

Guidelines



**Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und
Artikel 46 Absatz 3 Buchstabe b der Verordnung (EU)
2016/679 für die Übermittlung personenbezogener Daten
zwischen **Behörden und Einrichtungen des EWR** und des
Nicht-EWR**

Version 2.0

**Verabschiedet am 15.
Dezember 2020**

[Nicholas Vollmer: Fußnoten entfernt, um Lesbarkeit und
Übersetzungsqualität zu verbessern]

Versionsgeschichte

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

Inhaltsübersicht

1	Allgemein	5
1.1	Zweck	5
1.2	Allgemeine Regeln für internationale Überweisungen	6
1.3	Definition einer öffentlichen Behörde oder Einrichtung	6
2	Allgemeine Empfehlungen für die angemessenen Schutzmaßnahmen sowohl nach Artikel 46 (2) (a) als auch nach 46 (3) (b) GDPR	7
2.1	Zweck und Umfang	8
2.2	Definitionen	8
2.3	Grundsätze des Datenschutzes	8
2.3.1	Grundsatz der Zweckbindung	8
2.3.2	Grundsätze der Datengenauigkeit und -minimierung	8
2.3.3	Prinzip der Speicherbegrenzung	9
2.3.4	Sicherheit und Vertraulichkeit der Daten	9
2.4	Rechte der betroffenen Personen	9
2.4.1	Recht auf Transparenz	10
2.4.2	Auskunftsrecht, Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Recht auf Widerspruch	10
2.4.3	Automatisierte individuelle Entscheidungsfindung	11
2.4.4	Recht auf Entschädigung	11
2.4.5	Einschränkung der Rechte der betroffenen Personen	11
2.5	Beschränkungen der Weitergabe und des Austauschs von Daten (einschließlich Offenlegung und staatlicher Zugriff)	12
2.6	Sensible Daten	13
2.7	Rechtsbehelfsmechanismen	13
2.8	Überwachungsmechanismen	15
2.9	Kündigungsklausel	16
3	Spezifische Informationen zu Artikel 46 GDPR	17
3.1	Spezifische Informationen zu rechtsverbindlichen und vollstreckbaren Instrumenten - Artikel 46 (2) (a) GDPR	17
3.2	Spezifische Informationen über Verwaltungsvereinbarungen - Artikel 46 (3) (b) GDPR	17
4	Verfahrenstechnische Fragen	19

Der Europäische Datenschutzausschuss

gestützt auf Artikel 70 (1e) 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, (im Folgenden "DSGVO"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

HAT DIE FOLGENDEN RICHTLINIEN VERABSCHIEDET

¹ Verweise auf "Mitgliedstaaten" in diesen Leitlinien sind als Verweise auf "EWR-Mitgliedstaaten" zu verstehen.

1 ALLGEMEINES

1.1 Zweck

1. Dieses Dokument soll als Leitfaden für die Anwendung von Artikel 46 Absatz 2 Buchstabe a und Artikel 46 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung (DSGVO) auf die Übermittlung personenbezogener Daten **von Behörden oder Einrichtungen des EWR (im Folgenden "öffentliche Stellen") an öffentliche Stellen in Drittländern oder an internationale Organisationen** dienen, soweit diese nicht durch eine Angemessenheitsfeststellung der Europäischen Kommission² abgedeckt sind. Öffentliche Stellen können sich dafür entscheiden, diese Mechanismen zu nutzen, die die Datenschutz-Grundverordnung für ihre Situation als angemessener erachtet, es steht ihnen aber auch frei, sich auf andere einschlägige Instrumente zu stützen, die angemessene Garantien gemäß Artikel 46 der Datenschutz-Grundverordnung vorsehen.
2. Die Leitlinien sollen einen Hinweis auf die Erwartungen des Europäischen Datenschutzausschusses (EDSB) an die Garantien geben, die durch ein rechtsverbindliches und durchsetzbares Instrument zwischen öffentlichen Stellen gemäß Artikel 46 Absatz 2 Buchstabe a DSGVO oder, vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde, durch Bestimmungen, die in Verwaltungsvereinbarungen zwischen öffentlichen Stellen gemäß Artikel 46 Absatz 3 Buchstabe b DSGVO einzufügen sind, zu schaffen sind.³ Der EDSB empfiehlt den Parteien dringend, die Leitlinien frühzeitig als Referenz zu verwenden, wenn sie den Abschluss oder die Änderung solcher Instrumente oder Vereinbarungen in Betracht ziehen.⁴
3. Die Leitlinien sind in Verbindung mit anderen früheren Arbeiten des EDSB (einschließlich der von seinem Vorgänger, der Artikel-29-Datenschutzgruppe⁵ ("WP29"), gebilligten Dokumente) zu den zentralen Fragen des territorialen Anwendungsbereichs und der Übermittlung personenbezogener Daten an Drittländer⁶ zu lesen. Die Leitlinien werden auf der Grundlage der praktischen Erfahrungen mit der Anwendung der Datenschutz-Grundverordnung überprüft und gegebenenfalls aktualisiert.
4. Die vorliegenden Leitlinien beziehen sich auf internationale Datenübermittlungen zwischen öffentlichen Stellen, die zu verschiedenen Zwecken der Verwaltungszusammenarbeit erfolgen und in den Anwendungsbereich der DS-GVO fallen. Infolgedessen und in Übereinstimmung mit Artikel 2 Absatz 2 der DSGVO decken sie keine Übermittlungen im Bereich der öffentlichen Sicherheit, der Verteidigung oder der Staatssicherheit ab. Darüber hinaus befassen sie sich nicht mit der Datenverarbeitung und -übermittlung durch die zuständigen Behörden zu Strafverfolgungszwecken, da dies in einem separaten spezifischen Rechtsakt, der Strafverfolgungsrichtlinie⁷, geregelt ist. Schließlich konzentrieren sich die Leitlinien nur auf Übermittlungen zwischen öffentlichen Stellen und decken nicht die Übermittlung personenbezogener Daten von einer öffentlichen Stelle an eine private Einrichtung oder von einer privaten Einrichtung an eine öffentliche Stelle ab.

1.2 Allgemeine Regeln für internationale Überweisungen

5. Gemäß Artikel 44 der DSGVO muss der Datenexporteur, der personenbezogene Daten an Drittländer oder internationale Organisationen übermittelt, neben der Einhaltung von Kapitel V der DSGVO auch die Bedingungen der anderen Bestimmungen der DSGVO erfüllen. Insbesondere muss jede Verarbeitungstätigkeit mit den Datenschutzgrundsätzen in Artikel 5 DSGVO übereinstimmen, gemäß Artikel 6 DSGVO rechtmäßig sein und im Falle besonderer Datenkategorien mit Artikel 9 DSGVO übereinstimmen. Daher muss ein zweistufiger Test durchgeführt werden: Zunächst muss eine Rechtsgrundlage für die Datenverarbeitung als solche zusammen mit allen relevanten Bestimmungen der DSGVO gelten; und in einem zweiten Schritt müssen die Bestimmungen von Kapitel V der DSGVO eingehalten werden.

6. In Artikel 46 der DSGVO heißt es: "Liegt keine Entscheidung nach Artikel 45 Absatz 3 vor, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten nur dann in ein Drittland oder an eine internationale Organisation übermitteln, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und unter der Bedingung, dass durchsetzbare Rechte der betroffenen Person und wirksame Rechtsbehelfe für die betroffenen Personen zur Verfügung stehen". Solche angemessenen Garantien können durch eine rechtsverbindliche und durchsetzbare Übereinkunft zwischen öffentlichen Stellen (Artikel 46 Absatz 2 Buchstabe a) DSGVO) oder, vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde, durch Bestimmungen vorgesehen werden, die in Verwaltungsvereinbarungen zwischen öffentlichen Stellen einzufügen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen enthalten (Artikel 46 Absatz 3 Buchstabe b) DSGVO). Wie der Gerichtshof der Europäischen Union (EuGH) klargestellt hat, müssen solche angemessenen Garantien geeignet sein, den betroffenen Personen, deren personenbezogene Daten übermittelt werden, ein Schutzniveau zu gewährleisten, das im Wesentlichen demjenigen entspricht, das innerhalb des EWR gewährleistet ist.⁸
7. Abgesehen von dieser Lösung und in Ermangelung einer solchen bietet Artikel 49 der DSGVO auch eine begrenzte Anzahl spezifischer Situationen, in denen internationale Datenübermittlungen stattfinden können, wenn keine Angemessenheitsfeststellung durch die Europäische Kommission vorliegt⁹. Eine Ausnahmeregelung betrifft insbesondere Übermittlungen, die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, die im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sind, auch im Sinne der Gegenseitigkeit der internationalen Zusammenarbeit¹⁰. Wie in früheren Leitlinien des EDPB erläutert, sind die Ausnahmen nach Artikel 49 DSGVO jedoch restriktiv auszulegen und beziehen sich hauptsächlich auf gelegentliche und nicht wiederholte Verarbeitungen¹¹.

1.3 Definition einer öffentlichen Behörde oder Einrichtung

8. In der Datenschutz-Grundverordnung wird nicht definiert, was eine "öffentliche Behörde oder Einrichtung" ist. Der EDSB ist der Ansicht, dass dieser Begriff weit genug 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 Einrichtungen staatliche Behörden auf verschiedenen Ebenen (z. B. nationale, regionale und lokale Behörden), können aber auch andere Einrichtungen des öffentlichen Rechts umfassen (z. B. Exekutivagenturen, Universitäten, Krankenhäuser usw.).¹³ In Übereinstimmung mit Artikel 4 (26) GDPR sind "internationale

Organisation" bezieht sich auf eine Organisation und ihre untergeordneten Organe, die dem Völkerrecht unterliegen, oder auf jede andere Einrichtung, die durch eine Vereinbarung zwischen zwei Ländern oder auf der Grundlage einer solchen Vereinbarung geschaffen wurde.

9. Der EDSB weist darauf hin, dass die Anwendung der DSGVO unbeschadet der Bestimmungen des internationalen Rechts erfolgt, wie z. B. derjenigen, die die Vorrechte und Befreiungen internationaler Organisationen regeln. Gleichzeitig ist es wichtig, daran zu erinnern, dass jede öffentliche Einrichtung des EWR, die Daten an internationale Organisationen übermittelt, die Bestimmungen der DSGVO über die Übermittlung an Drittländer oder internationale Organisationen einhalten muss.¹⁴

2 ALLGEMEINE EMPFEHLUNGEN FÜR ANGEMESSENE SICHERHEITSVORSCHRIFTEN GEMÄSS ARTIKEL 46 (2) (a) UND

46 (3) (b) DSGVO

10. Im Gegensatz zu Artikel 26 (2) der Richtlinie 95/46/EG sieht Artikel 46 der Datenschutz-Grundverordnung zusätzliche angemessene Garantien als Instrumente für Übermittlungen zwischen öffentlichen Stellen vor:
 - (i) ein rechtsverbindliches und vollstreckbares Instrument, Artikel 46 (2) (a) GDPR oder
 - (ii) Bestimmungen, die in Verwaltungsvereinbarungen einzufügen sind, Artikel 46 (3)

(b) GDPR. Diese Instrumente und Vereinbarungen können bilateraler oder multilateraler Natur sein.
11. Der folgende Abschnitt enthält einige allgemeine Empfehlungen, die dazu beitragen sollen, dass rechtsverbindliche Instrumente oder Verwaltungsvereinbarungen (im Folgenden "internationale Vereinbarungen") zwischen öffentlichen Stellen mit der DSGVO in Einklang stehen.
12. Obwohl Artikel 46 und Erwägungsgrund 108 der DSGVO keine spezifischen Angaben zu den Garantien enthalten, die in solche internationalen Vereinbarungen aufzunehmen sind, hat der EDSB unter Berücksichtigung von Artikel 44 der DSGVO15 und der jüngsten Rechtsprechung des EuGH16 eine Liste von Mindestgarantien erstellt, die in internationale Vereinbarungen zwischen öffentlichen Stellen, die unter Artikel 46 Absatz 2 Buchstabe a oder Artikel 46 Absatz 3 Buchstabe b DSGVO fallen, aufzunehmen sind. Mit diesen Garantien soll sichergestellt werden, dass das Schutzniveau natürlicher Personen nach der DSGVO nicht untergraben wird, wenn ihre personenbezogenen Daten in Länder außerhalb des EWR übermittelt werden, und dass den betroffenen Personen ein Schutzniveau gewährt wird, das im Wesentlichen dem durch die DSGVO garantierten Schutzniveau innerhalb der EU entspricht.¹⁷
13. Nach der jüngsten Rechtsprechung des EuGH18 obliegt es der übermittelnden öffentlichen Stelle in einem Mitgliedstaat, gegebenenfalls mit Hilfe der empfangenden öffentlichen Stelle, zu prüfen, ob das nach EU-Recht erforderliche Schutzniveau in dem Drittland eingehalten wird, um festzustellen, ob die in dem internationalen Abkommen enthaltene Liste von Schutzmaßnahmen in der Praxis eingehalten werden kann, wobei die möglichen Beeinträchtigungen der Einhaltung dieser Schutzmaßnahmen durch die Rechtsvorschriften des Drittlands zu berücksichtigen sind.

14. In diesem Zusammenhang ist auch anzumerken, dass internationale Vereinbarungen zur Gewährleistung der in diesen Leitlinien aufgeführten Schutzmaßnahmen auf bereits bestehenden Elementen im nationalen Recht eines Drittlandes oder den internen Regeln/Regelwerken einer internationalen Organisation aufbauen können.

2.1 Zweck und Umfang

15. Internationale Abkommen sollten ihren Anwendungsbereich definieren und ihre Zwecke sollten ausdrücklich und konkret festgelegt werden. Darüber hinaus sollten sie die betroffenen Kategorien personenbezogener Daten und die Art der Verarbeitung der personenbezogenen Daten, die im Rahmen des Abkommens übermittelt und verarbeitet werden, eindeutig angeben.

2.2 Definitionen

16. Internationale Vereinbarungen sollten Definitionen der grundlegenden Konzepte und Rechte für personenbezogene Daten in Übereinstimmung mit der DSGVO enthalten, die für die betreffende

Vereinbarung relevant sind. Als Beispiel sollten solche Vereinbarungen, wenn darauf verwiesen wird, die folgenden wichtigen Definitionen enthalten: "personenbezogene Daten", "Verarbeitung personenbezogener Daten", "Datenverantwortlicher", "Datenverarbeiter", "Empfänger" und "sensible Daten".

2.3 Grundsätze des Datenschutzes

17. Internationale Abkommen müssen einen spezifischen Wortlaut enthalten, der verlangt, dass die Kernprinzipien des Datenschutzes von beiden Parteien gewährleistet werden.

2.3.1 Prinzip der Zweckbindung

18. In internationalen Vereinbarungen müssen die Zwecke angegeben werden, für die personenbezogene Daten übermittelt und verarbeitet werden sollen, einschließlich kompatibler Zwecke für die weitere Verarbeitung, sowie um sicherzustellen, dass die Daten nicht für unvereinbare Zwecke weiterverarbeitet werden. Zu den kompatiblen Zwecken kann die Speicherung zu Archivierungszwecken im öffentlichen Interesse gehören, ebenso wie die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken. Zur besseren Übersichtlichkeit wird empfohlen, die spezifischen Zwecke für die Verarbeitung und Übermittlung der Daten in dem internationalen Abkommen selbst aufzuführen.
19. Um jegliches Risiko eines "Function Creep" zu vermeiden, sollte in solchen Vereinbarungen auch festgelegt werden, dass übermittelte Daten nicht für andere als die ausdrücklich in der Vereinbarung genannten Zwecke verwendet werden dürfen, mit Ausnahme der im folgenden Absatz genannten.
20. Wollen beide Parteien des internationalen Abkommens der empfangenden öffentlichen Stelle eine weitere kompatible Nutzung der übermittelten personenbezogenen Daten gestatten, so ist die weitere Nutzung durch die empfangende öffentliche Stelle nur zulässig, wenn sie mit der ursprünglichen Nutzung vereinbar ist und zuvor der übermittelnden öffentlichen Stelle mitgeteilt wurde, die aus bestimmten Gründen widersprechen kann.

2.3.2 Grundsätze der Datengenauigkeit und -minimierung

21. In dem internationalen Abkommen muss festgelegt werden, dass die übermittelten und weiterverarbeiteten Daten den Zwecken entsprechen, für die sie übermittelt und weiterverarbeitet werden, dafür erheblich sind und sich auf das beschränken, was im Hinblick auf die Zwecke, für die sie übermittelt und weiterverarbeitet werden, erforderlich ist.
22. In der Praxis ist dieser Grundsatz der Datenminimierung wichtig, um die Übermittlung von personenbezogenen Daten zu vermeiden, wenn diese unangemessen oder übermäßig sind.
23. Außerdem sollten die Daten im Hinblick auf die Zwecke, für die sie verarbeitet werden, richtig und aktuell sein. Ein internationales Abkommen muss daher vorsehen, dass die übermittelnde Partei Folgendes sicherstellt

dass die im Rahmen der Vereinbarung übermittelten personenbezogenen Daten richtig und gegebenenfalls auf dem neuesten Stand sind. Darüber hinaus sollte die Vereinbarung vorsehen, dass eine der Parteien, wenn sie feststellt, dass unrichtige oder veraltete Daten übermittelt wurden oder verarbeitet werden, die andere Partei unverzüglich benachrichtigen muss. Schließlich sollte die Vereinbarung sicherstellen, dass jede Partei, die die Daten verarbeitet, alle angemessenen Schritte unternimmt, um die Informationen zu berichtigen oder zu löschen, wenn bestätigt wird, dass die übermittelten oder verarbeiteten Daten unrichtig sind.

2.3.3 Prinzip der Speicherbegrenzung

24. Die Parteien müssen sicherstellen, dass das internationale Abkommen eine Datenaufbewahrungsklausel enthält. In dieser Klausel sollte insbesondere festgelegt werden, dass personenbezogene Daten nicht unbegrenzt aufbewahrt werden, sondern in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, nur so lange aufbewahrt werden, wie es für den Zweck, für den sie übermittelt und anschließend verarbeitet wurden, erforderlich ist. Dies kann die Speicherung so lange einschließen, wie es für im öffentlichen Interesse liegende Archivierungszwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke erforderlich ist, sofern geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden, wie z. B. zusätzliche technische Maßnahmen (z. B. Sicherheitsmaßnahmen, Pseudonymisierung) und Zugangsbeschränkungen. Wenn eine maximale Aufbewahrungsfrist nicht bereits in der nationalen Gesetzgebung oder den internen Regeln/Regelwerken einer internationalen Organisation festgelegt ist, sollte eine maximale Aufbewahrungsfrist im Text des Abkommens festgelegt werden.

2.3.4 Sicherheit und Vertraulichkeit der Daten

25. Die Parteien sollten sich verpflichten, die Sicherheit und Vertraulichkeit der von ihnen durchgeführten Verarbeitung und Übertragung personenbezogener Daten zu gewährleisten. Insbesondere sollten sich die Parteien verpflichten, geeignete technische und organisatorische Maßnahmen zu ergreifen, um personenbezogene Daten vor versehentlichem oder unrechtmäßigem Zugriff, Zerstörung, Verlust, Änderung oder unbefugter Offenlegung zu schützen. Diese Maßnahmen können z. B. Verschlüsselung, auch während der Übertragung, Pseudonymisierung, Kennzeichnung von Informationen als personenbezogene Daten, die aus dem EWR übermittelt werden, Beschränkung des Zugriffs auf personenbezogene Daten, sichere Speicherung personenbezogener Daten oder die Umsetzung von Richtlinien, die die Sicherheit und Vertraulichkeit personenbezogener Daten gewährleisten, umfassen.
Das Sicherheitsniveau sollte die Risiken, den Stand der Technik und die damit verbundenen Kosten berücksichtigen.
26. In dem internationalen Abkommen kann ferner festgelegt werden, dass eine der Parteien, wenn sie von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt, die andere(n) Partei(en) so schnell wie möglich unterrichtet und angemessene und geeignete Mittel einsetzt, um die Verletzung des Schutzes personenbezogener Daten zu beheben und die potenziellen nachteiligen Auswirkungen so gering wie möglich zu halten, einschließlich der unverzüglichen Unterrichtung der betroffenen Person über die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der natürlichen Person führt.
Es wird empfohlen, dass der Zeitrahmen für die Benachrichtigung bei einer Verletzung des Schutzes personenbezogener Daten sowie die Verfahren für die Kommunikation mit der betroffenen Person in dem internationalen Abkommen festgelegt werden.

2.4 Rechte der betroffenen Personen

27. Das internationale Abkommen muss durchsetzbare und wirksame Rechte der Betroffenen gemäß Artikel 46 (1) und Erwägungsgrund 108 der DSGVO gewährleisten.
28. Die Rechte, die den betroffenen Personen zur Verfügung stehen, einschließlich der spezifischen Verpflichtungen, die die Parteien eingegangen sind, um diese Rechte zu gewährleisten, sollten in dem Abkommen aufgeführt werden. Um wirksam zu sein, muss das internationale Abkommen Mechanismen vorsehen, die ihre Anwendung in der Praxis gewährleisten. Außerdem muss jede Verletzung der Rechte der betroffenen Person mit einem angemessenen Rechtsbehelf einhergehen.

2.4.1 Recht auf Transparenz

29. Die Parteien müssen sicherstellen, dass die internationale Vereinbarung einen klaren Wortlaut enthält, der die Transparenzpflichten der Parteien beschreibt.
30. Solche Verpflichtungen sollten einerseits einen allgemeinen Informationshinweis enthalten, der mindestens Informationen darüber enthält, wie und warum die öffentlichen Stellen personenbezogene Daten verarbeiten und übermitteln dürfen, das für die Übermittlung verwendete Instrument, die Stellen, an die solche Daten übermittelt werden dürfen, die den betroffenen Personen zur Verfügung stehenden Rechte und geltenden Einschränkungen, verfügbare Rechtsbehelfsmechanismen und Kontaktdaten für die Einreichung einer Streitigkeit oder Forderung.
31. Es ist jedoch wichtig, daran zu erinnern, dass für die übertragende öffentliche Stelle ein allgemeiner Informationshinweis auf der Website der betreffenden öffentlichen Stelle nicht ausreicht. Die individuelle Information der betroffenen Personen sollte von der übertragenden öffentlichen Stelle gemäß den Meldevorschriften der Artikel 13 und 14 DSGVO19 erfolgen.
Das internationale Abkommen kann auch einige Ausnahmen für solche individuellen Informationen vorsehen. Diese Ausnahmen sind begrenzt und sollten im Einklang mit den in Artikel 14 (5) DSGVO vorgesehenen Ausnahmen stehen, z. B. wenn die betroffene Person bereits über die Informationen verfügt oder wenn sich die Bereitstellung dieser Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand bedeuten würde.
32. Die Parteien müssen sich verpflichten, das internationale Abkommen den betroffenen Personen auf Anfrage zur Verfügung zu stellen und das internationale Abkommen oder die einschlägigen Bestimmungen, die angemessene Garantien vorsehen, auf ihrer Website öffentlich zugänglich zu machen. Soweit dies zum Schutz sensibler oder sonstiger vertraulicher Informationen erforderlich ist, kann der Text des internationalen Abkommens vor der Weitergabe einer Kopie oder der öffentlichen Zugänglichmachung geschwärzt werden. Soweit dies erforderlich ist, damit die betroffene Person den Inhalt des internationalen Abkommens verstehen kann, müssen die Parteien eine aussagekräftige Zusammenfassung desselben bereitstellen.

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

33. Das internationale Abkommen sollte das Recht der betroffenen Person auf Information über und Zugang zu allen sie betreffenden personenbezogenen Daten, die verarbeitet werden, sowie das Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung und gegebenenfalls das Recht auf Widerspruch gegen die Datenverarbeitung aus Gründen, die sich aus ihrer besonderen Situation ergeben, gewährleisten.
34. In Bezug auf das Auskunftsrecht sollte in dem internationalen Abkommen festgelegt werden, dass Personen gegenüber der empfangenden öffentlichen Stelle das Recht haben, eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht, und wenn dies der Fall ist, Zugang zu diesen Daten zu erhalten, sowie spezifische Informationen über die Verarbeitung zu erhalten, einschließlich des Zwecks der Verarbeitung, der betroffenen Kategorien personenbezogener Daten, der Empfänger, an die personenbezogene Daten weitergegeben werden, der vorgesehenen Aufbewahrungsdauer und der Rechtsbehelfsmöglichkeiten.
35. Das Abkommen sollte außerdem festlegen, wann diese Rechte geltend gemacht werden können, und die Modalitäten enthalten, wie die betroffenen Personen diese Rechte vor beiden Parteien ausüben können und wie die Parteien auf solche Anfragen reagieren. In Bezug auf die Löschung könnte das internationale Abkommen beispielsweise festlegen, dass die Daten zu löschen sind, wenn die

Informationen unrechtmäßig verarbeitet wurden oder für den Zweck der Verarbeitung nicht mehr erforderlich sind. Darüber hinaus sollte das internationale Abkommen festlegen, dass die Parteien in angemessener und zeitnaher Weise auf Anfragen von betroffenen Personen reagieren. In der internationalen Vereinbarung könnte auch festgelegt werden, dass die Parteien geeignete Maßnahmen ergreifen können, wie z. B. die Erhebung angemessener Gebühren zur Deckung der Verwaltungskosten, wenn die Anfragen einer betroffenen Person offensichtlich unbegründet oder überzogen sind, insbesondere aufgrund ihres wiederholten Charakters.

36. Das internationale Abkommen sollte auch eine Verpflichtung der übermittelnden öffentlichen Stelle vorsehen, die betroffene Person nach der Übermittlung ihrer personenbezogenen Daten unverzüglich über die Maßnahmen zu unterrichten, die auf ihren Antrag im Rahmen der in dem internationalen Abkommen vorgesehenen Rechte ergriffen wurden, indem eine angemessene Frist (z. B. ein Monat) gesetzt wird. Schließlich sollte die betroffene Person, wenn die Parteien auf ihr Ersuchen hin nicht tätig werden, unverzüglich unter Setzung einer angemessenen Frist (z. B. innerhalb eines Monats nach Eingang des Ersuchens) über die Gründe für das Nichttätigwerden und über die Möglichkeit, eine Beschwerde einzureichen und einen gerichtlichen Rechtsbehelf einzulegen, unterrichtet werden.
37. Das internationale Abkommen kann auch Ausnahmen von diesen Rechten vorsehen. So könnten beispielsweise Ausnahmen vom Recht auf Auskunft und Löschung vorgesehen werden, wie sie in Artikel 15 Absatz 4 und Artikel 17 Absatz 3 DS-GVO vorgesehen sind. Ebenso könnten Ausnahmen von den Rechten des Einzelnen vorgesehen werden, wenn personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken, zu statistischen Zwecken oder zu Archivierungszwecken verarbeitet werden, sofern diese Rechte die Erreichung dieser spezifischen Zwecke wahrscheinlich unmöglich machen oder ernsthaft beeinträchtigen würden und sofern geeignete Garantien vorgesehen sind (z. B. technische und organisatorische Maßnahmen, einschließlich Pseudonymisierung). Schließlich kann die Vereinbarung vorsehen, dass die Parteien es ablehnen können, einem Ersuchen nachzukommen, das offenkundig unbegründet oder übertrieben ist.

2.4.3 Automatisierte individuelle Entscheidungsfindung

38. Sofern dies für das betreffende Abkommen relevant ist, sollten internationale Abkommen grundsätzlich eine Klausel enthalten, die besagt, dass die empfangende öffentliche Stelle keine Entscheidungen trifft, die ausschließlich auf einer automatisierten individuellen Entscheidungsfindung, einschließlich Profiling, beruhen und Rechtswirkungen für die betroffene Person entfalten oder diese in ähnlicher Weise beeinträchtigen. Beinhaltet der Zweck der Übermittlung die Möglichkeit für die empfangende öffentliche Stelle, Entscheidungen ausschließlich auf der Grundlage einer automatisierten Verarbeitung im Sinne von Artikel 22 DSGVO zu treffen, sollte dies nur unter bestimmten, in der internationalen Vereinbarung festgelegten Bedingungen erfolgen, wie etwa der Notwendigkeit, die ausdrückliche Einwilligung der betroffenen Person einzuholen. Entspricht die Entscheidung nicht diesen Bedingungen, sollte die betroffene Person das Recht haben, ihr nicht unterworfen zu werden. Wenn das internationale Abkommen eine automatisierte individuelle Entscheidungsfindung zulässt, sollte es auf jeden Fall die notwendigen Garantien vorsehen, einschließlich des Rechts, über die spezifischen Gründe für die Entscheidung und die damit verbundene Logik informiert zu werden, unrichtige oder unvollständige Informationen zu berichtigen und die Entscheidung anzufechten und ein menschliches Eingreifen zu erhalten.

2.4.4 Recht auf Entschädigung

39. Die gesicherten Betroffenenrechte müssen durchsetzbar und wirksam sein. Daher muss die betroffene Person Zugang zu Rechtsbehelfen haben. Verschiedene Beispiele für Möglichkeiten, Rechtsbehelfsmechanismen anzubieten, sind unten unter den Abschnitten 2.7 und 3 angegeben.

2.4.5 Einschränkung der Rechte der betroffenen Personen

40. Das internationale Abkommen kann auch Einschränkungen der Rechte der betroffenen Personen vorsehen. Diese Einschränkungen sollten im Einklang mit den in Artikel 23 DSGVO vorgesehenen Einschränkungen stehen. Eine solche Einschränkung muss in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme sein, um wichtige Ziele von öffentlichem Interesse zu schützen, die mit den in Artikel 23 Absatz 1 DSGVO aufgeführten Zielen übereinstimmen, einschließlich der Rechte und Freiheiten anderer, der nationalen Sicherheit, der Verteidigung oder der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten. Sie muss gesetzlich vorgesehen sein oder, im Falle von internationalen

Organisationen, den geltenden internen Regeln/Rechtsvorschriften und gilt nur so lange, wie der Grund für die Beschränkung fortbesteht.

2.5 Beschränkungen der Weitergabe und des Austauschs von Daten (einschließlich Offenlegung und staatlicher Zugriff)

41. Weiterübermittlungen durch die empfangende öffentliche Stelle oder internationale Organisation an Empfänger, die nicht durch die Vereinbarung gebunden sind, sollten in der Regel durch die internationale Vereinbarung ausdrücklich ausgeschlossen werden. Je nach dem Gegenstand und den besonderen Umständen können die Parteien es für notwendig erachten, Weiterübermittlungen zuzulassen. In diesem Fall sollte das internationale Abkommen unter der Voraussetzung, dass der Grundsatz der Zweckbindung beachtet wird²⁰, vorsehen, dass solche Weiterübermittlungen nur stattfinden können, wenn die übermittelnde öffentliche Stelle ihre vorherige und ausdrückliche Genehmigung erteilt hat und die empfangenden Dritten sich verpflichten, dieselben Datenschutzgrundsätze und -garantien einzuhalten, wie sie in dem internationalen Abkommen enthalten sind. Dazu sollte die Verpflichtung gehören, den betroffenen Personen dieselben Datenschutzrechte und -garantien zu gewähren, wie sie in dem internationalen Abkommen vorgesehen sind, um sicherzustellen, dass das Schutzniveau bei der Weiterübermittlung von Daten nicht verringert wird.
42. In der Regel sollten für die Weitergabe personenbezogener Daten innerhalb desselben Landes dieselben Garantien gelten wie für die Weitergabe, d. h. das internationale Abkommen schließt diese Weitergabe aus, und Ausnahmen sollten im Allgemeinen nur dann zulässig sein, wenn die übermittelnde öffentliche Stelle ihre vorherige und ausdrückliche Genehmigung erteilt hat und die empfangenden Dritten sich verpflichten, dieselben Datenschutzgrundsätze und -garantien einzuhalten, wie sie in dem internationalen Abkommen vorgesehen sind.
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 zu übermitteln/ weiterzugeben beabsichtigt, die Gründe und Zwecke, für die sie die Übermittlung/ Weitergabe der personenbezogenen Daten für erforderlich hält, sowie - im Falle von Weiterübermittlungen - die Länder oder internationalen Organisationen, an die sie personenbezogene Daten weiterzugeben beabsichtigt, bereitstellt, um die Rechtsvorschriften des Drittlandes bzw. - im Falle internationaler Organisationen - die anwendbaren internen Vorschriften/Rechtsrahmen beurteilen zu können.
44. In Fällen, in denen es notwendig ist, die Weitergabe personenbezogener Daten an einen Dritten im selben Land wie die empfangende öffentliche Stelle oder eine andere internationale Organisation zu gestatten, könnte die Weitergabe unter bestimmten Umständen entweder mit vorheriger und ausdrücklicher Genehmigung der übermittelnden öffentlichen Stelle oder solange es eine verbindliche Verpflichtung des empfangenden Dritten gibt, die in dem internationalen Abkommen enthaltenen Grundsätze und Garantien einzuhalten, gestattet werden.
45. Darüber hinaus könnten in dem internationalen Abkommen außergewöhnliche Umstände festgelegt werden, unter denen eine Weitergabe ohne vorherige Genehmigung oder die oben genannten Verpflichtungen im Einklang mit den in Artikel 49 der DSGVO aufgeführten Ausnahmen erfolgen könnte, z. B. wenn diese spezifische Weitergabe zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich wäre. Solche außergewöhnlichen Umstände könnten auch vorliegen, wenn die Weitergabe nach dem Recht der empfangenden Partei erforderlich ist, da sie für unmittelbar damit zusammenhängende Ermittlungen/Gerichtsverfahren notwendig ist.
46. In den im obigen Absatz genannten Fällen sollte das internationale Abkommen die besonderen und Angenommenen

außergewöhnlichen Umstände, unter denen eine solche gemeinsame Nutzung von Daten zulässig ist, eindeutig festlegen. Die empfangende öffentliche Stelle oder internationale Organisation sollte auch verpflichtet sein, die übermittelnde öffentliche Stelle vor der gemeinsamen Nutzung zu benachrichtigen und Informationen über die gemeinsam genutzten Daten, den empfangenden Dritten und die Rechtsgrundlage für die gemeinsame Nutzung anzugeben. Die übermittelnde öffentliche Stelle sollte ihrerseits Aufzeichnungen über solche Benachrichtigungen der empfangenden öffentlichen Stelle oder der internationalen Organisation führen und ihrer SA auf Anfrage diese Informationen zur Verfügung stellen. Wenn eine solche Benachrichtigung vor der Weitergabe gegen gesetzlich vorgesehene Geheimhaltungspflichten verstößt, z. B. zur Wahrung der Vertraulichkeit einer Untersuchung, 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 Anfragen, einschließlich Informationen über die angeforderten Datenkategorien, die anfragende Stelle und die Rechtsgrundlage für die Weitergabe, übermittelt werden.

47. In allen oben genannten Szenarien sollte das internationale Abkommen nur die Weitergabe personenbezogener Daten an andere Behörden im Drittland der empfangenden öffentlichen Stelle erlauben, die nicht über das hinausgeht, was in einer demokratischen Gesellschaft zur Wahrung wichtiger Ziele von öffentlichem Interesse im Einklang mit den in Artikel 23 Absatz 1 DSGVO aufgeführten Zielen und im Einklang mit der Rechtsprechung des EuGH erforderlich und verhältnismäßig ist. Um einen möglichen Zugriff von Drittlandsbehörden zu Überwachungszwecken zu beurteilen, sollte die übermittelnde Behörde die Elemente berücksichtigen, die in den vier europäischen Grundgarantien²¹ genannt werden. Dazu gehört die Verfügbarkeit eines wirksamen Rechtsbehelfs für die betroffenen Personen im Drittland der empfangenden öffentlichen Stelle, wenn öffentliche Behörden auf ihre personenbezogenen Daten zugreifen.²² Im Falle von Übermittlungen an internationale Organisationen muss ein solcher Zugriff im Einklang mit dem Völkerrecht und insbesondere unbeschadet der Vorrechte und Befreiungen der internationalen Organisation erfolgen.
48. Je nach Fall kann es sinnvoll sein, die Aufnahme eines Anhangs in das internationale Abkommen zu verlangen, in dem die Gesetze aufgeführt sind, die die Weitergabe an andere öffentliche Stellen, auch zu Überwachungszwecken im Zielland, regeln. Alle Änderungen dieses Anhangs sollten der übermittelnden Partei innerhalb eines bestimmten Zeitraums mitgeteilt werden.

2.6 Sensible Daten

49. Wenn ein internationales Abkommen die Übermittlung sensibler personenbezogener Daten im Sinne von Artikel 9 (1) der DSGVO vorsieht, sollten zusätzliche Garantien zur Bewältigung der spezifischen Risiken enthalten sein, die von der empfangenden öffentlichen Stelle oder internationalen Organisation umzusetzen sind. Diese könnten z. B. Beschränkungen wie Zugangsbeschränkungen, Beschränkungen der Zwecke, für die die Informationen verarbeitet werden dürfen, Beschränkungen bei der Weiterübermittlung usw. oder spezifische Garantien, z. B. zusätzliche Sicherheitsmaßnahmen, die eine spezielle Schulung des Personals erfordern, das auf die Informationen zugreifen darf, umfassen.

2.7 Abhilfemechanismen

50. Um durchsetzbare und wirksame Rechte der betroffenen Personen zu gewährleisten, muss das internationale Abkommen ein System vorsehen, das es den betroffenen Personen ermöglicht, nach der Übermittlung ihrer Daten an ein Nicht-EWR-Land oder eine internationale Organisation weiterhin Rechtsbehelfsmechanismen in Anspruch zu nehmen. Diese Rechtsbehelfsmechanismen müssen

einen Rechtsbehelf für Personen vorsehen, die von der Nichteinhaltung der Bestimmungen des gewählten Instruments betroffen sind, und somit die Möglichkeit für betroffene Personen, deren personenbezogene Daten aus dem EWR übermittelt wurden, Beschwerden über eine solche Nichteinhaltung einzureichen und eine Lösung für diese Beschwerden zu finden. Insbesondere muss sichergestellt werden, dass die betroffene Person einen wirksamen Weg hat, um sich bei den öffentlichen Stellen, die Vertragsparteien des internationalen Abkommens sind, und (entweder direkt oder nachdem sie sich an die betreffende Partei gewandt hat) bei einem unabhängigen Aufsichtsmechanismus zu beschweren. Außerdem sollte grundsätzlich ein gerichtlicher Rechtsbehelf zur Verfügung stehen.

51. Erstens sollte sich die empfangende öffentliche Stelle verpflichten, einen Mechanismus einzurichten, um Beschwerden von betroffenen Personen über die Einhaltung der vereinbarten Datenschutzgarantien wirksam und zeitnah zu bearbeiten und zu lösen. Darüber hinaus sollten die betroffenen Personen die Möglichkeit haben, einen wirksamen verwaltungsrechtlichen Rechtsbehelf bei einer unabhängigen Aufsichtsbehörde, einschließlich - sofern vorhanden - einer unabhängigen Datenschutzbehörde²³, einzulegen.
52. Zweitens sollte das Abkommen einen gerichtlichen Rechtsbehelf einschließlich des Ersatzes von Schäden - sowohl materieller als auch immaterieller Art - als Folge der unrechtmäßigen Verarbeitung der personenbezogenen Daten ermöglichen. Besteht keine Möglichkeit, einen wirksamen gerichtlichen Rechtsbehelf zu gewährleisten, z. B. aufgrund von Beschränkungen im innerstaatlichen Recht oder des besonderen Status der empfangenden öffentlichen Stelle, z. B. einer internationalen Organisation, muss das internationale Abkommen alternative Garantien vorsehen. Diese alternativen Garantien müssen der betroffenen Person Garantien bieten, die im Wesentlichen den in Artikel 47 der Charta der Grundrechte der Europäischen Union (EU-Charta) geforderten Garantien ^{entsprechen²⁴}.
53. In diesem Fall könnte das internationale Abkommen eine Struktur schaffen, die es der betroffenen Person ermöglicht, ihre Rechte außerhalb der Gerichte durchzusetzen, z. B. durch quasi-gerichtliche, verbindliche Mechanismen wie Schiedsverfahren oder alternative Streitbeilegungsmechanismen wie Mediation, die eine unabhängige Überprüfung gewährleisten und die empfangende öffentliche Stelle binden würden²⁵. Darüber hinaus könnte sich die öffentliche Stelle, die die personenbezogenen Daten übermittelt, dazu verpflichten, für Schäden durch unrechtmäßige Verarbeitung der personenbezogenen Daten, die durch die unabhängige Überprüfung bezeugt werden, zu haften. Ausnahmsweise könnten durch die Vereinbarung andere, ebenso unabhängige und wirksame Rechtsbehelfsmechanismen geschaffen werden, z. B. wirksame Rechtsbehelfsmechanismen, die von internationalen Organisationen umgesetzt werden.
54. Für alle oben genannten Rechtsbehelfsmechanismen sollte das internationale Abkommen eine Verpflichtung für die Parteien enthalten, sich gegenseitig über den Ausgang des Verfahrens zu informieren, insbesondere wenn eine Beschwerde einer Einzelperson abgewiesen oder nicht gelöst wird.
55. Der Rechtsbehelfsmechanismus muss mit der Möglichkeit für die übermittelnde öffentliche Stelle verbunden sein, die Übermittlung personenbezogener Daten im Rahmen des internationalen Abkommens auszusetzen oder zu beenden, wenn es den Parteien nicht gelingt, eine Streitigkeit gütlich beizulegen, bis sie der Ansicht ist, dass die Frage von der empfangenden öffentlichen Stelle zufriedenstellend gelöst wurde. Eine solche Aussetzung oder Beendigung muss, wenn sie durchgeführt wird, mit einer Verpflichtung der empfangenden öffentlichen Stelle zur Rückgabe oder Löschung der personenbezogenen Daten verbunden sein. Die übermittelnde öffentliche Stelle muss die Aussetzung oder Beendigung der zuständigen nationalen SA mitteilen.

2.8 Überwachungsmechanismen

56. Um sicherzustellen, dass alle durch das internationale Abkommen entstandenen Verpflichtungen erfüllt werden, muss das internationale Abkommen eine unabhängige Aufsicht vorsehen, die die ordnungsgemäße Anwendung des Abkommens und Eingriffe in die durch das Abkommen gewährten Rechte überwacht.
 57. Erstens sollte die Vereinbarung eine interne Überwachung vorsehen, die die Einhaltung der Vereinbarung sicherstellt. Jede Vertragspartei sollte regelmäßige interne Kontrollen der eingerichteten Verfahren und der wirksamen Anwendung der im Abkommen vorgesehenen Garantien durchführen. Bei den regelmäßigen internen Kontrollen sollten auch etwaige Änderungen der Rechtsvorschriften überprüft werden, die die Partei(en) daran hindern würden, die in dem internationalen Abkommen enthaltenen Datenschutzgrundsätze und -garantien einzuhalten. Darüber hinaus könnte vorgesehen werden, dass eine Partei des Abkommens auch von einer anderen Partei des Abkommens verlangen kann, eine solche Überprüfung durchzuführen. Das internationale Abkommen muss vorschreiben, dass die Parteien auf Anfragen der anderen Partei bezüglich der effektiven Umsetzung der Garantien des Abkommens antworten müssen. Jede Partei, die eine Überprüfung durchführt, sollte der (den) anderen Partei(en) des Abkommens die Ergebnisse der Überprüfungen mitteilen. Idealerweise sollte eine solche Mitteilung auch an den unabhängigen Aufsichtsmechanismus erfolgen, der die Vereinbarung überwacht.
 58. Darüber hinaus muss das internationale Abkommen die Verpflichtung enthalten, dass eine Partei die andere Partei unverzüglich informiert, wenn sie aus irgendeinem Grund nicht in der Lage ist, die Garantien des Abkommens wirksam umzusetzen. Für diesen Fall muss das internationale Abkommen die Möglichkeit vorsehen, dass die übermittelnde öffentliche Stelle die Übermittlung personenbezogener Daten im Rahmen des internationalen Abkommens an die empfangende öffentliche Stelle so lange aussetzen oder beenden kann, bis die empfangende öffentliche Stelle die übermittelnde öffentliche Stelle darüber informiert, dass sie wieder in der Lage ist, im Einklang mit den Garantien zu handeln. Die übermittelnde Stelle muss die Änderung der Situation sowie die Aussetzung von Übermittlungen oder die Beendigung des Abkommens der zuständigen nationalen SA mitteilen.
 59. Zweitens muss die Vereinbarung eine unabhängige Aufsicht vorsehen, die dafür zuständig ist, sicherzustellen, dass die Parteien die in der Vereinbarung festgelegten Bestimmungen einhalten. Dies ergibt sich unmittelbar aus der EU-Charta²⁶ und der Europäischen Menschenrechtskonvention (EMRK)²⁷ in Übereinstimmung mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) und den im ^{Primärrecht²⁸ sowie in der} entsprechenden Rechtsprechung festgelegten Bedingungen.
-

60. Der EuGH hat seit 2015²⁹ die Notwendigkeit eines unabhängigen Rechtsbehelfs und Überwachungsmechanismus bekräftigt.³⁰ Ebenso hat der EGMR in seinen Urteilen häufig hervorgehoben, dass jeder Eingriff in das Recht auf Achtung des Privatlebens, wie es in Artikel 8 EMRK verankert ist, einem wirksamen, unabhängigen und unparteiischen Aufsichtssystem unterliegen muss³¹.
61. Die Vereinbarung könnte sich beispielsweise auf die Aufsicht durch eine zuständige Aufsichtsbehörde berufen, wenn es im Land der öffentlichen Stelle, die die personenbezogenen Daten aus dem EWR erhält, eine solche gibt, auch wenn in der DSGVO nicht festgelegt ist, dass die zuständige Aufsichtsbehörde die externe Aufsichtsbehörde sein muss. Darüber hinaus könnte die Vereinbarung die freiwillige Verpflichtung der empfangenden Partei zur Zusammenarbeit mit den EWR-Aufsichtsbehörden enthalten.
62. In Ermangelung einer Aufsichtsbehörde, die speziell mit der Überwachung des Datenschutzrechts in dem Drittland oder bei der internationalen Organisation betraut ist, muss der Bedarf an einem unabhängigen, wirksamen und unparteiischen Aufsichtsmechanismus auf andere Weise gedeckt werden. Welche Art von unabhängigem Aufsichtsmechanismus eingerichtet wird, kann vom jeweiligen Fall abhängen.
63. Die Vereinbarung könnte z. B. auf bestehende Aufsichtsorgane im Drittland verweisen, die keine Aufsichtsbehörde im Bereich des Datenschutzes sind. Wenn aus struktureller oder institutioneller Sicht keine externe unabhängige Aufsicht gewährleistet werden kann, z. B. aufgrund der Vorrechte und Immunitäten bestimmter internationaler Organisationen, könnte die Aufsicht außerdem durch funktionell autonome Mechanismen gewährleistet werden. Dabei muss es sich um ein Gremium handeln, das zwar selbst nicht extern ist, aber seine Aufgaben unabhängig, d.h. frei von Weisungen, mit ausreichenden personellen, technischen und finanziellen Ressourcen etc. wahrnimmt. Die empfangende Partei ist an die Entscheidungen der Aufsichtsbehörde gebunden.

2.9 Kündigungsklausel

64. Das internationale Abkommen sollte vorsehen, dass alle personenbezogenen Daten, die vor der wirksamen Beendigung des internationalen Abkommens aus dem EWR gemäß dem internationalen Abkommen übermittelt wurden, weiterhin gemäß den Bestimmungen des internationalen Abkommens verarbeitet werden.
-

3 SPEZIFISCHE INFORMATIONEN ZU ARTIKEL 46 GDPR

3.1 Spezifische Informationen zu rechtsverbindlichen und durchsetzbaren Instrumenten

- Artikel 46 (2) (a) GDPR

65. Artikel 46 (2) (a) DSGVO erlaubt es öffentlichen Stellen des EWR, Übermittlungen an öffentliche Stellen in einem Drittland oder an eine internationale Organisation auf Instrumente zu stützen, die zwischen ihnen geschlossen wurden, ohne eine vorherige Genehmigung einer ORKB einzuholen. Solche Instrumente müssen rechtsverbindlich und durchsetzbar sein. Daher können internationale Verträge, öffentlich-rechtliche Verträge oder selbstausführende Verwaltungsvereinbarungen gemäß dieser Bestimmung verwendet werden.
66. Jedes rechtsverbindliche und durchsetzbare Instrument sollte den Kernsatz der Datenschutzgrundsätze und die Rechte der betroffenen Personen gemäß der DSGVO umfassen.
67. Die Parteien sind verpflichtet, sich zu verpflichten, ausreichende Datenschutzgarantien für die Übermittlung von Daten einzurichten. Folglich sollte in der Vereinbarung auch festgelegt werden, wie die empfangende öffentliche Stelle den Kernbestand der grundlegenden Datenschutzprinzipien und die Rechte der betroffenen Personen auf alle übermittelten personenbezogenen Daten anwenden wird, um sicherzustellen, dass das Schutzniveau natürlicher Personen nach der DSGVO nicht untergraben wird.
68. Wenn es keine Möglichkeit gibt, einen wirksamen gerichtlichen Rechtsbehelf in rechtsverbindlichen und vollstreckbaren Instrumenten zu gewährleisten, so dass alternative Rechtsbehelfsmechanismen vereinbart werden müssen, sollten die öffentlichen Stellen des EWR vor Abschluss dieser Instrumente die zuständige SA konsultieren.
69. Auch wenn die Form des Instruments nicht entscheidend ist, solange es rechtsverbindlich und durchsetzbar ist, wäre es nach Ansicht des EDPB die beste Option, detaillierte Datenschutzklauseln direkt in das Instrument aufzunehmen. Sollte diese Lösung jedoch aufgrund der besonderen Umstände nicht durchführbar sein, empfiehlt der EDSB nachdrücklich, zumindest eine allgemeine Klausel mit den Datenschutzgrundsätzen direkt in den Text des Instruments aufzunehmen und die detaillierteren Bestimmungen und Garantien in einen Anhang zum Instrument einzufügen.

3.2 Spezifische Informationen über Verwaltungsvereinbarungen - Artikel 46 (3) (b) GDPR

70. Die DSGVO sieht in ihrem Artikel 46 (3) (b) auch alternative Instrumente in Form von Verwaltungsvereinbarungen vor, z. B. Memorandum of Understanding "MOU", die Schutz durch die von beiden Parteien eingegangenen Verpflichtungen bieten, um ihre gemeinsame Vereinbarung in Kraft zu setzen.
71. In diesem Zusammenhang wird in Artikel 46 (1) und Erwägungsgrund 108 der DSGVO festgelegt, dass diese Vereinbarungen durchsetzbare Rechte der betroffenen Person und wirksame Rechtsbehelfe gewährleisten müssen. Wenn in nicht rechtsverbindlichen Verwaltungsvereinbarungen Garantien vorgesehen sind, muss die Genehmigung der zuständigen Aufsichtsbehörde eingeholt werden.
72. Es sollte sorgfältig geprüft werden, ob angesichts des Zwecks der Verarbeitung und der Art der betreffenden Daten auf nicht rechtsverbindliche Verwaltungsvereinbarungen zurückgegriffen werden soll, um Garantien im öffentlichen Sektor zu bieten. Wenn Datenschutzrechte und Rechtsbehelfe für EWR-Personen nicht im innerstaatlichen Recht des Drittlandes oder in den internen

Vorschriften/Regelungen der internationalen Organisation vorgesehen sind, sollte dem Abschluss einer rechtsverbindlichen Vereinbarung der Vorzug gegeben werden. Unabhängig von der Art des angenommenen Instruments müssen die vorhandenen Maßnahmen wirksam sein, um eine angemessene Umsetzung, Durchsetzung und Überwachung zu gewährleisten.

73. Bei Verwaltungsvereinbarungen müssen besondere Schritte unternommen werden, um wirksame Rechte des Einzelnen, Rechtsbehelfe und Aufsicht zu gewährleisten. Um wirksame und durchsetzbare Rechte zu gewährleisten, sollte eine nicht verbindliche Übereinkunft insbesondere Zusicherungen der öffentlichen Stelle enthalten, die die personenbezogenen Daten aus dem EWR erhält, dass die Rechte des Einzelnen durch ihr innerstaatliches Recht in vollem Umfang gewährleistet sind und von EWR-Personen unter denselben Bedingungen ausgeübt werden können, wie dies für Bürger und Einwohner des betreffenden Drittlands der Fall ist. Das Gleiche gilt, wenn EWR-Personen im innerstaatlichen Rechtsrahmen der empfangenden öffentlichen Stelle administrative und gerichtliche Rechtsbehelfe zur Verfügung stehen. In ähnlicher Weise sollten internationale Organisationen Zusicherungen über die in ihren internen Vorschriften vorgesehenen Rechte des Einzelnen sowie die verfügbaren Rechtsbehelfsmechanismen geben.
74. Ist dies nicht der Fall, sollten die Rechte des Einzelnen durch spezifische Verpflichtungen der Parteien garantiert werden, kombiniert mit Verfahrensmechanismen, um ihre Wirksamkeit zu gewährleisten und dem Einzelnen Rechtsschutz zu bieten. Diese spezifischen Verpflichtungen und Verfahrensmechanismen müssen es in der Praxis ermöglichen, die Einhaltung des Schutzniveaus zu gewährleisten, das im Wesentlichen dem entspricht, das innerhalb der EU durch die DSGVO garantiert wird.
Solche Verfahrensmechanismen können z. B. die Verpflichtung der Parteien beinhalten, sich gegenseitig über Anfragen von EWR-Personen zu informieren und Streitigkeiten oder Ansprüche zeitnah beizulegen.
75. Darüber hinaus muss für den Fall, dass solche Streitigkeiten oder Ansprüche nicht auf gutlichem Wege zwischen den Parteien selbst gelöst werden können, dem Einzelnen ein unabhängiger und wirksamer Rechtsbehelf durch alternative Mechanismen zur Verfügung gestellt werden, z. B. durch eine Möglichkeit für den Einzelnen, einen alternativen Streitbeilegungsmechanismus wie ein Schiedsgericht oder eine Mediation in Anspruch zu nehmen. Ein solcher alternativer Streitbeilegungsmechanismus muss verbindlich sein³².
76. Je nach Fall sollte in der Verwaltungsvereinbarung eine Kombination aus allen oder einigen der oben genannten Maßnahmen vorgesehen werden, um einen wirksamen Rechtsbehelf zu gewährleisten. Andere Maßnahmen, die nicht in diesen Leitlinien enthalten sind, könnten ebenfalls akzeptabel sein, solange sie für einen unabhängigen und wirksamen Rechtsbehelf sorgen.
77. Jede Verwaltungsvereinbarung, die gemäß Artikel 46 (3) (b) DSGVO entwickelt wurde, wird von der zuständigen ORKB von Fall zu Fall geprüft, gefolgt von dem entsprechenden EDPB-Verfahren, falls anwendbar. Die zuständige ORKB stützt sich bei ihrer Prüfung auf die allgemeinen Empfehlungen in diesen Leitlinien, kann aber je nach Einzelfall auch weitere Garantien verlangen.
-

4 VERFAHRENSTECHNISCHE FRAGEN

78. Verwaltungsvereinbarungen gemäß Artikel 46 (3) (b) DSGVO werden aufgrund der Anforderungen für eine Genehmigung durch die zuständige Aufsichtsbehörde, die gemäß Artikel 46 (4) DSGVO das Kohärenzverfahren gemäß Artikel 64 (2) DSGVO anwendet, von Fall zu Fall geprüft. Bei der Integration alternativer Rechtsbehelfsmechanismen in verbindliche und vollstreckbare Instrumente gemäß Artikel 46 (2) (a) DSGVO empfiehlt der EDPB, auch den Rat der zuständigen Aufsichtsbehörde einzuholen. Der EDSB rät dringend dazu, die zuständige Aufsichtsbehörde frühzeitig zu konsultieren.

Für den Europäischen

Datenschutzausschuss Der Vorsitzende

(Andrea Jelinek)