Empfehlungen 01/2021 zu der Referenzgrundlage für Angemessenheit nach der Datenschutz-Richtlinie für den Bereich Justiz und Inneres

Angenommen am 2. Februar 2021

Inhalt

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 51 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[1] (im Folgenden: JI-Richtlinie),

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung —

HAT FOLGENDE EMPFEHLUNGEN ANGENOMMEN:

1. EINFÜHRUNG

1. Die Artikel-29-Datenschutzgruppe (WP29) hat eine Arbeitsunterlage[2] zur Referenzgrundlage für den Begriff „Angemessenheit" gemäß der Datenschutz-Grundverordnung (DSGVO)[3] veröffentlicht. Diese Arbeitsunterlage wurde vom Europäischen Datenschutzausschuss (EDSA) auf seiner ersten Plenarsitzung gebilligt.

2. Gemäß der dem Vertrag von Lissabon beigefügten Erklärung Nr. 21 können sich in den Bereichen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit aufgrund der Besonderheiten in diesen Bereichen spezifische, auf Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gestützte Vorschriften über den Schutz personenbezogener Daten und den freien Datenverkehr als erforderlich erweisen.

3. Auf dieser Grundlage hat der EU-Gesetzgeber die JI-Richtlinie erlassen, in der die spezifischen Vorschriften bezüglich der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit,** festgelegt sind.

4. In der JI-Richtlinie sind die Bedingungen aufgeführt, nach denen die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation in diesem Zusammenhang zulässig ist. Eine solche Übermittlung darf u.a. dann vorgenommen werden, wenn die Europäische Kommission beschlossen hat, dass das betreffende Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau gewährleistet.

[1] ABl. L 119 vom 4.5.2016, S. 89.
[2] WP254.rev01, von der Artikel-29-Datenschutzgruppe am 28. November 2017 angenommen, zuletzt überarbeitet und angenommen am 6. Februar 2018. Sie enthält eine Aktualisierung von Kapitel I der Arbeitsunterlage „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU", WP12, von der Artikel-29-Datenschutzgruppe am 24. Juli 1998 angenommen.
[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 26. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

5. Mit der Arbeitsunterlage WP254.rev01 zur Referenzgrundlage für Angemessenheit sollten der Europäischen Kommission Leitlinien zum Datenschutzniveau in Drittländern und internationalen Organisationen im Rahmen der DSGVO an die Hand gegeben werden; das vorliegende Dokument soll nun ähnliche Leitlinien im Rahmen der JI-Richtlinie bieten. Vor diesem Hintergrund legt dieses Dokument die wichtigsten datenschutzrechtlichen Grundsätze fest, die im Rechtsrahmen eines Drittlands oder einer internationalen Organisation gegeben sein müssen, damit sichergestellt werden kann, dass dieser Rechtsrahmen im Hinblick auf den Anwendungsbereich der JI-Richtlinie (d. h. für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung) der Sache nach gleichwertig mit dem Rechtsrahmen der EU ist. Darüber hinaus kann das Dokument auch Drittländern und internationalen Organisationen als Richtschnur dienen, die ein Interesse daran haben, Angemessenheit zu erreichen.

6. In dem Dokument werden ausschließlich Angemessenheitsbeschlüsse behandelt. Dabei handelt sich um Durchführungsrechtsakte der Europäischen Kommission nach Maßgabe von Artikel 36 Absatz 3 der JI-Richtlinie.

2. DER BEGRIFF DER „ANGEMESSENHEIT“

7. Die JI-Richtlinie enthält die Vorschriften für die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen, soweit die betreffende Übermittlung in den Anwendungsbereich der Richtlinie fällt. Die Vorschriften für die grenzüberschreitende Übermittlung personenbezogener Daten sind in Kapitel V der JI-Richtlinie, insbesondere in den Artikeln 35 bis 39, festgelegt.

8. Nach Artikel 36 der JI-Richtlinie dürfen personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden, wenn das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Aus der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH)[4] geht hervor, dass diese Bestimmung im Lichte von Artikel 35 der JI-Richtlinie („Allgemeine Grundsätze für die Übermittlung personenbezogener Daten“) zu lesen ist, in dem es heißt: „Sämtliche Bestimmungen [des Kapitels V der JI-Richtlinie] werden angewendet, um sicherzustellen, dass das durch diese Richtlinie gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.“

9. Hat die Europäische Kommission beschlossen, dass ein angemessenes Schutzniveau gewährleistet ist, können personenbezogene Daten ohne besondere Genehmigung an das betreffende Drittland, das betreffende Gebiet, den betreffenden Sektor oder die betreffende internationale Organisation übermittelt werden, es sei denn, ein anderer Mitgliedstaat, von dem die Daten stammen, muss die Übermittlung gemäß Artikel 35 und 36 sowie Erwägungsgrund 66 der JI-Richtlinie genehmigen. Dies gilt unbeschadet der Tatsache, dass die Verarbeitung von Daten durch die Behörden der betreffenden Mitgliedstaaten im Einklang mit den gemäß der Richtlinie (EU) 2016/680 erlassenen nationalen Bestimmungen erfolgen muss.

[4] Rechtssache C-311/18, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems, 16. Juli 2020, ECLI:EU:C:2020:559, Rn. 92 („Schrems II“).

10. Dieser Begriff des „angemessenen Schutzniveaus“, der bereits in der Richtlinie 95/46/EG[5] und im Rahmenbeschluss 2008/977/JI des Rates[6] verwendet wurde, wurde vom EuGH in diesem Zusammenhang und kürzlich im Rahmen der DSGVO weiterentwickelt.

11. Dem EuGH zufolge muss das Schutzniveau in dem Drittland zwar dem in der Union garantierten Niveau der Sache nach gleichwertig sein, doch können „sich die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden […], die in der Union herangezogen werden“. Gleichwohl „müssen sich diese Mittel […] in der Praxis als wirksam erweisen“.[7] Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Rechtsvorschriften der Union, sondern es müssen die wesentlichen Kernanforderungen dieser Vorschriften festgelegt werden.

12. In diesem Zusammenhang hat der Gerichtshof außerdem klargestellt, dass ein Angemessenheitsbeschluss der Kommission eine Feststellung dazu enthalten sollte, ob es in dem Drittland staatliche Regeln gibt, die dazu dienen, etwaige Eingriffe – zu denen die staatlichen Stellen dieses Landes in Verfolgung berechtigter Ziele wie der nationalen Sicherheit *berechtigt* wären – in die Grundrechte der Personen, deren Daten aus der Union in dieses Drittland übermittelt werden, zu begrenzen.[8]

13. Zweck der Angemessenheitsbeschlüsse der Europäischen Kommission ist es, gegenüber den Mitgliedstaaten[9], einschließlich ihrer zuständigen Datenschutzbehörden[10], verbindlich zu bestätigen, dass das Datenschutzniveau in einem Drittland oder in einer internationalen Organisation der Sache nach gleichwertig mit dem Datenschutzniveau in der Europäischen Union ist. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist, insbesondere in Fällen, in denen Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden.[11]

14. Angemessenheit kann durch eine Kombination von gegenüber den Betroffenen eingeräumten Rechten, bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt, und der Aufsicht durch unabhängige Behörden erreicht werden. Datenschutzvorschriften sind allerdings nur dann wirksam, wenn sie durchsetzbar sind und in der Praxis eingehalten werden. Daher gilt es nicht nur den Inhalt der Vorschriften zu bewerten, die für die an ein Drittland oder eine internationale Organisation übermittelten personenbezogenen Daten gelten, sondern auch das System, mit dem die Wirksamkeit dieser Regeln sichergestellt werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit von Datenschutzvorschriften von wesentlicher Bedeutung.[12]

---

[5] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

[6] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

[7] Rechtssache C−362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015, ECLI:EU:C:2015:650, Rn. 73 und 74 („Schrems I“).

[8] Schrems I, Rn 88.

[9] Artikel 288 Absatz 2 AEUV.

[10] Schrems I, Rn. 52.

[11] Erwägungsgrund 67 der JI-Richtlinie.

[12] Schrems I, Rn. 72 bis 74 und Gutachten 1/15 des EuGH zum geplanten Abkommen zwischen Kanada und der Europäischen Union, 26. Juli 2017, ECLI:EU:C:2017:592 (Gutachten 1/15), Rn. 134: „Das Recht auf Schutz personenbezogener Daten verlangt u. a., dass im Fall der Übermittlung personenbezogener Daten aus der Union

3. VERFAHRENSRECHTLICHE ASPEKTE VON ANGEMESSENHEITSFESTSTELLUNGEN GEMÄß DER JI-RICHTLINIE

15. Damit der EDSA seine Aufgabe nach Artikel 51 Absatz 1 Buchstabe g der JI-Richtlinie, die Kommission zu beraten, erfüllen kann, sollten ihm alle relevanten Dokumente, darunter einschlägige Korrespondenz und die Feststellungen der Europäischen Kommission, vorgelegt werden. Damit vor der endgültigen Annahme von Angemessenheitsbeschlüssen fundierte und nützliche Diskussionen geführt werden können, ist es unbedingt erforderlich, dass alle relevanten Dokumente dem EDSA rechtzeitig vorab übermittelt und ins Englische übersetzt werden. Bei komplexen Rechtsrahmen sollte auch ein Bericht über das Datenschutzniveau in dem betreffenden Drittland oder in der betreffenden internationalen Organisation beiliegen. In jedem Fall sollten die von der Europäischen Kommission bereitgestellten Informationen umfassend sein und es dem EDSA ermöglichen, die von der Kommission durchgeführte Analyse des Datenschutzniveaus in dem Drittland oder der internationalen Organisation zu bewerten.

16. Der EDSA wird zu den Feststellungen der Europäischen Kommission rechtzeitig Stellung nehmen und dabei auf etwaige Mängel des Angemessenheitsrahmens hinweisen und gegebenenfalls Empfehlungen aussprechen.

17. Nach Artikel 36 Absatz 4 der JI-Richtlinie ist die Europäische Kommission dafür verantwortlich, jegliche Entwicklungen, die die Wirkungsweise eines Angemessenheitsbeschlusses beeinträchtigen könnten, fortlaufend zu überwachen.

18. Artikel 36 Absatz 3 der JI-Richtlinie sieht eine regelmäßige Überprüfung vor, die mindestens alle vier Jahre erfolgt. Hierbei handelt es sich allerdings um einen allgemeinen Zeitrahmen, der je nach Drittland oder internationaler Organisation, für die ein Angemessenheitsbeschluss vorliegt, anzupassen ist. Je nach den besonderen Umständen des Einzelfalls kann ein kürzerer Überprüfungszyklus gerechtfertigt sein. Zudem können einzelne Vorfälle oder andere Informationen über den Rechtsrahmen des betreffenden Drittlands bzw. der betreffenden internationalen Organisation oder diesbezügliche Änderungen eine vorzeitige Überprüfung erforderlich machen. Außerdem erscheint es angebracht, bei gänzlich neuen Angemessenheitsbeschlüssen recht zeitnah eine erste Überprüfung durchzuführen und den Überprüfungszyklus dann ergebnisabhängig nach und nach anzupassen.

19. Angesichts seiner Aufgabe, gegenüber der Europäischen Kommission dazu Stellung zu nehmen, ob ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau mehr gewährleisten, ist der EDSA darauf angewiesen, rechtzeitig aussagekräftige Informationen über die von der Kommission durchgeführte Überwachung der relevanten Entwicklungen in dem betreffenden Drittland oder in der internationalen Organisation zu erhalten. Der EDSA sollte daher über alle Überprüfungsverfahren und -missionen in einem betreffenden Drittland oder bei einer internationalen Organisation informiert werden. Der EDSA empfiehlt, dass man, wie es im

in ein Drittland der Fortbestand des durch das Unionsrecht gewährten hohen Niveaus des Schutzes der Grundfreiheiten und Grundrechte gewährleistet wird. Auch wenn sich die Mittel zur Gewährleistung eines solchen Schutzniveaus von denen unterscheiden können, die in der Union herangezogen werden, um die Wahrung der Anforderungen, die sich aus dem Unionsrecht ergeben, zu gewährleisten, müssen sie sich gleichwohl in der Praxis als wirksam erweisen, um einen Schutz zu gewährleisten, der dem in der Union garantierten der Sache nach gleichwertig ist."

Beschluss zum Privacy Shield vorgesehen war und im Angemessenheitsbeschluss zu Japan vorgesehen ist, ihn zur Teilnahme an diesen Überprüfungsverfahren und -missionen einlädt.

20. Ferner sei darauf hingewiesen, dass die Europäische Kommission nach Artikel 36 Absatz 5 der JI-Richtlinie befugt ist, bestehende Angemessenheitsbeschlüsse zu widerrufen, zu ändern oder auszusetzen, wenn das Drittland oder die internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet. An dem Verfahren zur Widerrufung, Änderung oder Aussetzung ist der EDSA insofern beteiligt, als er gemäß Artikel 51 Absatz 1 Buchstabe g der JI-Richtlinie um eine Stellungnahme ersucht wird.

21. Unbeschadet der Befugnisse der Strafverfolgungsbehörden sollten die Aufsichtsbehörden außerdem befugt sein, Verstöße gegen diese Richtlinie den Justizbehörden zur Kenntnis zu bringen oder Gerichtsverfahren anzustrengen.[13] Insbesondere aus dem „Schrems-I"-Urteil des EuGH ergibt sich, dass Datenschutzbehörden die Möglichkeit haben müssen, vor den nationalen Gerichten zu klagen, wenn sie eine Eingabe einer Person gegen einen Angemessenheitsbeschluss für begründet halten.[14] Diese Einschätzung wurde durch das „Schrems-II"-Urteil bestätigt.[15]

4. EU-STANDARDS FÜR ANGEMESSENHEIT IM BEREICH DER POLIZEILICHEN ZUSAMMENARBEIT UND DER JUSTIZIELLEN ZUSAMMENARBEIT IN STRAFSACHEN

22. Inhaltlich sollte der Schwerpunkt der Angemessenheitsbeschlüsse darauf liegen, die bestehenden Rechtsvorschriften des betreffenden Drittlandes als Ganzes sowohl in der Theorie als auch in der Praxis anhand der in Artikel 36 der JI-Richtlinie festgelegten Bewertungskriterien zu beurteilen. Jedes System eines Drittlands oder einer internationalen Organisation muss die nachfolgend genannten allgemeinen, verfahrensrechtlichen und durchsetzungsbezogenen Datenschutzgrundsätze und -mechanismen vorsehen.

23. In Artikel 36 Absatz 2 der JI-Richtlinie sind die verschiedenen Elemente festgelegt, welche die Europäische Kommission bei der Beurteilung der Angemessenheit des Schutzniveaus in einem Drittland oder in einer internationalen Organisation berücksichtigen soll.

24. Dabei handelt es sich insbesondere um die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten[16], die einschlägigen Vorschriften sowie die Durchsetzung dieser Vorschriften,

[13] Siehe Artikel 47 Absatz 5 sowie Erwägungsgrund 82 der JI-Richtlinie.
[14] Siehe Schrems I, Rn. 65: „Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen."
[15] Siehe Schrems II, Rn. 120: „Auch wenn die Kommission einen Angemessenheitsbeschluss erlassen hat, muss die zuständige nationale Aufsichtsbehörde, an die sich eine Person mit einer Beschwerde bezüglich des Schutzes ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten wendet, daher in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung dieser Daten die in der DSGVO aufgestellten Anforderungen gewahrt werden, und gegebenenfalls Klage vor den nationalen Gerichten erheben können, damit diese, wenn sie die Zweifel der Aufsichtsbehörde an der Gültigkeit des Angemessenheitsbeschlusses teilen, um eine Vorabentscheidung über dessen Gültigkeit ersuchen."
[16] Bei der Bewertung des Rechtsrahmens des Drittlandes sollte die Möglichkeit berücksichtigt werden, dass die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung auf der Grundlage von aus der EU übermittelten Daten verhängt werden könnte. Sollte eine solche Strafe oder Behandlung im Recht des Drittlandes

wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden, die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen.

25. Vor diesem Hintergrund wird deutlich, dass jede sinnvolle Analyse des angemessenen Schutzniveaus die beiden folgenden Grundelemente umfassen muss: Den Inhalt der geltenden Vorschriften und die Mittel zur Sicherstellung ihrer wirksamen Umsetzung in der Praxis. Die Europäische Kommission ist dafür verantwortlich, regelmäßig zu überprüfen, ob die bestehenden Vorschriften in der Praxis wirksam sind.

26. Der Kern der allgemeinen datenschutzrechtlichen Grundsätze sowie die verfahrensrechtlichen und durchsetzungsbezogenen Anforderungen, die als Mindestanforderung für die Angemessenheit des Schutzniveaus betrachtet werden können, ergeben sich aus der Charta der Grundrechte der Europäischen Union (Charta) sowie aus der JI-Richtlinie. Allgemeine Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre im Drittland sind nicht ausreichend. Der Rechtsrahmen des Drittlands bzw. der internationalen Organisation muss vielmehr spezifische Bestimmungen beinhalten, die sich konkret auf das Recht auf Datenschutz im Bereich der Strafverfolgung beziehen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist. Diese Bestimmungen müssen durchsetzbar sein.

27. Darüber hinaus hat der EuGH in Bezug auf den Grundsatz der Verhältnismäßigkeit[17] entschieden, dass die Frage, ob eine Beschränkung des Rechts auf Privatsphäre und Datenschutz gerechtfertigt ist, beurteilt werden muss, indem einerseits **die Schwere des** mit einer solchen Beschränkung verbundenen **Eingriffs** bestimmt[18] und andererseits geprüft wird, ob die damit verfolgte, **dem Gemeinwohl dienende Zielsetzung** in angemessenem Verhältnis zur Schwere des Eingriffs steht.[19]

28. Gemäß der Rechtsprechung des EuGH muss eine gesetzliche Grundlage für Eingriffe in Grundrechte, um dem Grundsatz der Verhältnismäßigkeit zu genügen, den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen.[20] Die Ausnahmen und Beschränkungen in Bezug auf den Schutz personenbezogener Daten müssen sich auf das absolut Notwendige beschränken.[21] Um diesem Erfordernis zu genügen, muss die fragliche Regelung nicht nur klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme

vorgesehen sein, sollten im Rechtsrahmen des Drittlandes zusätzliche Garantien vorgesehen sein, mit denen sichergestellt wird, dass aus der EU übermittelte Daten nicht dazu verwendet werden, um die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken (z. B. ein internationales Abkommen, durch das die Übermittlung an Bedingungen geknüpft wird, eine Verpflichtung des Drittlandes, auf der Grundlage von aus der EU übermittelten Daten keine Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu verhängen, oder ein Moratorium für die Todesstrafe).

[17] Artikel 52 Absatz 1 der Charta.

[18] Der Gerichtshof hat u.a. Folgendes festgestellt: „Der Eingriff, der mit einer Erhebung von Daten, die es ermöglichen, den Standort eines Endgeräts zu ermitteln, in Echtzeit verbunden ist, ist besonders schwerwiegend, denn diese Daten versetzen die zuständigen nationalen Behörden in die Lage, die Ortsveränderungen der Nutzer von Mobiltelefonen präzise und permanent nachzuverfolgen“ (verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., 6. Oktober 2020, ECLI:EU:C:2020:791, Rn. 187 sowie die dort angeführte Rechtsprechung).

[19] La Quadrature du Net u. a., Rn. 131.

[20] Siehe Schrems II, Rn. 180.

[21] Schrems II, Rn 176 sowie die dort angeführte Rechtsprechung.

vorsehen, sondern auch Mindesterfordernisse aufstellen, damit die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. „Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden.“[22]

29. Der EDSA hat Empfehlungen angenommen, in denen wesentliche Garantien aufgeführt sind, die auf der Rechtsprechung des EuGH und des Europäischen Gerichtshofs für Menschenrechte (EGMR) im Bereich der Überwachung beruhen und die im Recht des Drittlandes gegeben sein müssen, wenn es darum geht, die Eingriffe solcher Überwachungsmaßnahmen des Drittlands in die Rechte betroffener Personen zu bewerten, wenn die Daten gemäß der DSGVO an dieses Drittland übermittelt werden.[23] Um zu beurteilen, ob die Bedingungen nach Artikel 36 Absatz 2 Buchstabe a der JI-Richtlinie erfüllt sind, müssen die in diesen Empfehlungen dargelegten Garantien nach Ansicht des EDSA berücksichtigt werden, wenn die Angemessenheit des von einem Drittland gebotenen Schutzniveaus im Rahmen dieser Richtlinie im Bereich der Überwachung beurteilt wird, wobei in diesem Zusammenhang weitere spezifische Bedingungen im Bereich der Überwachung zu berücksichtigen sind.

30. Mit Blick auf die Anforderung nach Artikel 36 Absatz 2 Buchstabe b der JI-Richtlinie sollte das Drittland nicht nur eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten, sondern auch Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen.[24]

31. Mit Blick auf die Anforderung nach Artikel 36 Absatz 2 Buchstabe c der JI-Richtlinie sollten neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Pflichten, die sich aus der Teilnahme des Drittlandes oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Pflichten berücksichtigt werden; insbesondere sollte der Beitritt des Drittlandes zu anderen internationalen Datenschutzübereinkommen, z. B. zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll (Übereinkommen Nr. 108[25] und seine modernisierte Fassung, Übereinkommen Nr. 108+), berücksichtigt werden. Ferner kann berücksichtigt werden, inwieweit das Drittland die Grundsätze einhält, die in einschlägigen internationalen Dokumenten wie dem praktischen Leitfaden des Europarats zum Thema Nutzung personenbezogener Daten im Polizeibereich („Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime“) niedergelegt sind.

32. Durch einen Angemessenheitsbeschluss sollte sichergestellt werden, dass das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre und Datenschutz sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz bietet; dies gilt auch für Daten während ihrer Übermittlung in dieses Drittland. Wie der

[22] Schrems II, Rn 176 sowie die dort angeführte Rechtsprechung.
[23] Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020.
[24] Erwägungsgrund 67 der JI-Richtlinie.
[25] Erwägungsgrund 68 der JI-Richtlinie.

EuGH im „Schrems-II"-Urteil betont hat, sollte das hohe Schutzniveau auch bei der Übermittlung personenbezogener Daten in ein Drittland gewährleistet sein.[26]

33. Schließlich sollte die Europäische Kommission bei der Annahme eines Angemessenheitsbeschlusses, der sich nur auf ein Gebiet oder einen bestimmten Sektor in einem Drittland bezieht, eindeutige und objektive Kriterien berücksichtigen, etwa bestimmte Verarbeitungsvorgänge oder den Anwendungsbereich anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland.[27]

A. Allgemeine Grundsätze und Garantien

a) Begriffe

34. Es sollten grundlegende Datenschutzbegriffe bestehen. Diese müssen zwar nicht mit der in der JI-Richtlinie verwendeten Terminologie identisch sein, sollten jedoch die im europäischen Datenschutzrecht verankerten Begriffe widerspiegeln und mit diesen im Einklang stehen. Die JI-Richtlinie enthält beispielsweise folgende wichtige Begriffe: „personenbezogene Daten", „Verarbeitung personenbezogener Daten", „zuständige Behörden", „Verantwortlicher", „Auftragsverarbeiter", „Empfänger", „sensible Daten", „sachliche Richtigkeit", „Profiling", „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen", „Aufsichtsbehörde" und „Pseudonymisierung".

b) Verarbeitung personenbezogener Daten auf rechtmäßige Weise und nach Treu und Glauben (Artikel 4 – Erwägungsgrund 26)

35. Nach Artikel 8 Absatz 2 der Charta sollten personenbezogene Daten unter anderem nur „für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage" verarbeitet werden.[28] Im Zusammenhang mit der Strafverfolgung ist jedoch darauf hinzuweisen, dass die zuständigen Behörden bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, natürliche Personen auffordern oder anweisen können, ihren Anordnungen nachzukommen. In einem solchen Fall sollte die Einwilligung der betroffenen Person keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen.[29]

36. Diese Rechtsgrundlage sollte klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Datenverarbeitungstätigkeiten vorsehen und Mindesterfordernisse aufstellen.[30]

---

[26] Siehe Rn. 93.
[27] Erwägungsgrund 67 der JI-Richtlinie.
[28] Siehe Schrems II, Rn. 173.
[29] In Erwägungsgrund 35 der JI-Richtlinie heißt es zudem: „Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung."
[30] Siehe Schrems II, Rn. 175 und 180, und Gutachten 1/15, Rn 139, sowie die dort angeführte Rechtsprechung.

Darüber hinaus wies der EuGH darauf hin, dass „[d]ie Regelung […] nach nationalem Recht bindend“ sein muss.[31]

37. Die Datenverarbeitung[32] sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausführt.[33] Diese Zwecke sollten im nationalen Recht vorgesehen sein.

38. Personenbezogene Daten müssen nach Treu und Glauben verarbeitet werden. Der Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben ist ein anderes Konzept als das Recht auf ein faires Verfahren im Sinne des Artikels 47 der Charta und des Artikels 6 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK).[34]

c) Der Grundsatz der Zweckbindung (Artikel 4)

39. Die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, sollten eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung dieser Daten feststehen.[35]

40. Die Daten sollten für einen bestimmten, eindeutigen und rechtmäßigen Zweck im Rahmen der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen[36], einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit innerhalb des Drittlandes, verarbeitet werden und können anschließend für einen weiteren Zweck im Rahmen der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen verwendet werden, sofern dieser Zweck nicht mit dem ursprünglichen Zweck der Verarbeitung unvereinbar ist (z. B. für parallele Vollstreckungsverfahren oder die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für derartige Zwecke) und sofern geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorhanden sind. Werden personenbezogene Daten von demselben oder einem anderen Verantwortlichen

[31] Siehe Rechtssache C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs u. a., 6. Oktober 2020, ECLI:EU:C:2020:790, Rn. 68; dabei sei darauf hingewiesen, dass der EuGH in der französischen Fassung des Urteils den Begriff „*réglementation*“ verwendet, der mehr umfasst als die vom Parlament erlassenen Gesetze.

[32] Die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

[33] Zuständige Behörden sind staatliche Stellen, die für derartige Zwecke zuständig sind, oder andere Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für derartige Zwecke übertragen wurde.

[34] Erwägungsgrund 26 der JI-Richtlinie.

[35] Erwägungsgrund 26 der JI-Richtlinie.

[36] Dazu zählen auch „polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist“ (Erwägungsgrund 12 der JI-Richtlinie). Dies ist zu unterscheiden von Zwecken der nationalen Sicherheit oder von Tätigkeiten, die in den Anwendungsbereich des Titels V Kapitel 2 des Vertrags über die Europäische Union (EUV) fallen (Erwägungsgrund 14 der JI-Richtlinie).

(zuständige Behörde[37]) für einen Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung verarbeitet, der nicht dem Zweck entspricht, für den sie erhoben wurden, so sollte diese Verarbeitung unter der Bedingung erlaubt sein, dass sie nach den geltenden Rechtsvorschriften zulässig ist und dass sie für diesen anderen Zweck erforderlich und verhältnismäßig ist.[38] Darüber hinaus sollte berücksichtigt werden, ob ein Mechanismus existiert, mit dem die zuständigen Behörden der jeweiligen Mitgliedstaaten über eine solche Weiterverarbeitung von Daten unterrichtet werden.[39] Ferner sollte in keinem Falle das durch die JI-Richtlinie unionsweit gewährleistete Schutzniveau für natürliche Personen untergraben werden, und zwar auch dann nicht, wenn aus dem Drittland personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben Drittland übermittelt werden.[40]

d) Besondere Bedingungen für die Weiterverarbeitung zu anderen Zwecken (Artikel 9)

41. Die Weiterverarbeitung oder Offenlegung von aus der EU übermittelten Daten zu anderen Zwecken als zu Strafverfolgungszwecken, z. B. zu Zwecken der nationalen Sicherheit, sollte ebenfalls gesetzlich geregelt, erforderlich und verhältnismäßig sein. Darüber hinaus sollte berücksichtigt werden, ob ein Mechanismus existiert, mit dem die zuständigen Behörden der jeweiligen Mitgliedstaaten über eine solche Weiterverarbeitung von Daten unterrichtet werden.[41] Auch in diesem Fall sollte für die Daten nach ihrer Weiterverarbeitung oder Offenlegung das gleiche Schutzniveau gelten wie bei ihrer ursprünglichen Verarbeitung durch die empfangende zuständige Behörde.

e) Der Grundsatz der Datenminimierung

42. Die Daten sollten angemessen, relevant und im Hinblick auf die Zwecke, für die sie verarbeitet werden, nicht exzessiv sein. Insbesondere sollte berücksichtigt werden, ob Anforderungen in Bezug auf den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen – etwa begrenzte Eingabefelder (strukturierte Kommunikation) oder automatisierte und nicht automatisierte Qualitätsprüfungen – gelten.

f) Der Grundsatz der sachlichen Richtigkeit der Daten

43. Die Daten sollten sachlich richtig sein und erforderlichenfalls auf dem neuesten Stand gehalten werden. Gleichwohl sollte der Grundsatz der sachlichen Richtigkeit der Daten unter Berücksichtigung von Art und Zweck der jeweiligen Verarbeitung angewandt werden. Aussagen, die personenbezogene Daten enthalten, basieren gerade in Gerichtsverfahren auf der subjektiven Wahrnehmung von natürlichen Personen und sind nicht immer nachprüfbar. Infolgedessen sollte sich der Grundsatz der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aussage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.[42]

[37] Siehe Fußnote 33.
[38] Erwägungsgrund 29 der JI-Richtlinie.
[39] Ein solcher Mechanismus könnte beispielsweise in Form von einvernehmlich vereinbarten Bearbeitungscodes, einer Mitteilungspflicht im Rahmen eines internationalen Instruments – unter anderem auch durch automatische Mitteilungen – oder anderen ähnlichen Transparenzmaßnahmen bestehen.
[40] Erwägungsgrund 64 der JI-Richtlinie.
[41] Siehe Fußnote 39.
[42] Erwägungsgrund 30 der JI-Richtlinie.

44. Es sollte dafür gesorgt werden, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden[43] und dass Verfahren zur Berichtigung oder Löschung unrichtiger Daten vorhanden sind. Insbesondere sollte berücksichtigt werden, ob ein System zur Klassifizierung der verarbeiteten Informationen im Hinblick auf die Zuverlässigkeit der Quelle und die Überprüfbarkeit der Fakten[44] besteht.

g) Der Grundsatz der Datenspeicherung

45. Die Daten sollten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Es sollten geeignete Mechanismen für die Löschung personenbezogener Daten eingerichtet werden; dabei kann ein fester Zeitraum für die Speicherung der Daten oder eine regelmäßige Überprüfung der Notwendigkeit der Speicherung vorgesehen werden (oder eine Kombination aus beidem: eine festgelegte Höchstdauer und eine regelmäßige Überprüfung in bestimmten Abständen).[45] Für personenbezogene Daten, die zum Zwecke der Archivierung im öffentlichen Interesse und der wissenschaftlichen, statistischen oder historischen Verwendung für längere Zeiträume gespeichert werden, sollten geeignete Garantien (z. B. bezüglich des Zugangs) gelten.[46]

h) Der Grundsatz der Sicherheit und der Vertraulichkeit (Artikel 29, Erwägungsgründe 28 und 71)

46. Jede Stelle, die personenbezogene Daten verarbeitet, sollte sicherstellen, dass die Daten so verarbeitet werden, dass die Sicherheit der personenbezogenen Daten gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben bzw. erhalten und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können. Hierzu zählt auch der Schutz vor unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Bei der Bestimmung des Sicherheitsniveaus sollten der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden.

47. Es sollte für sichere Kommunikationskanäle zwischen den Behörden der Mitgliedstaaten, die die personenbezogenen Daten übermitteln, und den empfangenden Behörden von Drittstaaten gesorgt werden.

i) Der Grundsatz der Transparenz (Artikel 13, Erwägungsgründe 26, 39, 42, 43, 44 und 46)

48. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.[47]

49. Ihnen sollten zudem Informationen über alle wesentlichen Elemente der Verarbeitung ihrer personenbezogenen Daten zur Verfügung gestellt werden. Diese Informationen sollten leicht zugänglich und verständlich, also in klarer und einfacher Sprache abgefasst sein. Diese Informationen sollten den Zweck der Verarbeitung, die Identität des Verantwortlichen, die Rechte

[43] Erwägungsgrund 32 der JI-Richtlinie.
[44] Beispielsweise 4x4-Gitter für Zuverlässigkeitsprüfungen und Bearbeitungscodes.
[45] Artikel 5 der JI-Richtlinie.
[46] Erwägungsgrund 26 der JI-Richtlinie.
[47] Erwägungsgrund 26 der JI-Richtlinie.

der betroffenen Person[48] und andere Informationen erhalten, die zur Sicherstellung der Verarbeitung nach Treu und Glauben erforderlich sind.

50. Es können Ausnahmen von diesem Informationsrecht bestehen. Eine solche Beschränkung sollte jedoch auf Grundlage einer gesetzgeberischen Maßnahme zulässig sein sowie erforderlich und verhältnismäßig sein, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen, soweit und solange wie diese teilweise oder vollständige Beschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird. Derartige Beschränkungen sollten zudem unter Berücksichtigung der Möglichkeit erwogen und bewertet werden, bei einer Aufsichtsbehörde Beschwerde einzureichen oder einen gerichtlichen Rechtsbehelf einzulegen. In jedem Falle sollte eine mögliche Beschränkung zeitlich begrenzt und nicht pauschal gelten und ähnlichen Bedingungen, Garantien und Beschränkungen unterliegen, wie sie nach der Charta und der EMRK in der Auslegung durch die Rechtsprechung des EuGH bzw. des EGMR erforderlich sind, und insbesondere den Wesensgehalt dieser Rechte und Freiheiten achten.

j) Das Recht auf Auskunft, Berichtigung und Löschung (Artikel 14 und 16)

51. Die betroffene Person sollte das Recht haben, eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Auskunft über ihre Daten zu erhalten. Dieses Recht sollte zumindest bestimmte Informationen über die Verarbeitung umfassen, etwa die Zwecke der Verarbeitung und deren Rechtsgrundlage, das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde oder die Kategorien personenbezogener Daten, die verarbeitet werden.[49] Dies ist besonders dann wichtig, wenn der Grundsatz der Transparenz durch allgemeine Bekanntmachung (z. B. Informationen auf der Website der Behörde) erfüllt wird.

52. Die betroffene Person sollte das Recht haben, aus bestimmten Gründen, z. B. wenn sich ihre Daten als unrichtig oder unvollständig erweisen, die Berichtigung dieser Daten zu verlangen. Die betroffene Person sollte zudem das Recht auf Löschung ihrer Daten haben, z. B. wenn deren Verarbeitung nicht mehr erforderlich oder aber unrechtmäßig ist.

53. Die Ausübung dieser Rechte sollte für die betroffene Person nicht übermäßig aufwendig sein.

k) Beschränkungen der Rechte betroffener Personen

54. Die Rechte betroffener Personen können beschränkt werden, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen, soweit und solange wie diese teilweise oder vollständige Beschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird. Werden Beschränkungen dieser Art in Erwägung gezogen oder bewertet, sollte dabei auch die Möglichkeit

[48] Sowohl die materiellen Rechte (Recht auf Auskunft, auf Berichtigung usw.) als auch das Recht auf einen Rechtsbehelf.
[49] Artikel 14 der JI-Richtlinie.

berücksichtigt werden, eine Beschwerde bei einer Aufsichtsbehörde einzureichen oder einen Rechtsbehelf einzulegen.

l) Beschränkungen bei der Weiterübermittlung von Daten (Artikel 35, Erwägungsgründe 64 und 65)

55. Bei einer Weiterübermittlung personenbezogener Daten durch den ursprünglichen Empfänger an ein anderes Drittland oder eine andere internationale Organisation darf das in der Union vorgesehene Schutzniveau für natürliche Personen, deren Daten übermittelt werden, nicht untergraben werden. Daher sollte eine Weiterübermittlung von Daten nur dann zulässig sein, wenn der Fortbestand des nach Unionsrecht gebotenen Schutzniveaus gewährleistet ist.[50] Insbesondere sollte es sich bei dem späteren Empfänger (d. h. dem Empfänger der Weiterübermittlung) um eine für Strafverfolgungszwecke zuständige Behörde[51] handeln; ferner dürfen solche Weiterübermittlungen von Daten nur für begrenzte und bestimmte Zwecke und so lange erfolgen, wie es eine Rechtsgrundlage für diese Verarbeitung gibt.

56. Darüber hinaus muss berücksichtigt werden, ob ein Mechanismus existiert, mit dem die zuständigen Behörden des jeweiligen Mitgliedstaats über eine solche Weiterübermittlung von Daten unterrichtet werden und diese genehmigen können. Der ursprüngliche Empfänger der aus der EU übermittelten Daten sollte dazu verpflichtet und in der Lage sein, nachzuweisen, dass die jeweils zuständige Behörde des Mitgliedstaats die Weiterübermittlung genehmigt hat[52] und dass geeignete Garantien für die Weiterübermittlung von Daten gegeben sind, wenn kein Angemessenheitsbeschluss für das Drittland vorliegt, in das die Daten weiterübermittelt werden sollen.[53]

m) Der Grundsatz der Rechenschaftspflicht (Artikel 4 Absatz 4)

57. Der Verantwortliche sollte für die Einhaltung der datenschutzrechtlichen Grundsätze gemäß Artikel 4 der JI-Richtlinie verantwortlich sein und deren Einhaltung nachweisen können.

[50] Siehe auch Gutachten 1/15.
[51] Siehe Fußnote 33.
[52] In diesem Zusammenhang sollte berücksichtigt werden, ob eine Pflicht oder eine Selbstverpflichtung zur Anwendung einschlägiger, von den Behörden der übertragenden Mitgliedstaaten festgelegter Bearbeitungscodes besteht.
[53] Die genannten Anforderungen gelten unbeschadet der in der JI-Richtlinie (Artikel 35 Absatz 1 Buchstaben c und e) festgelegten besonderen Bedingungen für die Weiterübermittlung an ein geeignetes Land.

B. Beispiele für zusätzliche Grundsätze für bestimmte Arten der Verarbeitung

a) Besondere Kategorien von Daten (Artikel 10 und Erwägungsgrund 37)

58. Betrifft die Verarbeitung „besondere Kategorien personenbezogener Daten“[54], sollten besondere Garantien[55] bestehen, die den damit verbundenen besonderen Risiken Rechnung tragen. Diese Kategorien sollten die in Artikel 10 der JI-Richtlinie verankerten Kategorien abbilden. Die Verarbeitung besonderer Kategorien von Daten sollte daher mit besonderen Garantien verbunden und nur dann zulässig sein, wenn sie unter bestimmten Bedingungen, beispielsweise zur Wahrung lebenswichtiger Interessen einer Person, unbedingt erforderlich ist.

b) Automatisierte Entscheidungen und Profiling (Artikel 11 und Erwägungsgrund 38)

59. Entscheidungen, die allein auf der Grundlage der automatisierten Verarbeitung (automatisierte Entscheidungen im Einzelfall) einschließlich Profiling beruhen, die eine nachteilige rechtliche Wirkung für die betroffene Person entfalten oder sie erheblich beeinträchtigen, sollten nur unter bestimmten Bedingungen ergehen, die im Rechtsrahmen des Drittlands festzulegen sind.[56]

60. Im Rechtsrahmen der Europäischen Union umfassen diese Bedingungen beispielsweise die spezifische Unterrichtung der betroffenen Person und das Recht auf persönliches Eingreifen vonseiten des Verantwortlichen, insbesondere das Recht auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder auf Anfechtung der Entscheidung.

61. Im Recht des Drittlandes sollten in jedem Fall die erforderlichen Garantien für die Rechte und Freiheiten der betroffenen Person vorgesehen sein. In dieser Hinsicht sollte zudem berücksichtigt werden, ob ein Mechanismus existiert, mit dem die zuständigen Behörden des jeweiligen Mitgliedstaats über jede Weiterverarbeitung der übermittelten Daten – beispielsweise für ein umfangreiches Profiling – unterrichtet werden können.

c) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Artikel 20)

62. Bei der Beurteilung der Angemessenheit sollte darauf geachtet werden, ob die Verantwortlichen verpflichtet sind, interne Richtlinien festzulegen und Maßnahmen zu ergreifen, die den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Genüge tun, und ob sie verpflichtet sind, – unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung – angemessene technische und organisatorische Maßnahmen (z. B. Pseudonymisierung) zu treffen, die dafür ausgelegt sind, Datenschutzgrundsätze wie die Datenminimierung wirksam umzusetzen und die notwendigen Garantien in den Verarbeitungsprozess zu integrieren.

---

[54] Diese besonderen Kategorien von Daten werden in Erwägungsgrund 37 der JI-Richtlinie auch als „sensible Daten“ bezeichnet.
[55] Beispiele für derartige zusätzliche Garantien sind spezifische Sicherheitsmaßnahmen, eingeschränkte Auskunftsrechte von Mitarbeitern und Beschränkungen in Bezug auf Weiterverarbeitung, automatisierte Entscheidungen, Weitergabe oder Weiterübermittlung.
[56] Gutachten 1/15, Rn. 173.

C. Verfahrens- und Durchsetzungsmechanismen

63. Die Mittel, auf die ein Drittland zur Sicherstellung eines angemessenen Schutzniveaus zurückgreifen kann, dürfen durchaus von den Mitteln der Europäischen Union abweichen[57]. Jedoch muss jedes System, das im Einklang mit dem europäischen System steht, folgende Elemente aufweisen:

a) Zuständige unabhängige Aufsichtsbehörde (Artikel 36 Absatz 2 Buchstabe b und Artikel 36 Absatz 3 sowie Erwägungsgrund 67)

64. Es sollte eine oder mehrere unabhängige Aufsichtsbehörden geben, die mit der Sicherstellung und Durchsetzung der Einhaltung von Bestimmungen über den Datenschutz und den Schutz der Privatsphäre im Drittland beauftragt sind. Diese Aufsichtsbehörde muss bei der Erfüllung ihrer Pflichten und bei der Ausübung ihrer Befugnisse völlig unabhängig handeln und darf dabei weder Anweisungen einholen noch entgegennehmen. In diesem Zusammenhang sollte die Aufsichtsbehörde über alle geeigneten Durchsetzungsbefugnisse verfügen, die es ihr ermöglichen, die Einhaltung der Datenschutzrechte wirksam sicherzustellen und das Bewusstsein für diese Rechte zu fördern. Auch der Personal- und Haushaltsausstattung der Aufsichtsbehörde sollte Rechnung getragen werden. Ferner sollte die Aufsichtsbehörde befugt sein, von sich aus eigene Untersuchungen durchzuführen. Auch sollte sie die Aufgabe haben, die betroffenen Personen bei der Ausübung ihrer Rechte zu unterstützen und zu beraten (siehe auch den nachstehenden Buchstaben c). In den Angemessenheitsbeschlüssen sollte(n) diese Aufsichtsbehörde(n) und die zur Durchsetzung der Datenschutzvorschriften bestehenden Mechanismen der Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten gegebenenfalls genannt werden.

b) Wirksame Umsetzung von Datenschutzvorschriften

65. Im Rahmen des Systems eines Drittlands sollte sichergestellt sein, dass die Verantwortlichen und diejenigen, die in ihrem Auftrag personenbezogene Daten verarbeiten, umfassend über ihre Pflichten, Aufgaben und Verantwortlichkeiten informiert sind und dass die betroffenen Personen umfassend über ihre Rechte und über die Mittel zu deren Ausübung aufgeklärt werden. Das Vorhandensein wirksamer und abschreckender Sanktionen kann ebenso eine wichtige Rolle für die Vorschrifteneinhaltung spielen wie systematische unmittelbare Überprüfungen durch Behörden, Prüfer oder unabhängige Datenschutzbeauftragte.

66. Der Datenschutzrahmen eines Drittlands sollte die Verantwortlichen oder diejenigen, die in ihrem Auftrag personenbezogene Daten verarbeiten, dazu verpflichten, diesen einzuhalten und gegenüber der zuständigen Aufsichtsbehörde den Nachweis seiner Einhaltung erbringen zu können. Solche Maßnahmen sollten das Führen von Aufzeichnungen oder Protokolldateien der Datenverarbeitungstätigkeiten für einen angemessenen Zeitraum einschließen. Darüber hinaus können sie beispielsweise Datenschutz-Folgenabschätzungen, die Benennung eines Datenschutzbeauftragten oder Maßnahmen zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen umfassen.

c) Das Datenschutzsystem muss die Ausübung der Rechte der betroffenen Person erleichtern (Artikel 12, 17 und 46 der JI-Richtlinie)

[57] Schrems I, Rn. 74.

67. Der Datenschutzrahmen eines Drittlandes sollte die Verantwortlichen dazu verpflichten, die Ausübung der in Abschnitt A Buchstabe j genannten Rechte der betroffenen Person zu erleichtern, und vorsehen, dass die Aufsichtsbehörde des Drittlandes auf Antrag jeder betroffenen Person Informationen über die Ausübung ihrer Rechte[58] zur Verfügung stellt.

d) Das Datenschutzsystem muss geeignete Rechtsbehelfsmechanismen umfassen

68. Es gibt zwar (noch) keine Rechtsprechung in Bezug auf die Angemessenheit eines Rechtssystems eines Drittlandes gemäß der JI-Richtlinie, aber der EuGH hat bereits das in Artikel 47 der Charta verankerte Grundrecht auf wirksamen gerichtlichen Rechtsschutz ausgelegt. Nach Artikel 47 Absatz 1 der Charta hat jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht auf einen wirksamen Rechtsbehelf bei einem Gericht[59] nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen.

69. Nach ständiger Rechtsprechung des EuGH ist es dem Wesen eines Rechtsstaats inhärent, dass eine wirksame, zur Gewährleistung der Einhaltung des Unionsrechts dienende gerichtliche Kontrolle vorhanden sein muss. Somit verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.[60]

70. Die betroffene Person sollte in der Lage sein, zur Durchsetzung ihrer Rechte sowie zur Sicherstellung der Einhaltung der Vorschriften schnell und wirksam sowie ohne prohibitive Kosten Rechtsbehelfe in Anspruch zu nehmen.

71. Dazu sind Überwachungsmechanismen erforderlich, die eine unabhängige Untersuchung von Beschwerden ermöglichen und dafür sorgen, dass Verletzungen des Rechts auf Datenschutz und auf die Achtung der Privatsphäre in der Praxis identifiziert und bestraft werden.

72. Bei etwaigen Verstößen gegen die geltenden Vorschriften sollten der betroffenen Person, deren personenbezogene Daten in das Drittland übermittelt werden, auch in dem Drittland wirksame administrative und gerichtliche Abhilfen zur Verfügung stehen, einschließlich zur Forderung von Schadensersatz wegen unrechtmäßiger Verarbeitung ihrer personenbezogenen Daten. Hierbei handelt es sich um einen zentralen Aspekt, der die Existenz eines Systems unabhängiger Rechtsprechung oder Schlichtung beinhalten muss, welches die Zahlung von Schadensersatz oder die Verhängung von Sanktionen ermöglicht.

[58] Die Ausübung der Rechte der betroffenen Person kann entweder direkt oder indirekt erfolgen.
[59] Der EuGH ist der Auffassung, dass ein wirksamer gerichtlicher Rechtsschutz nicht nur durch ein Gericht, sondern auch durch ein Organ gewährleistet werden kann, das Garantien bietet, die den nach Artikel 47 der Charta erforderlichen Garantien der Sache nach gleichwertig sind (siehe Schrems II, Rn. 197). Dies könnte insbesondere für internationale Organisationen relevant sein.
[60] Schrems II, Rn 187 und 194 sowie die dort angeführte Rechtsprechung.