Verarbeitungskette, z. B. Unterauftragsverarbeiter und Unter-Unterauftragsverarbeiter. Artikel 24 Absatz 1 und Artikel 28 Absatz 1 DSGVO sollten so ausgelegt werden, dass der Verantwortliche sicherstellen muss, dass die Verarbeitungskette nur aus Auftragsverarbeitern, Unterauftragsverarbeitern, Unter-

---

[31] Vgl. Feststellung des EuGH: „*Hierzu führt Art. 24 Abs. 1 DSGVO eine Reihe von Kriterien auf, die für die Beurteilung der Geeignetheit solcher Maßnahmen zu berücksichtigen sind, nämlich Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen*", Urteil vom 14. Dezember 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, Rn. 25. In demselben Urteil hat der EuGH ausgeführt: „*Die Geeignetheit solcher Maßnahmen ist konkret zu bewerten, indem geprüft wird, ob der Verantwortliche diese Maßnahmen unter Berücksichtigung der verschiedenen (...) aufgeführten Kriterien und der Datenschutzbedürfnisse getroffen hat, die speziell mit der betreffenden Verarbeitung sowie den davon ausgehenden Risiken verbunden sind.*", Rn. 30; dies erinnert an das Urteil vom 25. Januar 2024, *BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, Rn. 38: „*Somit ergibt sich aus dem Wortlaut der Art. 24 und 32 DSGVO, dass die Geeignetheit der vom Verantwortlichen umgesetzten Maßnahmen konkret zu bewerten ist, unter Berücksichtigung der verschiedenen in diesen Artikeln aufgeführten Kriterien und der Datenschutzbedürfnisse, die speziell mit der betreffenden Verarbeitung sowie den davon ausgehenden Risiken verbunden sind. Dies gilt umso mehr, als der Verantwortliche die Möglichkeit haben muss, den Nachweis zu erbringen, dass seine Maßnahmen im Einklang mit der DSGVO stehen; diese Möglichkeit bliebe ihm verwehrt, wenn von einer unwiderlegbaren Vermutung ausgegangen würde*". Es sei darauf hingewiesen, dass sich die Analyse des EuGH auch auf Artikel 32 der DSGVO bezieht.

[32] Urteil vom 27. Oktober 2022, *Proximus NV gegen Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, Rn. 81. Siehe auch EDSA-Leitlinien 07/2020, Absatz 9.

[33] EDSA-Leitlinien 07/2020, Absatz 94.

[34] EDSA-Leitlinien 07/2020, Absatz 8.

Unterauftragsverarbeitern (usw.) besteht, die „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen [...] durchgeführt werden“. Zudem sollte der Verantwortliche nachweisen können, dass er alle in der DSGVO vorgesehenen Elemente ernsthaft berücksichtigt hat[35]. Diese Erwägungen gelten auch dann, wenn die Verarbeitungskette lang und komplex sein kann und verschiedene Auftragsverarbeiter, Unterauftragsverarbeiter usw. an verschiedenen Phasen der Verarbeitungstätigkeiten beteiligt sind. Der Verantwortliche sollte bei der Auswahl und Beaufsichtigung seiner Auftragsverarbeiter mit der gebotenen Sorgfalt vorgehen.

40. Bei der Wahl des **ursprünglichen Auftragsverarbeiters** sollte der Verantwortliche von Fall zu Fall unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen auf der Grundlage der Art der dem Auftragsverarbeiter anvertrauten Verarbeitung prüfen, ob die gebotenen Garantien hinreichend sind[36]. Gemäß Artikel 28 Absatz 5 DSGVO kann die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DSGVO durch einen Auftragsverarbeiter als Faktor herangezogen werden, um hinreichende Garantien nachzuweisen.

41. Wie der EDSA bereits erwähnt hat, sollte der Verantwortliche bei der Überprüfung der von den Auftragsverarbeitern gebotenen Garantien verschiedene Elemente berücksichtigen[37], und häufig ist ein Austausch einschlägiger Unterlagen erforderlich[38]. In jedem Fall gilt: „*Die Garantien, die der Auftragsverarbeiter ‚bietet‘, sind diejenigen, die der Auftragsverarbeiter zur Zufriedenheit des Verantwortlichen nachweisen kann, da diese die einzigen Garantien sind, die der Verantwortliche bei der Prüfung der Erfüllung seiner Pflichten wirksam berücksichtigen kann*“[39]. Weder Artikel 28 Absatz 1 DSGVO selbst noch frühere Dokumente des EDSA enthalten eine erschöpfende Liste der Dokumente oder Maßnahmen, die der Auftragsverarbeiter vorlegen oder nachweisen sollte, da dies weitgehend von den spezifischen Umständen der Verarbeitung abhängt[40]. Beispielsweise kann der Verantwortliche beschließen, einen Fragebogen zu erstellen, um Informationen von seinem Auftragsverarbeiter einzuholen und die einschlägigen Garantien zu überprüfen, die entsprechenden Unterlagen anzufordern, sich auf öffentlich zugängliche Informationen und/oder Zertifizierungen oder Prüfberichte vertrauenswürdiger Dritter zu stützen und/oder Prüfungen vor Ort durchzuführen.

42. Der EDSA hat bereits klargestellt, dass es sich bei der in Artikel 28 Absatz 1 DSGVO enthaltenen Verpflichtung, nur Auftragsverarbeiter zu nutzen, die „hinreichende Garantien bieten“, um eine

[35] EDSA-Leitlinien 07/2020, Absatz 94.
[36] EDSA-Leitlinien 07/2020, Absatz 96.
[37] EDSA-Leitlinien 07/2020, Absätze 97-98 (betreffend das Fachwissen, die Zuverlässigkeit und die Ressourcen des Auftragsverarbeiters sowie den Ruf des Auftragsverarbeiters auf dem Markt und die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsmechanismus).
[38] EDSA-Leitlinien 07/2020, Absatz 95 (wo einige Beispiele angeführt werden: Datenschutzerklärung, Dienstleistungsbedingungen, Verzeichnis von Verarbeitungstätigkeiten, Richtlinien zum Dokumentenmanagement, Informationssicherheitskonzept, Berichte über externe Datenschutzaudits, anerkannte internationale Zertifizierungen wie die ISO 27000-Reihe).
[39] EDSA-Leitlinien 07/2020, Absatz 95.
[40] EDSA-Leitlinien 07/2020, Absatz 96: „*Die Beurteilung durch den Verantwortlichen, ob die Garantien hinreichend sind, ist eine Form der Risikobeurteilung, die in hohem Maße von der Art der dem Auftragsverarbeiter anvertrauten Verarbeitung abhängt und von Fall zu Fall unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen erfolgen muss. Folglich kann der EDSA keine abschließende Liste der Dokumente oder Maßnahmen bereitstellen, die der Auftragsverarbeiter in einem bestimmten Szenario vorlegen oder nachweisen muss, da dies weitgehend von den besonderen Umständen der Verarbeitung abhängt*“.

kontinuierliche Verpflichtung handelt und dass der Verantwortliche in angemessenen Abständen die Garantien des Auftragsverarbeiters kontrollieren sollte[41].

43. Im Hinblick auf die von der dänischen Aufsichtsbehörde in ihrem Ersuchen aufgeworfene Frage 1.3 bezüglich des mit der Verarbeitung verbundenen Risikos betont der EDSA, dass der Begriff „Risiko" in einer Reihe von Bestimmungen der DSGVO eine wichtige Rolle spielt, insbesondere in den Bestimmungen, die sich auf Kapitel IV der DSGVO beziehen[42].

44. Es ist wichtig zu betonen, dass der Verweis auf das „Risiko" in Artikel 24 Absatz 1 und Erwägungsgrund 74 DSGVO nicht so ausgelegt werden sollte, dass der Verantwortliche seine Verpflichtungen aus der DSGVO vernachlässigen oder von ihnen abweichen kann, nur weil er das Risiko für die Rechte und Freiheiten der betroffenen Personen als „gering" einstuft. Die Verpflichtung, „geeignete technische und organisatorische Maßnahmen" zu ergreifen, um die Einhaltung der DSGVO gemäß Artikel 24 Absatz 1 DSGVO zu gewährleisten, gilt immer, doch die Maßnahmen, die erforderlich sind, um dies zu erreichen, können je nach Risiko variieren.[43]

45. Auch wenn in Artikel 28 Absatz 1 DSGVO nicht ausdrücklich auf das „Risiko" Bezug genommen wird, impliziert diese Bestimmung die Notwendigkeit, das Ausmaß des Risikos für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen. Die Anforderung in Artikel 28 Absatz 1, nur Auftragsverarbeiter einzusetzen, die „hinreichende Garantien" für die Durchführung „geeigneter technischer und organisatorischer Maßnahmen" bieten, sollte dahingehend verstanden werden, dass zu prüfen ist, ob die Auftragsverarbeiter hinreichende Garantien für die Durchführung solcher Maßnahmen im Hinblick auf die Risiken der Verarbeitung bieten, da beispielsweise das Niveau der zu ergreifenden Sicherheitsmaßnahmen auch von den Risiken abhängt.

46. Das mit der Verarbeitungstätigkeit verbundene Risiko spielt eine wichtige Rolle bei der Bestimmung der Geeignetheit der technischen und organisatorischen Maßnahmen, zusammen mit den anderen in Artikel 24 Absatz 1 DSGVO genannten Kriterien[44]. Je nach Höhe des mit der Verarbeitungstätigkeit verbundenen Risikos (z. B. wenn besondere Kategorien personenbezogener Daten verarbeitet werden) kann der Verantwortliche strengere oder umfangreichere technische und organisatorische Maßnahmen festlegen. Jeder Auftragsverarbeiter sollte daher hinreichende Garantien bieten, um die von dem Verantwortlichen festgelegten „geeigneten" Maßnahmen wirksam umzusetzen.

47. Der Ausschuss ist der Auffassung, dass **die *Verpflichtung* des Verantwortlichen, zu überprüfen, ob die (Unter-)Auftragsverarbeiter hinreichende Garantien für die Umsetzung der von dem Verantwortlichen festgelegten Maßnahmen bieten, unabhängig von dem Risiko für die Rechte und Freiheiten der betroffenen Personen gelten sollte.**

48. **Der *Umfang* dieser Überprüfung wird jedoch in der Praxis variieren, je nach Art dieser organisatorischen und technischen Maßnahmen, die der Verantwortliche unter anderem auf der**

[41] EDSA-Leitlinien 07/2020, Absatz 99: „*gegebenenfalls auch durch Überprüfungen und Inspektionen*".
[42] Der Begriff „Risiko" wird in den Artikeln 24, 25, 27, 30, 32, 33, 34, 35, 36 und 39 DSGVO verwendet.
[43] EuGH, Urteil vom 14. Dezember 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, Rn. 35: „*Zudem sollte der Verantwortliche nach dem 74. Erwägungsgrund der DSGVO geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit der DSGVO stehen und die Maßnahmen auch wirksam sind, wobei er die Kriterien berücksichtigen sollte, die mit den ebenfalls in den Art. 24 und 32 DSGVO genannten Merkmalen der betreffenden Verarbeitung und dem von ihr ausgehenden Risiko zusammenhängen*".
[44] Artikel 24 Absatz 1 bezieht sich auf die „*Art, [den] Umfang, [die] Umstände und [die] Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen*".

Grundlage des mit der Verarbeitung verbundenen Risikos festlegt. Wenn beispielsweise die Verarbeitungstätigkeiten ein geringeres Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen, werden die entsprechenden „geeigneten Maßnahmen" weniger streng sein. Somit kann der Umfang der Überprüfung durch den Verantwortlichen in der Praxis weniger umfangreich sein. Umgekehrt kann bei höheren Risiken, die sich aus der betreffenden Verarbeitung ergeben, das Ausmaß der Überprüfung durch den Verantwortlichen größer sein, um zu beurteilen, ob die gesamte Verarbeitungskette hinreichende Garantien bietet, da die zu ergreifenden „geeigneten Maßnahmen" umfassender und robuster sind, um die Risiken für die betroffenen Personen zu bewältigen.

49. In diesem Zusammenhang kann der Verantwortliche je nach Ausmaß des mit der Verarbeitungstätigkeit verbundenen Risikos den Umfang seiner Überprüfung erhöhen, indem er die Unterauftragsverarbeitungsvereinbarungen selbst überprüft und/oder auch dem ursprünglichen Auftragsverarbeiter eine erweiterte Überprüfung und Dokumentation auferlegt.

50. Gemäß dem Grundsatz der Rechenschaftspflicht sollte der Verantwortliche jede Maßnahme, die zur Einhaltung der DSGVO – auch auf der Grundlage des mit der Verarbeitung verbundenen Risikos - als notwendig angesehen wird, angemessen dokumentieren[45]. Erleichtert wird diese Pflicht zum einen durch die den Auftragsverarbeitern auferlegten **Unterstützungs- und Prüfverpflichtungen** und zum anderen durch die **Informationen, die der ursprüngliche Auftragsverarbeiter** dem Verantwortlichen vor der Beauftragung weiterer Auftragsverarbeiter **zur Verfügung stellt**.

51. Erstens stellt der Ausschuss fest, dass Auftragsverarbeiter verpflichtet sind, den Verantwortlichen bei der Erfüllung bestimmter Anforderungen der DSGVO zu unterstützen (gemäß Artikel 28 Absatz 3 Buchstaben e und f)[46]. Ganz allgemein ist der Auftragsverarbeiter verpflichtet, dem Verantwortlichen alle Informationen zur Verfügung zu stellen, die zum Nachweis der Einhaltung der in Artikel 28 niedergelegten Pflichten erforderlich sind (Artikel 28 Absatz 3 Buchstabe h)[47]. Der Verantwortliche sollte umfassend über die Einzelheiten der Verarbeitung informiert sein, die für den Nachweis der Einhaltung der in Artikel 28 DSGVO festgelegten Pflichten relevant sind, und der Auftragsverarbeiter sollte alle Informationen darüber bereitstellen, wie die Verarbeitungstätigkeit im Auftrag des Verantwortlichen durchgeführt wird[48]. Im Vertrag sollte festgelegt werden, wie oft und auf welche Weise dieser Informationsfluss stattfinden soll[49].

---

[45] Zur Beweislast des Verantwortlichen, siehe EuGH, Urteil vom 14. Dezember 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, Rn. 52: „*Aus dem Wortlaut von Art. 5 Abs. 2, Art. 24 Abs. 1 und Art. 32 Abs. 1 DSGVO geht eindeutig hervor, dass die Beweislast dafür, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten im Sinne von Art. 5 Abs. 1 Buchst. f und Art. 32 DSGVO gewährleistet, dem für die betreffende Verarbeitung Verantwortlichen obliegt*"; siehe auch EuGH-Urteil vom 25. Januar 2024, BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, Rn. 42 „*Insoweit ergibt sich aus einer Gesamtbetrachtung der Art. 5, 24 und 32 DSGVO im Licht ihres 74. Erwägungsgrundes, dass im Rahmen einer auf Art. 82 DSGVO gestützten Schadensersatzklage der für die betreffende Verarbeitung Verantwortliche die Beweislast dafür trägt, dass die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten im Sinne von Art. 5 Abs. 1 Buchst. f und Art. 32 DSGVO gewährleistet. Eine solche Beweislastverteilung ist nicht nur geeignet, die für die Verarbeitung dieser Daten Verantwortlichen dazu anzuhalten, die nach der DSGVO erforderlichen Sicherheitsmaßnahmen zu ergreifen, sondern auch, die praktische Wirksamkeit des in Art. 82 DSGVO vorgesehenen Schadensersatzanspruchs zu schützen und die in ihrem elften Erwägungsgrund genannten Absichten des Unionsgesetzgebers zu wahren*".

[46] Siehe EDSA-Leitlinien 07/2020, Absätze 130-138.

[47] Siehe EDSA-Leitlinien 07/2020, Absätze 143-145.

[48] EDSA-Leitlinien 07/2020, Absatz 143.

[49] EDSA-Leitlinien 07/2020, Absatz 143.

52. Daher kann sich der Verantwortliche bei der Erfüllung seiner Pflicht zur Dokumentation der getroffenen Maßnahmen auf die vom Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Buchstabe h DSGVO vorgelegten Informationen stützen, sofern die vom Auftragsverarbeiter vorgelegten Informationen die Einhaltung der Vorschriften tatsächlich belegen. Da der Auftragsverarbeiter sehr wohl in der Lage ist, die Einzelheiten der von ihm durchgeführten Verarbeitung und der von den Unterauftragsverarbeitern durchgeführten Verarbeitung zu kennen, sollte er dem Verantwortlichen proaktiv alle relevanten Informationen zur Verfügung stellen[50].

53. Das Vorstehende gilt auch für Unterauftragsverarbeiter. Auftragsverarbeiter sind nämlich verpflichtet, die Unterstützungspflichten in der Verarbeitungskette weiterzugeben (Artikel 28 Absatz 4 DSGVO).

54. Zweitens ist die **Beauftragung von Unterauftragsverarbeitern**, wie bereits erwähnt, nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen möglich, die gesondert oder allgemein sein kann. Entscheidet sich der Verantwortliche für die Erteilung einer allgemeinen Genehmigung, so sollte diese *„um Kriterien als Richtschnur für die Entscheidung des Auftragsverarbeiters ergänzt werden [...] (z. B. Garantien in Bezug auf technische und organisatorische Maßnahmen, Fachwissen, Zuverlässigkeit und Ressourcen)"*[51].

55. Wie vom EDSA erläutert, gilt Folgendes: *„Zum Zweck der Prüfung und Entscheidung über die Genehmigung einer Unterauftragsvergabe muss der Auftragsverarbeiter dem Verantwortlichen eine Liste potenzieller Unterauftragsverarbeiter (jeweils mit Angabe des Standorts, ihrer künftigen Aufgabe und einem Nachweis für die von ihnen durchgeführten Sicherheitsmaßnahmen) vorlegen"*[52]. Diese Informationen sind erforderlich, damit der Verantwortliche dem Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 sowie den Bestimmungen von Artikel 28 Absatz 1, Artikel 32 und Kapitel V der DSGVO genügen kann.[53] In Bezug auf die Übermittlung personenbezogener Daten in Länder außerhalb des EWR verweist der Ausschuss auf die nachstehende Antwort auf Frage 1.2 der DK-AB.

56. Wie der EDSA in Erinnerung ruft, sollte der ursprüngliche Auftragsverarbeiter sicherstellen, dass er Unterauftragsverarbeiter vorschlägt, die hinreichende Garantien bieten.[54] Die Anforderung, dass der ursprüngliche Auftragsverarbeiter die oben genannten Informationen zur Verfügung stellen muss, zeigt, dass der **Auftragsverarbeiter bei der Auswahl der Unterauftragsverarbeiter und bei der Überprüfung der von ihnen gebotenen Garantien eine Rolle spielt und dem Verantwortlichen hinreichende Informationen zur Verfügung stellen sollte**. Dies steht auch in Einklang mit der Tatsache, dass der ursprüngliche Auftragsverarbeiter ungeachtet der Kriterien, die der Verantwortliche für die Auswahl weiterer Auftragsverarbeiter vorgibt, gegenüber dem Verantwortlichen in vollem Umfang für

[50] EDSA-Leitlinien 07/2020, Absatz 143 betreffend Artikel 28 Absatz 3 Buchstabe h: *„So können beispielsweise die maßgeblichen Teile des Verzeichnisses von Verarbeitungstätigkeiten des Auftragsverarbeiters an den Verantwortlichen weitergegeben werden. Der Auftragsverarbeiter sollte alle Informationen darüber bereitstellen, wie die Verarbeitungstätigkeit im Auftrag des Verantwortlichen durchgeführt wird. Diese Informationen sollten folgende Angaben umfassen: Funktionsweise der verwendeten Systeme, Sicherheitsmaßnahmen, Gewährleistung der Speicher-/ Aufbewahrungspflichten, Speicherort der Daten, Datenübermittlungen, Personen, die Zugriff auf die Daten haben, Empfänger der Daten, eingesetzte Unterauftragsverarbeiter usw."* Die Möglichkeit für den Verantwortlichen, eine Überprüfung durchzuführen, ist ebenfalls in Absatz 144 festgelegt: *„Mit solchen Überprüfungen soll sichergestellt werden, dass der Verantwortliche über alle Informationen über die in seinem Auftrag durchgeführte Verarbeitungstätigkeit und die vom Auftragsverarbeiter gebotenen Garantien verfügt"*.

[51] EDSA-Leitlinien 07/2020, Absatz 156.

[52] EDSA-Leitlinien 07/2020, Absatz 152.

[53] EDSA-Leitlinien 07/2020, Fußnote 69.

[54] EDSA-Leitlinien 07/2020, Absatz 159.

die Erfüllung der Verpflichtungen der Unterauftragsverarbeiter haftbar bleibt (Artikel 28 Absatz 4 DSGVO).

57. Auch wenn der Auftragsverarbeiter, der einen Unterauftragsverarbeiter beauftragt, gemäß Artikel 28 Absatz 4 DSGVO unmittelbar dafür verantwortlich ist, dass diesem weiteren Auftragsverarbeiter dieselben Datenschutzverpflichtungen auferlegt werden, wie sie im ursprünglichen Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, entbindet dies den Verantwortlichen nicht von seiner Verantwortung, für die Einhaltung der Anforderungen von Artikel 28 Absatz 1 und Artikel 24 Absatz 1 DSGVO zu sorgen und diese Einhaltung nachweisen zu können.

58. **Die endgültige Entscheidung über die Beauftragung eines bestimmten (Unter-)Unterauftragsverarbeiters und die damit verbundene Verantwortung verbleibt – auch hinsichtlich der Überprüfung der Hinlänglichkeit der vom (Unter-)Auftragsverarbeiter bereitgestellten Garantien – beim Verantwortlichen.** Wie bereits erwähnt, muss der Verantwortliche im Falle einer allgemeinen oder gesonderten Genehmigung immer entscheiden, ob er die Beauftragung des Unterauftragsverarbeiters genehmigt oder dagegen Einspruch erhebt.

59. Bei der Bewertung der Einhaltung von Artikel 24 Absatz 1 und Artikel 28 Absatz 1 DSGVO sollten die Aufsichtsbehörden beurteilen, ob der Verantwortliche nachweisen kann, dass die Überprüfung der Hinlänglichkeit der von seinen Unterauftragsverarbeitern gebotenen Garantien zur Zufriedenheit des Verantwortlichen erfolgt ist. Dies bedeutet, dass sich der Verantwortliche dafür entscheiden kann, sich auf die von seinem Auftragsverarbeiter erhaltenen Informationen zu stützen und diese bei Bedarf zu ergänzen. Wenn beispielsweise die Informationen, die der Verantwortliche erhält, unvollständig oder unzutreffend erscheinen oder Fragen aufwerfen, oder wenn dies aufgrund der Sachlage, einschließlich des mit der Verarbeitung verbundenen Risikos, angezeigt ist, sollte der Verantwortliche zusätzliche Informationen anfordern und/oder die Informationen überprüfen und erforderlichenfalls vervollständigen/berichtigen.

60. Insbesondere bei Verarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten betroffener Personen darstellen, sollte der Verantwortliche seine Überprüfung hinsichtlich der Informationen zu den Garantien der verschiedenen Auftragsverarbeiter in der Verarbeitungskette vertiefen.

2.1.3 Überprüfung des Vertrags zwischen dem ursprünglichen Auftragsverarbeiter und den weiteren Auftragsverarbeitern

61. Die DK-AB fragt im Wesentlichen, ob und inwieweit der Verantwortliche die Pflicht hat, zu überprüfen und zu dokumentieren, dass die Verträge über die Unterauftragsverarbeitung den weiteren Auftragsverarbeitern die gleichen Verpflichtungen auferlegen.

62. Artikel 28 Absatz 4[55] erlegt den Auftragsverarbeitern in dieser Hinsicht eine unmittelbare Verpflichtung auf. Außerdem müssen der Verantwortliche und der Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Buchstabe d in ihrem Vertrag die Verpflichtung des Auftragsverarbeiters zur Einhaltung der in Artikel 28 Absatz 4 genannten Bedingungen „vorsehen“, wodurch diese Anforderung

[55] Artikel 60 Absatz 4 DSGVO: „*Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt.*“

zu einer vertraglichen Verpflichtung des Auftragsverarbeiters wird. Anders formuliert bedeutet dies: **Der ursprüngliche Auftragsverarbeiter ist gesetzlich und vertraglich verpflichtet, in den Unter-Auftragsverarbeitungsvereinbarungen, die er mit weiteren Auftragsverarbeitern abschließt, dieselben Datenschutzpflichten weiterzureichen.**

63. Ebenso werden die weiteren Auftragsverarbeiter (vom ursprünglichen Auftragsverarbeiter) vertraglich verpflichtet, ihren eigenen Auftragsverarbeitern die gleichen Datenschutzpflichten aufzuerlegen (was sich entsprechend entlang der Verarbeitungskette fortsetzt).[56] Es ist nicht erforderlich, dass die Unterauftragsverarbeitungsvereinbarung denselben Wortlaut hat wie der Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter.[57]

64. Der Ausschuss erinnert daran, dass für den Fall, dass ein Unterauftragsverarbeiter seinen Verpflichtungen nicht nachkommt, die letztendliche Verantwortung für die Erfüllung der Verpflichtungen dieses weiteren Unterauftragsverarbeiters beim Verantwortlichen liegt. Der ursprüngliche Auftragsverarbeiter bleibt jedoch gegenüber dem Verantwortlichen haftbar, sodass der Verantwortliche die Möglichkeit hat, einen vertraglichen Anspruch gegenüber seinem ursprünglichen Auftragsverarbeiter geltend zu machen, wenn dieser es versäumt, in den Unterauftragsverarbeitungsvereinbarungen dieselben Datenschutzverpflichtungen weiterzureichen.

65. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 Absatz 3 Buchstabe h DSGVO niedergelegten Pflichten zur Verfügung zu stellen. Daher muss der ursprüngliche Auftragsverarbeiter auf Verlangen des Verantwortlichen die Unterauftragsverarbeitungsvereinbarungen zwischen dem ursprünglichen Auftragsverarbeiter und den weiteren Auftragsverarbeitern vorlegen.

66. In diesem Zusammenhang bieten die Standardvertragsklauseln der Europäischen Kommission zwischen Verantwortlichen und Auftragsverarbeitern[58] und die Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer[59] dem

[56] In der gemeinsamen Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer hoben der EDSA und der EDSA hervor, dass die Anforderung gemäß Artikel 28 Absatz 4 der DSGVO von den Parteien in Verträgen zwischen Auftragsverarbeitern und Auftragsverarbeitern berücksichtigt werden muss (Absatz 66).

[57] EDSA-Leitlinien 07/2020, Absatz 160: „*Die Auferlegung ‚derselben' Verpflichtungen sollte vielmehr funktional als formal ausgelegt werden: Es ist nicht erforderlich, dass der Vertrag denselben Wortlaut hat wie der Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter, aber er sollte sicherstellen, dass die Verpflichtungen materiell identisch sind*". Der EDSA stellt ferner fest, dass in Fällen, in denen sich zwei Auftragsverarbeiter auf Modul drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) der Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer stützen, der ursprüngliche Auftragsverarbeiter eine zusätzliche Garantie stellt. Nach Klausel 8.1.d dieser Standardvertragsklauseln sichert der Datenexporteur (ursprünglicher Auftragsverarbeiter) zu, dass er dem Datenimporteur (Unterauftragsverarbeiter) dieselben Datenschutzpflichten auferlegt hat, die im Vertrag oder in einem anderen Rechtsinstrument nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zwischen dem Verantwortlichen und dem Datenexporteur festgelegt sind.

[58] In Abschnitt 7 über den Einsatz von Unterauftragsverarbeitern ist in Klausel 7.7.c der Standardvertragsklauseln der Europäischen Kommission zwischen Verantwortlichen und Auftragsverarbeitern Folgendes vorgesehen: „*Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen*". Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (im Folgenden „Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern").

[59] Modul zwei (Übermittlung von Verantwortlichen an Auftragsverarbeiter), Klausel 9 Buchstabe c der Standardvertragsklauseln der Kommission für die Übermittlung personenbezogener Daten an Drittländer sieht

Verantwortlichen die Möglichkeit, eine Kopie der Unterauftragsverarbeitungsvereinbarung zwischen dem ursprünglichen Auftragsverarbeiter und den weiteren Auftragsverarbeitern zu verlangen. Diese Möglichkeit ist auch in drei von Aufsichtsbehörden angenommenen Standardvertragsklauseln zwischen Verantwortlichem und Auftragsverarbeiter vorgesehen.[60] Diese Möglichkeit ist Ausdruck des Rechts des Verantwortlichen auf Überprüfung gemäß Artikel 28 Absatz 3 Buchstabe h DSGVO. Auf Verlangen des Verantwortlichen legt der Auftragsverarbeiter eine solche Kopie vor.

67. Der EDSA stellt jedoch fest, dass in den Standardvertragsklauseln nicht geregelt ist, ob ein Verantwortlicher eine solche Kopie anfordern *muss*, um Artikel 28 Absatz 1 DSGVO nachzukommen.

68. Dementsprechend kann der Umstand, ob der Verantwortliche eine solche Kopie anfordert, sich nicht auf die Verantwortung des Verantwortlichen auswirken. Der Auftragsverarbeiter hat in jedem Fall auch rechtliche und vertragliche Verpflichtungen, die ihn verpflichten, dieselben Datenschutzverpflichtungen aufzuerlegen wie im ursprünglichen Vertrag.

69. In Anbetracht dessen **ist der Verantwortliche nicht verpflichtet, systematisch die Unterauftragsverarbeitungsvereinbarungen anzufordern, um zu prüfen, inwiefern die im ursprünglichen Vertrag vorgesehenen Datenschutzverpflichtungen in der Verarbeitungskette weitergereicht wurden**. Der Verantwortliche sollte von Fall zu Fall prüfen, ob die Anforderung einer Kopie solcher Verträge oder deren Überprüfung zu einem bestimmten Zeitpunkt erforderlich ist, damit er die Einhaltung der Verträge im Hinblick auf den Grundsatz der Rechenschaftspflicht nachweisen kann. Im Rahmen der Ausübung seines Überprüfungsrechts gemäß Artikel 28 Absatz 3 Buchstabe h sollte der Verantwortliche über ein Verfahren zur Durchführung von Überprüfungsmaßnahmen verfügen, um stichprobenartig zu überprüfen, ob die Verträge mit seinen Unterauftragsverarbeitern den erforderlichen Datenschutzverpflichtungen genügen.

70. Die Notwendigkeit, eine Kopie der Unterauftragsverarbeitungsvereinbarung anzufordern, hängt daher von den Umständen des Einzelfalls ab. So sollte der Verantwortliche bei Zweifeln an der Einhaltung der Anforderungen gemäß Artikel 28 Absatz 1 und Artikel 28 Absatz 4 durch den Auftragsverarbeiter oder Unterauftragsverarbeiter oder auf Ersuchen der Aufsichtsbehörde den Vertrag zur Überprüfung anfordern (z. B. wenn der weitere Auftragsverarbeiter von einer Datenschutzverletzung betroffen ist oder wenn andere Informationen öffentlich zugänglich sind oder dem Verantwortlichen andere Informationen vorliegen); z. B. können Muster für den Datenverarbeitungsvertrag des

---

Folgendes vor: „*Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen*“. Darüber hinaus sieht Modul drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) Folgendes vor: „*Auf Verlangen des Datenexporteurs oder des Verantwortlichen stellt der Datenimporteur eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen*“. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (im Folgenden „Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer“).

[60] Standardvertragsklauseln der dänischen Aufsichtsbehörde für die Zwecke der Einhaltung von Artikel 28 DSGVO, insbesondere Klausel 7.5; Standardvertragsklauseln der litauischen Aufsichtsbehörde für die Zwecke der Einhaltung von Artikel 28 DSGVO, insbesondere Klausel 18; Standardvertragsklauseln der slowenischen Aufsichtsbehörde für die Zwecke der Einhaltung von Artikel 28 DSGVO, insbesondere Klausel 6.5.

Unterauftragsverarbeiters vorhanden sein, die nicht den Anforderungen von Artikel 28 Absatz 3 DSGVO entsprechen.

71. Um die Einhaltung von Artikel 28 Absatz 1 vor dem Hintergrund des Grundsatzes der Rechenschaftspflicht zu gewährleisten, kann eine Kopie der Unterauftragsverarbeitungsvereinbarungen dem Verantwortlichen helfen nachzuweisen, dass seine Auftragsverarbeiter und Unterauftragsverarbeiter hinreichende Garantien bieten, einschließlich der Einhaltung von Artikel 28 Absatz 4 DSGVO durch den Auftragsverarbeiter. Der EDSA stellt fest, dass ein Verantwortlicher möglicherweise nicht beurteilen kann, ob die in Bezug auf einen Unterauftragsverarbeiter gegebenen Garantien ausreichen oder nicht, ohne den Inhalt der Unterauftragsverarbeitungsvereinbarung eingesehen und diesen bewertet zu haben. Zwar können Garantien schriftlich im Vertrag vorgesehen werden, doch können Vertragsklauseln für sich genommen nicht belegen, dass die hinreichenden Garantien von den Vertragsparteien tatsächlich erfüllt werden.

2.2 Auslegung von Artikel 28 Absatz 1 DSGVO in Verbindung mit Artikel 44 DSGVO (Übermittlungen entlang der Verarbeitungskette – Fragen 1.2 und 1.3)

72. Frage 1.2 des Ersuchens zielt darauf ab, in Fällen von Übermittlungen oder Weiterübermittlungen von einem (Unter-)Auftragsverarbeiter an einen weiteren (Unter-)Auftragsverarbeiter zu klären, inwieweit der Verantwortliche im Rahmen seiner Verpflichtung nach Artikel 28 Absatz 1 DSGVO in Verbindung mit Artikel 44 DSGVO die Dokumentation von (Unter-)Auftragsverarbeitern dahingehend prüfen sollte, dass das Schutzniveau für personenbezogene Daten durch die Erst- oder Weiterübermittlung nicht untergraben wird.

73. Mit Frage 1.3 soll geklärt werden, ob der Umfang der Verpflichtungen nach Artikel 28 Absatz 1 DSGVO in Verbindung mit Artikel 5 Absatz 2 und Artikel 24 DSGVO in Verbindung mit der Antwort auf Frage 1.2 je nach dem mit der Verarbeitungstätigkeit verbundenen Risiko variiert. Wenn diese Frage bejaht wird, so bittet die DK-AB um Auskunft über den Umfang dieser Verpflichtungen bei Verarbeitungstätigkeiten mit „geringem“ und „hohem“ Risiko.

Einleitende Erläuterungen

74. Der Klarheit halber werden im Rahmen dieser Stellungnahme einige einleitende Erläuterungen zu diesen Fragen gegeben.

75. Erstens versteht der EDSA den Begriff „Übermittlung" in der Bedeutung, die in den EDSA-Leitlinien 05/2021 über das Zusammenspiel zwischen Artikel 3 und Kapitel V der DSGVO[61] (nachfolgend „EDSA-Leitlinien 05/2021 (Zusammenspiel)") dargelegt ist, die auch auf die EDSA-Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3)[62] verweisen. Wie der EDSA bereits hervorgehoben hat, stellt der Fernzugriff aus einem Drittland eine Übermittlung dar, wenn er die in den EDSA-Leitlinien 05/2021 (Zusammenspiel) festgelegten Kriterien erfüllt[63]. In jedem Fall löst das Vorhandensein einer Übermittlung die Anwendung von Kapitel V der DSGVO aus.

76. Zweitens: Da sich Frage 1.2 auf eine Situation bezieht, in der ein (Unter-)Auftragsverarbeiter eine Erst- oder Weiterübermittlung an einen weiteren (Unter-)Auftragsverarbeiter vornimmt, ist der Verantwortliche nicht der Datenexporteur; der Datenexporteur ist vielmehr ein Auftragsverarbeiter, der die personenbezogenen Daten im Namen des Verantwortlichen an einen weiteren Auftragsverarbeiter entlang der Kette und nicht an einen separaten Verantwortlichen übermittelt. Ausgeschlossen sind daher personenbezogene Daten, die an separate Verantwortliche, einschließlich Gerichten oder Verwaltungsbehörden in Drittländern, übermittelt werden. Daher fällt die Auslegung von Artikel 48 DSGVO nicht in den Anwendungsbereich dieser Fragen.

77. Drittens stellt der EDSA fest, dass sich Frage 1.2 auf Übermittlungen bezieht, die gemäß den dokumentierten Weisungen des Verantwortlichen nach Artikel 28 Absatz 3 Buchstabe a DSGVO entlang der Verarbeitungskette erfolgen. Es ist hervorzuheben, dass es dem Verantwortlichen obliegt, zu entscheiden, ob eine Übermittlung personenbezogener Daten außerhalb des EWR im Rahmen der den (Unter-)Auftragsverarbeitern übertragenen Verarbeitungstätigkeiten möglich ist. Der Auftragsverarbeiter sollte davon absehen, eine Erst- oder Weiterübermittlung außerhalb der Weisungen des Verantwortlichen vorzunehmen[64]. Die dokumentierten Weisungen des Verantwortlichen in Bezug auf die Erstübermittlung oder Weiterübermittlung personenbezogener Daten sind entlang der Verarbeitungskette weiterzugeben[65].

78. Viertens stellt der EDSA klar, dass der Risikobegriff, auf den in Frage 1.3 Bezug genommen wird, als das Risiko für die Rechte und Freiheiten der betroffenen Personen zu verstehen ist, deren

[61] EDSA-Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO, Version 2.0, angenommen am 14. Februar 2023, in deren Absatz 9 die drei kumulativen Kriterien für die Einstufung eines Verarbeitungsvorgangs als Übermittlung festlegt werden und in deren Abschnitt 2 diese Kriterien allgemeiner erläutert werden.

[62] EDSA-Leitlinien 05/2021 (Zusammenspiel), Absatz 12 mit Verweis auf die EDSA-Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO, Version 2.1, angenommen am 12. November 2019 (mit Berichtigung vom 7. Januar 2020), S. 5 und Abschnitte 1-3. Siehe insbesondere Abschnitt 2, „d) Nicht in der Union ansässiger Auftragsverarbeiter".

[63] EDSA-Leitlinien 05/2021 (Zusammenspiel), Absatz 16.

[64] Artikel 29 der DSGVO. Der EDSA ruft Folgendes in Erinnerung: „*In dem Vertrag sollten unter Berücksichtigung der Bestimmungen von Kapitel V der DSGVO die Anforderungen an die Übermittlung an Drittländer oder internationale Organisationen festgelegt werden*" (EDSA-Leitlinien 07/2020, Absatz 119). So kann sich der Verantwortliche beispielsweise dafür entscheiden, Übermittlungen zu verbieten oder nur in bestimmte Länder zuzulassen.

[65] Artikel 28 Absatz 4 DSGVO.

personenbezogene Daten im Sinne der Erwägungsgründe 75 und 76 der DSGVO (und wie in Absatz 35 oben erwähnt) verarbeitet werden.

Die Verantwortung des Verantwortlichen besteht selbst dann, wenn die (Unter-)Auftragsverarbeiter die Erst- oder Weiterübermittlungen vornehmen

79. Was den Inhalt des Antrags betrifft, so hat der EDSA bereits präzisiert, dass „(…) *es Übermittlungssituationen [gibt], in denen ein Auftragsverarbeiter (der entweder nach Artikel 3 Absatz 1 oder nach Artikel 3 Absatz 2 für eine bestimmte Verarbeitung [...]) auf Weisung seines Verantwortlichen Daten an einen anderen Auftragsverarbeiter oder sogar an einen Verantwortlichen in einem Drittland sendet. In diesen Fällen handelt der Auftragsverarbeiter als Datenexporteur im Auftrag des Verantwortlichen und muss sicherstellen, dass die Bestimmungen des Kapitels V bei der betreffenden Übermittlung entsprechend den Weisungen des Verantwortlichen eingehalten werden, einschließlich dessen, dass ein geeignetes Übermittlungsinstrument verwendet wird. Da es sich bei der Übermittlung um eine im Auftrag des Verantwortlichen vorgenommene Verarbeitungstätigkeit handelt,* ***ist der Verantwortliche hierfür ebenfalls verantwortlich und könnte gemäß Kapitel V haftbar sein; außerdem muss er sicherstellen, dass der Auftragsverarbeiter hinreichend Garantien nach Artikel 28 bietet***“.[66]

80. Anders ausgedrückt: Im Falle einer Übermittlung unterliegt der Verantwortliche auch dann noch den Pflichten, die sich sowohl aus Artikel 44 DSGVO als auch aus Artikel 28 Absatz 1 DSGVO[67] ergeben, wenn diese Übermittlung nicht direkt von dem Verantwortlichen, sondern von einem Auftragsverarbeiter im Namen des Verantwortlichen durchgeführt wird[68].

Verantwortung aufgrund von Artikel 44 der DSGVO

81. Die sich aus Artikel 44 DSGVO[69] ergebenden Verpflichtungen richten sich sowohl an Auftragsverarbeiter (die im Rahmen der Stellungnahme als Datenexporteure fungieren) als auch an Verantwortliche[70]. Sowohl der Auftragsverarbeiter als auch der Verantwortliche sollten daher unabhängig vom Übermittlungsgrund sicherstellen, dass das Schutzniveau der personenbezogenen Daten durch die Erst- oder Weiterübermittlung nicht untergraben wird[71]. So bleiben beispielsweise sowohl der Verantwortliche als auch der Auftragsverarbeiter nach Kapitel V der DSGVO grundsätzlich

[66] EDSA-Leitlinien 05/2021 (Zusammenspiel), Absatz 19, Hervorhebung hinzugefügt.

[67] Es ist auch darauf hinzuweisen, dass sich Artikel 28 Absatz 1 DSGVO auf die Erfüllung der Anforderungen der DSGVO bezieht und daher dahin auszulegen ist, dass er Bestimmungen des Kapitels V über die Erst- oder Weiterübermittlung personenbezogener Daten an Drittländer umfasst. Dies gilt sowohl für Erstübermittlungen als auch für Weiterübermittlungen, siehe Artikel 44 DSGVO.

[68] Für die Zwecke dieses Abschnitts der Stellungnahme werden die sich aus Artikel 44 und Artikel 28 Absatz 1 DSGVO ergebenden Pflichten behandelt, wobei klargestellt wird, dass der Verantwortliche weiterhin allen Pflichten unterliegt, die für Verantwortliche gemäß der DSGVO gelten.

[69] In Artikel 44 DSGVO wird auf die Bestimmungen von Kapitel V DSGVO verwiesen.

[70] Artikel 44 DSGVO betrifft im Hinblick auf die Einhaltung von Kapitel V sowohl den „Verantwortlichen“ als auch den „Auftragsverarbeiter“, vgl. Erwägungsgrund 101. Aus diesem Grund gelten die am 18. Juni 2021 angenommenen EDSA-Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0 (im Folgenden „EDSA-Empfehlungen 01/2020„) für „Datenexporteure“ (seien es Verantwortliche oder [Unter-]Auftragsverarbeiter, die personenbezogene Daten verarbeiten).

[71] Urteil des EuGH vom 16. Juli 2020, *Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems* (im Folgenden „Schrems-II-Urteil“), C-311/18, ECLI:EU:C:2020:559, Rn. 92.

für eine unrechtmäßige Erst- oder Weiterübermittlung verantwortlich[72] und könnten daher im Falle eines Verstoßes beide und einzeln haftbar gemacht werden.

Verantwortung aufgrund von Artikel 28 Absatz 1 der DSGVO

82. Nach dem Grundsatz der Rechenschaftspflicht sind die Verantwortlichen verpflichtet, „geeignete Maßnahmen" zu ergreifen, um Verstöße gegen die Vorschriften der DSGVO zu verhindern, damit das Recht auf Datenschutz zu gewährleistet ist[73]. Dies schließt die Verhinderung von Verstößen gegen Kapitel V der DSGVO ein. Diese Verantwortung gilt vor Beginn der Übermittlung und solange, wie die übermittelten personenbezogenen Daten in dem Drittland verarbeitet werden.

83. Wie oben in den Absätzen 47-48 erläutert, sollte die *Verpflichtung des Verantwortlichen*, zu überprüfen, ob die (Unter-)Auftragsverarbeiter hinreichende Garantien für die Durchführung der von dem Verantwortlichen gemäß Artikel 28 Absatz 1 DSGVO[74] festgelegten Maßnahmen bieten, unabhängig von dem Risiko für die Rechte und Freiheiten der betroffenen Personen gelten. Der *Umfang* dieser Überprüfung wird jedoch in der Praxis variieren, je nach Art der organisatorischen und technischen Maßnahmen, die der Verantwortliche bestimmt, und zwar unter anderem auf der Grundlage des mit der Verarbeitung verbundenen Risikos[75]. Insoweit kann das Vorliegen einer Erst- oder Weiterübermittlung an Drittländer entlang der Verarbeitungskette die mit der Verarbeitung verbundenen Risiken erhöhen und sich somit auf die vom Verantwortlichen festgelegten „geeigneten" Maßnahmen auswirken[76].

84. Auf Anfrage sollte der Verantwortliche – mit Unterstützung des Auftragsverarbeiters und der Unterauftragsverarbeiter – in der Lage sein, der zuständigen Aufsichtsbehörde nachzuweisen, dass er die Anforderungen von Artikel 28 Absatz 1 DSGVO erfüllt. Die entsprechende Dokumentation kann sich unter anderem auf die Informationen stützen, die von den Auftragsverarbeitern im Rahmen der Beauftragung von (Unter-)Auftragsverarbeitern[77] (siehe Absätze 54-56), aber auch mit Unterstützung

[72] Der Verantwortliche kann von seinem Auftragsverarbeiter Schadenersatz verlangen, der seinem Teil der Verantwortung entspricht, sofern die in Artikel 82 Absatz 5 DSGVO festgelegten Bedingungen erfüllt sind.

[73] Siehe den obigen Abschnitt zu Artikel 5 Absatz 2 und Artikel 24 Absatz 1 in Verbindung mit Artikel 28 Absatz 1 DSGVO.

[74] Hinweis: Die in Artikel 24 Absatz 1 und Artikel 28 Absatz 1 DSGVO genannten „geeigneten technischen und organisatorischen Maßnahmen" sind nicht mit den in den Empfehlungen 01/2020 des EDSA genannten „zusätzlichen Maßnahmen" zu verwechseln (Absatz 50:„ *‚Zusätzliche Maßnahmen' sind per definitionem eine Ergänzung der Garantien, die bereits in dem in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrument enthalten sind, sowie aller anderen anwendbaren Sicherheitsanforderungen (z. B. technischen Sicherheitsmaßnahmen), die in der DSGVO festgelegt sind*", wobei auf Erwägungsgrund 109 der DSGVO und das Schrems-II-Urteil, Rn. 133 verwiesen wird.

[75] Siehe die Definition des Begriffs „Risiko" in den Ziffern 35 und 78.

[76] In Erwägungsgrund 116 der DSGVO heißt es: „*Wenn personenbezogene Daten in ein anderes Land außerhalb der Union übermittelt werden, besteht eine erhöhte Gefahr, dass natürliche Personen ihre Datenschutzrechte nicht wahrnehmen können und sich insbesondere nicht gegen die unrechtmäßige Nutzung oder Offenlegung dieser Informationen zu schützen.*"

[77] Siehe auch Klausel 9 Buchstabe a von Modul drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) und Anhang III der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer; siehe zudem Klausel 9 Buchstabe a von Modul zwei (Übermittlung von Verantwortlichen an Auftragsverarbeiter) und Klausel 7.7 Buchstabe a der Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern und deren Anhang IV „Liste der Unterauftragsverarbeiter". Sowohl Anhang II der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer als auch Anhang IV der Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern sind im Falle einer gesonderten Genehmigung durch den Verantwortlichen mit folgenden Informationen über die Unterauftragsverarbeiter zu ergänzen: Name, Anschrift, Name, Funktion und Kontaktdaten der Kontaktperson

ihrer Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Buchstabe h DSGVO vorgelegt wurden (siehe Absätze 51-52).

85. Der Verantwortliche benötigt außerdem alle relevanten Informationen, um die erforderlichen Weisungen für die Übermittlung der personenbezogenen Daten in die jeweiligen Drittländer zu erteilen und um dem Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 DSGVO sowie den Bestimmungen von Artikel 28 Absatz 1, Artikel 32 und Kapitel V der DSGVO nachkommen zu können[78]. Der Verantwortliche kann auf der Grundlage der erhaltenen Informationen der Beauftragung eines zusätzlichen Auftragsverarbeiters widersprechen oder diese nicht genehmigen, wenn dies eine Übermittlung personenbezogener Daten vom ursprünglichen Auftragsverarbeiter (als Exporteur) an den vorgesehenen zusätzlichen Auftragsverarbeiter (als Importeur) zur Folge hätte.

86. Gemäß dem obigen Absatz 58 ist der Verantwortliche letztlich für jeden Verstoß gegen Artikel 28 Absatz 1 DSGVO im Zusammenhang mit dem Einsatz von (Unter-)Auftragsverarbeitern verantwortlich und könnte dafür haftbar gemacht werden. Der EDSA hebt hervor, dass praktische Schwierigkeiten, die von Verantwortlichen in Bezug auf die Kontrolle der Beauftragung von Unterauftragsverarbeitern durch ihren Auftragsverarbeiter geltend gemacht werden – die es ihnen erschweren kann, die „hinreichenden Garantien" zu überprüfen, vor allem für Übermittlungen in Drittländer – den Verantwortlichen nicht von seinen Verantwortlichkeiten bei der Verarbeitung entbinden[79].

87. Im Folgenden werden nicht erschöpfende Beispiele für die Dokumentation beschrieben, die der Verantwortliche bewerten und der zuständigen Aufsichtsbehörde vorlegen können sollte: Übersicht über die Übermittlungen, Übermittlungsgrundlage und gegebenenfalls „Transfer Impact Assessment" und zusätzliche Maßnahmen.

Übersicht über die Übermittlungen:

88. In einem ersten Schritt sollte der Verantwortliche in Fällen, in denen personenbezogene Daten im Zusammenhang mit dem Einsatz von (Unter-)Auftragsverarbeitern in Drittländer übermittelt werden, die Dokumentation der Übermittlungsübersicht[80] prüfen und vorlegen können. Der Verantwortliche sollte sicherstellen, dass der Datenexporteur (der personenbezogene Daten in seinem Auftrag verarbeitet) eine Übermittlungsübersicht erstellt, aus der hervorgeht, welche personenbezogenen Daten übermittelt werden (einschließlich Fällen des Fernzugriffs) und wo und für welche Zwecke diese Übermittlungen erfolgen.[81] Der Verantwortliche kann sich auf diese Übersicht stützen und sie bei Bedarf ergänzen. Wenn beispielsweise die von dem Verantwortlichen erhaltene Übersicht

sowie Beschreibung der Verarbeitung. Darüber hinaus enthält Anhang I der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer, Abschnitt B „Beschreibung der Datenübermittlung" die Anweisung „Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben". In ähnlicher Weise enthält Anhang II der Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern die Formulierung „Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben".

[78] EDSA-Leitlinien 07/2020, Absatz 152, Fußnote 69.

[79] CEF Report on Cloud Services, S. 16.

[80] „Übermittlungsübersicht" bezieht sich auf den ersten Schritt (der vollen Kenntnis aller Übermittlungen bzw. das sogenannte „Know your Transfers") der EDSA-Empfehlungen 01/2020, Abschnitt 2.1 „Schritt 1: Die Datenübermittlungen kennen". Dieser erste Schritt gilt unabhängig vom Übermittlungsgrund.

[81] Es sollte präzisiert werden, dass die Zwecke von dem Verantwortlichen festgelegt werden, ebenso wie die „wesentlichen Mittel" der Verarbeitung (siehe EDSA-Leitlinien 07/2020, Absatz 40).

unvollständig oder ungenau erscheint[82] oder Fragen aufwirft, sollte der Verantwortliche zusätzliche Informationen anfordern, die Informationen überprüfen und bei Bedarf ergänzen/korrigieren.

89. Der Verantwortliche sollte diese Informationen erhalten,[83] bevor ein weiterer Auftragsverarbeiter beauftragt wird. Es sei auch daran erinnert, dass der Verantwortliche besonderen Transparenzanforderungen in Bezug auf Übermittlungen in Drittländer gemäß Artikel 13 Absatz 1 Buchstabe f, Artikel 14 Absatz 1 Buchstabe f, Artikel 15 Absatz 1 Buchstabe c und Artikel 15 Absatz 2 DSGVO sowie der Verpflichtung zur Führung von Verzeichnissen von Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 1 Buchstaben d und e DSGVO unterliegt. Um diese Anforderungen zu erfüllen, sollte der Verantwortliche wissen, wo sich die Unterauftragsverarbeiter befinden und wo die Übermittlungen – einschließlich des Fernzugriffs – stattfinden[84].

Verwendete Übermittlungsgrundlage und gegebenenfalls „Transfer Impact Assessment" sowie zusätzliche Maßnahmen:

90. Der Verantwortliche sollte die Dokumentation über die Grundlage für die Übermittlung,[85] auf die sich der Exporteur stützt, gemäß den Weisungen des Verantwortlichen bewerten und vorlegen können[86]. Das bedeutet, dass der Verantwortliche diese Informationen von den (Unter-)Auftragsverarbeitern/Exporteuren erhalten sollte, bevor die Übermittlungen stattfinden. Der EDSA erinnert in diesem Zusammenhang daran, dass der Verantwortliche besonderen Transparenzanforderungen in Bezug auf „das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses" gemäß Artikel 45 DSGVO oder „geeigneten Garantien" gemäß Artikel 46 DSGVO unterliegt (Artikel 13 Absatz 1 Buchstabe f, Artikel 14 Absatz 1 Buchstabe f und Artikel 15 Absatz 2 DSGVO[87]).

91. Der Umfang der Pflicht des Verantwortlichen, diese Unterlagen zu bewerten, hängt von der Art des Grundes ab, der für die Erst- oder Weiterübermittlung durch die (Unter-)Auftragsverarbeiter (als Datenexporteur) genutzt wird[88]:

92. Übermittlungen können auf der Grundlage eines **Angemessenheitsbeschlusses** erfolgen, wenn die Kommission gemäß Artikel 45 DSGVO beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Bei der Beurteilung der Angemessenheit des Schutzniveaus berücksichtigt die Kommission – neben anderen Kriterien – die Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die in diesem Land oder dieser internationalen Organisation eingehalten werden, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Personen und

[82] Z. B. wenn in der Übermittlungsübersicht die Standorte der Unterauftragsverarbeiter nicht angegeben sind oder wenn Übermittlungen in Form eines Fernzugriffs in der Übermittlungsübersicht nicht aufgeführt werden, während sie stattfinden.

[83] Wie oben in den Absätzen 54-56 erläutert.

[84] Eine solche Übermittlungsübersicht ist auch erforderlich, wenn die Parteien die einschlägigen Anhänge der Standardvertragsklauseln der Kommission für die Übermittlung in Drittländer und der Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern ausfüllen (siehe Fußnote 80 oben).

[85] EDSA-Empfehlungen 01/2020, Abschnitt 2.2. „Schritt 2: Auswahl der eingesetzten Übermittlungsinstrumente".

[86] Artikel 65 Absatz 1 Buchstabe a DSGVO.

[87] EDSA-Leitlinien 01/2022 (Auskunftsrecht), Absatz 122.

[88] Im Einklang mit den dokumentierten Weisungen des Verantwortlichen in Bezug auf die Übermittlung personenbezogener Daten entlang der Verarbeitungskette.

wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für die betroffenen Personen, deren personenbezogene Daten übermittelt werden.[89]

93. Vor diesem Hintergrund sollte, wenn eine Übermittlung von einem (Unter-)Auftragsverarbeiter (im Auftrag des Verantwortlichen) auf der Grundlage eines Angemessenheitsbeschlusses gemäß Artikel 45 DSGVO vorgenommen wird, der gemäß Artikel 28 Absatz 1 DSGVO vom Verantwortlichen geforderte Überprüfungsumfang, dass sein (Unter-)Auftragsverarbeiter hinreichende Garantien hinsichtlich der Einhaltung von Kapitel V der DSGVO bietet, folgende Aspekte umfassen:

- ob der Angemessenheitsbeschluss in Kraft ist[90],

- und ob die im Auftrag des Verantwortlichen vorgenommenen Übermittlungen in den Anwendungsbereich eines solchen Beschlusses fallen (z. B. in den Geltungsbereich fallende Kategorien personenbezogener Daten oder Sektoren)[91].

94. Wenn personenbezogene Daten, die von einem (Unter-)Auftragsverarbeiter (im Auftrag des Verantwortlichen) auf der Grundlage eines Angemessenheitsbeschlusses übermittelt werden, Gegenstand einer **Weiterübermittlung** aus diesem Drittland sind, darf das durch die DSGVO garantierte Schutzniveau für natürliche Personen bei dieser Weiterübermittlung ebenfalls nicht untergraben werden[92]. In diesem Zusammenhang erstreckt sich gemäß Artikel 45 Absatz 2 Buchstabe a DSGVO jeder von der Europäischen Kommission erlassene Angemessenheitsbeschluss unter anderem auf die Vorschriften von Drittländern für Weiterübermittlungen. Daher muss der Verantwortliche gemäß Artikel 44 DSGVO diese Anforderungen nicht selbst überprüfen.

95. In Bezug auf die Verpflichtung des Verantwortlichen gemäß Artikel 28 Absatz 1 DSGVO bedeutet dies, dass der Verantwortliche sicherstellen sollte, dass der (Unter-)Auftragsverarbeiter „hinreichende Garantien" auch in Bezug auf Weiterübermittlungen bietet, die von einem (Unter-)Auftragsverarbeiter aus einem für angemessen befundenen Land durchgeführt werden.

96. In Ermangelung eines Angemessenheitsbeschlusses können Übermittlungen von „**geeigneten Garantien**" im Sinne von **Artikel 46 DSGVO** abhängig gemacht werden. In diesem Fall sollte der

---

[89] Siehe Artikel 45 der DSGVO und WP29-Referendum zur Angemessenheit (WP29 Adequacy Referential), angenommen am 28. November 2017, WP 254, gebilligt vom EDSA am 25. Mai 2018, Seite 7: „Die Weiterleitung *der personenbezogenen Daten des ursprünglichen Empfängers der ursprünglichen Datenübermittlung sollte nur zulässig sein, wenn der weitere Empfänger (d. h. der Empfänger der weitergeleiteten Daten) ebenfalls Vorschriften (einschließlich vertraglichen Bestimmungen) unterliegt und dadurch ein angemessenes Schutzniveau gewährleistet und die einschlägigen Anweisungen für die Verarbeitung von Daten im Namen des Verantwortlichen befolgt. Das Schutzniveau natürlicher Personen, deren Daten übermittelt werden, darf durch die Weiterleitung der Daten nicht untergraben werden. Der ursprüngliche Empfänger von aus der EU übermittelten Daten ist verpflichtet sicherzustellen, dass ohne Vorliegen eines Angemessenheitsbeschlusses geeignete Garantien für die Weiterleitung der Daten gegeben sind. Solche Weiterleitungen von Daten sollten nur für begrenzte und bestimmte Zwecke erfolgen und solange es eine Rechtsgrundlage für die Verarbeitung gibt*."

[90] EDSA-Empfehlungen 01/2020, Absatz 19: „*Ein Datenexporteur, der personenbezogene Daten in ein Drittland, ein Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland übermittelt, für welche(s) die Kommission einen einschlägigen Angemessenheitsbeschluss erlassen hat, muss keine der weiteren in diesen Empfehlungen beschriebenen Schritte befolgen. Allerdings muss er fortlaufend überwachen, ob die für seine Übermittlungen relevanten Angemessenheitsbeschlüsse möglicherweise widerrufen oder für ungültig erklärt worden sind.*"

[91] EDSA-Empfehlungen 01/2020, Absatz 19.

[92] Siehe Artikel 44 der DSGVO: „*die in diesem Kapitel niedergelegten Bedingungen einhalten [...]; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation*".

Verantwortliche die geeigneten Garantien bewerten und auf etwaige problematische Rechtsvorschriften achten, die den Unterauftragsverarbeiter daran hindern könnten, die in seinem Vertrag mit dem ursprünglichen Auftragsverarbeiter festgelegten Verpflichtungen zu erfüllen[93]. Insbesondere sollte der Verantwortliche sicherstellen, dass ein solches „Transfer Impact Assessment[94] im Einklang mit der Rechtsprechung[95] und wie in den EDSA-Empfehlungen 01/2020 erläutert durchgeführt wird. Die Dokumentation über die getroffenen geeigneten Garantien, das „Transfer Impact Assessment" und die möglichen ergänzenden Maßnahmen sollte der Auftragsverarbeiter/Exporteur[96] (gegebenenfalls in Zusammenarbeit mit dem Auftragsverarbeiter/Importeur) erstellen[97]. Der Verantwortliche kann sich auf die vom (Unter-)Auftragsverarbeiter erstellte Bewertung stützen und diese bei Bedarf ergänzen. Erscheint beispielsweise die bei dem Verantwortlichen eingegangene Bewertung unvollständig, ungenau oder wirft sie Fragen auf, sollte der Verantwortliche zusätzliche Informationen anfordern, die Informationen überprüfen und sie bei Bedarf vervollständigen/korrigieren, wobei zu beachten ist, dass die Bewertung im Einklang mit den EDSA-Empfehlungen 01/2020 und den darin dargelegten Schritten stehen sollte[98]. Dazu gehört die Ermittlung von Rechtsvorschriften und Praktiken, die unter Berücksichtigung sämtlicher Umstände der Übermittlung relevant sind,[99] und gegebenenfalls die Feststellung geeigneter zusätzlicher Maßnahmen[100]. In diesem Zusammenhang sollte der Verantwortliche besonders darauf achten, ob der Datenexporteur, d. h. der Auftragsverarbeiter oder Unterauftragsverarbeiter, geprüft hat, ob es in den Rechtsvorschriften und/oder Praktiken des Drittlandes eine Bestimmung gibt, die die Wirksamkeit der geeigneten Garantien der Übermittlungsgrundlage, auf die sich der Exporteur beruft,

[93] Siehe hierzu das Schrems-II-Urteil, Rn. 132 und 133, in denen der EuGH den vertraglichen Charakter der Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer betont.

[94] Diese Bewertung wird in den EDSA-Empfehlungen 01/2020, Schritt 3 mit dem Titel „Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments gemäß Artikel 46 DSGVO im Hinblick auf die Gesamtumstände der Übermittlung", näher erläutert.[95] Schrems-II-Urteil, Rn. 134.

[95] Schrems-II-Urteil, Rn. 134.

[96] Empfehlungen 1/2022 des EDSA zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für Verantwortliche enthalten sein sollten (Art. 47 DSGVO), angenommen am 20. Juni 2023, Version 2.1, Absatz 10: „(...) *[es obliegt] beispielsweise jedem Datenexporteur, bei jeder Übermittlung auf Einzelfallbasis zu prüfen, ob zusätzliche Maßnahmen ergriffen werden müssen, um ein Schutzniveau zu gewährleisten, das dem der DSGVO der Sache nach gleichwertig ist.*"

[97] In seinem Urteil in der Rechtssache Schrems II, Rn. 134, stellte der EuGH fest, dass eine solche Überprüfung gegebenenfalls in Zusammenarbeit mit dem Datenimporteur erfolgen kann. Siehe auch EDSA-Empfehlungen 01/2020, Abschnitt 4.

[98] Bitte beachten Sie insbesondere „Schritt 3: Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments gemäß Artikel 46 DSGVO im Hinblick auf die Gesamtumstände der Übermittlung", „Schritt 4: Zusätzliche Maßnahmen ergreifen" und „Schritt 6: Neubewertung in angemessenen Abständen", wie in den EDSA-Empfehlungen 01/2020 erläutert.

[99] Schrems-II-Urteil, Rn. 126. Siehe auch EDSA-Empfehlungen 01/2020, Abschnitt 2.3. „Schritt 3: Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments gemäß Artikel 46 DSGVO im Hinblick auf die Gesamtumstände der Übermittlung" und insbesondere Absatz 33. Im Schrems-II-Urteil, Rn. 134, stellte der EuGH fest, dass eine solche Überprüfung gegebenenfalls in Zusammenarbeit mit dem Datenimporteur erfolgen kann. (siehe auch EDSA-Empfehlungen 01/2020, Rn. 30).

[100] Der Rechtsprechung zufolge obliegt es dem Datenexporteur, in jedem Einzelfall – falls angemessen, in Zusammenarbeit mit dem Datenempfänger – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des EU-Rechts einen im Wesentlichen gleichwertigen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren (Schrems-II-Urteil, Rn. 134). Siehe auch EDSA-Empfehlungen 01/2020, Abschnitt 2.4, „Schritt 4: Zusätzliche Maßnahmen ergreifen".

beeinträchtigen könnte[101], insbesondere aufgrund der Rechtsvorschriften und Praktiken, die den Zugang der Behörden des Drittlandes zu den übermittelten personenbezogenen Daten regeln[102].

97. Darüber hinaus und ähnlich wie bei Übermittlungen auf der Grundlage eines Angemessenheitsbeschlusses (Artikel 45 DSGVO, siehe oben Absätze 94 und 95), bei denen personenbezogene Daten von einem (Unter-)Auftragsverarbeiter auf der Grundlage geeigneter Garantien gemäß Artikel 46 DSGVO übermittelt werden, erstreckt sich die Verpflichtung des Verantwortlichen nach Artikel 28 Absatz 1 DSGVO auch darauf, sich zu vergewissern, dass der (Unter-)Auftragsverarbeiter hinreichende Garantien in Bezug auf **Weiterübermittlungen** bietet. Zu den geeigneten Garantien gemäß Artikel 46 DSGVO gehören in der Regel auch Bestimmungen, in denen Regeln für die Weiterübermittlung festgelegt werden[103]. Dies bedeutet, dass die Verantwortlichen nicht überprüfen müssen, ob diese Regeln als solche den Anforderungen von Kapitel V der DSGVO entsprechen. Die Verantwortlichen sollten jedoch die Dokumentation im Zusammenhang mit solchen Weiterübermittlungen vorweisen können. Dies bedeutet, dass der Verantwortliche diese Informationen von den (Unter-)Auftragsverarbeitern/Exporteuren erhalten sollte, aus denen hervorgeht, dass die Importeure, die im Instrument für die geeigneten Garantien festgelegten Anforderungen für Weiterübermittlungen, tatsächlich erfüllen.

2.3 Auslegung von Artikel 28 Absatz 3 Buchstabe a DSGVO (Frage 2)

98. Um eine transparente Aufteilung der Verantwortlichkeiten und Haftung sowohl intern (zwischen Verantwortlichen und Auftragsverarbeitern) als auch extern gegenüber den betroffenen Personen und den Aufsichtsbehörden zu gewährleisten, muss gemäß Artikel 28 Absatz 3 DSGVO jede Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem EU-Recht oder dem Recht eines Mitgliedstaats[104] erfolgen. Gemäß Artikel 28 Absatz 3 Buchstabe a DSGVO muss in diesem Vertrag vor allem festgelegt werden, dass der Auftragsverarbeiter *„die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*“. Zudem sieht die Bestimmung vor: *„in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet*“.

99. Das Ersuchen bezieht sich auf bestehende Verträge, die die Verpflichtung enthalten, personenbezogene Daten nur auf Weisung des Verantwortlichen zu verarbeiten, *„sofern er [der Auftragsverarbeiter] nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*“ (wobei der Verweis auf das Unionsrecht oder das Recht eines Mitgliedstaats weggelassen wird). In diesem Zusammenhang wurden mehrere Fragen an den EDSA gerichtet, die im folgenden Abschnitt gemeinsam behandelt werden:

> 2 Muss ein Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht eines Mitgliedstaats gemäß Artikel 28 Absatz 3 DSGVO die in Artikel 28 Absatz 3 Buchstabe a

[101] Siehe EDSA-Empfehlungen 01/2020, Abschnitt 2.3 („Schritt 3“).
[102] Siehe EDSA-Empfehlungen 01/2020, Absätze 41 ff.
[103] Siehe z. B. Klausel 8.7 (Modul eins) bzw. 8.8 (Module zwei und drei) der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer (Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021).
[104] Im Folgenden wird der Begriff „**Vertrag**“ verwendet, um „einen Vertrag oder ein anderes Rechtsinstrument nach dem EU-Recht oder dem Recht eines Mitgliedstaats“ zu bezeichnen.

vorgesehene Ausnahme „*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*“ (wörtlich übernommen oder sehr ähnlich formuliert) enthalten, damit er bzw. es mit der DSGVO in Einklang steht?

2a Wenn Frage 2 verneint wird, ist es für sich genommen ein Verstoß gegen Artikel 28 Absatz 3 Buchstabe a DSGVO, wenn ein Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, die Ausnahme nach Artikel 28 Absatz 3 Buchstabe a DSGVO auf das Recht von Drittländern ausweitet (z. B. „sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist“)?

100. In den EDSA-Leitlinien 07/2020 wird daran erinnert, „*wie wichtig es ist, Datenverarbeitungsvereinbarungen [im Hinblick auf alle rechtlichen Anforderungen der EU oder eines Mitgliedstaats, denen der Auftragsverarbeiter unterliegt] sorgfältig auszuhandeln und abzufassen*“[105]. Bezüglich des Inhalts der Verträge heißt es dort: „*Eine Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter muss den Anforderungen von Artikel 28 DSGVO genügen, damit sichergestellt ist, dass der Auftragsverarbeiter personenbezogene Daten im Einklang mit der DSGVO verarbeitet. Eine solche Vereinbarung sollte den konkreten Verantwortlichkeiten von Verantwortlichen und Auftragsverarbeitern Rechnung tragen. Artikel 28 enthält zwar eine Liste von Punkten, die in jedem Vertrag behandelt werden müssen, der das Verhältnis zwischen Verantwortlichen und Auftragsverarbeitern regelt, doch lässt er den Parteien solcher Verträge Raum für Verhandlungen.*“[106] Der Verhandlungsspielraum ist durch die in Artikel 28 Absatz 3 DSGVO festgelegten Anforderungen begrenzt.

[105] EDSA-Leitlinien 07/2020, Absatz 121.
[106] EDSA-Leitlinien 07/2020, Absatz 109.

101. Zunächst ist die Verpflichtung des Auftragsverarbeiters, personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, ein Kernelement des Vertrags.

102. Gemäß Artikel 28 Absatz 3 Buchstabe a DSGVO dürfen Auftragsverarbeiter personenbezogene Daten – außer auf dokumentierte Weisung des Verantwortlichen – jedoch rechtmäßig verarbeiten, um rechtlichen Verpflichtungen nach dem Recht der EU oder der Mitgliedstaaten nachzukommen (im Folgenden „**EU-/MS-rechtliche Anforderung**"). Diese Bestimmung verlangt außerdem, dass der Auftragsverarbeiters den Verantwortlichen im Voraus informiert, wenn eine EU-/MS-rechtliche Anforderung die Verarbeitung / Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation vorschreibt, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Diese Verpflichtung ist mit einer Formulierung, die dem Wortlaut von Artikel 28 Absatz 3 Buchstabe a DSGVO sehr ähnlich ist, in den Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern[107] sowie in mehreren Standardvertragsklauseln enthalten, insbesondere in den Standardvertragsklauseln, die von der dänischen[108], slowenischen[109] und litauischen[110] Aufsichtsbehörde zum Zwecke der Einhaltung von Artikel 28 DSGVO angenommen wurden.

[107] Siehe insbesondere Klausel 7.1 Buchstabe a und Klausel 7.8 Buchstabe a:
– Klausel 7.1 Buchstabe a: „*Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren*." (Hervorhebung hinzugefügt). In ihrer gemeinsamen Stellungnahme zum Entwurf der Standardvertragsklauseln der Kommission empfahlen der EDSA und der EDSA, den vollständigen Wortlaut von Artikel 28 Absatz 3 Buchstabe a aufzunehmen (und somit einen Verweis auf die Pflicht des Auftragsverarbeiters hinzuzufügen, den Verantwortlichen über die rechtliche Anforderung zu informieren), um die Kohärenz zu erhöhen. Gemeinsame Stellungnahme 1/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern für die in Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 genannten Aspekte, Absatz 38. Die Formulierung „*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*" [bzw. „*es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet*", je nach Übersetzung] war bereits im Entwurf der Standardvertragsklauseln enthalten.
– Klausel 7.8 Buchstabe a: „*Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen*". In Bezug auf Klausel 7.8 Buchstabe a empfahlen der EDSA und der EDSB die Aufnahme eines Verweises auf die Möglichkeit für den Auftragsverarbeiter, Datenübermittlungen auf der Grundlage einer spezifischen Anforderung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der der Auftragsverarbeiter unterliegt, vorzunehmen, was ursprünglich in den Entwürfen der Standardvertragsklauseln nicht vorgesehen war. Anhang 2 zur Gemeinsamen Stellungnahme 1/2021 des EDSA und des EDSB, Anmerkungen zu Klausel 7.7 Buchstabe a.

[108] Standardvertragsklauseln der dänischen Aufsichtsbehörde für die Zwecke der Einhaltung von Artikel 28 der DSGVO, insbesondere der Klauseln 4.1 und 8.2. In der Stellungnahme 14/2019 des EDSA zu dem von der DK-AB vorgelegten Entwurf von Standardvertragsklauseln (Art. 28(8) DSGVO) empfahl der EDSA, den Wortlaut von Art. 28 Absatz 3 Buchstabe a aufzunehmen, um Rechtssicherheit zu gewährleisten.

[109] Standardvertragsklauseln der slowenischen Aufsichtsbehörde für die Zwecke der Einhaltung von Artikel 28 der DSGVO, insbesondere Klauseln 3.1 und 7.2.

[110] Standardvertragsklauseln der litauischen Aufsichtsbehörde für die Zwecke der Einhaltung von Artikel 28 der DSGVO, insbesondere Klauseln 4.1, 22 und 23.

103. Neben der Verpflichtung, Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, enthält Artikel 28 Absatz 3 Buchstabe a DSGVO somit drei wesentliche Elemente: (a) eine Regelung für Situationen, in denen der Auftragsverarbeiter aufgrund einer Rechtsvorschrift verpflichtet ist, eine Verarbeitung personenbezogener Daten durchzuführen, die nicht auf den Weisungen des Verantwortlichen beruht und daher nicht im Auftrag des Verantwortlichen erfolgt, (b) die Notwendigkeit, dass der Auftragsverarbeiter den Verantwortlichen informiert[111], und (c) die Bezugnahme darauf, dass sich die rechtliche Verpflichtung aus dem Unionsrecht oder dem Recht der Mitgliedstaaten ergibt.

104. In diesem Zusammenhang erinnert der EDSA an den allgemeinen Grundsatz, dass Verträge das Gesetz nicht außer Kraft setzen können. Das bedeutet, dass unabhängig davon, ob die in Artikel 28 Absatz 3 Buchstabe a DSGVO vorgesehene Klausel („*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*“) in einem Vertrag enthalten ist oder nicht, diese Klausel nicht verhindern kann, dass gesetzliche Anforderungen zusätzlich zu den vertraglichen Anforderungen gelten oder in einigen Fällen sogar im Widerspruch zu diesen stehen. Gemäß dem allgemeinen Grundsatz, dass ein Vertrag keine Verpflichtungen gegenüber Dritten begründet, kann ein Vertrag beispielsweise nicht die Behörden eines Mitgliedstaates oder eines Drittlandes binden[112].

105. In allen Verträgen zwischen einem Verantwortlichen und einem Auftragsverarbeiter müssen Situationen geregelt werden, in denen der Auftragsverarbeiter aufgrund von Rechtsvorschriften verpflichtet werden kann, personenbezogene Daten auf andere Weise als auf der Grundlage der Weisungen des Verantwortlichen zu verarbeiten. Darüber hinaus ist die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen zu informieren, bevor er eine Verarbeitung vornimmt, die nicht auf seinen Weisungen beruht, ebenfalls ein Kernelement des Vertrags, das aufzunehmen ist[113].

106. Bei personenbezogenen Daten, die außerhalb des EWR verarbeitet werden, ist der Verweis auf das Unionsrecht oder das Recht der Mitgliedstaaten möglicherweise nicht sehr sinnvoll, da ein Auftragsverarbeiter außerhalb des EWR nur in Ausnahmefällen den rechtlichen Anforderungen der EU oder der Mitgliedstaaten unterliegt. In diesem Zusammenhang stellt der EDSA fest, dass die Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer, die neben den Anforderungen von Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe d DSGVO die Anforderungen

[111] Art. 28 Absatz 3 Buchstabe a DSGVO sieht vor, dass der Auftragsverarbeiter in Fällen, in denen das Unionsrecht oder das Recht der Mitgliedstaaten den Auftragsverarbeiter verpflichtet, personenbezogene Daten zu verarbeiten, „*dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung [mitteilt], sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet*“.

[112] Aus diesem Grund enthalten die Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer mehrere Garantien, nach denen der Exporteur und der Importeur verpflichtet sind, vor der Übermittlung der Daten die verbindlichen Anforderungen der Rechtsvorschriften eines Drittlandes zu prüfen, um sicherzustellen, dass sie nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist (Klausel 14 Buchstaben a bis d), wobei der Importeur verpflichtet wird, den Exporteur im Falle von Änderungen zu benachrichtigen und der Exporteur verpflichtet wird, entsprechend zu handeln (Klausel 14 Buchstaben e und f); dem Importeur werden für den Fall des Zugangs von Behörden zu den Daten Verpflichtungen auferlegt (Klausel 15). Siehe Schrems-II-Urteil, Rn. 125 und 141.

[113] In der Stellungnahme 18/2021 des EDSA zu dem von der litauischen Aufsichtsbehörde vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO) empfahl der EDSA, das letzte Element von Artikel 28 Absatz 3 Buchstabe a in die Standardvertragsklauseln aufzunehmen (d. h. die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen über die geltende rechtliche Anforderung zu informieren), EDSA-Stellungnahme 18/2021, Absatz 19.

von Artikel 28 Absätze 3 und 4 DSGVO erfüllen sollen,[114] keine Formulierung enthalten, die der „Sofern-nicht"-Klausel in Artikel 28 Absatz 3 Buchstabe a DSGVO vergleichbar ist. Die Verpflichtung, personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, sofern dies nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgeschrieben ist, wird jedoch bereits indirekt in Klausel 8.1 der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer geregelt.[115] Darüber hinaus bedeutet dies nicht, dass die Informationspflicht nach Artikel 28 Absatz 3 Buchstabe a DSGVO nicht berücksichtigt wird, da die Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer ausdrücklich vorsehen, dass der Datenimporteur den Datenexporteur informieren muss, wenn er nicht in der Lage ist, den Weisungen des Verantwortlichen Folge zu leisten[116]. Folglich ergibt sich die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen zu informieren, wenn eine rechtliche Verpflichtung zur Verarbeitung besteht (unabhängig davon, ob sie sich aus dem Recht der EU oder der Mitgliedstaaten oder aus dem Recht eines Drittlandes ergibt), aus den Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer, ohne dass der genaue Wortlaut „*sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist*" von Artikel 28 Absatz 3 Buchstabe a DSGVO verwendet wird (oben erwähntes Element c).

---

[114] Siehe Erwägungsgrund 9 der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer: „*Umfasst die Verarbeitung Datenübermittlungen von der Verordnung (EU) 2016/679 unterliegenden Verantwortlichen an Auftragsverarbeiter außerhalb des räumlichen Anwendungsbereichs dieser Verordnung oder von der Verordnung (EU) 2016/679 unterliegenden Auftragsverarbeitern an Unterauftragsverarbeiter außerhalb des räumlichen Anwendungsbereichs dieser Verordnung, so sollten die Standardvertragsklauseln im Anhang dieses Beschlusses auch die Erfüllung der Anforderungen in Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 ermöglichen.*"

[115] Klausel 8 zu Datenschutzgarantien (Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter) enthält in Klausel 8.1 (Weisungen) folgende Bestimmung:
„*a) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.*
b) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann."
Modul drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) enthält in Klausel 8 (Datenschutzgarantien) unter Klausel 8.1 (Weisungen) eine ähnliche Bestimmung:
„*a) Der Datenexporteur hat dem Datenimporteur mitgeteilt, dass er als Auftragsverarbeiter nach den Weisungen seines/seiner Verantwortlichen fungiert, und der Datenexporteur stellt dem Datenimporteur diese Weisungen vor der Verarbeitung zur Verfügung.*
b) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, sowie auf der Grundlage aller zusätzlichen dokumentierten Weisungen des Datenexporteurs. Diese zusätzlichen Weisungen dürfen nicht im Widerspruch zu den Weisungen des Verantwortlichen stehen. Der Verantwortliche oder der Datenexporteur kann während der gesamten Vertragslaufzeit weitere dokumentierte Weisungen im Hinblick auf die Datenverarbeitung erteilen.
c) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann. Ist der Datenimporteur nicht in der Lage, die Weisungen des Verantwortlichen zu befolgen, setzt der Datenexporteur den Verantwortlichen unverzüglich davon in Kenntnis."

[116] Zusätzlich zu Klausel 8.1 (siehe vorherige Fußnote) besagt Klausel 14 unter 14.e Folgendes: „*Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht. [In Bezug auf Modul drei: Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.]*"

107. Dies steht im Einklang mit dem Ziel gemäß Artikel 28 Absatz 3 Buchstabe a DSGVO sicherzustellen, dass der Verantwortliche informiert wird, wenn der Auftragsverarbeiter gesetzlich verpflichtet ist, personenbezogene Daten auf andere Weise als auf Weisung des Verantwortlichen zu verarbeiten.

108. In Anbetracht der vorstehenden Analyse ist der EDSA der Ansicht, dass dringend empfohlen, aber nicht zwingend erforderlich ist, die in Artikel 28 Absatz 3 Buchstabe a DSGVO vorgesehenen Ausnahme, „sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist" (wörtlich übernommen oder sehr ähnlich formuliert) in einen Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter[117] aufzunehmen, um Artikel 28 Absatz 3 Buchstabe a DSGVO einzuhalten. Dieser Standpunkt berührt nicht die Notwendigkeit einer vertraglichen Verpflichtung zur Unterrichtung des Verantwortlichen, wenn der Auftragsverarbeiter gesetzlich verpflichtet ist, personenbezogene Daten auf andere Weise als auf Weisung des Verantwortlichen zu verarbeiten, wie sie in Artikel 28 Absatz 3 Buchstabe a DSGVO vorgesehen ist. Wenn klar ist, dass die rechtlichen Anforderungen der EU oder der Mitgliedstaaten für die Verarbeitung relevant sind, würde die Verwendung des Wortlauts von Artikel 28 Absatz 3 Buchstabe a DSGVO helfen, dessen Einhaltung nachzuweisen.

109. Der EDSA befasst sich nun mit der Frage, ob der Vertrag, der eine weitergehende Ausnahme enthält, die auch das Recht eines Drittlands abdeckt, wie beispielsweise eine Ausnahme von der Verpflichtung, die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen zu verarbeiten, „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*", an sich einen Verstoß gegen Artikel 28 Absatz 3 Buchstabe a DSGVO darstellt.

110. Diese Formulierung kann, wenn sie nicht konkretisierend ergänzt wird, zwei unterschiedliche Situationen umfassen, die im Lichte des rechtlichen Kontextes getrennt analysiert werden sollten:

- die betreffende gesetzliche Verpflichtung oder verbindliche Anordnung ergibt sich aus dem Unionsrecht oder dem Recht der Mitgliedstaaten des Europäischen Wirtschaftsraums (EWR);
- die betreffende gesetzliche Verpflichtung oder verbindliche Anordnung ergibt sich aus anderen Rechtsvorschriften als dem Unionsrecht oder dem Recht der Mitgliedstaaten des EWR.

[117] Dies gilt insbesondere für den Fall, dass sich der Verantwortliche und der Auftragsverarbeiter auf ihren eigenen Verarbeitungsvertrag statt auf die Standardvertragsklauseln der Kommission zwischen Verantwortlichen und Auftragsverarbeitern stützen, auf Standardvertragsklauseln, die von den Aufsichtsbehörden für die Zwecke der Einhaltung von Artikel 28 der DSGVO angenommen wurden, oder die Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer. Siehe auch Erwägungsgrund 109 und Erwägungsgrund 28 Absatz 6 der Verordnung (EU) 2016/679.

111. Der erstgenannte Fall fällt unter die ausdrücklichen Bestimmungen von Artikel 28 Absatz 3 Buchstabe a DSGVO, der eine vertragliche Verpflichtung des Auftragsverarbeiters vorsieht, die Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, *„sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist"*. Dies gilt unabhängig davon, ob die Verarbeitung personenbezogener Daten innerhalb oder außerhalb des EWR erfolgt.

112. Das EU-Recht, einschließlich der DSGVO und der Rechtsvorschriften der Mitgliedstaaten, steht in derselben Verfassungstradition wie die DSGVO, die den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten als Grundrecht in Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union („**AEUV**") und Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union („**Charta**") festschreibt[118].

113. Wenn die Parteien auf der Grundlage anderer Elemente ihres Vertrags bzw. ihrer Verträge nachweisen können, dass nur diese erstgenannte Situation von der Formulierung *„sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*" abgedeckt wird, hat diese Formulierung keine Auswirkungen auf die in Artikel 28 Absatz 3 Buchstabe a DSGVO vorgesehenen Garantien.

114. Es wird Fälle geben, in denen der Vertrag bzw. die Verträge der Parteien über diese erstgenannte Situation hinausgehen, was bedeutet, dass ein Verweis auf *„das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle*" auch gesetzliche Verpflichtungen / verbindliche Anordnungen umfasst, die sich aus anderen Gesetzen als dem Unionsrecht oder dem Recht der (EWR-)Mitgliedstaaten ergeben (zweitgenannte Situation).

115. Der EDSA stellt fest, dass Anforderungen an die Verarbeitung von Daten, die auf anderen Gesetzen als dem Unionsrecht oder dem Recht der (EWR-)Mitgliedstaaten beruhen, nicht per se die gleiche verfassungsrechtliche Tradition haben und nicht automatisch mit jenen innerhalb der EU-Rechtsordnung gleichgesetzt werden können (im Lichte von Artikel 44 DSGVO). In diesem Zusammenhang erinnert der EDSA daran, dass sich die Begriffe „rechtliche Verpflichtung", „öffentliches Interesse" und „öffentliche Gewalt" gemäß Artikel 6 DSGVO auf das Recht der Union oder der Mitgliedstaaten beziehen[119]. Ebenso stellt der EDSA fest, dass Artikel 29 DSGVO über die Verarbeitung durch dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen Folgendes vorsieht: *„Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem*

[118] In Erwägungsgrund 1 der DSGVO wird auf Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") verwiesen. Nach Artikel 52 Absatz 1 der Charta muss jede *„Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten [...] gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Vorbehaltlich des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der EU anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen."*

[119] Art. 6 Absatz 3 DSGVO sieht vor, dass in Fällen, in denen die Rechtsgrundlage für die Verarbeitung eine „rechtliche Verpflichtung" (Artikel 6 Absatz 1 Buchstabe c DSGVO) oder „eine Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde" (Artikel 6 Absatz 1 Buchstabe e DSGVO) ist, sich dies auf Bestimmungen des Unionsrechts oder des Rechts der Mitgliedstaaten bezieht, denen der Verantwortliche unterliegt. Unter Bezugnahme auf Artikel 6 DSGVO wird in Erwägungsgrund 40 der DSGVO erläutert, dass, wenn die Rechtsgrundlage für die Verarbeitung gesetzlich geregelt ist, dies *„sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt*" bedeutet. Nach Artikel 49 Absatz 4 DSGVO können nur öffentliche Interessen, die im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sind, zur Anwendung dieser Ausnahmeregelung führen.

Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind" (Hervorhebungen hinzugefügt).

116. Im Zusammenhang mit Übermittlungen ist vorhersehbar, dass sich gesetzliche Verpflichtungen auch aus anderen Rechtsvorschriften als dem Unionsrecht oder dem Recht der Mitgliedstaaten ergeben können. Der EDSA erinnert daran, dass im Falle von Übermittlungen zusätzlich zu Artikel 28 DSGVO auch Kapitel V der DSGVO gilt. Der EDSA ist der Ansicht, dass Artikel 28 Absatz 3 Buchstabe a DSGVO in Bezug auf personenbezogene Daten, die außerhalb des EWR verarbeitet werden, nicht per se der Aufnahme von Bestimmungen in den Vertrag entgegensteht, die die Verpflichtungen des Rechts eines Drittlandes in Bezug auf die Verarbeitung übermittelter personenbezogener Daten betreffen. Solche Bestimmungen können insbesondere aufgenommen werden, um die Einhaltung von Kapitel V der DSGVO zu gewährleisten, jedoch ist es sehr unwahrscheinlich, dass die bloße Aufnahme des Wortlauts „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*" ausreicht.

117. In diesem Zusammenhang stellt der EDSA fest, dass in den Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer ausdrücklich auf „lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken" in Klausel 14 und auf „Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten" in Klausel 15 eingegangen wird. Vor der Unterzeichnung von Standardvertragsklauseln müssen die Parteien prüfen, ob es lokale Rechtsvorschriften und Gepflogenheiten gibt, die sich auf die Einhaltung der Klauseln auswirken (Klausel 14 der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer). Nach Klausel 14 müssen die Parteien gewährleisten, dass sie sich keiner Rechtsvorschriften und Gepflogenheiten in dem Drittland, in dem der Importeur seinen Sitz hat, bewusst sind, die ihn daran hindern würden, seinen Verpflichtungen aus den Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer nachzukommen, nachdem der Importeur diese Rechtsvorschriften und Gepflogenheiten geprüft hat; zudem verpflichtet die Klausel den Importeur, dem Exporteur unverzüglich jede Änderung mitzuteilen; in diesem Fall legt der Exporteur entweder geeignete Abhilfemaßnahmen fest, oder Klausel 14 erlaubt es ihm, die Übermittlung auszusetzen und sogar den Vertrag zu kündigen. Klausel 15 erlegt dem Datenimporteur im Falle des Zugriffs von Drittlandbehörden auf die Daten bestimmte Verpflichtungen auf. Sie legt eine Reihe von Schritten fest, die der Datenimporteur umsetzen muss, wenn er mit dem Zugriff durch Drittlandbehörden (entweder auf Ersuchen oder direkt) konfrontiert wird, um (letztendlich) sicherzustellen, dass der Verantwortliche informiert wird. Neben der Verpflichtung, den Datenexporteur zu benachrichtigen, ist der Importeur unter anderem verpflichtet, die Rechtmäßigkeit des Zugriffsersuchens zu prüfen und diese rechtliche Bewertung zu dokumentieren, und er ist verpflichtet, das Ersuchen in bestimmten Fällen anzufechten. Der Datenexporteur ist dann in der Lage – in Absprache mit dem Verantwortlichen, sofern es sich bei dem Datenexporteur nicht um den Verantwortlichen handelt, die erforderlichen Maßnahmen zu ergreifen, einschließlich einer möglichen Aussetzung der Übermittlung oder Beendigung der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer. Ob (Weiter-)Übermittlungen an staatliche Stellen des Drittlandes mit der DSGVO im Einklang stehen, hängt von einer Einzelfallanalyse ab (unter anderem in Bezug auf die Rechtsgrundlage, die Verantwortlichkeit und die Einhaltung von Kapitel V der DSGVO). Gemäß Modul 3 der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) ist der Datenimporteur/Auftragsverarbeiter verpflichtet, dem Datenexporteur die rechtliche Beurteilung zur Verfügung zu stellen. In diesem Zusammenhang verweist der EDSA auch auf die vorstehenden Absätze 88 bis 89 und 106.

118. Darüber hinaus sind sowohl der Datenexporteur als auch der Datenimporteur nach den Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer verpflichtet, sich vor der Übermittlung personenbezogener Daten in ein bestimmtes Drittland zu vergewissern, dass das Recht dieses Drittlands es dem Empfänger erlaubt, die Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer einzuhalten[120]. Exportiert der Auftragsverarbeiter personenbezogene Daten im Namen des Verantwortlichen, so obliegt diese Verpflichtung auch dem Verantwortlichen (siehe auch Absätze 79 ff.).

119. Ebenso enthalten die Empfehlungen für BCR (binding corporate rules, dt. verbindliche interne Datenschutzvorschriften) für Verantwortliche und die Empfehlungen für BCR für Auftragsverarbeiter eine Reihe von Verpflichtungen für den Fall, dass ein BCR-Mitglied einem Konflikt zwischen seinen lokalen Rechtsvorschriften und den verbindlichen internen Datenschutzvorschriften unterliegt[121] und/oder von einer Strafverfolgungsbehörde oder einer für die nationale Sicherheit zuständigen Stelle zur Offenlegung aufgefordert wird[122]. Konkret wird in den Empfehlungen 1/2022 des EDSA[123] darauf hingewiesen, dass verbindliche interne Datenschutzvorschriften für Verantwortliche (BCR-C) Klauseln enthalten sollten, die sich auf lokale Rechtsvorschriften und Gepflogenheiten beziehen, die sich auf die Einhaltung der BCR-C auswirken (Abschnitt 5.4.1). Zudem sollten sie die Pflichten des Datenimporteurs bei Auskunftsersuchen staatlicher Stellen enthalten (Abschnitt 5.4.2). BCR-C können als Übermittlungsmechanismus für Übermittlungen an Auftragsverarbeiter innerhalb der Gruppe dienen.

120. In Fällen, in denen die Übermittlungen durch Angemessenheitsbeschlüsse abgedeckt sind, gehören die Rechtsvorschriften über den „*Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften*“ zu den Elementen, die die Europäische Kommission bei der Bewertung der Angemessenheit des Schutzniveaus gemäß Artikel 45 Absatz 2 Buchstabe a DSGVO berücksichtigen muss[124].

[120] Schrems-II-Urteil, Rn. 141. Siehe auch Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer, Klausel 14 Buchstaben a bis d.

[121] Abschnitt 5.4.1 „Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der BCR-C auswirken“, Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO). Abschnitt 6.3 „Transparenzerfordernis bei nationalen Rechtsvorschriften, die die Gruppe an der Einhaltung der BCR hindern“ des Arbeitsdokuments der Artikel-29-Datenschutzgruppe, Arbeitspapier mit einer Übersicht der Bestandteile und Grundsätze in verbindlichen internen Datenschutzvorschriften, WP 257 rev.01, am 25. Mai 2018 vom EDSA angenommen.

[122] Abschnitt 5.4.2 „Pflichten des Datenimporteurs bei Auskunftsersuchen staatlicher Stellen“, EDSA-Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO); siehe auch Abschnitt 6.3 „Transparenzerfordernis bei nationalen Rechtsvorschriften, die die Gruppe an der Einhaltung der VID hindern“, Arbeitspapier mit einer Übersicht der Bestandteile und Grundsätze in verbindlichen internen Datenschutzvorschriften, WP 257 rev.01.

[123] EDSA-Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO).

[124] Der EuGH hat sich in seinen Urteilen in den Rechtssachen Schrems I und Schrems II mit diesem Aspekt befasst. Urteil des EuGH vom 6. Oktober 2015, *Maximillian Schrems gegen Data Protection Commissioner* (im Folgenden „Schrems-I-Urteil“), C-362/14, ECLI:EU:C:2015:650, Rn. 91 ff. Schrems-II-Urteil, Rn. 141, 174-177, 187-189.

121. Was den Angemessenheitsbeschlüssen[125], den Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer[126] und den BCR-Empfehlungen[127] gemeinsam ist, ist das Verständnis, dass Rechtsvorschriften und Gepflogenheiten eines Drittlands, die den Wesensgehalt der im AEUV, in der Charta und in der DSGVO verankerten Grundrechte und Grundfreiheiten achten und nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist, um eines der in Artikel 23 Absatz 1 DSGVO aufgeführten Ziele zu schützen, das durch die DSGVO gewährleistete Schutzniveau nicht untergraben[128]. Aus diesem Grund enthalten die Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer[129] und die BCR-Empfehlungen[130] Bestimmungen, die Rechtsvorschriften und Gepflogenheiten in Abhängigkeit davon, ob sie das durch die DSGVO gewährleistete Schutzniveau untergraben, unterschiedliche Folgen beimessen. Ad-hoc-Vertragsklauseln auf der Grundlage von Artikel 46 Absatz 3 Buchstabe a DSGVO sollten ebenfalls ähnliche Bestimmungen enthalten.[131]

122. Aus den obigen Ausführungen geht eindeutig hervor, dass dann, wenn Rechtsvorschriften des Drittlandes den Auftragsverarbeiter verpflichten, personenbezogene Daten außerhalb der Weisungen des Verantwortlichen zu verarbeiten, das in der DSGVO verankerte Schutzniveau nur dann eingehalten wird, wenn diese Rechtsvorschriften die oben genannten Bedingungen erfüllen. In jedem Fall sollte der Auftragsverarbeiter zusätzliche Maßnahmen ergreifen, falls die genannten Bedingungen nicht erfüllt sind, und der Vertrag sollte sicherstellen, dass diese Bedingungen erfüllt sind.

123. Wenn der Auftragsverarbeiter personenbezogene Daten innerhalb des EWR verarbeitet, kann er unter bestimmten Umständen dennoch mit dem Recht eines Drittlandes konfrontiert werden. Der EDSA

---

[125] Siehe Artikel 45 Absatz 2 Buchstabe a DSGVO, wonach die Europäische Kommission Folgendes berücksichtigen muss: „*die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, und der Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden*“. Siehe auch Artikel-29-Arbeitsgruppe, Arbeitspapier der Artikel-29-Datenschutzgruppe „Referenzgrundlage für Angemessenheit“ (WP 254 rev.01), angenommen am 6. Februar 2018, gebilligt vom EDSA am 25. Mai 2018. Das Konzept des „angemessenen Schutzniveaus“ wurde vom EuGH in seinen Urteilen im Schrems-I-Urteil (Rn. 73 und 74) und im Schrems-II-Urteil (Rn. 94) weiter ausgeführt.

[126] Klausel 14 Buchstabe a der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer.

[127] Dies wird in den EDSA-Empfehlungen 1/2022 („VID-V-Empfehlungen“), Version 2.1, in den Abschnitten 5.4.1 und 5.4.2 ausdrücklich beschrieben. Dasselbe Verständnis bildet die Grundlage von Abschnitt 6.3 „Transparenzerfordernis bei nationalen Rechtsvorschriften, die die Gruppe an der Einhaltung der VID hindern“ des Arbeitsdokuments der Artikel-29-Datenschutzgruppe, Arbeitspapier mit einer Übersicht der Bestandteile und Grundsätze in verbindlichen internen Datenschutzvorschriften, WP 257 rev.01, am 25. Mai 2018 vom EDSA angenommen.

[128] Siehe EDSA-Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Absatz 38, und Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, Absätze 22 und 24.

[129] Klausel 14 der Standardvertragsklauseln der Kommission für die Übermittlung an Drittländer.

[130] Siehe Fußnote 127.

[131] Siehe EDSA-Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Absatz 66.

unterstreicht, dass die Aufnahme eines Verweises auf das Recht eines Drittlandes in den Vertrag den Auftragsverarbeiter nicht von seinen Verpflichtungen gemäß der DSGVO entbindet.

124. In Anbetracht der obigen Analyse ist der EDSA der Ansicht, dass Formulierungen, die dem Wortlaut „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*“ ähneln, im Rahmen der Vertragsfreiheit der Parteien liegen und an sich nicht gegen Artikel 28 Absatz 3 Buchstabe a der DSGVO verstoßen. Dies gilt unbeschadet der Verpflichtung, bei der Verarbeitung personenbezogener Daten die Bestimmungen der DSGVO einzuhalten. Darüber hinaus entbindet eine solche Klausel den Verantwortlichen und den Auftragsverarbeiter nicht von der Einhaltung ihrer Verpflichtungen gemäß der DSGVO, insbesondere hinsichtlich der Informationen, die dem Verantwortlichen zur Verfügung zu stellen sind, und - soweit anwendbar - der Bedingungen für die Übermittlung personenbezogener Daten, die im Auftrag des Verantwortlichen verarbeitet werden, an Drittländer[132].

125. Schließlich wird im Ersuchen eine darauf aufbauende Frage gestellt:

> Wenn Frage 2a verneint wird, sollte eine solche erweiterte Ausnahme stattdessen als dokumentierte Weisung des Verantwortlichen im Sinne von Artikel 28 Absatz 3 Buchstabe a DSGVO verstanden werden?

126. In Anbetracht der oben gegebenen Antwort versteht der EDSA die verbleibende Frage dahingehend, ob die Parteien behaupten können, dass die Formulierung „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*“ (wörtlich übernommen oder sehr ähnlich formuliert) in ihrem Vertrag als eine dokumentierte Weisung des Verantwortlichen im Sinne von Artikel 28 Absatz 3 Buchstabe a DSGVO auszulegen ist.

127. Der EDSA prüft zunächst, ob dieses Argument stichhaltig ist, wenn sich die gesetzliche Anforderung oder die verbindliche Anordnung aus dem Unionsrecht oder dem Recht eines (EWR-)Mitgliedstaats ergibt.

128. Der EDSA stellt fest, dass sich der Begriff „Weisungen“, wie er in Artikel 28 Absatz 3 Buchstabe a DSGVO verwendet wird, speziell auf den Verantwortlichen bezieht, der festlegt, welche Datenverarbeitung der Auftragsverarbeiter in seinem Auftrag wie vornimmt[133]. Jede Bestimmung, die der Verantwortliche in den Vertrag mit seinem Dienstleister/Auftragsverarbeiter aufnimmt und die nicht in einer Aufforderung zur Verarbeitung personenbezogener Daten im Namen des Verantwortlichen besteht, gilt auch nicht als Weisung im Sinne von Artikel 28 Absatz 3 Buchstabe a DSGVO. Darüber hinaus müssten die Weisungen des Verantwortlichen hinreichend genau sein, um eine bestimmte Verarbeitung personenbezogener Daten abzudecken, was bei der fraglichen Formulierung nicht der Fall ist. Darüber hinaus wäre der Verantwortliche immer in der Lage (müsste immer in der Lage sein) – und rechtlich verpflichtet, soweit eine Weisung zur Verarbeitung personenbezogener Daten im Namen des Verantwortlichen gegen die DSGVO verstoßen würde –, eine solche Weisung zu widerrufen. Der Auftragsverarbeiter sollte dann der Rücknahme seiner Weisung durch den Verantwortlichen Folge leisten und die Verarbeitung einstellen.

129. Durch die Erteilung von Weisungen an den Auftragsverarbeiter setzt der Verantwortliche seine Festlegung der Zwecke und Mittel der Datenverarbeitung in die Praxis um, indem er insbesondere

---

[132] Hierzu zählt insbesondere die Verpflichtung des Verantwortlichen, sicherzustellen, dass in Bezug auf die Verarbeitung außerhalb des EWR nur Rechtsvorschriften von Drittländern, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleisten, eine Verarbeitung durch den Auftragsverarbeiter erfordern. Vgl. auch Absätze 116 bis 122.

[133] EDSA-Leitlinien 07/2020, Absatz 116.

Einfluss auf die Schlüsselelemente der Verarbeitung ausübt.[134] Grundsätzlich erlischt der Einfluss des Verantwortlichen auf die Verarbeitung personenbezogener Daten, wenn das Unionsrecht oder das Recht der Mitgliedstaaten Anforderungen an den Auftragsverarbeiter hinsichtlich der Durchführung der Verarbeitung personenbezogener Daten festlegen, die der Verantwortliche nicht steuern oder einstellen kann.[135] Auch wenn der Verantwortliche den Auftragsverarbeiter daran erinnern könnte, sich an das Unionsrecht oder das Recht der Mitgliedstaaten zu halten, kann dies nicht als Weisung im Sinne von Artikel 28 Absatz 3 Buchstabe a DSGVO verstanden werden[136]. Die DSGVO selbst erkennt diesen Sachverhalt an, indem sie darauf hinweist, dass der Auftragsverarbeiter die Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten darf, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (Artikel 28 Absatz 3 Buchstabe a DSGVO), und dass er den Verantwortlichen unverzüglich unterrichten muss, wenn eine Weisung gegen die DSGVO verstößt (Artikel 28 Absatz 3 letzter Unterabsatz DSGVO).

130. Der EDSA ist der Ansicht, dass die obige Argumentation auch dann gilt, wenn sich die gesetzliche Anforderung oder verbindliche Anordnung aus dem Recht eines Drittlandes ergibt. In diesem Fall begrenzt das betreffende Recht den Einfluss, den der Verantwortliche auf die Datenverarbeitung ausüben kann.

131. Darüber hinaus zeigt eine Klausel, mit der sich ein Auftragsverarbeiter verpflichtet, personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*“, dass die Verarbeitung auf Weisung des Verantwortlichen die Regel ist, während die Ausnahme gerade für die Verarbeitung ohne Weisung des Verantwortlichen gilt (wie die Formulierung „sofern nicht“ zeigt). Darüber hinaus ist es nach wie vor die Entscheidung des Auftragsverarbeiters, ob er der gesetzlichen Anforderung oder der verbindlichen Anordnung, an die er gebunden ist, nachkommt oder ob er die rechtlichen Folgen einer Nichtbefolgung trägt.

132. Auf dieser Grundlage kommt der EDSA zu dem Schluss, dass „*sofern er nicht durch das geltende Recht oder eine verbindliche Anordnung einer staatlichen Stelle hierzu verpflichtet ist*“ (wörtlich übernommen oder sehr ähnlich formuliert) nicht als dokumentierte Weisung des Verantwortlichen verstanden werden kann. Der Verantwortliche bleibt verantwortlich, wenn er nicht sichergestellt hat, dass der (Unter-)Auftragsverarbeiter personenbezogene Daten nur auf seine dokumentierten Weisungen hin verarbeitet. Dies gilt jedoch nicht, wenn die Verarbeitung nach dem EU-Recht oder dem Recht der Mitgliedstaaten oder für die Verarbeitung außerhalb des EWR nach dem Recht eines Drittlandes, dem der (Unter-)Auftragsverarbeiter unterliegt, vorgeschrieben ist und dieses Recht ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet.

Für den Europäischen Datenschutzausschuss

Der Vorsitz

[134] EDSA-Leitlinien 07/2020, Absatz 20.

[135] In diesem Zusammenhang könnte es sich um die in Artikel 4 Nummer 7 der DSGVO vorgesehene Situation handeln, wonach der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung in Fällen, in denen die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind, nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden können. Siehe Urteil des EuGH vom 11. Januar 2024, *État belge (Amtsblatt eines Mitgliedstaats),* Rechtssache C-231/22, ECLI:EU:C:2024:7, Rn. 28-30, 35 und 39; EDSA-Leitlinien 07/2020, Absätze 22-24.

[136] Vielmehr wird eine solche Erinnerung als vertragliche Garantien vonseiten des Verantwortlichen angesehen, die sicherstellen, dass die Verarbeitung im Namen des Verantwortlichen alle Anforderungen der DSGVO erfüllt und den Schutz der Rechte der betroffenen Person gewährleistet.

(Anu Talus)