Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen

Angenommen am 10. November 2020

[Vollmer: Es geht hier wohl über Überwachungsmaßnahmen von ausländischen Regierungen... und nicht um die Überwachung von Website-Nutzern.]

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[1] (im Folgenden: DSGVO),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und das Protokoll 37 in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,[2]

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

gestützt auf die Arbeitsunterlage 01/2016 über die Rechtfertigung von Eingriffen in die Grundrechte auf Schutz der Privatsphäre und Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (wesentliche europäische Garantien), WP 237 der Artikel-29-Datenschutzgruppe

HAT FOLGENDE EMPFEHLUNG ANGENOMMEN:

1. EINLEITUNG

1. In Reaktion auf das Schrems I-Urteil haben die in der Artikel-29-Datenschutzgruppe versammelten Datenschutzbehörden auf Grundlage der Rechtsprechung die wesentlichen europäischen Garantien aufgestellt, die einzuhalten sind, um sicherzustellen, dass Eingriffe in die Grundrechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten, die im Zuge von Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten erfolgen, nicht über das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß hinausgehen.

2. Der Europäische Datenschutzausschuss (im Folgenden: EDSA) möchte hervorheben, dass die wesentlichen europäischen Garantien auf der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden: EuGH) zu den Artikeln 7, 8, 47 und 52 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) bzw. auf der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (im Folgenden: EGMR) zu Artikel 8 der Europäischen Menschenrechtskonvention (im Folgenden: EMRK), die sich mit Überwachungsfragen in Vertragsstaaten der EMRK befasst, beruhen.[3]

[1] Dieses Dokument befasst sich nicht mit der Situation bei Übermittlungen oder Weiterleitung im Sinne der JI-Richtlinie (Richtlinie (EU) 2016/680)

[2] Soweit in diesem Dokument auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

[3] Der in diesen Empfehlungen verwendete Begriff „Grundrechte“ leitet sich aus der Charta der Grundrechte der Europäischen Union ab. Er umfasst jedoch auch die „Menschenrechte“ im Sinne der Europäischen Menschenrechtskonvention.

3. Mit der Aktualisierung dieses Dokuments ist beabsichtigt, die ursprünglich in Reaktion auf das Schrems I-Urteil[4] aufgestellten wesentlichen europäischen Garantien im Lichte der Klarstellungen weiterzuentwickeln, die nach dessen Erstveröffentlichung vom EuGH, insbesondere in dessen Grundsatzurteil in der Rechtssache Schrems II[5], sowie vom EMRK gegeben wurden.

4. In seinem Schrems II-Urteil hat der EuGH entschieden, dass die Prüfung des Beschlusses 2010/87/EU der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern anhand der Artikel 7, 8 und 47 der Charta nichts ergeben hat, was dessen Gültigkeit berühren könnte, der Durchführungsbeschluss zum EU-US-Datenschutzschild (im Folgenden: DSS-Beschluss) wurde jedoch für ungültig befunden. Der EuGH befand, dass der DSS-Beschluss den Anforderungen nach Artikel 45 Absatz 1 DSGVO im Lichte der Artikel 7, 8 und 47 der Charta nicht genügt. Das Urteil kann somit als Beispiel für Überwachungsmaßnahmen in einem Drittland (hier die USA und Section 702 FISA und Executive Order 12 333) dienen, die weder hinreichend beschränkt sind noch den betroffenen Personen wirksamen Rechtsschutz zur Durchsetzung ihrer Rechte bieten, so wie es nach dem Unionsrecht erforderlich ist, um das Schutzniveau in einem Drittland dem in der Europäischen Union garantierten Niveau für „der Sache nach gleichwertig" im Sinne von Artikel 45 Absatz 1 DSGVO befinden zu können.

5. Die Gründe für die Ungültigkeit des Datenschutzschildes haben auch Auswirkungen auf andere Übermittlungsinstrumente[6]. Auch wenn der Gerichtshof Artikel 46 Absatz 1 DSGVO lediglich im Zusammenhang mit der Gültigkeit von Standardvertragsklauseln (im Folgenden: SVK) ausgelegt hat, ist diese Auslegung doch auf jede Übermittlung in Drittländer anwendbar, die auf eines der in Artikel 46 DSGVO genannten Instrumente gestützt ist[7].

6. Letztendlich ist die Entscheidung, ob ein Grundrechtseingriff gerechtfertigt ist, Sache des EuGH. Solange jedoch kein Urteil ergangen ist, sind die Datenschutzbehörden nach ständiger Rechtsprechung gehalten, von Amts wegen oder auf eine Beschwerde hin eine Einzelfallbeurteilung vorzunehmen und die Sache, wenn ein Angemessenheitsbeschluss vorliegt, an ein nationales Gericht zu verweisen, falls sie vermuten, dass die Übermittlung nicht Artikel 45 genügt, oder die Übermittlung aussetzen oder verbieten, falls sie feststellen, dass Artikel 46 DSGVO nicht eingehalten werden kann und der nach Unionsrecht erforderliche Schutz der übermittelten Daten sich nicht auf andere Weise sicherstellen lässt.

7. Die aktualisierte Fassung der wesentlichen europäischen Garantien soll Kriterien für die Prüfung angeben, ob Überwachungsmaßnahmen, die den Behörden (sei es nationalen Sicherheitsbehörden oder Strafverfolgungsbehörden) den Zugriff auf personenbezogene Daten gestatten, als gerechtfertigter Eingriff angesehen werden können oder nicht.

8. Dabei bilden die wesentlichen europäischen Garantien einen Teil der Bewertung, die für die Feststellung, ob im Drittland ein Schutzniveau besteht, das dem in der Union garantierten der Sache nach gleichwertig ist, vorzunehmen ist; sie sind allerdings nicht als vollständige Festlegung sämtlicher

[4] Urteil des EuGH vom 6. Oktober 2015, Schrems (C-362/14, EU:C:2015:650, im Folgenden: Schrems I).

[5] Urteil des EuGH vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18, ECLI:EU:C:2020:559, im Folgenden: Schrems II).

[6] Vgl. Schrems II, Rn. 105.

[7] Vgl. Schrems II, Rn. 92.

Kriterien gedacht, die bei der Prüfung, ob ein Drittland ein solches Schutzniveau im Sinne von Artikel 45 DSGVO bietet, zu berücksichtigen sind. Genauso wenig ist beabsichtigt, dass sie für sich genommen sämtliche Kriterien festlegen, die für die Bewertung erforderlich sind, ob die Rechtsordnung des Drittlands Datenexporteure und Datenimporteure daran hindert, geeignete Garantien im Sinne von Artikel 46 DSGVO vorzusehen.

9. Die in diesem Dokument genannten Kriterien sind daher als die wesentlichen Garantien anzusehen, die im Drittland gegeben sein müssen, auf die bei der Prüfung des mit den Überwachungsmaßnahmen des Drittlands verbundenen Eingriffs in die Rechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten abzustellen ist – nicht jedoch als eine Liste von Kriterien, die zeigen, dass die Rechtsordnung des Drittlands im Ganzen ein im Wesentlichen gleichwertiges Schutzniveau bietet.

10. In Artikel 6 Absatz 3 des Vertrags über die Europäische Union ist niedergelegt, dass die Grundrechte, wie sie in der EMRK gewährleistet sind, als allgemeine Grundsätze Teil des Unionsrechts sind. In seiner Rechtsprechung erinnert der EuGH allerdings daran, dass die EMRK, solange die Union ihr nicht beigetreten ist, kein formell in die Unionsrechtsordnung übernommenes Rechtsinstrument darstellt.[8] Das nach Artikel 46 Absatz 1 DSGVO erforderliche Grundrechtsschutzniveau muss daher auf Grundlage der Bestimmungen der genannten Verordnung ermittelt werden, die im Lichte der in der Charta verankerten Grundrechte zu lesen sind. Nach Artikel 52 Absatz 3 der Charta soll jedoch den in der Charta enthaltenen Rechten, die den durch die EMRK garantierten Rechten entsprechen, dieselbe Bedeutung und derselbe Anwendungsbereich wie den in der Konvention niedergelegten Rechten zukommen, weshalb, woran der EuGH erinnert hat, die Rechtsprechung des EGMR zu den auch in der Charta der Grundrechte der Europäischen Union vorgesehenen Rechten als Mindestschutzstandard für die Auslegung der entsprechenden Rechte in der Charta zu berücksichtigen ist[9]. Dabei gilt allerdings gemäß Artikel 52 Absatz 3 Satz 2 der Charta, dass „[d]iese Bestimmung […] dem nicht [entgegensteht], dass das Recht der Union einen weiter gehenden Schutz gewährt."

11. Der substanzielle Gehalt der wesentlichen Garantien wird daher weiterhin zum Teil auf der Rechtsprechung des EGMR beruhen, soweit nicht die Charta in ihrer vom EuGH vorgenommenen Auslegung ein höheres Schutzniveau bietet, das andere Anforderungen als die nach der Rechtsprechung des EGMR vorschreibt.

12. In diesem Dokument werden der Hintergrund und die näheren Einzelheiten der vier wesentlichen europäischen Garantien erklärt.

2. GRUNDRECHTSEINGRIFFE

13. Die Grundrechte auf Achtung des Privat- und Familienlebens (einschließlich der Kommunikation) sowie auf den Schutz personenbezogener Daten sind in den Artikeln 7 und 8 der Charta festgelegt und gelten für jeden. Des Weiteren sind in Artikel 8 nicht nur die Anforderungen an eine rechtmäßige Verarbeitung personenbezogener Daten und die Anerkennung des Rechts auf Auskunft und

[8] Vgl. Schrems II, Rn. 98.

[9] Vgl. Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791) (im Folgenden: La Quadrature du Net u. a.), Rn. 124.

Berichtigung geregelt, sondern auch die Überwachung der Einhaltung dieser Vorschriften durch eine unabhängige Stelle.

14. „Folglich stellt die Übermittlung personenbezogener Daten aus einem Mitgliedstaat in ein Drittland als solche eine Verarbeitung personenbezogener Daten […] dar“[10]. Da die Artikel 7 und 8 der Charta auf diesen spezifischen Vorgang Anwendung finden und ihr Schutz sich auf die übermittelten Daten erstreckt, muss für betroffene Personen, deren personenbezogene Daten in ein Drittland übermittelt werden, ein Schutzniveau gewährleistet sein, das dem in der Europäischen Union garantierten Schutzniveau der Sache nach gleichwertig ist.[11]

15. Nach der Rechtsprechung des EuGH ist, wenn die Verarbeitung personenbezogener Daten einer natürlichen Person das in Artikel 7 der Charta verankerte Grundrecht auf Achtung des Privatlebens berührt, das Recht auf Schutz personenbezogener Daten ebenfalls berührt, da eine solche Verarbeitung im Anwendungsbereich von Artikel 8 der Charta liegt und deshalb zwangsläufig die dort vorgesehenen Erfordernisse des Schutzes personenbezogener Daten erfüllen muss.[12]

16. Die den Anbietern elektronischer Kommunikationsdienste auferlegte Pflicht, Verkehrsdaten zu speichern, um sie erforderlichenfalls den zuständigen nationalen Behörden zur Verfügung zu stellen, greift möglicherweise in unionsrechtliche Grundrechte ein, was Fragen hinsichtlich der Vereinbarkeit mit den Artikeln 7 und 8 der Charta aufwirft.[13.] Dasselbe gilt für andere Arten der Datenverarbeitung, etwa die Datenübermittlung an andere Personen als die Nutzer oder den Zugriff auf solche Daten im Hinblick auf ihre Nutzung[14], welche somit mit einem Eingriff in die betreffenden Grundrechte verbunden sind. Nach ständiger Rechtsprechung stellt der Zugang von Behörden zu den Daten zudem einen zusätzlichen Eingriff in dieses Grundrecht dar[15].

17. Dabei kommt es für die Feststellung eines Eingriffs „nicht darauf [an], ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten“[16]. Der EuGH hat auch hervorgehoben, dass unerheblich ist, ob die gespeicherten Daten später verwendet werden oder nicht.[17]

18. Die in den Artikeln 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden.[18]

[10] EuGH, Schrems II, Rn. 83.
[11] EuGH, Schrems II, Rn. 96.
[12] EuGH, Schrems II, Rn. 170-171.
[13] EuGH, Urteil vom 6. Oktober 2020, Privacy International (C-623/17, ECLI:EU:C:2020:790) (im Folgenden: Privacy International), Rn. 60.
[14] EuGH, Privacy International, Rn. 61.
[15] EGMR, 26. März 1987, Leander (9248/81), Rn. 48; EGMR, 4. Mai 2000 Rotaru (28341/95), Rn. 46; EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a. (C-293/12, ECLI:EU:C:2014:238), Rn. 35.
[16]EuGH, Schrems II, Rn. 171 sowie die dort angeführte Rechtsprechung.
[17]EuGH, Schrems II, Rn. 171 sowie die dort angeführte Rechtsprechung.
[18] EuGH, Privacy International, Rn. 63.

19. Die Charta sieht zur Begrenzung von Einschränkungen der durch sie geschützten Rechte eine Erforderlichkeits- und Angemessenheitsprüfung vor. In Artikel 52 Absatz 1 der Charta ist der Umfang möglicher Einschränkungen der Artikel 7 und 8 wie folgt festgelegt: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen."

20. Der EuGH hat erneut darauf hingewiesen, dass „eine Unionsregelung, die einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte enthält, nach ständiger Rechtsprechung des Gerichtshofs klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken […] ermöglichen", was umso bedeutsamer ist, „wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht".[19]

21. Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt nach ständiger Rechtsprechung des EuGH, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen „auf das absolut Notwendige beschränken müssen". Des Weiteren muss die dem Gemeinwohl dienende Zielsetzung mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden, indem einerseits das Ziel und andererseits die Rechte „angemessen abgewogen" werden.[20]

22. Folglich dürfen Zugriff, Speicherung und weitere Verwendung personenbezogener Daten, soweit diese im Rahmen von Überwachungsmaßnahmen staatlicher Stellen erfolgen, nicht über die Grenzen dessen hinausgehen, was im Lichte der Charta absolut notwendig ist, da sie sonst nicht als in einer demokratischen Gesellschaft gerechtfertigter Eingriff in die Grundrechte angesehen werden können.[21]

23. Die vier wesentlichen europäischen Garantien, die im nächsten Kapitel näher erläutert werden, sollen weitere Orientierung geben für die bei der Übermittlung personenbezogener Daten vorzunehmende Prüfung von Eingriffen in die Grundrechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten im Zusammenhang mit Überwachungsmaßnahmen staatlicher Stellen in einem Drittland, insbesondere dazu, nach welchen rechtlichen Anforderungen zu beurteilen ist, ob derartige Eingriffe nach der Charta zulässig sind oder nicht.

3. DIE WESENTLICHEN EUROPÄISCHEN GARANTIEN

24. Aus der Rechtsprechung ergibt sich nach Auffassung des EDSA, dass sich die einschlägigen rechtlichen Voraussetzungen, unter denen Einschränkungen der in der Charta anerkannten Rechte auf Schutz personenbezogener Daten und Schutz der Privatsphäre gerechtfertigt sein können, in den folgenden vier wesentlichen europäischen Garantien zusammenfassen lassen:

[19] EuGH, Privacy International, Rn. 68 sowie die dort angeführte Rechtsprechung.
[20] EuGH, Privacy International, Rn. 68 sowie die dort angeführte Rechtsprechung.
[21] EuGH, Privacy International, Rn. 81.

A. Auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung
B. Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele
C. Vorhandensein eines unabhängigen Aufsichtsmechanismus
D. Vorhandensein wirksamer Rechtsbehelfe für den Bürger

25. Die Garantien beruhen auf den für alle, unabhängig von ihrer Staatsangehörigkeit, geltenden Grundrechten auf Schutz der Privatsphäre und Schutz personenbezogener Daten.

Garantie A – Auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung

26. Nach Artikel 8 Absatz 2 der Charta dürfen personenbezogene Daten, wie der EuGH im Schrems II-Urteil ausgeführt hat, unter anderem „für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“[22]. Nach Artikel 52 Absatz 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten innerhalb der Union gesetzlich vorgesehen sein. Ein Eingriff ist also nur gerechtfertigt, wenn er mit dem Gesetz im Einklang steht.

27. Die gesetzliche Grundlage muss klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen.[23] Darüber hinaus ist nach der Rechtsprechung des EuGH erforderlich, dass die gesetzliche Grundlage nach dem inländischen Recht rechtsverbindlich ist[24]. Diesbezüglich hat der EuGH klargestellt, dass bei der Beurteilung des Rechts des Drittlands darauf abzustellen ist, ob betroffene Personen das Recht gerichtlich geltend machen und durchsetzen können[25]. Der EuGH verlangt also, dass die den betroffenen Personen verliehenen Rechte gerichtlich durchsetzbar sein müssen; werden den betroffenen Personen keine gegen die Behörden durchsetzbaren Rechte verliehen, kann das Schutzniveau nicht als dem aus der Charta resultierenden Niveau der Sache nach gleichwertig angesehen werden, sodass die Anforderungen von Artikel 45 Absatz 2 Buchstabe a der DSGVO nicht erfüllt sind.[26]

28. Des Weiteren hat der EuGH betont, dass das einschlägige Gesetz Angaben dazu enthalten muss, unter welchen Umständen und unter welchen Bedingungen eine Maßnahme beschlossen werden darf, die die Verarbeitung derartiger Daten regelt[27] (zum Verhältnis zwischen diesen Anforderungen und den Grundsätzen der Erforderlichkeit und Angemessenheit wird auf nachstehende Garantie B verwiesen).

[22] Vgl. Schrems II, Rn. 173.

[23] Vgl. Schrems II, Rn. 175 und 180, sowie Gutachten 1/15 vom 26. Juli 2017 zum PNR-Abkommen zwischen Kanada und der Europäischen Union (ECLI:EU:C:2017:592), Rn. 139, und die dort angeführte Rechtsprechung.

[24] Vgl. Privacy International Rn. 68. Dabei ist auch klarzustellen, dass der EuGH in der französischen Fassung des Urteils das Wort „réglementation“ verwendet, dessen Bedeutung über Parlamentsgesetze hinausgeht.

[25] Vgl. Schrems II, Rn. 181, wo der EuGH auf die US Presidential Policy Directive 28 (PPD-28) eingeht.

[26] Vgl. Schrems II, Rn. 181.

[27] Vgl. Privacy International Rn. 68 in Bezug auf das mitgliedstaatliche Recht.

29. Des Weiteren hat der EuGH ausgeführt, „dass das Erfordernis einer gesetzlichen Grundlage für jede Einschränkung der Ausübung der Grundrechte bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang der Einschränkung der Ausübung des betreffenden Rechts selbst festlegen muss“[28].

30. Und schließlich gibt es nach Auffassung des Europäischen Gerichtshofs für Menschenrechte „keinen Grund, auf die Zugänglichkeit und Klarheit der Vorschriften für die Überwachung der Kommunikation Einzelner einerseits und für allgemeinere Überwachungsprogramme andererseits unterschiedliche Grundsätze anzuwenden“[29]. Der EGMR hat auch klargestellt, dass in der gesetzlichen Regelung mindestens eine Definition der Personengruppen, die überwacht werden können, der zeitlichen Begrenzung der Maßnahme, des Verfahrens für die Auswertung, Verwendung und Speicherung der gewonnenen Daten sowie der bei der Übermittlung der Daten an andere Parteien zu treffenden Vorsichtsmaßnahmen enthalten sein sollte[30].

31. Außerdem muss der Eingriff hinsichtlich seiner Auswirkungen auf den Bürger vorhersehbar sein, um diesem angemessenen und wirksamen Schutz vor willkürlichen Eingriffen und vor Missbrauchsrisiken zu bieten. Die Datenverarbeitung muss deshalb auf einer präzisen, aber auch klaren und zugänglichen (d. h. öffentlichen) Rechtsgrundlage erfolgen[31]. Der EGMR hat zu dieser Frage in der Rechtssache Zakharov daran erinnert, dass „Vorhersehbarkeit“ im Zusammenhang mit der Überwachung des Kommunikationsverkehrs nicht dasselbe sein kann wie in vielen anderen Bereichen. Gerade im Falle geheimer Überwachungsmaßnahmen wie der Überwachung des Kommunikationsverkehrs kann Vorhersehbarkeit nicht bedeuten, dass der Bürger vorhersehen können sollte, wann die Behörden wahrscheinlich Maßnahmen zur Überwachung seiner Kommunikation treffen werden, sodass er sein Verhalten entsprechend anpassen kann. Da jedoch unter solchen Umständen die Gefahr von Willkür offensichtlich ist, sind klare, ausführliche Vorschriften für das Abhören von Telefongesprächen unerlässlich, insbesondere da sich die hierfür zur Verfügung stehende Technologie ständig weiterentwickelt. Das inländische Recht muss hinreichend klar formuliert sein, damit die Bürger angemessenen Hinweis darauf haben, unter welchen Umständen und Voraussetzungen die Behörden zu derartigen Maßnahmen befugt sind.[32]

Garantie B – Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele

32. Nach Artikel 52 Absatz 1 Satz 1 der Charta muss jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten den Wesensgehalt dieser Rechte und Freiheiten achten. Nach Artikel 52 Absatz 1 Satz 2 der Charta dürfen Einschränkungen dieser Rechte und Freiheiten unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.[33]

---

[28] Vgl. Schrems II, Rn. 175 und die dort angeführte Rechtsprechung, sowie Privacy International, Rn. 65.

[29] EGMR, 1. Juli 2008, Liberty (58243/00), Rn. 63.

[30] EGMR, 29. Juni 2006, Weber und Saravia (54934/00), Rn. 95.

[31] EGMR, 2. August 1984, Malone (8691/79), Rn. 65, 66.

[32] EGMR, 4. Dezember 2015, Zakharov (47143/06) (im Folgenden: Zakharov), Rn. 229.

[33] EuGH, Schrems II, Rn. 174.

33. Hinsichtlich des **Grundsatzes der Verhältnismäßigkeit** hat der EuGH in Bezug auf mitgliedstaatliche Gesetze entschieden, dass für die Frage, ob eine Einschränkung der Rechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten gerechtfertigt sein könnte, einerseits auf die **Schwere des Eingriffs**, der mit der betreffenden Einschränkung verbunden ist,[34] abzustellen ist und andererseits zu überprüfen ist, dass die **Bedeutung des Ziels des allgemeinen öffentlichen Interesses**, das mit der Einschränkung verfolgt wird, dieser Schwere angemessen ist.[35]

34. In der Rechtssache La Quadrature du Net u. a. hat der EuGH – in Bezug auf das Recht eines Mitgliedstaats, nicht eines Drittlands – entschieden, dass das Ziel des Schutzes der nationalen Sicherheit wegen seiner hohen Bedeutung Maßnahmen rechtfertigen kann, die mit Grundrechtseingriffen verbunden sind, die schwerer sind als diejenigen, die im Hinblick auf andere Ziele, etwa die Bekämpfung von Straftaten, gerechtfertigt sein mögen. Allerdings hat er ausgeführt, dass dies nur dann der Fall ist, wenn es ausreichend triftige Gründe dafür gibt, dass der betreffende Staat einer ernsthaften Gefährdung der nationalen Sicherheit ausgesetzt ist, die nachweislich echt sowie gegenwärtig oder vorhersehbar ist, und außerdem die weiteren in Artikel 52 Absatz 1 der Charta aufgeführten Anforderungen erfüllt sind.[36]

35. Diesbezüglich gilt nach ständiger Rechtsprechung des EuGH, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen[37]. Diese Anforderung ist nur erfüllt, wenn das betreffende Gesetz nicht nur klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsieht, sondern auch Mindesterfordernisse aufstellt, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. „[Die Regelung] 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."[38]

---

[34] In diesem Zusammenhang hat der EuGH z. B. ausgeführt, dass der Eingriff, der sich daraus ergibt, dass in Echtzeit Daten erfasst werden, anhand derer feststellbar ist, wo sich das Endgerät befindet, besonders schwer ist, da diese Daten den zuständigen nationalen Behörden ermöglichen, die Bewegungen der Benutzer von Mobiltelefonen genau und dauerhaft zu verfolgen. (La Quadrature du Net u. a., Rn. 187 und die dort angeführte Rechtsprechung).

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

[36] La Quadrature du Net u. a., Rn. 136 und 137. Vgl. auch Privacy International, wo der EuGH ausgeführt hat, dass derartige Gefährdungen nach ihrer Art und besonderen Schwere von der allgemeinen Gefahr abzugrenzen sind, dass es zu die öffentliche Sicherheit beeinträchtigenden Spannungen oder Unruhen, selbst solchen schwerer Art, kommt. Rn. 75. So hat z. B. der EuGH in der Rechtssache La Quadrature du Net u. a. festgestellt, dass die automatische Analyse von Verkehrs- und Standortdaten, die allgemein und unterschiedslos die Daten elektronische Kommunikationssysteme benutzender Personen erfassen einen besonders schweren Eingriff darstellen, weshalb eine solche Maßnahme der Anforderung der Verhältnismäßigkeit nur dann genügen kann, wenn der betroffene Mitgliedstaat einer ernsthaften Gefährdung der nationalen Sicherheit ausgesetzt ist, die nachweislich echt sowie gegenwärtig oder vorhersehbar ist, und wenn unter anderem die Dauer der Speicherung auf das absolut Notwendige beschränkt ist (Rn. 174-177).

[37] EuGH, Schrems II, Rn. 176 und die dort angeführte Rechtsprechung.

[38] EuGH, Schrems II, Rn. 175.

36. Im Schrems II-Urteil hat der EuGH hervorgehoben, dass die gesetzliche Grundlage eines Drittlands, die keine Einschränkungen für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung vorsieht, nicht geeignet ist, ein Schutzniveau zu gewährleisten, das dem durch die Charta garantierten Niveau der Sache nach gleichwertig ist. Nach der Rechtsprechung 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.[39]

37. Was den **Grundsatz der Erforderlichkeit** angeht, hat der EuGH festgestellt, dass eine Regelung, „die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union […] übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen“, dem Grundsatz der Erforderlichkeit nicht genügt[40]. Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Artikel 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.[41]

38. Entsprechend hat der EuGH in seiner Entscheidung in der Sache La Quadrature du Net u. a., allerdings bezüglich der gesetzlichen Regelung eines Mitgliedstaats, nicht eines Drittlands, entschieden, dass Gesetze, die die Aufbewahrung personenbezogener Daten vorschreiben, stets objektiven Kriterien genügen müssen, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen[42]. Im selben Kontext hat der EuGH in der Rechtssache Privacy International auch entschieden, dass sich der Gesetzgeber bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den Daten von Teilnehmern oder registrierten Nutzern zu gewähren ist, auf objektive Kriterien stützen muss[43].

---

[39] EuGH, Schrems II, Rn. 180.

[40] EuGH, Schrems I, Rn. 93 mit weiteren Hinweisen. Vgl. jedoch in diesem Fall bezüglich der gesetzlichen Regelung eines Mitgliedstaats, nicht eines Drittlands, Privacy International, Rn. 71 und die dort angeführte Rechtsprechung. In der Sache hat der EuGH dort festgestellt, dass mitgliedstaatliche Gesetze, die die Anbieter elektronischer Kommunikationsdienste dazu anhalten, Verkehrsdaten und Standortdaten allgemein und unterschiedslos den Sicherheitsbehörden und Nachrichtendiensten zu übermitteln, über das absolut Notwendige hinausgehen und in einer demokratischen Gesellschaft nicht als gerechtfertigt angesehen werden können, so wie es nach der im Lichte der Charta ausgelegten Datenschutzrichtlinie für elektronische Kommunikation erforderlich ist (Rn. 81).

[41] EuGH, Schrems I, Rn. 94.

[42] La Quadrature du Net u. a., Rn. 133. In diesem Kontext hat der EuGH bestätigt, dass gesetzgeberische Maßnahmen, die – als Präventionsmaßnahme – die allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten vorsehen, nach der im Lichte der Charta ausgelegten Datenschutzrichtlinie für elektronische Kommunikation ausgeschlossen sind. Im Gegensatz dazu kann der Gesetzgeber nach der Rechtsprechung des EuGH in Situationen einer ernsthaften Gefährdung der nationalen Sicherheit, die nachweislich echt sowie gegenwärtig oder vorhersehbar ist, zum Schutz der nationalen Sicherheit auf eine Anweisung zurückgreifen, die die Anbieter elektronischer Kommunikationsdienste zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten verpflichtet. Eine solche Maßnahme muss jedoch bestimmte Voraussetzungen erfüllen. Insbesondere darf die Anweisung nur für einen Zeitraum erteilt werde, der zeitlich auf das absolut Notwendige beschränkt ist, wobei jedoch eine Verlängerung möglich ist, falls die Gefährdung andauert (Rn. 168).

[43] Privacy International, Rn. 78 und die dort angeführte Rechtsprechung. Im Privacy International-Urteil hat der EuGH bezüglich des in einem Gesetz eines Mitgliedsstaates vorgesehenen Zugriffs einer Behörde auf

Garantie C – Vorhandensein eines unabhängigen Aufsichtsmechanismus

39. Der EDSA erinnert daran, dass ein Eingriff sowohl zum Zeitpunkt der Datenerhebung als auch zu dem Zeitpunkt stattfindet, zu dem eine staatliche Behörde zum Zwecke der Weiterverarbeitung auf die Daten zugreift. Der EGMR hat mehrfach die Auffassung vertreten, dass jeder Eingriff in die Rechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten der wirksamen, unabhängigen und unparteiischen Aufsicht durch einen Richter oder eine andere unabhängige Stelle[44] (z. B. eine Verwaltungsbehörde oder ein parlamentarisches Gremium) unterliegen muss. Die unabhängige Aufsicht über die Durchführung der Überwachungsmaßnahmen wurde auch vom EuGH im Schrems II-Urteil berücksichtigt[45].

40. Der EGMR führt aus, dass die vorherige (gerichtliche) Genehmigung von Überwachungsmaßnahmen zwar eine wichtige Garantie gegen Willkür ist, dass aber auch der tatsächliche Betrieb des Überwachungssystems zu berücksichtigen ist, einschließlich der für die Ausübung der Befugnisse vorgesehenen Kontrollen und des Vorliegens oder Nichtvorliegens tatsächlichen Missbrauchs[46]. In der Rechtssache Schrems II hat der EuGH auch den Umfang der Aufsichtsfunktion des Kontrollmechanismus berücksichtigt, welcher sich nicht auf die einzelnen Überwachungsmaßnahmen erstreckte.[47]

41. In Bezug auf mitgliedstaatliche Gesetze hat der EuGH befunden, dass einige Maßnahmen nur dann mit dem Unionsrecht vereinbar sind, wenn sie einer wirksamen Kontrolle durch Gerichte oder unabhängige Verwaltungsstellen unterliegen, deren Entscheidung bindend ist. Diese Kontrolle bezweckt die Überprüfung, dass eine Situation gegeben ist, in der die Maßnahme gerechtfertigt ist, und dass die dafür vorgesehenen Voraussetzungen und Garantien eingehalten sind[48]. Im Falle der Echtzeit-Erfassung von Verkehrs- und Standortdaten sollte die Kontrolle es ermöglichen, vorab unter anderem zu prüfen, ob die genehmigte Maßnahme auf das absolut Notwendige beschränkt ist. In Fällen, in denen Eile geboten ist, können die Maßnahmen ohne eine solche Vorabprüfung ergriffen werden; der EuGH verlangt jedoch, dass die spätere Überprüfung kurzfristig erfolgt.[49]

42. Was die Unabhängigkeit von Aufsichtsmechanismen im Zusammenhang mit Überwachungsmaßnahmen angeht, könnten die Feststellungen des EuGH über die Unabhängigkeit einer Stelle im Zusammenhang mit dem Rechtsschutz berücksichtigt werden (siehe nachstehend unter Garantie D). Auch die Rechtsprechung des EGMR könnte weitere Hinweise liefern. Dieser hat zum Ausdruck gebracht, dass die Aufsicht vorzugsweise durch einen Richter ausgeübt werden sollte. Es ist jedoch nicht ausgeschlossen, dass die Verantwortung einer anderen Stelle übertragen wird, sofern diese über hinreichende Unabhängigkeit von der Exekutive verfügt[50] und auch „von den Behörden, welche

---

personenbezogene Daten entschieden, dass der allgemeine Zugang zu allen gespeicherten Daten, unabhängig vom Bestehen eines – zumindest indirekten – Zusammenhangs mit dem verfolgten Ziel, nicht als auf das absolut Notwendige beschränkt angesehen werden kann (Rn. 77-78).

[44] EGMR, 6. September 1978, Klass (5029/71) (im Folgenden: Klass), Rn. 17, 51.

[45] EuGH, Schrems II, Rn. 179, 183.

[46] EGMR, 13. September, Big Brother Watch (58170/13, 62322/14, 24960/15) (im Folgenden: Big Brother Watch), Rechtsmittel anhängig, Rn. 319-320.

[47] EuGH, Schrems II, Rn. 179.

[48] EuGH, La Quadrature du Net u. a., Rn. 168, 189.

[49] EuGH, La Quadrature du Net u. a., Rn. 189.

[50] EGMR, Zakharov, Rn. 258; 10. Februar 2009, Iordachi and Others v. Moldova (25198/02), Rn. 40 und 51; sowie 26.04.2007, Dumitru Popescu v. Romania (71525/01), Rn. 70-73.

die Überwachung durchführen, unabhängig und mit ausreichenden Machtbefugnissen und Kompetenzen ausgestattet [ist], um eine wirksame und ständige Kontrolle ausüben zu können“[51]. Der EGMR hat dazu des Weiteren ausgeführt, dass bei der Prüfung der Unabhängigkeit auch die Modalitäten der Ernennung und die Rechtsstellung der Mitglieder des Aufsichtsgremiums[52] zu berücksichtigen sind. „Dies schließt Personen mit Befähigung zum Richteramt ein, die entweder vom Parlament oder vom Regierungschef ernannt werden. Dagegen wurde ein Innenminister – der nicht nur ein politisches Amt innehatte und der Exekutive angehörte, sondern auch direkt an der Beschaffung besonderer Überwachungsmittel beteiligt war – für nicht hinreichend unabhängig befunden.“[53] Wie der EGMR ferner anmerkt, ist es unerlässlich, dass die Aufsichtsstelle Zugang zu sämtlichen relevanten Schriftstücken hat, unter anderem auch zu Verschlusssachen[54]. Abschließend berücksichtigt der EGMR, ob die Tätigkeit der Aufsichtsstelle der öffentlichen Kontrolle unterliegt[55].

Garantie D – Vorhandensein wirksamer Rechtsbehelfe für den Bürger

43. Die letzte der vier wesentlichen europäischen Garantien betrifft den Rechtsschutz für den Bürger. Ihm muss ein wirksamer Rechtsbehelf zur Wahrung seiner Rechte zur Verfügung stehen, wenn er den Eindruck hat, diese würden nicht geachtet. Im Schrems I-Urteil hat der EuGH erklärt, dass „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 Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz [verletzt]. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen.“[56]

44. Im Rahmen der Prüfung eines mitgliedstaatlichen Gesetzes, das die Echtzeiterfassung von Verkehrs- und Standortdaten gestattete, hat der EuGH entschieden, dass die Mitteilung erforderlich ist, damit die betroffenen Personen ihre Rechte aus den Artikeln 7 und 8 der Charta auf Auskunft über die sie betreffenden personenbezogenen Daten und gegebenenfalls auf Berichtigung oder Löschung der Daten sowie ihr Recht, gemäß Artikel 47 der Charta bei einem Gericht einen wirksamen Rechtsbehelf einzulegen, ausüben können[57]. Allerdings hat der EuGH auch anerkannt, dass die Mitteilung an die Personen, deren Daten erfasst oder analysiert wurden, nur insoweit und erst zu dem Zeitpunkt erfolgt darf, zu dem die Mitteilung die Aufgaben, für die diese Behörden verantwortlich sind, nicht mehr gefährdet[58].

45. Auch für den EGMR ist die Frage des wirksamen Rechtsbehelfs untrennbar damit verbunden, dass der Bürger nach der Beendigung einer Überwachungsmaßnahme darüber benachrichtigt wird. Dazu hat der EMGR ausgeführt, dass der betroffene Bürger grundsätzlich kaum Möglichkeiten hat, den

[51] EGMR, Klass, Rn. 56 und Big Brother Watch, Rechtsmittel anhängig, Rn. 318.
[52] EGMR, Zakharov, Rn. 278.
[53] EGMR, Zakharov, Rn. 278.
[54] EGMR, Zakharov, Rn. 281.
[55] EGMR, Zakharov, Rn. 283.
[56] EuGH, Schrems I, Rn. 95.
[57] Vgl. La Quadrature du Net u. a., Rn. 190, sowie Gutachten 1/15 des EuGH, Nr. 220.
[58] Rechtssache La Quadrature du Net u. a., Rn. 191.

Rechtsweg zu beschreiten, es sei denn, er wird über die ohne sein Wissen durchgeführten Maßnahmen in Kenntnis gesetzt und kann so deren Rechtmäßigkeit im Nachhinein anfechten, oder er kann, wenn er den Verdacht hat, dass seine Kommunikation überwacht wurde oder wird, die Gerichte anrufen, sodass die Zuständigkeit der Gerichte nicht von der Benachrichtigung der überwachten Person über die Überwachung ihrer Kommunikation abhängt[59]. Der EGMR hat somit anerkannt, dass in einigen Fällen möglicherweise keine Benachrichtigung erfolgt, dass aber ein wirksamer Rechtsschutz gegeben sein muss. Für den Fall, dass keine Benachrichtigung erfolgt, hat der EGMR beispielsweise in der Rechtssache Kennedy klargestellt, dass ein Gericht seiner Auffassung nach hinreichende Rechtsschutzmöglichkeiten bietet, sofern es eine Reihe von Kriterien erfüllt: Es muss sich um eine unabhängige und unparteiische Stelle handeln, die sich eine Verfahrensordnung gegeben hat und aus Mitgliedern besteht, die ein hohes Richteramt bekleiden oder bekleidet haben oder erfahrene Juristen sein müssen, und es darf keine der Geltendmachung des Rechtsschutzes entgegenstehende Beweislasthürden geben[60]. Bei der Prüfung von Beschwerden Einzelner sollte das Gericht Zugang zu allen relevanten Informationen haben[61], auch zu Verschlusssachen. Und schließlich sollte es befugt sein, bei Rechtsverletzungen Abhilfe zu schaffen.[62]

46. In der englischen Fassung von Artikel 47 der Charta wird der Begriff „Tribunal“ verwendet, wobei jedoch andere Sprachfassungen dem Wort Vorzug geben, das dem englischen Wort „court“ entspricht[63]; nach der EMRK sind die Mitgliedstaaten jedoch lediglich verpflichtet, zu gewährleisten, dass „[j]ede Person, die in ihren […] Rechten oder Freiheiten verletzt worden ist, […] das Recht [hat], bei einer innerstaatlichen Instanz eine wirksame Beschwerde zu erheben“[64], wobei diese Instanz nicht notwendigerweise eine gerichtliche Instanz sein muss[65].

47. Der EuGH hat im Schrems II-Urteil hinsichtlich der Beurteilung der Angemessenheit des im Drittland gebotenen Schutzniveaus wiederholt, dass betroffene Personen „über die Möglichkeit verfügen müssen, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken“[66]. Im selben Zusammenhang zieht der EuGH in Betracht, dass ein wirksamer Rechtsschutz gegen derartige Eingriffe nicht nur durch ein Gericht, sondern auch durch ein Organ[67] gewährleistet werden kann, das Garantien böte, die den nach Artikel 47 der Charta erforderlichen Garantien der Sache nach gleichwertig wären. In seinem Schrems II-Urteil hat der EuGH hervorgehoben, dass zum einen die Unabhängigkeit des Gerichts oder Organs, insbesondere gegenüber der Exekutive, gewährleistet sein muss, einschließlich aller notwendigen Garantien, auch in Bezug auf die

[59] EGMR, Zakharov, Rn. 234.

[60] EGMR, 18. Mai 2010, Kennedy (26839/05) (im Folgenden: Kennedy), Rn. 190.

[61] Der EDSA weist darauf hin, dass nach Auffassung des Menschenrechtskommissars des Europarats die sogenannte Third-Party-Rule – nach der Nachrichtendienste eines Landes, die Nachrichtendiensten eines anderen Landes Daten übermitteln, der Empfängerseite die Verpflichtung auferlegen können, die übermittelten Daten Dritten gegenüber nicht offenzulegen – für Aufsichtsstellen nicht gelten sollte, damit die Möglichkeit eines wirksamen Rechtsbehelfs nicht beeinträchtigt wird (Themenpapier „Democratic and effective oversight of national security services“).

[62] EGMR, Kennedy, Rn. 167.

[63] In der deutschen Fassung ist z. B. das für „tribunal“ gewählte Wort „Gericht“, in der niederländischen „gerecht“.

[64] Artikel 13 EMRK.

[65] EGMR, Klass, Rn. 67.

[66] Vgl. Schrems II, Rn. 194.

[67] Vgl. Schrems II, Rn. 197, wo der EuGH ausdrücklich dieses Wort verwendet.

Voraussetzungen für seine Abberufung oder den Widerruf seiner Ernennung[68], und dass zum anderen die dem Gericht gewährten Befugnisse den Anforderungen nach Artikel 47 der Charta genügen müssen. Danach ist das Organ[69] zu ermächtigen, gegenüber den Nachrichtendiensten verbindliche Entscheidungen zu treffen, und zwar gemäß gesetzlichen Garantien, auf die sich die betroffenen Personen berufen könnten.[70]

4. ABSCHLIESSENDE BEMERKUNGEN

48. Die vier wesentlichen europäischen Garantien sind als die Hauptvoraussetzungen anzusehen, auf die bei der Beurteilung des Grades des Eingriffs in die Grundrechte auf den Schutz der Privatsphäre und Schutz personenbezogener Daten abzustellen ist. Sie sollten, da sie in engem Zusammenhang stehen, nicht unabhängig voneinander geprüft werden, sondern in ihrer Gesamtheit und unter Berücksichtigung der einschlägigen Rechtsvorschriften zu Überwachungsmaßnahmen, zum Mindestmaß an Garantien für den Schutz der Rechte der betroffenen Personen sowie zu den nach dem nationalen Recht des Drittlands zur Verfügung stehenden Rechtsbehelfen.

49. Diese Garantien sind in gewissem Maß auslegungsbedürftig, nicht zuletzt, weil die Gesetze des Drittlands nicht unbedingt mit dem unionsrechtlichen Rechtsrahmen vergleichbar sind.

50. Wie der EGMR in der Rechtssache Kennedy festgestellt hat, hängt die Prüfung von allen Umständen des Falles ab, unter anderem von Art, Umfang und Dauer der möglichen Maßnahmen, von den für deren Anordnung erforderlichen Gründen, von den für deren Genehmigung, Durchführung und Aufsicht zuständigen Behörden sowie von der Art der im nationalen Recht vorgesehenen Rechtsbehelfe.[71]

51. Die anhand der wesentlichen europäischen Garantien vorgenommene Beurteilung der Überwachungsmaßnahmen eines Drittlands kann danach zu zwei Ergebnissen führen:

- dass die in Rede stehende gesetzliche Regelung des Drittlands den Anforderungen der wesentlichen europäischen Garantien nicht genügt: In diesem Falle wäre diese nicht geeignet, ein Schutzniveau zu gewährleisten, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist;

- dass die in Rede stehende gesetzliche Regelung des Drittlands den Anforderungen der wesentlichen europäischen Garantien genügt.

52. Bei der Bewertung der Angemessenheit des Schutzniveaus wird die Kommission nach Artikel 45 der DSGVO zu beurteilen haben, ob die wesentlichen europäischen Garantien, die Teil der zu berücksichtigenden Kriterien sind, erfüllt sind, so dass die gesetzliche Regelung des Drittlands im Ganzen ein Schutzniveau gewährleistet, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist.

---

[68] Vgl. Schrems II, Rn. 195.

[69] Vgl. Schrems II, Rn. 197, wo der EuGH ausdrücklich dieses Wort verwendet.

[70] Vgl. Schrems II, Rn. 196.

[71] EGMR, Kennedy, Rn. 153.

53. Wenn sich Datenexporteure, ebenso wie Datenimporteure, auf geeignete Garantien im Sinne von Artikel 46 der DSGVO stützen, müssen sie wegen der Anforderungen, die speziell im Hinblick auf die übermittelten Daten an die gesetzliche Regelung des Drittlands zu stellen sind, sicherstellen, dass tatsächlich ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet ist. Wenn die gesetzliche Regelung des Drittlands den sich aus den wesentlichen europäischen Garantien ergebenden Anforderungen nicht genügt, wäre deshalb sicherzustellen, dass das betreffende Gesetz die für die Übermittlung geltenden Garantien und Schutzmaßnahmen nicht beeinträchtigt, damit dennoch ein Schutzniveau erreicht wird, das dem in der Union gewährleisteten im Wesentlichen gleichwertig ist.

54. Der EDSA hat weitere - bei der Bewertung zu berücksichtigende - Leitlinien und Empfehlungen erlassen, je nachdem, welches Übermittlungsinstrument verwendet wird und ob die Notwendigkeit besteht, geeignete Garantien zu geben, u. a. ggf. zusätzliche Maßnahmen.[72]

55. Des Weiteren ist zu beachten, dass die wesentlichen europäischen Garantien auf rechtlichen Anforderungen beruhen. Der EDSA weist darauf hin, dass die wesentlichen europäischen Garantien auf die Grundrechte gestützt sind, die für jeden unabhängig von seiner Staatsangehörigkeit gelten.

56. Der EDSA bekräftigt, dass die wesentlichen europäischen Garantien ein Maßstab für die Bewertung von Grundrechtseingriffen sind, die im Rahmen internationaler Datenübermittlung in Verbindung mit Überwachungsmaßnahmen eines Drittlands erfolgen. Diese Standards ergeben sich aus dem Unionsrecht und der für die Mitgliedstaaten verbindlichen Rechtsprechung des EuGH und des EGMR.

[72] Referenzgrundlage für Angemessenheit, WP 254/rev.01, zuletzt überarbeitet und angenommen am 6. Februar 2018; EDSA Empfehlungen 01/2020 vom 10. November 2020 (EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020).