

Leitlinien



Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten zwischen Behörden und öffentlichen Stellen im EWR und Behörden und öffentlichen Stellen außerhalb des EWR

Version 2.0

Angenommen am 15. Dezember 2020

Versionsverlauf

Version 2.0	15. Dezember 2020	Annahme der Leitlinien nach öffentlicher Konsultation
Version 1.0	18. Februar 2020	Annahme der Leitlinien für die öffentliche Konsultation

Inhaltsverzeichnis

1	Allgemeines	5
1.1	Zweck	5
1.2	Allgemeine Vorschriften für internationale Datenübermittlungen.....	6
1.3	Definition einer Behörde oder öffentlichen Stelle.....	6
2	Allgemeine Empfehlungen für die geeigneten Garantien gemäß Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b DSGVO.....	7
2.1	Zweck und Anwendungsbereich	8
2.2	Begriffsbestimmungen.....	8
2.3	Datenschutzgrundsätze	8
2.3.1	Zweckbindung	Error! Bookmark not defined.
2.3.2	Datenrichtigkeit und -minimierung	9
2.3.3	Speicherbegrenzung	9
2.3.4	Sicherheit und Vertraulichkeit von Daten	10
2.4	Rechte der betroffenen Personen	10
2.4.1	Recht auf Transparenz.....	11
2.4.2	Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch.....	11
2.4.3	Automatisierte Entscheidungen im Einzelfall.....	12
2.4.4	Recht auf Rechtsbehelf.....	13
2.4.5	Beschränkungen der Rechte der betroffenen Person.....	13
2.5	Beschränkungen der Weiterübermittlung und der Weitergabe von Daten (einschließlich der Offenlegung und des staatlichen Zugriffs).....	13
2.6	Sensible Daten	15
2.7	Rechtsbehelfsmechanismen	15
2.8	Überwachungsmechanismen.....	17
2.9	Kündigungsklausel	18
3	Besondere Hinweise zu Artikel 46 DSGVO	19
3.1	Besondere Hinweise zu rechtlich bindenden und durchsetzbaren Dokumenten – Artikel 46 Absatz 2 Buchstabe a DSGVO	19
3.2	Besondere Hinweise zu Verwaltungsvereinbarungen – Artikel 46 Absatz 3 Buchstabe b DSGVO.....	19
4	Verfahrensfragen.....	21

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e 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 (Datenschutz-Grundverordnung, im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung¹,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

¹ Soweit in diesen Leitlinien auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

1 ALLGEMEINES

1.1 Zweck

1. Dieses Dokument soll eine Anleitung für die Anwendung von Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b der Datenschutz-Grundverordnung (DSGVO) für die Übermittlung personenbezogener Daten von Behörden oder öffentlichen Stellen im EWR (im Folgenden „öffentliche Stellen“) an öffentliche Stellen in Drittländern oder internationale Organisationen bieten, soweit solche Übermittlungen nicht durch einen von der Europäischen Kommission angenommenen Angemessenheitsbeschluss abgedeckt sind.² Öffentliche Stellen können diese Mechanismen, die ihren Rahmenbedingungen laut DSGVO besser Rechnung tragen, nutzen, dürfen aber auch andere für sie anwendbare Instrumente einsetzen, die geeignete Garantien im Sinne von Artikel 46 DSGVO vorsehen.
2. Mit diesen Leitlinien sollen die Erwartungen des Europäischen Datenschutzausschusses (EDSA) hinsichtlich der Garantien klargestellt werden, die durch rechtlich bindende und durchsetzbare Dokumente gemäß Artikel 46 Absatz 2 Buchstabe a DSGVO zwischen öffentlichen Stellen oder – vorbehaltlich der Genehmigung der zuständigen Aufsichtsbehörde – durch Bestimmungen zu gewähren sind, die in Verwaltungsvereinbarungen zwischen öffentlichen Stellen gemäß Artikel 46 Absatz 3 Buchstabe b DSGVO aufzunehmen sind.³ Der EDSA empfiehlt den Parteien nachdrücklich, diese Leitlinien frühzeitig als Referenz heranzuziehen, sofern sie beabsichtigen, solche Dokumente oder Vereinbarungen abzuschließen oder zu ändern.⁴
3. Die Leitlinien sind in Verbindung mit der bisherigen Arbeit des EDSA (einschließlich der von seinem Vorgänger, der Artikel-29-Datenschutzgruppe⁵, gebilligten Dokumente) zu den zentralen Fragen des räumlichen Anwendungsbereichs und der Übermittlung personenbezogener Daten an Drittländer zu lesen.⁶ Die Leitlinien werden auf der Grundlage der praktischen Erfahrung mit der Anwendung der DSGVO überprüft und bei Bedarf aktualisiert.
4. Diese Leitlinien betreffen internationale Datenübermittlungen zwischen öffentlichen Stellen für verschiedene Zwecke der Verwaltungszusammenarbeit, die in den Anwendungsbereich der DSGVO fallen. Folglich finden sie gemäß Artikel 2 Absatz 2 DSGVO keine Anwendung auf Übermittlungen im Bereich der öffentlichen Sicherheit, der Landesverteidigung oder der nationalen Sicherheit. Darüber hinaus betreffen sie nicht die Verarbeitung und Übermittlung von Daten durch zuständige Behörden zu Strafverfolgungszwecken, da hierfür ein gesondertes spezifisches Rechtsinstrument, die Richtlinie zum Datenschutz bei der Strafverfolgung⁷, gilt. Die Leitlinien beziehen sich nur auf Übermittlungen

² Beispielsweise japanische öffentliche Stellen, die nicht unter den Angemessenheitsbeschluss für Japan fallen, da dieser nur Organisationen des privaten Sektors abdeckt.

³ In diesen Leitlinien wird der Begriff „internationale Übereinkünfte“ verwendet, um rechtlich bindende und durchsetzbare Dokumente gemäß Artikel 46 Absatz 2 Buchstabe a DSGVO und Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b DSGVO zu bezeichnen.

⁴ Gemäß Artikel 96 DSGVO bleiben Übereinkünfte, die vor dem 24. Mai 2016 abgeschlossen wurden, in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

⁵ Die Arbeitsgruppe der EU-Datenschutzbehörden, die gemäß Artikel 29 der Datenschutzrichtlinie 95/46/EG eingesetzt wurde.

⁶ Siehe Artikel-29-Datenschutzgruppe, Referenzgrundlage für Angemessenheit (WP254 rev.01, vom EDSA am 25. Mai 2018 gebilligt), EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, und EDSA, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3).

⁷ Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.

zwischen öffentlichen Stellen und nicht auf Übermittlungen personenbezogener Daten von einer öffentlichen Stelle an eine private Einrichtung oder von einer privaten Einrichtung an eine öffentliche Stelle.

1.2 Allgemeine Vorschriften für internationale Datenübermittlungen

5. Gemäß Artikel 44 DSGVO muss der Datenexporteur, der personenbezogene Daten an Drittländer oder internationale Organisationen übermittelt, nicht nur Kapitel V der DSGVO einhalten, sondern auch die sonstigen Bestimmungen der DSGVO erfüllen. Insbesondere muss jede Verarbeitungstätigkeit mit den Datenschutzgrundsätzen in Artikel 5 DSGVO übereinstimmen, im Einklang mit Artikel 6 DSGVO rechtmäßig sein und im Falle besonderer Kategorien personenbezogener Daten Artikel 9 DSGVO entsprechen. Daher ist eine zweistufige Prüfung durchzuführen: Zunächst gilt es zu prüfen, ob eine für die Datenverarbeitung als solche geltende Rechtsgrundlage existiert, die zusammen mit allen einschlägigen Bestimmungen der DSGVO angewendet wird; zudem ist zu prüfen, ob die Bestimmungen des Kapitels V der DSGVO eingehalten werden.
6. In Artikel 46 Absatz 1 der DSGVO heißt es: *„Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.“* Solche geeigneten Garantien können durch rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen (Artikel 46 Absatz 2 Buchstabe a DSGVO) oder – vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde – durch Bestimmungen gewährt werden, die in Verwaltungsvereinbarungen zwischen öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen (Artikel 46 Absatz 3 Buchstabe b DSGVO). Wie der Gerichtshof der Europäischen Union (EuGH) klargestellt hat, müssen die geeigneten Garantien so beschaffen sein, dass sie für Personen, deren personenbezogene Daten übermittelt werden, ein Schutzniveau gewährleisten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist.⁸
7. Neben dieser Lösung und in ihrer Ermangelung sind in Artikel 49 DSGVO auch eine begrenzte Anzahl bestimmter Fälle aufgeführt, in denen internationale Datenübermittlungen stattfinden können, wenn keine Angemessenheitsfeststellung der Europäischen Kommission vorliegt.⁹ Eine Ausnahme gilt beispielsweise, wenn sich aus dem Unionsrecht oder dem Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, ergibt, dass derartige Datenübermittlungen zum Zwecke der Wahrung wichtiger öffentlicher Interessen zulässig sind, was auch den Grundsatz der Gegenseitigkeit der internationalen Zusammenarbeit mit einschließt.¹⁰ Wie in früheren Leitlinien des EDSA erläutert, müssen die in Artikel 49 DSGVO vorgesehenen Ausnahmen jedoch restriktiv ausgelegt werden und beziehen sich hauptsächlich auf Verarbeitungstätigkeiten, die gelegentlich und nicht wiederholt erfolgen.¹¹

1.3 Definition einer Behörde oder öffentlichen Stelle

⁸ Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland und Maximilian Schrems („Schrems II“), C-311/18, ECLI:EU:C:2020:559, Rn. 96.

⁹ Weitere Informationen zu Artikel 49 und dessen Zusammenspiel mit Artikel 46 im Allgemeinen sind in den Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung (EG) Nr. 2016/679 des EDSA enthalten.

¹⁰ Siehe EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung (EU) 2016/679, S. 12.

¹¹ Siehe EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung (EU) 2016/679, S. 5.

8. In der DSGVO ist nicht definiert, was eine „Behörde oder öffentliche Stelle“ ist. Der EDSA ist der Auffassung, dass dieser Begriff weit genug gefasst ist, um sowohl öffentliche Stellen in Drittländern als auch internationale Organisationen zu erfassen.¹² In Bezug auf öffentliche Stellen in Drittländern ist der Begriff nach innerstaatlichem Recht zu bestimmen. Dementsprechend umfassen öffentliche Stellen Regierungsbehörden auf verschiedenen Ebenen (z. B. nationale, regionale und lokale Behörden), aber unter Umständen auch Einrichtungen des öffentlichen Rechts (z. B. Exekutivagenturen, Universitäten oder Krankenhäuser).¹³ Nach Artikel 4 Nummer 26 DSGVO bezeichnet der Begriff „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.
9. Der EDSA erinnert daran, dass die Anwendung der DSGVO die Bestimmungen des Völkerrechts, wie die Bestimmungen über die Vorrechte und Befreiungen internationaler Organisationen, unberührt lässt. Gleichzeitig ist darauf hinzuweisen, dass jede öffentliche Stelle im EWR, die Daten an internationale Organisationen übermittelt, die Vorschriften der DSGVO über die Übermittlung an Drittländer oder internationale Organisationen einhalten muss.¹⁴

2 ALLGEMEINE EMPFEHLUNGEN FÜR DIE GEEIGNETEN GARANTIEEN GEMÄß ARTIKEL 46 ABSATZ 2 BUCHSTABE A UND ABSATZ 3 BUCHSTABE B DSGVO

10. Im Gegensatz zu Artikel 26 Absatz 2 der Richtlinie 95/46/EG sind in Artikel 46 DSGVO zusätzliche geeignete Garantien als Instrumente für Übermittlungen zwischen öffentlichen Stellen vorgesehen, nämlich
 - (i) ein rechtlich bindendes und durchsetzbares Dokument gemäß Artikel 46 Absatz 2 Buchstabe a DSGVO oder
 - (ii) in Verwaltungsvereinbarungen aufzunehmende Bestimmungen gemäß Artikel 46 Absatz 3 Buchstabe b DSGVO.

Diese Dokumente und Vereinbarungen können bilateraler oder multilateraler Art sein.

11. Der folgende Abschnitt enthält einige allgemeine Empfehlungen, mit denen sichergestellt werden soll, dass rechtlich bindende Dokumente oder Verwaltungsvereinbarungen (im Folgenden „internationale Übereinkünfte“) zwischen öffentlichen Stellen mit der DSGVO im Einklang stehen.
12. Obwohl Artikel 46 und Erwägungsgrund 108 der DSGVO keine spezifischen Angaben zu den Garantien enthalten, die in solche internationalen Übereinkünfte aufzunehmen sind, hat der EDSA unter

¹² Siehe hierzu auch Erwägungsgrund 108 der DSGVO.

¹³ Siehe z. B. die Bestimmung der Begriffe „öffentliche Stelle“ und „Einrichtung des öffentlichen Rechts“ in Artikel 2 Nummern 1 und 2 der Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

¹⁴ Siehe EDSA, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO, S. 27.

Berücksichtigung von Artikel 44 DSGVO¹⁵ und der jüngsten Rechtsprechung des EuGH¹⁶ hiermit eine Liste von Mindestgarantien erstellt bzw. ausgearbeitet, die in internationale Übereinkünfte zwischen öffentlichen Stellen, die unter Artikel 46 Absatz 2 Buchstabe a oder Absatz 3 Buchstabe b DSGVO fallen, aufzunehmen sind. Diese Garantien müssen gewährleisten, dass das im Rahmen der DSGVO bestehende Schutzniveau für natürliche Personen nicht untergraben wird, wenn ihre personenbezogenen Daten außerhalb des EWR übermittelt werden, und dass die Rechte der betroffenen Personen ein Schutzniveau genießen, das dem in der Union durch die DSGVO garantierten Niveau der Sache nach gleichwertig ist.¹⁷

13. Im Einklang mit der jüngsten Rechtsprechung des EuGH¹⁸ ist es Sache der übertragenden öffentlichen Stelle in einem Mitgliedstaat, gegebenenfalls mithilfe der empfangenden öffentlichen Stelle zu beurteilen, ob das nach EU-Recht erforderliche Schutzniveau in dem Drittland gewährleistet wird, um festzustellen, ob die Liste der in der internationalen Übereinkunft enthaltenen Garantien in der Praxis eingehalten werden kann, wobei zu berücksichtigen ist, dass die Rechtsvorschriften des Drittlands die Einhaltung dieser Garantien beeinträchtigen können.
14. In diesem Zusammenhang sei auch darauf hingewiesen, dass sich internationale Übereinkünfte zur Gewährleistung der in diesen Leitlinien aufgeführten Garantien auf bereits bestehende Elemente im nationalen Recht eines Drittlandes oder auf interne Vorschriften oder Regelungsrahmen einer internationalen Organisation stützen können.

2.1 Zweck und Anwendungsbereich

15. Internationale Übereinkünfte sollten eine Definition ihres Anwendungsbereichs enthalten, und ihre Zwecke sollten ausdrücklich und konkret festgelegt werden. Darüber hinaus sollten die betroffenen Kategorien personenbezogener Daten und die Art der Verarbeitung der personenbezogenen Daten, die im Rahmen der Übereinkunft übermittelt und verarbeitet werden, klar angegeben werden.

2.2 Begriffsbestimmungen

16. Internationale Übereinkünfte sollten Definitionen der grundlegenden Konzepte und Rechte in Bezug auf personenbezogene Daten gemäß der DSGVO enthalten, die für die betreffende Übereinkunft relevant sind. Beispielsweise sollten solche Übereinkünfte, sofern auf sie verwiesen wird, die folgenden wichtigen Begriffsbestimmungen enthalten: „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „Empfänger“ und „sensible Daten“.

2.3 Datenschutzgrundsätze

17. Internationale Übereinkünfte sollten spezifische Formulierungen enthalten, welche vorsehen, dass die zentralen Datenschutzgrundsätze von beiden Parteien einzuhalten sind.

¹⁵ In Artikel 44 der DSGVO heißt es: „Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.“

¹⁶ Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems („Schrems II“), C-311/18, ECLI:EU:C:2020:559.

¹⁷ Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems („Schrems II“), C-311/18, ECLI:EU:C:2020:559, Rn. 105.

¹⁸ Ebenda.

2.3.1 Zweckbindung

18. In internationalen Übereinkünften müssen die Zwecke festgelegt werden, zu denen personenbezogene Daten übermittelt und verarbeitet werden sollen, einschließlich vereinbar Zwecke einer Weiterverarbeitung, und es muss sichergestellt sein, dass die Daten nicht in einer Weise weiterverarbeitet werden, die nicht mit den ursprünglichen Verarbeitungszwecken vereinbar ist. Vereinbare Zwecke können die Speicherung für im öffentlichen Interesse liegende Archivzwecke sowie die Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sein. Aus Gründen der Klarheit wird empfohlen, die spezifischen Zwecke für die Verarbeitung und Übermittlung der Daten in der internationalen Übereinkunft selbst aufzuführen.
19. Um jegliches Risiko einer schleichenden Ausweitung der Zweckbestimmung zu vermeiden, sollte in diesen Übereinkünften auch festgelegt werden, dass übermittelte Daten nur für die in der Übereinkunft ausdrücklich genannten Zwecke verwendet werden dürfen; hierbei gilt die nachfolgend dargelegte Ausnahme.
20. Sofern beide Parteien der internationalen Übereinkunft der empfangenden öffentlichen Stelle gestatten wollen, die übermittelten personenbezogenen Daten in einer anderen vereinbarten Weise zu verwenden, so darf die durch die empfangende öffentliche Stelle erfolgende Weiterverwendung nur erlaubt werden, wenn diese mit der ursprünglichen Verwendung vereinbar ist und der übermittelnden öffentlichen Stelle zuvor zur Kenntnis gebracht wurde, wobei sich letztere dieser Weiterverwendung bei Vorliegen besonderer Gründe widersetzen kann.

2.3.2 Datenrichtigkeit und -minimierung

21. In der internationalen Übereinkunft muss festgelegt sein, dass die übermittelten und weiterverarbeiteten Daten angemessen und erheblich sowie auf das für die Zwecke ihrer Übermittlung und Weiterverarbeitung notwendige Maß beschränkt sein müssen.
22. In der Praxis ist dieser Grundsatz der Datenminimierung wichtig, um die Übermittlung personenbezogener Daten zu vermeiden, wenn diese unangemessen oder exzessiv sind.
23. Darüber hinaus sollten die Daten im Hinblick auf die Zwecke, für die sie verarbeitet werden, sachlich richtig und auf dem neuesten Stand sein. Daher muss in einer internationalen Übereinkunft vorgesehen werden, dass die übermittelnde Partei sicherstellt, dass die im Rahmen der Übereinkunft übermittelten personenbezogenen Daten sachlich richtig und gegebenenfalls auf dem neuesten Stand sind. Ferner sollte in der Übereinkunft festgeschrieben sein, dass wenn eine der Parteien feststellt, dass unrichtige oder veraltete Daten übermittelt wurden oder verarbeitet werden, sie dies der anderen Partei unverzüglich mitzuteilen hat. Schließlich sollte mit der Übereinkunft sichergestellt werden, dass jede Partei, die die Daten verarbeitet, alle angemessenen Maßnahmen trifft, um die Daten zu berichtigen oder zu löschen, wenn sich bestätigt, dass die übermittelten oder verarbeiteten Daten unrichtig sind.

2.3.3 Speicherbegrenzung

24. Die Parteien müssen sicherstellen, dass die internationale Übereinkunft eine Klausel über die Datenspeicherung enthält. In dieser Klausel sollte insbesondere festgelegt werden, dass personenbezogene Daten nicht unbegrenzt gespeichert werden dürfen, sondern in einer Form gespeichert werden, die die Identifizierung betroffener Personen nur so lange ermöglicht, wie es für den Zweck, zu dem die Daten übermittelt und anschließend verarbeitet wurden, erforderlich ist. Dies

kann eine Speicherung umfassen, die so lange erfolgt, wie dies für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich ist, sofern geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden, etwa zusätzliche technische Maßnahmen (z. B. Sicherheitsmaßnahmen, Pseudonymisierung) und Zugangsbeschränkungen. Ist in den nationalen Rechtsvorschriften oder in den internen Vorschriften bzw. im internen Regelungsrahmen einer internationalen Organisation noch keine Höchstdauer der Speicherung festgeschrieben, sollte in der Übereinkunft eine solche Höchstdauer festgelegt werden.

2.3.4 Sicherheit und Vertraulichkeit von Daten

25. Die Parteien sollten sich verpflichten, die Sicherheit und Vertraulichkeit der von ihnen vorgenommenen Verarbeitungen und Übermittlungen personenbezogener Daten zu gewährleisten.

Insbesondere sollten sich die Parteien verpflichten, geeignete technische und organisatorische Maßnahmen zu ergreifen, um personenbezogene Daten vor unbeabsichtigtem oder unrechtmäßigem Zugriff sowie vor Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung zu schützen. Diese Maßnahmen können beispielsweise die Verschlüsselung (auch im Transit), die Pseudonymisierung, die Kennzeichnung von aus dem EWR übermittelten Informationen als personenbezogene Daten, die Beschränkung des Zugangs zu personenbezogenen Daten, die sichere Speicherung personenbezogener Daten oder die Umsetzung von Leitlinien zur Gewährleistung der Sicherheit und Vertraulichkeit personenbezogener Daten umfassen.

Bei dem Schutzniveau sollten die Risiken, der Stand der Technik und die damit verbundenen Kosten berücksichtigt werden.

26. In der internationalen Übereinkunft kann ferner festgelegt werden, dass wenn eine der Parteien Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erhält, diese die andere(n) Partei(en) so schnell wie möglich benachrichtigt und angemessene und geeignete Mittel heranzieht, um der Verletzung des Schutzes personenbezogener Daten abzuwehren und die potenziellen nachteiligen Auswirkungen zu minimieren, auch indem sie der betroffenen Person unverzüglich eine Verletzung des Schutzes personenbezogener Daten mitteilt, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der natürlichen Person führt.

Es wird empfohlen, die Frist für die Meldung einer Verletzung des Schutzes personenbezogener Daten sowie die Verfahren für die Mitteilung an die betroffene Person in der internationalen Übereinkunft festzulegen.

2.4 Rechte der betroffenen Personen

27. Durch die internationale Übereinkunft müssen durchsetzbare und wirksame Rechte für betroffene Personen gemäß Artikel 46 Absatz 1 und Erwägungsgrund 108 DSGVO gewährleistet werden.
28. Die Rechte, über die die betroffenen Personen verfügen und die die von den Parteien eingegangenen besonderen Verpflichtungen, solche Rechte vorzusehen, einschließen, sollten in der Übereinkunft aufgeführt werden. Damit die Rechte wirksam sind, müssen in der internationalen Übereinkunft Mechanismen vorgesehen werden, mit denen ihre Umsetzung in der Praxis gewährleistet wird.

Darüber hinaus muss jede Verletzung der Rechte betroffener Personen mit einem angemessenen Rechtsbehelf einhergehen.

2.4.1 Recht auf Transparenz

29. Die Parteien müssen sicherstellen, dass die internationale Übereinkunft klare Formulierungen über die Transparenzpflichten der Parteien enthält.
30. Diese Pflichten sollten zum einen einen allgemeinen Hinweis umfassen, in dem mindestens dargelegt ist, wie und warum die öffentlichen Stellen personenbezogene Daten verarbeiten und übermitteln dürfen, welches einschlägige Instrument für die Übermittlung verwendet wird, an welche Einrichtungen solche Daten übermittelt werden dürfen, welche Rechte betroffene Personen besitzen und welchen Beschränkungen sie unterliegen, welche Rechtsbehelfsmechanismen zur Verfügung stehen und an wen sich betroffene Personen bei etwaigen Streitigkeiten oder Beschwerden wenden können.
31. Dabei ist jedoch unbedingt zu beachten, dass für die übertragende öffentliche Stelle ein allgemeiner Hinweis auf der Website der betreffenden öffentlichen Stelle nicht ausreicht. Den betroffenen Personen sollten individuelle Informationen von der übermittelnden öffentlichen Stelle gemäß der Informationspflicht nach Artikel 13 und 14 DSGVO übermittelt werden.¹⁹

Die internationale Übereinkunft kann auch Ausnahmen in Bezug auf solche individuellen Informationen vorsehen. Diese Ausnahmen sind begrenzt und sollten mit den in Artikel 14 Absatz 5 DSGVO vorgesehenen Ausnahmen im Einklang stehen, beispielsweise wenn die betroffene Person bereits über die betreffenden Informationen verfügt oder wenn sich die Erteilung dieser Informationen als unmöglich erweist oder einen unverhältnismäßig hohen Aufwand erfordern würde.

32. Die Parteien müssen sich verpflichten, den betroffenen Personen die internationale Übereinkunft auf Anfrage zur Verfügung zu stellen und die internationale Übereinkunft oder die einschlägigen Bestimmungen, die geeignete Garantien vorsehen, auf ihrer Website öffentlich zugänglich zu machen. Soweit es zum Schutz sensibler oder sonstiger vertraulicher Informationen erforderlich ist, kann der Wortlaut der internationalen Übereinkunft entsprechend geschwärzt werden, bevor das Dokument als Kopie weitergegeben oder öffentlich zugänglich gemacht wird. Damit die betroffene Person den Inhalt der internationalen Übereinkunft verstehen kann, müssen die Parteien eine aussagekräftige Zusammenfassung vorlegen, wenn dies erforderlich ist.

2.4.2 Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch

33. In der internationalen Übereinkunft sollten das Recht der betroffenen Person auf Information und Zugang zu allen sie betreffenden personenbezogenen Daten, die verarbeitet werden, sowie das Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung sowie gegebenenfalls das Recht auf Widerspruch gegen die Verarbeitung der Daten aus Gründen, die sich aus ihrer besonderen Situation ergeben, garantiert werden.
34. In Bezug auf das Auskunftsrecht sollte in der internationalen Übereinkunft festgelegt werden, dass Einzelpersonen gegenüber der empfangenden öffentlichen Stelle das Recht haben, eine Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so

¹⁹ Siehe EDSA, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 01, S. 13–22.

haben die betreffenden Einzelpersonen ein Recht auf Auskunft über diese Daten und spezifische Informationen über die Verarbeitung, einschließlich des Zwecks der Verarbeitung, die Kategorien personenbezogener Daten, die Empfänger personenbezogener Daten, die geplante Speicherdauer und die möglichen Rechtsbehelfe.

35. Überdies sollte in der Übereinkunft angegeben werden, wann diese Rechte geltend gemacht werden können, mittels welcher Modalitäten die betroffenen Personen diese Rechte vor beiden Parteien ausüben können und wie die Parteien auf solche Ersuchen reagieren. Beispielsweise könnte in Bezug auf die Löschung in der internationalen Übereinkunft festgeschrieben werden, dass Daten zu löschen sind, wenn sie unrechtmäßig verarbeitet wurden oder für die Zwecke der Verarbeitung nicht mehr benötigt werden. Darüber hinaus sollte in der internationalen Übereinkunft festgelegt werden, dass die Parteien Anträge betroffener Personen angemessen und rechtzeitig beantworten. Des Weiteren könnte in der internationalen Übereinkunft vorgesehen werden, dass die Parteien geeignete Maßnahmen ergreifen können, also beispielsweise angemessene Entgelte zur Deckung von Verwaltungskosten bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person erheben können.
36. Ebenso sollte der übermittelnden öffentlichen Stelle in der internationalen Übereinkunft die Pflicht auferlegt werden, die betroffene Person nach der Übermittlung ihrer personenbezogenen Daten unverzüglich über die Maßnahmen zu unterrichten, die nach ihrem Antrag aufgrund der in der internationalen Übereinkunft vorgesehenen Rechte ergriffen wurden, und hierfür eine angemessene Frist (z. B. ein Monat) vorgesehen werden. Werden die Parteien auf den Antrag der betroffenen Person hin nicht tätig, sollte die betroffene Person unverzüglich (d. h. innerhalb einer festzulegenden angemessenen Frist von beispielsweise einem Monat nach Eingang des Antrags) über die betreffenden Gründe und über die Möglichkeit, eine Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichtet werden.
37. In der internationalen Übereinkunft können auch Ausnahmen von diesen Rechten vorgesehen werden. Denkbar wären beispielsweise Ausnahmen vom Recht auf Auskunft und Löschung, so wie in Artikel 15 Absatz 4 und Artikel 17 Absatz 3 DSGVO vorgesehen. Ebenso könnten Ausnahmen von individuellen Rechten in Fällen vorgesehen werden, in denen personenbezogene Daten für wissenschaftliche oder historische Forschungszwecke, statistische Zwecke oder Archivzwecke verarbeitet werden, insofern diese Rechte voraussichtlich die Verwirklichung dieser spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und sofern geeignete Garantien (z. B. technische und organisatorische Maßnahmen einschließlich Pseudonymisierung) vorgesehen sind. Schließlich kann in der Übereinkunft vorgesehen werden, dass sich die Parteien bei einem offenkundig unbegründeten oder exzessiven Antrag weigern können, tätig zu werden.

2.4.3 Automatisierte Entscheidungen im Einzelfall

38. Sofern für die betreffende Übereinkunft relevant, sollten internationale Übereinkünfte grundsätzlich eine Klausel enthalten, welche vorsieht, dass die empfangende öffentliche Stelle keine Entscheidung trifft, die ausschließlich auf automatisierter Entscheidungsfindung im Einzelfall, einschließlich Profiling, beruht, rechtliche Wirkung gegenüber der betroffenen Person entfaltet oder diese betroffene Person in ähnlicher Weise erheblich beeinträchtigt. Falls der Zweck der Übermittlung die Möglichkeit einschließt, dass die empfangende öffentliche Stelle ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen im Sinne von Artikel 22 DSGVO treffen kann, sollte letzteres nur unter bestimmten in der internationalen Übereinkunft festgelegten Bedingungen erfolgen dürfen, beispielsweise falls es notwendig ist, die ausdrückliche Einwilligung der betroffenen Person

einzuholen. Erfüllt die Entscheidung diese Bedingungen nicht, so sollte die betroffene Person das Recht haben, der Entscheidung nicht unterworfen zu werden. Soweit nach der internationalen Übereinkunft automatisierte Entscheidungen im Einzelfall zulässig sind, sollten in der Übereinkunft in jedem Fall die erforderlichen Garantien vorgesehen werden, darunter das Recht, über die konkreten Gründe für die Entscheidung und die dahinter stehende Logik unterrichtet zu werden, fehlerhafte oder unvollständige Informationen zu berichtigen, die Entscheidung anzufechten und das Eingreifen einer Person zu erwirken.

2.4.4 Recht auf Rechtsbehelf

39. Die geschützten Rechte betroffener Personen müssen durchsetzbar und wirksam sein. Daher muss die betroffene Person Zugang zu Rechtsbehelfen haben. In den nachfolgenden Abschnitten 2.7 und 3 sind verschiedene Beispiele für die Bereitstellung von Rechtsbehelfsmechanismen aufgeführt.

2.4.5 Beschränkungen der Rechte der betroffenen Person

40. In der internationalen Übereinkunft können auch Beschränkungen der Rechte betroffener Personen vorgesehen werden. Diese Beschränkungen sollten im Einklang mit den in Artikel 23 DSGVO vorgesehenen Beschränkungen stehen. Eine solche Beschränkung muss eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellen, die dazu dient, wichtige Ziele des öffentlichen Interesses im Einklang mit den in Artikel 23 Absatz 1 DSGVO aufgeführten Zielen zu schützen, welche insbesondere die Rechte und Freiheiten Dritter, die nationale Sicherheit und Verteidigung oder die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten einschließen. Zudem muss sie gesetzlich oder im Falle internationaler Organisationen durch die anwendbaren internen Vorschriften bzw. den internen Regelungsrahmen geregelt sein und darf nur so lange aufrechterhalten werden, wie der Grund für die Beschränkung fortbesteht.

2.5 Beschränkungen der Weiterübermittlung und der Weitergabe von Daten (einschließlich der Offenlegung und des staatlichen Zugriffs)

41. Weiterübermittlungen durch die empfangende öffentliche Stelle oder internationale Organisation an Empfänger, die nicht der Übereinkunft unterliegen, sollten in der internationalen Übereinkunft generell ausdrücklich ausgeschlossen werden. Je nach Gegenstand und spezifischen Umständen kann es für die Parteien erforderlich sein, Weiterübermittlungen zuzulassen. In diesem Fall sollte in der internationalen Übereinkunft unter der Voraussetzung, dass der Grundsatz der Zweckbindung eingehalten wird²⁰, vorgesehen werden, dass eine solche Weiterübermittlung nur erfolgen darf, wenn die übermittelnde öffentliche Stelle ihre vorherige ausdrückliche Genehmigung erteilt hat und die empfangenden Dritten sich verpflichten, dieselben Datenschutzgrundsätze und -garantien wie die der internationalen Übereinkunft einzuhalten. Dies sollte mit der Verpflichtung einhergehen, betroffenen Personen die gleichen Datenschutzrechte und -garantien wie in der internationalen Übereinkunft einzuräumen, damit sichergestellt ist, dass das Schutzniveau nicht abnimmt, wenn Daten weiterübermittelt werden.
42. Für die Weitergabe personenbezogener Daten innerhalb desselben Landes sollten generell dieselben Garantien gelten wie für Weiterübermittlungen, d. h. die internationale Übereinkunft sollte eine solche Weitergabe ausschließen, und Ausnahmen sollten im Allgemeinen nur zulässig sein, wenn die übermittelnde öffentliche Stelle ihre vorherige ausdrückliche Genehmigung erteilt hat und die

²⁰ Siehe die vorstehenden Ausführungen unter 2.3.1.

empfangenden Dritten sich verpflichten, dieselben Datenschutzgrundsätze und -garantien wie die der internationalen Übereinkunft einzuhalten.

43. Es wird empfohlen, dass die empfangende öffentliche Stelle oder internationale Organisation vor der Beantragung der ausdrücklichen Genehmigung der übermittelnden öffentlichen Stelle ausreichende Informationen über die Art der personenbezogenen Daten, die sie übermitteln oder weitergeben möchte, die Gründe und Zwecke, aus denen bzw. für die sie die Übermittlung oder die Weitergabe der personenbezogenen Daten für erforderlich hält, sowie – im Falle von Weiterübermittlungen – die Länder oder internationalen Organisationen, an die sie personenbezogene Daten übermitteln möchte, offenlegt, damit die Rechtsvorschriften des Drittlands oder – im Falle internationaler Organisationen – die anwendbaren internen Vorschriften bzw. der geltende interne Regelungsrahmen bewertet werden können.
44. In Fällen, in denen es notwendig ist, die Weitergabe personenbezogener Daten an einen Dritten im Land der empfangenden öffentlichen Stelle oder an eine andere internationale Organisation zu gestatten, könnte die Weitergabe unter bestimmten Umständen entweder mit vorheriger und ausdrücklicher Genehmigung der übermittelnden öffentlichen Stelle oder unter der Voraussetzung gestattet werden, dass der empfangende Dritte eine verbindliche Verpflichtung zur Einhaltung der in der internationalen Übereinkunft enthaltenen Grundsätze und Garantien eingeht.
45. Darüber hinaus könnten in der internationalen Übereinkunft außergewöhnliche Umstände festgelegt werden, unter denen eine Weitergabe ohne vorherige Genehmigung oder ohne die oben genannten Verpflichtungen im Einklang mit den in Artikel 49 der DSGVO aufgeführten Ausnahmen erfolgen könnte, beispielsweise wenn diese spezifische Weitergabe zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich oder für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich wäre. Solche außergewöhnlichen Umstände könnten auch eintreten, wenn die Weitergabe nach dem für die empfangende Partei geltenden Recht erforderlich ist (wie bei unmittelbar damit zusammenhängenden Untersuchungen oder Gerichtsverfahren).
46. Mit Blick auf die im vorstehenden Absatz genannten Fälle sollte in der internationalen Übereinkunft eindeutig angegeben werden, unter welchen besonderen und außergewöhnlichen Umständen eine solche Weitergabe von Daten zulässig ist. Ebenso sollte die empfangende öffentliche Stelle oder internationale Organisation verpflichtet sein, die übermittelnde öffentliche Stelle vor der Weitergabe zu unterrichten und dabei auch Informationen über die weitergegebenen Daten, den empfangenden Dritten und die Rechtsgrundlage für die Weitergabe mitzuteilen. Die übermittelnde öffentliche Stelle sollte ihrerseits Aufzeichnungen über diese Meldungen der empfangenden öffentlichen Stelle oder internationalen Organisation führen und diese Informationen auf Anfrage an ihre Aufsichtsbehörde weiterleiten. Wenn eine solche der Weitergabe vorausgehende Meldung etwaigen gesetzlich vorgesehenen Vertraulichkeitspflichten (zum Beispiel zur Wahrung des Untersuchungsgeheimnisses) zuwiderläuft, sollten die spezifischen Informationen so bald wie möglich nach der Weitergabe bereitgestellt werden. In einem solchen Fall sollten der übermittelnden Stelle in regelmäßigen Abständen allgemeine Informationen über die Art der über einen bestimmten Zeitraum eingegangenen Ersuchen einschließlich Informationen über die Kategorien der angeforderten Daten, die ersuchende Stelle und die Rechtsgrundlage für die Offenlegung übermittelt werden.
47. In allen oben genannten Szenarien sollte die internationale Übereinkunft nur solche Offenlegungen personenbezogener Daten gegenüber anderen Behörden im Drittland der empfangenden öffentlichen Stelle zulassen, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um wichtige Ziele des öffentlichen Interesses im Einklang mit den in Artikel 23

Absatz 1 DSGVO aufgeführten Zielen und im Einklang mit der Rechtsprechung des EuGH zu schützen. Bei der Prüfung eines möglichen Zugangs von Behörden in Drittländern zu Überwachungszwecken sollte die übermittelnde Behörde die in den vier wesentlichen europäischen Garantien genannten Elemente berücksichtigen.²¹ Dazu gehört das Vorhandensein eines wirksamen Rechtsbehelfs für betroffene Personen im Drittland der empfangenden öffentlichen Stelle, wenn Behörden auf die personenbezogenen Daten dieser Personen zugreifen.²² Bei Übermittlungen an internationale Organisationen muss ein solcher Zugang im Einklang mit dem Völkerrecht stehen und insbesondere unbeschadet der Vorrechte und Befreiungen der internationalen Organisation erfolgen.

48. Je nach Fall kann es sinnvoll sein, die Aufnahme eines Anhangs zu der internationalen Übereinkunft vorzuschreiben, in dem die Rechtsvorschriften aufgeführt werden, die für die Weiterübermittlung an andere öffentliche Stellen, auch zu Überwachungszwecken im Bestimmungsland, gelten. Etwaige Änderungen dieses Anhangs sollten der übertragenden Partei innerhalb einer bestimmten Frist mitgeteilt werden müssen.

2.6 Sensible Daten

49. Ist in einer internationalen Übereinkunft die Übermittlung sensibler personenbezogener Daten im Sinne von Artikel 9 Absatz 1 DSGVO vorgesehen, sollten in die Übereinkunft zusätzliche Garantien für die spezifischen Risiken aufgenommen werden, die von der empfangenden öffentlichen Stelle oder internationalen Organisation umzusetzen sind. Diese könnten beispielsweise Beschränkungen des Zugangs, der Zwecke, zu denen die Informationen verarbeitet werden dürfen, der Weiterübermittlung usw. oder spezifische Garantien (beispielsweise zusätzliche Sicherheitsmaßnahmen) umfassen, die eine spezielle Schulung des Personals erfordern, das Zugang zu den Informationen erhält.

2.7 Rechtsbehelfsmechanismen

50. Um durchsetzbare und wirksame Rechte betroffener Personen zu gewährleisten, muss in der internationalen Übereinkunft ein System vorgesehen werden, das es betroffenen Personen ermöglicht, nach der Übermittlung ihrer Daten an ein Land außerhalb des EWR oder an eine internationale Organisation weiterhin Rechtsbehelfsmechanismen in Anspruch zu nehmen. Diese Rechtsbehelfsmechanismen müssen Einzelpersonen, die von der Nichteinhaltung der Bestimmungen des gewählten Instruments betroffen sind, und dementsprechend betroffenen Personen, deren personenbezogene Daten aus dem EWR übermittelt wurden, die Möglichkeit geben, Beschwerden über eine solche Nichteinhaltung einzureichen und diese Beschwerden beilegen zu lassen. Insbesondere muss für die betroffene Person ein wirksames Verfahren für die etwaige Beschwerde bei den öffentlichen Stellen, die Parteien der internationalen Übereinkunft sind, und für die (direkte oder nach Kontaktierung der betreffenden Partei erfolgende) Beschwerde bei einem unabhängigen Aufsichtsmechanismus gewährleistet sein. Darüber hinaus sollte grundsätzlich ein gerichtlicher Rechtsbehelf zur Verfügung stehen.
51. Erstens sollte sich die empfangende öffentliche Stelle verpflichten, einen Mechanismus einzurichten, mit dem Beschwerden betroffener Personen über die Einhaltung der vereinbarten Datenschutzgarantien wirksam und rechtzeitig bearbeitet und beigelegt werden können. Darüber hinaus sollten betroffene Personen die Möglichkeit erhalten, bei einem unabhängigen

²¹ Siehe EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen.

²² Siehe EDSA, Empfehlungen 02/2020, Garantie D, S. 14 ff.

Aufsichtsgremium wie gegebenenfalls einer unabhängigen Datenschutzbehörde wirksame verwaltungsrechtliche Rechtsbehelfe einzulegen.²³

52. Zweitens sollte in der Übereinkunft ein gerichtlicher Rechtsbehelf einschließlich einer Entschädigung für infolge der unrechtmäßigen Verarbeitung personenbezogener Daten entstandene materielle und immaterielle Schäden vorgesehen werden. Besteht - beispielsweise aufgrund von Beschränkungen im innerstaatlichen Recht oder aufgrund des spezifischen Status der empfangenden öffentlichen Stelle (wie bei internationalen Organisationen) - keine Möglichkeit, einen wirksamen gerichtlichen Rechtsbehelf zu gewährleisten, so muss die internationale Übereinkunft alternative Garantien vorsehen. Diese alternativen Garantien müssen so beschaffen sein, dass sie für die betroffene Person ein Schutzniveau gewährleisten, das den nach Artikel 47 der Charta der Grundrechte der Europäischen Union (EU-Charta) erforderlichen Garantien der Sache nach gleichwertig ist.²⁴
53. In diesem Fall könnte durch die internationale Übereinkunft eine Struktur geschaffen werden, die es der betroffenen Person ermöglicht, ihre Rechte außergerichtlich geltend zu machen, beispielsweise durch gerichtsähnliche, verbindliche Mechanismen wie Schiedsverfahren oder alternative Streitbeilegungsverfahren wie Mediation, die eine unabhängige Überprüfung gewährleisten würden und für die empfangende öffentliche Stelle verbindlich wären.²⁵ Darüber hinaus könnte sich die öffentliche Stelle, die die personenbezogenen Daten übermittelt, verpflichten, Schadenersatz zu leisten, falls bei der unabhängigen Überprüfung festgestellt wird, dass die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

In Ausnahmefällen könnten durch die Übereinkunft andere, gleichermaßen unabhängige und wirksame Rechtsbehelfsmechanismen eingesetzt werden, beispielsweise von internationalen Organisationen umgesetzte wirksame Rechtsbehelfsmechanismen.

54. In Bezug auf alle oben genannten Rechtsbehelfsmechanismen sollte die internationale Übereinkunft für alle Parteien die Pflicht vorsehen, sich gegenseitig über den Ausgang des Verfahrens zu unterrichten, insbesondere wenn eine Beschwerde einer Person abgewiesen oder nicht beigelegt wird.
55. Der Rechtsbehelfsmechanismus muss mit der Möglichkeit einhergehen, dass die übermittelnde öffentliche Stelle die Übermittlung personenbezogener Daten im Rahmen der internationalen Übereinkunft aussetzt oder beendet, wenn es den Parteien nicht gelingt, eine Streitigkeit gütlich beizulegen, und zwar so lange, bis sie der Auffassung ist, dass die empfangende öffentliche Stelle die Angelegenheit zufriedenstellend gelöst hat. Eine solche Aussetzung oder Beendigung muss mit einer Selbstverpflichtung der empfangenden öffentlichen Stelle zur Rückgabe oder zum Löschen der personenbezogenen Daten einhergehen. Die übertragende öffentliche Stelle muss die zuständige nationale Aufsichtsbehörde über die Aussetzung oder Beendigung unterrichten.

²³ Siehe ebenfalls Abschnitt 2.8 zum Aufsichtsmechanismus.

²⁴ Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems („Schrems II“), C-311/18, ECLI:EU:C:2020:559, Rn. 96, 186 ff.

²⁵ Urteil des Gerichtshofs vom 6. Oktober 2015, Maximilian Schrems/Data Protection Commissioner („Schrems“), C-362/14, ECLI:EU:C:2015:650, Rn. 41 und 95; Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems („Schrems II“), C-311/18, ECLI:EU:C:2020:559, Rn. 186, 187, 189 und 195 ff.

2.8 Überwachungsmechanismen

56. Um sicherzustellen, dass alle aus der internationalen Übereinkunft erwachsenden Pflichten erfüllt werden, muss die internationale Übereinkunft eine unabhängige Überwachung ihrer ordnungsgemäßen Anwendung und etwaiger Eingriffe in die in ihr vorgesehenen Rechte vorsehen.
57. Zunächst sollte in der Übereinkunft eine interne Aufsicht vorgesehen werden, mit der die Einhaltung der Übereinkunft sichergestellt wird. Jede Partei der Übereinkunft sollte regelmäßig interne Überprüfungen der eingerichteten Verfahren und der wirksamen Anwendung der in der Übereinkunft vorgesehenen Garantien durchführen. Bei den regelmäßigen internen Kontrollen sollten auch Änderungen der Rechtsvorschriften überprüft werden, die die Partei(en) daran hindern würden, die Datenschutzgrundsätze und -garantien der internationalen Übereinkunft einzuhalten. Darüber hinaus könnte vorgesehen werden, dass eine Partei der Übereinkunft von einer anderen Partei auch verlangen kann, eine solche Überprüfung vorzunehmen. Die internationale Übereinkunft muss vorsehen, dass jede Partei etwaige Anfragen der anderen Partei, die sich auf die wirksame Umsetzung der in der Übereinkunft enthaltenen Garantien beziehen, beantworten muss. Jede Partei, die eine Überprüfung durchführt, sollte die Ergebnisse ihrer Kontrollen der bzw. den anderen Partei(en) der Übereinkunft mitteilen. Im Idealfall sollte eine solche Mitteilung auch an den unabhängigen Aufsichtsmechanismus für die Übereinkunft erfolgen.
58. Darüber hinaus muss die internationale Übereinkunft die Pflicht vorsehen, dass jede Partei die andere Partei unverzüglich in Kenntnis setzt, wenn sie aus einem beliebigen Grund nicht in der Lage ist, die in der Übereinkunft vorgesehenen Garantien wirksam umzusetzen. Für diesen Fall muss in der internationalen Übereinkunft vorgesehen werden, dass die übermittelnde öffentliche Stelle die Übermittlung personenbezogener Daten an die empfangende öffentliche Stelle im Rahmen der internationalen Übereinkunft so lange aussetzen oder beenden kann, bis die empfangende öffentliche Stelle die übermittelnde öffentliche Stelle darüber unterrichtet, dass sie wieder in der Lage ist, im Einklang mit den Garantien zu handeln. Die übermittelnde Stelle hat der zuständigen nationalen Aufsichtsbehörde jede Änderung der Situation, jede Aussetzung der Übertragung sowie die etwaige Kündigung der Übereinkunft mitzuteilen.
59. Zweitens muss in der Übereinkunft eine unabhängige Kontrolle vorgesehen werden, mit der gewährleistet wird, dass die Parteien die Bestimmungen der Übereinkunft einhalten. Dies ergibt sich direkt aus der EU-Charta²⁶ und der Europäischen Konvention zum Schutze der Menschenrechte (EMRK)²⁷ im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR), aus den Bestimmungen des Primärrechts²⁸ und aus der einschlägigen Rechtsprechung.

²⁶ Artikel 7, 8 und 47 der EU-Charta.

²⁷ Artikel 8 EMRK.

²⁸ Artikel 6 des Vertrags von Lissabon.

„(1) Die Union erkennt die Rechte, Freiheiten und Grundsätze an, die in der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind; die Charta der Grundrechte und die Verträge sind rechtlich gleichrangig.

Durch die Bestimmungen der Charta werden die in den Verträgen festgelegten Zuständigkeiten der Union in keiner Weise erweitert.

Die in der Charta niedergelegten Rechte, Freiheiten und Grundsätze werden gemäß den allgemeinen Bestimmungen des Titels VII der Charta, der ihre Auslegung und Anwendung regelt, und unter gebührender Berücksichtigung der in der Charta angeführten Erläuterungen, in denen die Quellen dieser Bestimmungen angegeben sind, ausgelegt.

(2) Die Union tritt der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten bei. Dieser Beitritt ändert nicht die in den Verträgen festgelegten Zuständigkeiten der Union.

60. Der EuGH hat seit 2015²⁹ wiederholt die Notwendigkeit eines unabhängigen Rechtsbehelfs- und Überwachungsmechanismus bekräftigt.³⁰ Ebenso hat der EGMR in seinen Urteilen häufig betont, dass jeder Eingriff in das in Artikel 8 EMRK verankerte Recht auf Achtung des Privat- und Familienlebens einer wirksamen, unabhängigen und unparteiischen Aufsicht unterliegen muss.³¹
61. Wenngleich in der DSGVO nicht festgelegt ist, dass die zuständige Aufsichtsbehörde die externe Aufsichtsstelle sein muss, könnte in der Übereinkunft beispielsweise vereinbart werden, dass die Beaufsichtigung durch eine zuständige Aufsichtsbehörde erfolgt, sofern eine solche im Land der öffentlichen Stelle, die die personenbezogenen Daten aus dem EWR erhält, existiert. Darüber hinaus könnte die Übereinkunft die freiwillige Selbstverpflichtung der empfangenden Partei zur Zusammenarbeit mit den EWR-Aufsichtsbehörden enthalten.
62. In Ermangelung einer Aufsichtsbehörde, die speziell für die Überwachung des Datenschutzrechts in dem betreffenden Drittland oder bei der betreffenden internationalen Organisation zuständig ist, ist mit anderen Mitteln sicherzustellen, dass ein unabhängiger, wirksamer und unparteiischer Aufsichtsmechanismus vorhanden ist. Die Art des eingerichteten unabhängigen Aufsichtsmechanismus kann von Fall zu Fall unterschiedlich sein.
63. Beispielsweise könnte in der Übereinkunft auf in dem betreffenden Drittland bestehende Aufsichtsstellen verwiesen werden, bei denen es sich nicht um Aufsichtsbehörden im Bereich des Datenschutzes handelt. Zudem könnte die Aufsicht durch funktional autonome Mechanismen gewährleistet werden, falls (beispielsweise aufgrund der Vorrechte und Befreiungen bestimmter internationaler Organisationen) keine externe Aufsicht aus struktureller oder institutioneller Sicht gewährleistet werden kann. Dabei muss es sich gleichwohl um eine Stelle handeln, die zwar nicht externer Natur ist, aber ihre Aufgaben unabhängig - d. h. weisungsfrei und mit ausreichenden personellen, technischen und finanziellen Ressourcen usw. - erfüllt. Die empfangende Partei ist an die Entscheidungen des Aufsichtsgremiums gebunden.

2.9 Kündigungsklausel

64. In der internationalen Übereinkunft sollte vorgesehen werden, dass alle personenbezogenen Daten, die aus dem EWR auf der Grundlage der internationalen Übereinkunft vor deren wirksamer Beendigung übermittelt werden, weiterhin gemäß den Bestimmungen der internationalen Übereinkunft verarbeitet werden müssen.

(3) Die Grundrechte, wie sie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts."

²⁹ Urteil des Gerichtshofs vom 6. Oktober 2015, Maximilian Schrems/Data Protection Commissioner („Schrems“), C-362/14, ECLI:EU:C:2015:650, Rn. 41 und 95.

³⁰ Urteil des Gerichtshofs vom 27. Juli 2017, Gutachten 1/15 des Gerichtshofs vom 26. Juli 2017 zum geplanten Abkommen zwischen der Europäischen Union und Kanada über die Übermittlung und Verarbeitung von Fluggastdatensätzen, ECLI:EU:C:2017:592, Rn. 228 ff.; Urteil des Gerichtshofs vom 30. April 2019, Gutachten 1/17 des Gerichtshofs vom 30. April 2019 zum Umfassenden Wirtschafts- und Handelsabkommen zwischen Kanada einerseits und der Europäischen Union und ihren Mitgliedstaaten andererseits, ECLI:EU:C:2019:341, Rn. 190 ff.

³¹ Urteil des EGMR vom 6. September 1978, Klass/Deutschland, Rn. 55 und 56. Die auf den EGMR zurückgehende Anforderung gilt auch für jegliche Eingriffe in die Artikel 7 und 8 der EU-Charta, da die darin niedergelegten Grundrechte nach Artikel 52 Absatz 3 der EU-Charta die gleiche Bedeutung und Tragweite besitzen wie die Rechte nach Artikel 8 EMRK.

3 BESONDERE HINWEISE ZU ARTIKEL 46 DSGVO

3.1 Besondere Hinweise zu rechtlich bindenden und durchsetzbaren Dokumenten – Artikel 46 Absatz 2 Buchstabe a DSGVO

65. Nach Artikel 46 Absatz 2 Buchstabe a DSGVO dürfen öffentliche Stellen im EWR Übermittlungen an öffentliche Stellen in einem Drittland oder an eine internationale Organisation auf der Grundlage von zwischen diesen geschlossenen Dokumenten durchführen, ohne hierfür die vorherige Genehmigung einer Aufsichtsbehörde einholen zu müssen. Solche Dokumente müssen rechtlich bindend und durchsetzbar sein. Daher können im Rahmen dieser Bestimmung internationale Verträge, öffentlich-rechtliche Verträge oder unmittelbar anwendbare Verwaltungsvereinbarungen herangezogen werden.
66. Alle rechtlich bindenden und durchsetzbaren Dokumente sollten die wichtigsten Datenschutzgrundsätze und die Rechte betroffener Personen gemäß der DSGVO umfassen.
67. Die Parteien müssen sich verpflichten, für die Datenübermittlung ausreichende Datenschutzgarantien vorzusehen. Folglich sollte in der Übereinkunft auch festgelegt werden, wie die empfangende öffentliche Stelle die wichtigsten Datenschutzgrundsätze und Rechte betroffener Personen auf alle übermittelten personenbezogenen Daten anzuwenden hat, um sicherzustellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.
68. Falls keine Möglichkeit besteht, einen wirksamen gerichtlichen Rechtsbehelf in rechtlich bindenden und durchsetzbaren Dokumenten vorzusehen, und folglich alternative Rechtsbehelfsmechanismen vereinbart werden müssen, sollten die öffentlichen Stellen des EWR vor Abschluss dieser Dokumente die zuständige Aufsichtsbehörde zurate ziehen.
69. Zwar ist die Form des Dokuments nicht entscheidend, solange das Dokument rechtlich bindend und durchsetzbar ist, aber der EDSA ist der Auffassung, dass die beste Option darin besteht, detaillierte Datenschutzklauseln direkt in das Dokument aufzunehmen. Sollte diese Lösung jedoch aufgrund der besonderen Umstände nicht umsetzbar sein, empfiehlt der EDSA nachdrücklich, zumindest eine allgemeine Klausel in den Text aufzunehmen, mit der die Datenschutzgrundsätze direkt in den Text des Dokuments einfließen, und die detaillierteren Bestimmungen und Garantien in einem Anhang des Dokuments festzulegen.

3.2 Besondere Hinweise zu Verwaltungsvereinbarungen – Artikel 46 Absatz 3 Buchstabe b DSGVO

70. In der DSGVO werden in Artikel 46 Absatz 3 Buchstabe b auch alternative Dokumente in Form von Verwaltungsvereinbarungen (z. B. Absichtserklärungen) vorgesehen, bei denen der erforderliche Schutz durch die Verpflichtungen, die die beiden Parteien eingehen, um ihre gemeinsame Vereinbarung in Kraft zu setzen, geboten wird.
71. Diesbezüglich ist in Artikel 46 Absatz 1 und in Erwägungsgrund 108 der DSGVO festgelegt, dass durch derartige Vereinbarungen durchsetzbare Rechte betroffener Personen und wirksame Rechtsbehelfe gewährleistet werden müssen. Verwaltungsvereinbarungen, die keine rechtlich bindenden Garantien vorsehen, bedürfen der Genehmigung durch die zuständige Aufsichtsbehörde.
72. Es sollte sorgfältig geprüft werden, ob angesichts des Zwecks der Verarbeitung und der Art der betreffenden Daten von nicht rechtlich bindenden Verwaltungsvereinbarungen Gebrauch gemacht

werden sollte, um Garantien im öffentlichen Sektor zu bieten. Sind im innerstaatlichen Recht des Drittlands oder in den internen Vorschriften bzw. im internen Regelungsrahmen der internationalen Organisation keine Datenschutzrechte und Rechtsbehelfe für natürliche Personen im EWR vorgesehen, sollte dem Abschluss einer rechtlich bindenden Übereinkunft der Vorzug gegeben werden. Unabhängig von der Art des angenommenen Dokuments müssen die bestehenden Maßnahmen wirksam genug sein, um eine angemessene Umsetzung, Durchsetzung und Überwachung zu gewährleisten.

73. In Verwaltungsvereinbarungen müssen spezifische Maßnahmen vorgesehen werden, um wirksame individuelle Rechte, Rechtsbehelfe und eine wirksame Aufsicht zu gewährleisten. Um insbesondere wirksame und durchsetzbare Rechte sicherzustellen, sollte jedes nicht rechtlich bindende Dokument Garantien der öffentlichen Stelle, der die personenbezogenen Daten aus dem EWR übermittelt werden, dafür enthalten, dass die individuellen Rechte in vollem Umfang durch deren innerstaatliches Recht gewährleistet sind und von EWR-Bürgern unter denselben Bedingungen ausgeübt werden können wie sie für Bürger und Einwohner des betreffenden Drittlands gelten. Gleiches gilt, wenn natürlichen Personen aus dem EWR im innerstaatlichen Rechtsrahmen der empfangenden öffentlichen Stelle verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung stehen. In ähnlicher Weise sollten internationale Organisationen Garantien für in ihren internen Vorschriften vorgesehene individuelle Rechte sowie die verfügbaren Rechtsbehelfsmechanismen bieten.
74. Ist dies nicht der Fall, sollten individuelle Rechte durch spezifische Verpflichtungen der Parteien in Verbindung mit Verfahrensmechanismen gewährleistet werden, um ihre Wirksamkeit sicherzustellen und dem Einzelnen Rechtsbehelfe zur Verfügung zu stellen. Diese spezifischen Verpflichtungen und Verfahrensmechanismen müssen in der Praxis dazu geeignet sein, die Wahrung eines Schutzniveaus sicherzustellen, das dem innerhalb der Union durch die DSGVO gewährleisteten Schutzniveau der Sache nach gleichwertig ist.

Solche Verfahrensmechanismen können beispielsweise Selbstverpflichtungen der Parteien umfassen, einander über Anträge natürlicher Personen aus dem EWR zu unterrichten und Streitigkeiten oder Ansprüche zeitnah beizulegen.

75. Wenn solche Streitigkeiten oder Ansprüche nicht gütlich zwischen den Parteien beigelegt werden können, muss darüber hinaus für den Einzelnen ein unabhängiger und wirksamer Rechtsbehelf durch alternative Mechanismen gewährleistet sein, etwa durch die Möglichkeit, dass der Einzelne auf einen alternativen Streitbeilegungsmechanismus wie Schiedsverfahren oder Mediation zurückgreifen kann. Ein solcher alternativer Streitbeilegungsmechanismus muss verbindlich sein.³²
76. Je nach Fall sollte in der Verwaltungsvereinbarung eine Kombination aller oder einiger der oben genannten Maßnahmen vorgesehen werden, um einen wirksamen Rechtsbehelf zu gewährleisten. Andere, in diesen Leitlinien nicht genannte Maßnahmen könnten ebenfalls akzeptabel sein, wenn sie einen unabhängigen und wirksamen Rechtsbehelf vorsehen.
77. Jede gemäß Artikel 46 Absatz 3 Buchstabe b DSGVO ausgearbeitete Verwaltungsvereinbarung wird von der zuständigen Aufsichtsbehörde fallweise geprüft, gegebenenfalls gefolgt vom einschlägigen EDSA-Verfahren. Die zuständige Aufsichtsbehörde stützt sich bei ihrer Prüfung auf die in diesen Leitlinien enthaltenen allgemeinen Empfehlungen, kann aber je nach Einzelfall auch zusätzliche Garantien verlangen.

³² Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems („Schrems II“), C-311/18, ECLI:EU:C:2020:559, Rn. 189 und 196 ff.

4 VERFAHRENSFRAGEN

78. Die nach Artikel 46 Absatz 3 Buchstabe b DSGVO getroffenen Verwaltungsvereinbarungen werden aufgrund der Anforderung der Genehmigung durch die zuständige Aufsichtsbehörde, die gemäß Artikel 46 Absatz 4 DSGVO das Kohärenzverfahren nach Artikel 63 anwendet, fallweise geprüft. Der EDSA empfiehlt, bei der Aufnahme alternativer Rechtsbehelfsmechanismen in rechtlich bindende und durchsetzbare Dokumente gemäß Artikel 46 Absatz 2 Buchstabe a DSGVO auch die zuständige Aufsichtsbehörde zurate zu ziehen. Der EDSA empfiehlt nachdrücklich, die zuständige Aufsichtsbehörde frühzeitig zu konsultieren.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)