

Empfehlungen 02/2020 zu den Europäischen Grundlegenden Garantien für Überwachungsmassnahmen

**Angenommen am 10. November 2020**

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

Dieses Dokument wurde automatisiert von [www.Deepl.com](http://www.Deepl.com) übersetzt. Bedingt durch Seitenumbrüche werden einzelne Sätze schon mal künstlich getrennt und führen zu sinnlosen Übersetzungen.

Inhaltsverzeichnis

1. [INTRODUCTION 4](#_bookmark0)
2. [INTERFERENZEN MIT GRUNDLEGENDEN RIGHTS 6](#_bookmark1)
3. [DAS EUROPÄISCHE WESENTLICH GUARANTEES 8](#_bookmark2)

[Garantie A - Die Verarbeitung sollte auf klaren, präzisen und zugänglichen rules 8](#_bookmark3)

[Garantie B - Notwendigkeit und Verhältnismäßigkeit im Hinblick auf die verfolgten legitimen Ziele müssen nachgewiesen werden10](#_bookmark4)

[Garantie C - Unabhängige Aufsicht mechanism 12](#_bookmark5)

[Garantie D - Wirksame Rechtsmittel müssen für die individual 13](#_bookmark6)

1. [SCHLUSS REMARKS 15](#_bookmark7)

**Der Europäische Datenschutzrat**

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

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 20182 geänderten Fassung,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

gestützt auf das Arbeitsdokument der Artikel-29-Datenschutzgruppe zur Rechtfertigung von Eingriffen in die Grundrechte auf Privatsphäre und Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (European Essential Guarantees, im Folgenden "EEG"), WP237,

### HAT DIE FOLGENDEN EMPFEHLUNGEN ANGENOMMEN

# EINLEITUNG

1. Im Anschluss an das Urteil Schrems I haben die in der Arbeitsgruppe 29 versammelten Datenschutzbehörden der EU auf die Rechtsprechung zurückgegriffen, um die wesentlichen europäischen Garantien zu ermitteln, die eingehalten werden müssen, um sicherzustellen, dass Eingriffe in das Recht auf Privatsphäre und den Schutz personenbezogener Daten durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten nicht über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist.
2. Der EDPB möchte betonen, dass sich die wesentlichen europäischen Garantien auf die Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden: EuGH) in Bezug auf die Artikel 7, 8, 47 und 52 der Charta der Grundrechte der EU (im Folgenden: Charta) und gegebenenfalls auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (im Folgenden: EGMR) in Bezug auf Artikel 8 der Europäischen Menschenrechtskonvention (im Folgenden: EMRK) über Überwachungsfragen in Vertragsstaaten der EMRK stützen. 3

1 Dieses Papier befasst sich nicht mit Situationen der Übertragung oder Weitergabe, die in den Anwendungsbereich der Strafverfolgungsrichtlinie (Richtlinie (EU) 2016/680) fallen.

2 Bezugnahmen auf "Mitgliedstaaten" in diesem Dokument sind als Bezugnahmen auf "EWR-Mitgliedstaaten" zu verstehen.

3 In diesen Empfehlungen wird der Begriff "Grundrechte" aus der EU-Charta der Grundrechte der EU abgeleitet. Er wird jedoch auch für die "Menschenrechte" verwendet, wie sie in der Europäischen Menschenrechtskonvention enthalten sind.

1. Die Aktualisierung dieses Papiers soll die ursprünglich als Reaktion auf das Schrems-I-Urteil4 verfassten Europäischen Grundlegenden Garantien weiterentwickeln, indem sie die Klarstellungen widerspiegelt, die der EuGH (und der EGMR) seit seiner ersten Veröffentlichung, insbesondere in seinem wegweisenden Schrems-II-Urteil, vorgenommen hat. 5.
2. In seinem Schrems-II-Urteil stellte der EuGH fest, dass die Prüfung des Beschlusses 2010/87/EU der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern im Lichte der Artikel 7, 8 und 47 der Charta nichts ergeben hat, was die Gültigkeit dieses Beschlusses beeinträchtigen könnte, aber den Datenschutzschutzbeschluss für ungültig erklärt hat. Der CJEU befand, dass der Datenschutzschutzbeschluss im Lichte der Artikel 7, 8 und 47 der Charta mit Artikel 45 Absatz 1 GDPR unvereinbar sei. Das Urteil kann somit als Beispiel dienen, wenn Überwachungsmaßnahmen in einem Drittland (in diesem Fall die Vereinigten Staaten mit Abschnitt 702 FISA und Executive Order 12 333) weder ausreichend begrenzt sind noch Gegenstand eines wirksamen Rechtsbehelfs sind, der den betroffenen Personen zur Durchsetzung ihrer Rechte zur Verfügung steht, wie dies nach EU-Recht erforderlich ist, um das Schutzniveau in einem Drittland als "im Wesentlichen gleichwertig" mit dem in der Europäischen Union garantierten Schutzniveau im Sinne von Artikel 45 Absatz 1 GDPR zu betrachten.
3. Die Gründe für die Ungültigkeitserklärung des Datenschutzschildes haben auch Auswirkungen auf andere Übertragungsinstrumente. 6 Auch wenn der Gerichtshof Artikel 46 Absatz 1 GDPR im Zusammenhang mit der Gültigkeit der Standardvertragsklauseln (im Folgenden: SVK) ausgelegt hat, gilt seine Auslegung für jeden Transfer in Drittstaaten, der sich auf eines der in Artikel 46 GDPR7 genannten Instrumente stützt.
4. Es ist letztlich Sache des CJEU, zu beurteilen, ob Eingriffe in ein Grundrecht gerechtfertigt werden können. In Ermangelung eines solchen Urteils und in Anwendung der ständigen Rechtsprechung sind die Datenschutzbehörden jedoch verpflichtet, Einzelfälle entweder von Amts wegen oder aufgrund einer Beschwerde zu beurteilen und den Fall entweder an ein nationales Gericht zu verweisen, wenn sie den Verdacht haben, dass die Übermittlung nicht mit Artikel 45 in Einklang steht, wenn eine Entscheidung über die Angemessenheit vorliegt, oder die Übermittlung auszusetzen oder zu verbieten, wenn sie feststellen, dass Artikel 46 GDPR nicht eingehalten werden kann und der vom EU-Recht geforderte Schutz der übermittelten Daten nicht durch andere Mittel gewährleistet werden kann.
5. Das Ziel der aktualisierten Europäischen Grundlegenden Garantien ist es, Elemente zur Verfügung zu stellen, mit denen geprüft werden kann, ob Überwachungsmaßnahmen, die Behörden in einem Drittland, die nationale Sicherheitsbehörden oder Strafverfolgungsbehörden sind, den Zugang zu personenbezogenen Daten ermöglichen, als ein gerechtfertigter Eingriff angesehen werden können oder nicht.
6. In der Tat sind die wesentlichen europäischen Garantien Teil der Bewertung, die durchzuführen ist, um festzustellen, ob ein Drittland ein Schutzniveau bietet, das dem innerhalb der EU garantierten Schutzniveau im Wesentlichen gleichwertig ist, aber sie zielen nicht von sich aus darauf ab, alle Elemente zu definieren, die notwendig sind, um davon ausgehen zu können, dass ein Drittland ein solches Schutzniveau gemäß Artikel 45 des BIPR bietet. Ebenso wenig zielen sie allein darauf ab, alle Elemente zu definieren, die bei der Beurteilung der Frage, ob die Rechtsordnung eines Drittlandes den Datenexporteur und -importeur daran hindert, angemessene Schutzmaßnahmen gemäß Artikel 46 des BIPR zu gewährleisten, zu berücksichtigen sein könnten.

4 CJEU-Urteil vom 6. Oktober 2015, Maximillian Schrems gegen Datenschutzbeauftragte, Rechtssache C-362/14, EU:C:2015:650 (im Folgenden: Schrems I).

5 CJEU-Urteil vom 16. Juli 2020, Datenschutzbeauftragter gegen Facebook Ireland Ltd, Maximillian Schrems, Rechtssache C-311/18, ECLI:EU:C:2020:559 (im Folgenden: Schrems II).

6 Siehe §105 von Schrems II.

7 Siehe §92 von Schrems II.

1. Daher sollten die in diesem Papier dargelegten Elemente als die wesentlichen Garantien angesehen werden, die in dem Drittland zu finden sind, wenn es um die Beurteilung des Eingriffs geht, der durch Überwachungsmaßnahmen eines Drittlandes mit dem Recht auf Privatsphäre und Datenschutz verbunden ist, und nicht als eine Liste von Elementen, mit denen nachgewiesen werden soll, dass das Rechtssystem eines Drittlandes insgesamt ein im Wesentlichen gleichwertiges Schutzniveau bietet.
2. Artikel 6 Absatz 3 des Vertrags über die Europäische Union legt fest, dass die in der EMRK verankerten Grundrechte allgemeine Grundsätze des EU-Rechts darstellen. Wie der CJEU in seiner Rechtsprechung in Erinnerung ruft, stellt diese jedoch, solange die Europäische Union ihr nicht beigetreten ist, kein Rechtsinstrument dar, das formell in das EU-Recht übernommen wurde. 8 Folglich ist das in Artikel 46 Absatz 1 des BIPR geforderte Schutzniveau der Grundrechte auf der Grundlage der Bestimmungen dieser Verordnung unter Berücksichtigung der in der Charta verankerten Grundrechte zu bestimmen. Dessen ungeachtet haben gemäß Artikel 52 Absatz 3 der Charta die darin enthaltenen Rechte, die den durch die EMRK garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite wie die in dieser Konvention festgelegten Rechte, und folglich ist, wie der EuGH in Erinnerung gerufen hat, die Rechtsprechung des EGMR in Bezug auf Rechte, die auch in der Charta der Grundrechte der EU vorgesehen sind, als Mindestschutzschwelle für die Auslegung entsprechender Rechte in der Charta zu berücksichtigen. 9 Gemäß dem letzten Satz von Artikel 52 Absatz 3 der Charta "hindert diese Bestimmung jedoch nicht, dass das Unionsrecht einen weiter gehenden Schutz gewährt".
3. Daher wird der Inhalt der wesentlichen Garantien weiterhin teilweise auf der Rechtsprechung des EGMR beruhen, insofern als die Charta in der Auslegung durch den EuGH kein höheres Schutzniveau vorsieht, das andere Anforderungen als die Rechtsprechung des EGMR stellt.
4. In diesem Papier werden der Hintergrund und weitere Einzelheiten zu den vier Europäischen Grundlegenden Garantien erläutert.

# 2. EINGRIFFE IN DIE GRUNDRECHTE

1. Die Grundrechte auf Achtung des Privat- und Familienlebens, einschließlich der Kommunikation, und auf den Schutz personenbezogener Daten sind in den Artikeln 7 und 8 der Charta verankert und gelten für jedermann. Artikel 8 legt darüber hinaus die Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten fest und erkennt das Recht auf Zugang und Berichtigung an; ferner schreibt er vor, dass diese Vorschriften der Kontrolle einer unabhängigen Behörde unterliegen.
2. "(D)er Vorgang der Übermittlung personenbezogener Daten von einem Mitgliedstaat in ein Drittland stellt an sich schon eine Verarbeitung personenbezogener Daten dar". 10 Somit gelten die Artikel 7 und 8 der Charta für diesen spezifischen Vorgang, und ihr Schutz erstreckt sich auf die übermittelten Daten, weshalb die betroffenen Personen

8 Siehe § 98 von Schrems II.

9 Siehe § 124 der verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, La Quadrature du Net und andere (im Folgenden: La Quadrature du Net und andere).

10 CJEU, Schrems II, § 83.

deren personenbezogene Daten in ein Drittland übermittelt werden, muss ein Schutzniveau gewährt werden, das im Wesentlichen dem in der Europäischen Union garantierten Schutzniveau entspricht. 11

1. Nach Auffassung des EuGH wird, wenn das in Artikel 7 der Charta verankerte Grundrecht auf Achtung des Privatlebens durch die Verarbeitung personenbezogener Daten einer Person berührt wird, auch das Recht auf Datenschutz berührt, da eine solche Verarbeitung in den Anwendungsbereich von Artikel 8 der Charta fällt und daher notwendigerweise dem in diesem Artikel festgelegten Datenschutzerfordernis genügen muss. 12
2. Im Hinblick auf einen möglichen Eingriff in die Grundrechte nach dem EU-Recht wirft daher die den Anbietern elektronischer Kommunikationsdienste auferlegte Verpflichtung (...) zur Vorratsspeicherung von Verkehrsdaten mit dem Ziel, sie erforderlichenfalls den zuständigen nationalen Behörden zur Verfügung zu stellen, Fragen der Vereinbarkeit mit den Artikeln 7 und 8 der Charta auf. 13 Dasselbe gilt für andere Arten der Datenverarbeitung, wie die Übermittlung von Daten an andere Personen als die Nutzer oder den Zugang zu diesen Daten im Hinblick auf ihre Verwendung14 , was somit einen Eingriff in diese Grundrechte darstellt. Darüber hinaus stellt der Zugang zu den Daten durch eine öffentliche Behörde nach ständiger Rechtsprechung einen weiteren Eingriff dar. 15
3. Für die Feststellung eines Eingriffs ist es unerheblich, "ob die fraglichen Informationen über das Privatleben sensibel sind oder ob den betroffenen Personen durch diesen Eingriff in irgendeiner Weise Unannehmlichkeiten entstanden sind".16 Der CJEU betonte auch, dass es unerheblich ist, ob die auf Vorrat gespeicherten Daten anschließend verwendet wurden oder nicht. 17
4. Die Artikel 7 und 8 der Charta sind jedoch keine absoluten Rechte, sondern müssen im Zusammenhang mit ihrer Funktion in der Gesellschaft betrachtet werden. 18
5. Die Charta enthält eine Notwendigkeits- und Verhältnismäßigkeitsprüfung, um Einschränkungen der von ihr geschützten Rechte zu formulieren. In Artikel 52 Absatz 1 der Charta wird der Umfang möglicher Einschränkungen der Artikel 7 und 8 präzisiert, indem es heißt: "Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und das Wesen dieser Rechte und Freiheiten achten. Vorbehaltlich des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten Zielen von allgemeinem Interesse oder der Notwendigkeit, die Rechte und Freiheiten anderer zu schützen, tatsächlich entsprechen".
6. Der CJEU bekräftigte, dass EU-Rechtsvorschriften, die einen Eingriff in die durch Artikel 7 und 8 der Charta garantierten Grundrechte darstellen, "klare und präzise Regeln für den Anwendungsbereich und die Anwendung der Maßnahme sowie Mindestgarantien festlegen müssen, damit die Personen, deren personenbezogene Daten betroffen sind, ausreichende Garantien haben, dass die Daten wirksam gegen die Gefahr des Missbrauchs geschützt werden", insbesondere wenn personenbezogene Daten automatisch verarbeitet werden und "wenn ein erhebliches Risiko eines unrechtmäßigen Zugangs zu diesen Daten besteht". 19

11 CJEU, Schrems II, § 96.

12 CJEU, Schrems II, §§ 170-171.

13 CJEU, Rechtssache C-623/17, Privacy International (nachstehend: Privacy International), § 60.

14 CJEU, Datenschutz International, § 61.

15 EGMR, Leander, §48; EGMR, Rotaru §46; CJEU, Digital Rights Ireland, §35.

16 CJEU, Schrems II, § 171, einschließlich der zitierten Rechtsprechung. 17 CJEU, Schrems II, §171, einschließlich der zitierten Rechtsprechung. 18 CJEU, Datenschutz International, §63.

19 CJEU, Privacy International, §68 und die darin erwähnte Rechtsprechung.

1. Nach Ansicht des CJEU erfordert der Schutz des Rechts auf Privatsphäre, dass Ausnahmen und Einschränkungen des Rechts auf Datenschutz "insoweit gelten müssen, als dies unbedingt erforderlich ist". Darüber hinaus muss ein Ziel von allgemeinem Interesse mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden, "indem ein angemessenes Gleichgewicht zwischen diesem Ziel und den fraglichen Rechten hergestellt wird". 20
2. Folglich dürfen der Zugang zu personenbezogenen Daten sowie deren Speicherung und Weiterverwendung durch Behörden im Rahmen von Überwachungsmaßnahmen die Grenzen dessen, was im Lichte der Charta als unbedingt notwendig erachtet wird, nicht überschreiten, da sie sonst "in einer demokratischen Gesellschaft nicht als gerechtfertigt angesehen werden können". 21
3. Die vier grundlegenden europäischen Garantien, wie sie im nächsten Kapitel entwickelt werden, sollen näher erläutern, wie der Grad der Beeinträchtigung der Grundrechte auf Privatsphäre und Datenschutz im Zusammenhang mit Überwachungsmaßnahmen durch Behörden in einem Drittland bei der Übermittlung personenbezogener Daten zu beurteilen ist und welche rechtlichen Anforderungen folglich gelten müssen, um zu beurteilen, ob solche Eingriffe im Rahmen der Charta akzeptabel wären.

# 3. DIE EUROPÄISCHEN WESENTLICHEN GARANTIEN

1. Im Anschluss an die Analyse der Rechtsprechung ist der EDPB der Auffassung, dass sich die geltenden rechtlichen Anforderungen, um die in der Charta anerkannten Einschränkungen des Datenschutzes und des Rechts auf Privatsphäre zu rechtfertigen, in vier wesentlichen europäischen Garantien zusammenfassen lassen:
	1. Die Verarbeitung sollte auf klaren, präzisen und zugänglichen Regeln basieren
	2. Notwendigkeit und Verhältnismäßigkeit im Hinblick auf die verfolgten legitimen Ziele müssen nachgewiesen werden
	3. Es sollte ein unabhängiger Aufsichtsmechanismus existieren
	4. Wirksame Rechtsmittel müssen dem Einzelnen zur Verfügung stehen
2. Die Garantien basieren auf den Grundrechten auf Privatsphäre und Datenschutz, die für alle gelten, unabhängig von ihrer Nationalität.

## Garantie A - Die Verarbeitung sollte auf klaren, präzisen und zugänglichen Regeln basieren

1. Gemäß Artikel 8 Absatz 2 der Charta sollten personenbezogene Daten unter anderem "für festgelegte Zwecke und auf der Grundlage der Einwilligung der betroffenen Person oder auf einer anderen gesetzlich geregelten legitimen Grundlage" verarbeitet werden,22 wie der CJEU in der Entscheidung Schrems II in Erinnerung rief. Darüber hinaus muss gemäß Artikel 52 Absatz 1 der Charta jede Beschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten innerhalb der EU gesetzlich vorgesehen werden. Daher muss ein gerechtfertigter Eingriff im Einklang mit dem Gesetz stehen.

20 CJEU, Privacy International, §68 und die darin erwähnte Rechtsprechung.

21 CJEU, Datenschutz International, §81.

22 Siehe §173 Schrems II.

1. Diese Rechtsgrundlage sollte klare und präzise Regeln für den Anwendungsbereich und die Anwendung der fraglichen Maßnahme sowie Mindestgarantien festlegen. 23 Darüber hinaus erinnerte der Gerichtshof daran, dass "die Rechtsvorschriften nach innerstaatlichem Recht rechtsverbindlich sein müssen". 24 In diesem Zusammenhang stellte der CJEU klar, dass sich die Beurteilung des anwendbaren Drittlandsrechts darauf konzentrieren sollte, ob es von Einzelpersonen vor einem Gericht geltend gemacht und geltend gemacht werden kann. 25 Der Gerichtshof weist daher darauf hin, dass die den betroffenen Personen gewährten Rechte einklagbar sein müssen; wenn Einzelpersonen nicht mit durchsetzbaren Rechten gegenüber staatlichen Behörden ausgestattet sind, kann das gewährte Schutzniveau nicht als im Wesentlichen gleichwertig mit dem sich aus der Charta ergebenden Schutzniveau betrachtet werden, was im Widerspruch zu der Anforderung in Artikel 45 Absatz 2 Buchstabe a des BIPR steht. 26
2. Darüber hinaus betonte der Gerichtshof, dass das anwendbare Recht angeben muss, unter welchen Umständen und unter welchen Bedingungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden kann27 (siehe unten unter Garantie B das Verhältnis zwischen diesen Anforderungen und den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit).
3. Darüber hinaus hat der CJEU auch darauf hingewiesen, dass "das Erfordernis, dass jede Einschränkung der Ausübung von Grundrechten gesetzlich vorgesehen sein muss, impliziert, dass die Rechtsgrundlage, die den Eingriff in diese Rechte erlaubt, selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts definieren muss". 28
4. Schließlich ist der Europäische Gerichtshof für Menschenrechte "nicht der Ansicht, dass es keinen Grund gibt, unterschiedliche Prinzipien anzuwenden, die sich einerseits auf die Zugänglichkeit und Klarheit der Regeln für das Abhören individueller Kommunikation und andererseits auf allgemeinere Überwachungsprogramme beziehen". 29 Auch der EGMR hat klargestellt, dass die Rechtsgrundlage zumindest eine Definition der Kategorien von Personen, die überwacht werden könnten, eine Begrenzung der Dauer der Maßnahme, das Verfahren zur Prüfung, Verwendung und Speicherung der erhaltenen Daten sowie die Vorsichtsmaßnahmen bei der Übermittlung der Daten an andere Parteien enthalten sollte. 30
5. Schließlich muss der Eingriff in seiner Wirkung für den Einzelnen vorhersehbar sein, um ihn angemessen und wirksam vor willkürlichen Eingriffen und der Gefahr des Missbrauchs zu schützen. Folglich muss die Verarbeitung auf einer präzisen, klaren, aber auch zugänglichen (d.h. öffentlichen) Rechtsgrundlage beruhen. 31 Der EGMR erinnerte in dieser Frage im Fall Sacharow daran, dass "der Bezug auf die 'Vorhersehbarkeit' im Zusammenhang mit der Überwachung des Fernmeldeverkehrs nicht derselbe sein kann wie in vielen anderen Bereichen". Er präzisierte, dass im Zusammenhang mit geheimen Überwachungsmaßnahmen, wie z.B. dem Abhören von

23 Siehe §175 und §180 Schrems II und Gutachten 1/15 (Abkommen EU-Kanada über Fluggastdatensätze) vom 26. Juli 2017, § 139 und die zitierte Rechtsprechung.

24 Siehe § 68 Privacy International - Es sollte auch klar sein, dass das Gericht in der französischen Version des Urteils das Wort "réglementation" verwendet, das weiter gefasst ist als nur Akte des Parlaments.

25 Siehe § 181 Schrems II, in diesem Absatz bezieht sich der CJEU auf die US Presidential Policy Directive 28.

26 Siehe § 181 Schrems II.

27 Siehe § 68 von Privacy International, in Bezug auf das Recht der Mitgliedstaaten.

28 Siehe Schrems II, § 175 und die zitierte Rechtsprechung, sowie Privacy International, § 65.

29 EGMR, Freiheit, §63.

30 EGMR, Weber und Saravia, §95.

31 EGMR, Malone, §§65, 66.

Kommunikation, "Vorhersehbarkeit kann nicht bedeuten, dass ein Individuum in der Lage sein sollte, vorauszusehen, wann die Behörden wahrscheinlich seine Kommunikation abhören werden, so dass er sein Verhalten entsprechend anpassen kann". Wenn man jedoch bedenkt, dass in einer solchen Situation die Gefahr der Willkür offensichtlich ist, "ist es unerlässlich, klare, detaillierte Regeln für das Abhören von Telefongesprächen zu haben, zumal die zur Verfügung stehende Technologie immer ausgefeilter wird. Das innerstaatliche Recht muss ausreichend klar sein, um den Bürgern einen angemessenen Hinweis darauf zu geben, unter welchen Umständen und unter welchen Bedingungen die Behörden befugt sind, auf solche Maßnahmen zurückzugreifen". 32

## Garantie B - Notwendigkeit und Verhältnismäßigkeit im Hinblick auf die verfolgten legitimen Ziele müssen nachgewiesen werden

1. Nach Artikel 52 Absatz 1 Satz 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten das Wesen dieser Rechte und Freiheiten achten. Nach Artikel 52 Absatz 1 Satz 2 der Charta dürfen Einschränkungen dieser Rechte und Freiheiten vorbehaltlich des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten Zielen von allgemeinem Interesse oder der Notwendigkeit, die Rechte und Freiheiten anderer zu schützen, tatsächlich entsprechen. 33
2. In Bezug auf den **Grundsatz der Verhältnismäßigkeit** stellte der Gerichtshof in Bezug auf die Rechtsvorschriften der Mitgliedstaaten fest, dass die Frage, ob eine Beschränkung des Rechts auf Privatsphäre und Datenschutz gerechtfertigt sein kann, zum einen anhand der **Schwere des Eingriffs** zu beurteilen ist, **den** eine solche Beschränkung mit sich bringt34 , und zum anderen zu prüfen ist, ob die **Bedeutung des** mit dieser Beschränkung verfolgten **Ziels des Allgemeininteresses in** einem angemessenen Verhältnis zu dieser Schwere steht. 35
3. In der Rechtssache La Quadrature du net und anderen kann festgestellt werden, dass der EuGH in Bezug auf das Recht eines Mitgliedstaats und nicht auf das Recht eines Drittlandes entschieden hat, dass das Ziel der Wahrung der nationalen Sicherheit aufgrund seiner Bedeutung geeignet ist, Maßnahmen zu rechtfertigen, die schwerwiegendere Eingriffe in die Grundrechte nach sich ziehen als solche, die durch andere Ziele wie die Bekämpfung der Kriminalität gerechtfertigt werden könnten. Er stellte jedoch fest, dass dies der Fall ist, solange es hinreichend solide Gründe für die Annahme gibt, dass der betreffende Staat mit einer schwerwiegenden Bedrohung der nationalen Sicherheit konfrontiert ist, die nachweislich eine tatsächliche und gegenwärtige oder vorhersehbare Gefahr darstellt und vorbehaltlich der Erfüllung der anderen in Artikel 52 Absatz 1 der Charta festgelegten Anforderungen. 36

32 EGMR, Sacharow, §229.

33 Schrems II, § 174.

34 In diesem Zusammenhang stellte das Gericht beispielsweise fest, dass "die Beeinträchtigung durch die Echtzeiterfassung von Daten, die die Ortung von Endgeräten ermöglicht, besonders schwerwiegend erscheint, da diese Daten den zuständigen nationalen Behörden ein Mittel zur genauen und dauerhaften Verfolgung der Bewegungen der Benutzer von Mobiltelefonen (...) zur Verfügung stellen" (La Quadrature du Net und andere, § 187, einschließlich der zitierten Rechtsprechung).

35 La Quadrature du Net und andere, § 131.

36 §§136 und 137. Siehe auch Privacy International, wie der Gerichtshof ausgeführt hat, können solche Bedrohungen nach ihrer Art und besonderen Schwere von der allgemeinen Gefahr unterschieden werden, dass es zu Spannungen oder Störungen, auch schwerwiegender Art, kommt, die die öffentliche Sicherheit beeinträchtigen. § In La Quadrature du Net und anderen stellte der Gerichtshof zum Beispiel fest, dass die automatisierte Analyse von Verkehrs- und Standortdaten, die allgemein und unterschiedslos die Daten von Personen, die elektronische Kommunikationssysteme benutzen, erfasst, eine besonders schwerwiegende Störung darstellt, so dass eine solche Maßnahme

1. Nach ständiger Rechtsprechung des Gerichtshofs dürfen Ausnahmen und Einschränkungen des Schutzes personenbezogener Daten nur insoweit gelten, als dies unbedingt erforderlich ist. 37 Um diesem Erfordernis gerecht zu werden, müssen die fraglichen Rechtsvorschriften nicht nur klare und präzise Regeln für den Anwendungsbereich und die Anwendung der fraglichen Maßnahme festlegen, sondern auch Mindestgarantien vorsehen, damit die Personen, deren Daten übermittelt wurden, ausreichende Garantien haben, um ihre personenbezogenen Daten wirksam gegen die Gefahr des Missbrauchs zu schützen. "Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Bedingungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden kann, wodurch sichergestellt wird, dass der Eingriff auf das unbedingt notwendige Maß beschränkt bleibt. Der Bedarf an solchen Schutzmaßnahmen ist umso größer, wenn personenbezogene Daten automatisiert verarbeitet werden". 38
2. In Schrems II hat der CJEU betont, dass die Rechtsvorschriften eines Drittlandes, die keine Beschränkungen der Befugnisse angeben, die sie zur Durchführung von Überwachungsprogrammen für Zwecke des Auslandsgeheimdienstes übertragen, kein Schutzniveau gewährleisten können, das dem durch die Charta garantierten im Wesentlichen gleichwertig ist. In der Tat muss nach der Rechtsprechung eine Rechtsgrundlage, die einen Eingriff in die Grundrechte zulässt, selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts definieren, um den Erfordernissen des Grundsatzes der Verhältnismäßigkeit zu genügen. 39
3. Hinsichtlich des **Prinzips der Notwendigkeit** hat der CJEU klargestellt, dass Rechtsvorschriften, "die auf allgemeiner Basis die Speicherung aller personenbezogenen Daten aller Personen zulassen, deren Daten aus der Europäischen Union übermittelt wurden (...) ohne Differenzierung, Einschränkung oder Ausnahme im Hinblick auf den verfolgten Zweck und ohne Festlegung eines objektiven Kriteriums, anhand dessen die Grenzen des Zugangs der Behörden zu den Daten und ihrer anschließenden Verwendung für Zwecke festgelegt werden, die spezifisch, streng begrenzt und geeignet sind, den Eingriff zu rechtfertigen, den sowohl der Zugang zu den Daten als auch ihre Verwendung mit sich bringen", mit diesem Grundsatz nicht vereinbar sind. 40 Insbesondere ist davon auszugehen, dass Gesetze, die den Behörden einen allgemeinen Zugang zu den Inhalten der elektronischen Kommunikation gestatten, das Wesen des Grundrechts auf Achtung des Privatlebens, wie es durch Artikel 7 der Charta garantiert wird, beeinträchtigen. 41
4. Ebenso hat der CJEU in La Quadrature du Net und andere bei der Beurteilung der Gesetze eines Mitgliedstaates und nicht eines Drittlandes festgestellt, dass "Rechtsvorschriften, die die Vorratsspeicherung personenbezogener Daten vorschreiben, stets objektive Kriterien erfüllen müssen, die einen Zusammenhang zwischen den gespeicherten Daten und dem verfolgten Zweck herstellen". 42 In demselben Zusammenhang hat er in der Rechtssache Privacy International ebenfalls festgestellt, dass der Gesetzgeber "die

kann dem Erfordernis der Verhältnismäßigkeit nur in Situationen gerecht werden, in denen der betreffende Mitgliedstaat einer nachweislich tatsächlichen und gegenwärtigen oder vorhersehbaren ernsthaften Bedrohung der nationalen Sicherheit ausgesetzt ist, und unter anderem unter der Voraussetzung, dass die Dauer der Zurückhaltung auf das unbedingt erforderliche Maß beschränkt ist (§§ 174-177).

37 Schrems II, §176, einschließlich der zitierten Rechtsprechung.

38 Schrems II, § 175.

39 Schrems II, § 180.

40 Schrems I, § 93 mit weiteren Hinweisen. Siehe jedoch diesmal in Bezug auf ein Gesetz eines Mitgliedstaates und nicht eines Drittlandes, Privacy International, § 71, einschließlich der zitierten Rechtsprechung. In diesem Fall stellte der Gerichtshof fest, dass die Rechtsvorschriften eines Mitgliedstaates, die die Anbieter elektronischer Kommunikationsdienste verpflichten, Verkehrs- und Standortdaten an die Sicherheits- und Nachrichtendienste durch allgemeine und unterschiedslose Übermittlung weiterzugeben, die Grenzen des unbedingt Notwendigen überschreiten und nicht als gerechtfertigt angesehen werden können, wie es in einer demokratischen Gesellschaft gemäß der Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation, gelesen im Lichte der Charta, erforderlich ist (§81).

41 Schrems I, §94.

42 La Quadrature du Net und andere, § 133. In diesem Zusammenhang bestätigte das Gericht, dass gesetzgeberische Maßnahmen, die als Präventivmaßnahme die allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten vorsehen

sich auf objektive Kriterien stützen, um die Umstände und Bedingungen zu definieren, unter denen den zuständigen nationalen Behörden Zugang zu den fraglichen Daten gewährt werden soll". 43

## Garantie C - Unabhängiger Überwachungsmechanismus

1. Das EDPB erinnert daran, dass ein Eingriff zum Zeitpunkt der Datenerhebung erfolgt, aber auch zu dem Zeitpunkt, zu dem eine Behörde zur weiteren Verarbeitung auf die Daten zugreift. Der EGMR hat mehrfach festgelegt, dass jeder Eingriff in das Recht auf Privatsphäre und Datenschutz einem wirksamen, unabhängigen und unparteiischen Aufsichtssystem unterliegen sollte, das entweder von einem Richter oder einer anderen unabhängigen Stelle44 (z. B. einer Verwaltungsbehörde oder einem parlamentarischen Gremium) vorgesehen werden muss. Die unabhängige Aufsicht über die Durchführung von Überwachungsmaßnahmen wurde vom CJEU auch im Urteil Schrems II berücksichtigt. 45
2. Der EGMR legt fest, dass die vorherige (gerichtliche) Genehmigung von Überwachungsmaßnahmen zwar ein wichtiger Schutz vor Willkür ist, dass aber auch die tatsächliche Funktionsweise des Abhörsystems, einschließlich der Kontrolle der Machtausübung und des Vorliegens oder Nichtvorliegens eines tatsächlichen Missbrauchs, berücksichtigt werden muss. 46 Im Fall Schrems II berücksichtigte der CJEU auch den Umfang der Aufsichtsfunktion des Überwachungsmechanismus, der sich nicht auf die einzelnen Überwachungsmaßnahmen erstreckte. 47.
3. In Bezug auf das Recht der Mitgliedstaaten identifizierte der CJEU eine Reihe von Maßnahmen, die nur dann im Einklang mit dem EU-Recht stehen, wenn sie einer wirksamen Überprüfung durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterliegen, deren Entscheidung bindend ist. Ziel dieser Überprüfung ist es, zu überprüfen, ob eine Situation besteht, die die Maßnahme rechtfertigt, und ob die Bedingungen und Garantien, die festgelegt werden müssen, eingehalten werden. 48 Bei der Echtzeiterfassung von Verkehrs- und Standortdaten sollte die Überprüfung es unter anderem ermöglichen, ex ante zu prüfen, ob sie nur im Rahmen des unbedingt Notwendigen zulässig ist. In gebührend begründeten dringenden Fällen können die Maßnahmen ohne eine solche vorherige Überprüfung erfolgen; der Gerichtshof verlangt jedoch weiterhin, dass die anschließende Überprüfung innerhalb kurzer Zeit erfolgt. 49
4. Was die Unabhängigkeit der Aufsichtsmechanismen in Bezug auf die Überwachung anbelangt, so könnten die Feststellungen des CJEU bezüglich der Unabhängigkeit eines Organs im Zusammenhang mit Rechtsmitteln berücksichtigt werden (siehe

die von der Richtlinie über den Schutz der Privatsphäre und der elektronischen Kommunikation ausgeschlossen ist, im Lichte der Charta gelesen. Im Gegensatz dazu entschied der Gerichtshof, dass der Gesetzgeber in Situationen, in denen eine nachweislich tatsächliche und gegenwärtige oder vorhersehbare ernsthafte Gefahr für die nationale Sicherheit besteht, zum Schutz der nationalen Sicherheit den Rückgriff auf eine Anweisung zulassen kann, die die Anbieter elektronischer Kommunikationsdienste verpflichtet, Verkehrs- und Standortdaten allgemein und unterschiedslos aufzubewahren. Eine solche Maßnahme muss jedoch bestimmte Bedingungen erfüllen. Insbesondere darf die Weisung nur für einen Zeitraum erteilt werden, der zeitlich auf das unbedingt notwendige Maß beschränkt ist und verlängert werden kann, wenn diese Bedrohung fortbesteht (§168).

43 Privacy International, § 78, einschließlich der zitierten Rechtsprechung. In Privacy International entschied der Gerichtshof in Bezug auf den Zugang einer Behörde zu personenbezogenen Daten, die nach dem Recht eines Mitgliedstaates zur Verfügung gestellt werden, dass "ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten**,** unabhängig davon, ob ein zumindest indirekter Zusammenhang mit dem verfolgten Zweck besteht, nicht als auf das unbedingt erforderliche Maß beschränkt angesehen werden kann" (§77 -78).

44 EGMR, Klass, §§17, 51.

45 Schrems II, §§ 179, 183.

46 EGMR, Big Brother Watch unter Berufung auf §§319-320.

47 Schrems II, § 179.

48 CJEU, La Quadrature du Net und andere, §§ 168, 189.

49 CJEU, La Quadrature du Net und andere, § 189.

infra unter Garantie D). Darüber hinaus kann die Rechtsprechung des EGMR zusätzliche Elemente bieten. Dieses Gericht hat seine Präferenz für einen Richter zum Ausdruck gebracht, der für die Aufrechterhaltung der Aufsicht verantwortlich ist. Es ist jedoch nicht ausgeschlossen, dass ein anderes Organ verantwortlich sein kann, "solange es von der Exekutive"50 und "der die Überwachung durchführenden Behörden hinreichend unabhängig ist und mit ausreichenden Befugnissen und Kompetenzen ausgestattet ist, um eine wirksame und kontinuierliche Kontrolle auszuüben". 51 Der EGMR fügte hinzu, dass "die Art der Ernennung und der Rechtsstatus der Mitglieder des Überwachungsorgans"52 bei der Beurteilung der Unabhängigkeit berücksichtigt werden müssen. Dazu gehören "Personen, die für die Ausübung richterlicher Ämter qualifiziert sind und entweder vom Parlament oder vom Premierminister ernannt werden". Im Gegensatz dazu wurde ein Innenminister - der nicht nur ein politischer Beauftragter und ein Mitglied der Exekutive war, sondern direkt an der Beauftragung besonderer Überwachungsmittel beteiligt war - als nicht ausreichend unabhängig eingestuft.53 Der EGMR stellt ferner fest, "dass es von wesentlicher Bedeutung ist, dass das Aufsichtsorgan Zugang zu allen relevanten Dokumenten, einschließlich verschlossener Materialien, hat". 54 Schließlich berücksichtigt der EGMR, "ob die Tätigkeiten der Aufsichtsbehörde der öffentlichen Kontrolle zugänglich sind". 55

## Garantie D - Wirksame Rechtsmittel müssen dem Einzelnen zur Verfügung stehen

1. Die abschließende Europäische Grundlegende Garantie bezieht sich auf die Wiedergutmachungsrechte des Einzelnen. Er muss über einen wirksamen Rechtsbehelf verfügen, um seine Rechte zu befriedigen, wenn er der Ansicht ist, dass sie nicht eingehalten werden oder nicht eingehalten worden sind. Der CJEU erläuterte in Schrems I, dass "Rechtsvorschriften, die keine Möglichkeit für eine Person vorsehen, Rechtsbehelfe einzulegen, um Zugang zu sie betreffenden personenbezogenen Daten zu erhalten oder die Berichtigung oder Löschung solcher Daten zu erwirken, das Wesen des Grundrechts auf wirksamen Rechtsschutz, wie es in Artikel 47 der Charta verankert ist, nicht respektieren. Der erste Absatz von Artikel 47 der Charta schreibt vor, dass jede Person, deren durch das Recht der Europäischen Union garantierte Rechte und Freiheiten verletzt werden, das Recht auf einen wirksamen Rechtsbehelf vor einem Gericht unter Einhaltung der in diesem Artikel festgelegten Bedingungen hat."56
2. Bei der Beurteilung der Rechtsvorschriften eines Mitgliedstaates, die die Erhebung von Verkehrs- und Standortdaten in Echtzeit gestatten, vertrat der Gerichtshof die Auffassung, dass die Benachrichtigung erforderlich ist, "damit die betroffenen Personen ihre Rechte nach den Artikeln 7 und 8 der Charta wahrnehmen können, um Zugang zu ihren personenbezogenen Daten, die Gegenstand dieser Maßnahmen sind, zu beantragen und gegebenenfalls deren Berichtigung oder Löschung zu veranlassen sowie nach Artikel 47 Absatz 1 der Charta einen wirksamen Rechtsbehelf bei einem Gericht einzulegen". 57 Er erkannte jedoch auch an, daß die Benachrichtigung von Personen, deren Daten gesammelt oder analysiert worden sind, nur in dem Maße und sobald die Benachrichtigung die Aufgaben, für die diese Behörden zuständig sind, nicht mehr gefährdet, erfolgen darf. 58

50 EGMR, Sacharow, § 258, Iordachi und andere gegen Moldawien, §§ 40 und §§ 51 und Dumitru Popescu gegen Rumänien, §§ 70¬73.

51 EGMR, Klass §56 und Big Brother Watch in Berufung §318

52 EGMR, Sacharow, §278. 53 EGMR, Sacharow, §278. 54 EGMR, Sacharow, §281. 55 EGMR, Sacharow, Rdnr. 283. 56 EuGH, Schrems I, § 95.

57 Siehe § 190 von La Quadrature du Net und andere und CJEU, Gutachten 1/15, §220.

58 Siehe § 191 von La Quadrature du Net und andere.

1. Auch für den EGMR ist die Frage nach einem wirksamen Rechtsbehelf untrennbar mit der Benachrichtigung des Betroffenen über eine Überwachungsmaßnahme verbunden, sobald die Überwachung beendet ist. Insbesondere stellte der Gerichtshof fest, dass "grundsätzlich wenig Spielraum für die Anrufung der Gerichte durch die betroffene Person besteht, es sei denn, sie wird von den ohne ihr Wissen getroffenen Maßnahmen unterrichtet und kann somit deren Rechtmäßigkeit nachträglich anfechten, oder, hilfsweise, jede Person, die vermutet, dass ihre Kommunikation abgehört wird oder wurde, kann sich an die Gerichte wenden, so dass die Zuständigkeit der Gerichte nicht von der Benachrichtigung des Betroffenen über die erfolgte Überwachung seiner Kommunikation abhängt". 59 Der EGMR räumte somit ein, dass es in einigen Fällen keine Benachrichtigung geben kann, dass jedoch ein wirksamer Rechtsbehelf vorgesehen werden muss. In diesem Fall hat dieser Gerichtshof, z.B. im Fall Kennedy, klargestellt, dass ein Gericht ausreichende Abhilfemöglichkeiten bietet, wenn es eine Reihe von Kriterien erfüllt, d.h. ein unabhängiges und unparteiisches Gremium, das sich eine eigene Verfahrensordnung gegeben hat, die sich aus Mitgliedern zusammensetzt, die hohe richterliche Ämter bekleiden oder bekleidet haben müssen oder erfahrene Rechtsanwälte sind, und dass keine Beweislast zu überwinden ist, um einen Antrag bei ihm einzureichen. 60 Bei der Prüfung von Beschwerden von Einzelpersonen sollte das Gericht Zugang zu allen relevanten Informationen haben,61 einschließlich geschlossener Materialien. Schließlich sollte es die Befugnis haben, Verstöße zu beheben. 62
2. In Artikel 47 der Charta wird auf ein Gericht Bezug genommen, auch wenn in anderen Sprachfassungen als dem Englischen dem Wort "court" der Vorzug gegeben wird,63 während die EMRK die Mitgliedstaaten lediglich verpflichtet, dafür zu sorgen, dass "jeder, dessen Rechte und Freiheiten verletzt werden, einen wirksamen Rechtsbehelf bei einer innerstaatlichen Behörde einlegen kann"64 , die nicht notwendigerweise eine Justizbehörde sein muss. 65
3. Der CJEU hat im Zusammenhang mit dem Schrems-II-Urteil bei der Beurteilung der Angemessenheit des Schutzniveaus eines Drittlandes bekräftigt, dass "betroffene Personen die Möglichkeit haben müssen, vor einem unabhängigen und unparteiischen Gericht Klage zu erheben, um Zugang zu ihren personenbezogenen Daten zu erhalten oder die Berichtigung oder Löschung dieser Daten zu erwirken". 66 Im gleichen Zusammenhang ist der CJEU der Ansicht, dass ein wirksamer gerichtlicher Schutz gegen solche Eingriffe nicht nur durch ein Gericht, sondern auch durch eine Stelle67 gewährleistet werden kann, die Garantien bietet, die im Wesentlichen den in Artikel 47 der Charta geforderten Garantien entsprechen. In seinem Urteil in der Rechtssache Schrems II betonte der CJEU sowohl, dass die Unabhängigkeit des Gerichts oder Organs, insbesondere von der Exekutive, mit allen erforderlichen Garantien, auch im Hinblick auf die Bedingungen für seine Entlassung oder den Widerruf der Ernennung68 , gewährleistet werden muss, als auch, dass die Befugnisse, die einem Gericht erteilt werden sollten, den Anforderungen des Artikels 47 der Charta entsprechen müssen. In diesem

59 EGMR, Sacharow, §234.

60 EGMR, Kennedy, § 190.

61 Der EDPB stellt fest, dass der Menschenrechtskommissar des Europarates der Ansicht ist, dass die so genannte "Drittpartei"-Regel - nach der Nachrichtendienste in einem Land, die Daten an Nachrichtendienste in einem anderen Land weitergeben, die empfangenden Stellen verpflichten können, die übermittelten Daten nicht an Dritte weiterzugeben

- sollte nicht für Aufsichtsorgane gelten, um die Möglichkeit eines wirksamen Rechtsbehelfs nicht zu untergraben (Issue Paper on Democratic and effective oversight of national security services).

62 EGMR, Kennedy §167.

63 Das Wort "Tribunal" wird zum Beispiel im Deutschen mit "Gericht" und im Niederländischen mit "gerecht" übersetzt.

64 Artikel 13 EMRK.

65 EGMR, Klasse §67.

66 Siehe § 194 Schrems II.

67 Siehe §197 Schrems II, in dem der Gerichtshof dieses Wort ausdrücklich verwendet.

68 Siehe § 195 Schrems II.

Im Hinblick darauf wird dem Gremium69 die Befugnis eingeräumt, Entscheidungen zu treffen, die für die Nachrichtendienste bindend sind, und zwar in Übereinstimmung mit rechtlichen Garantien, auf die sich die betroffenen Personen verlassen können. 70

# 4. SCHLUSSBEMERKUNGEN

1. Die vier grundlegenden europäischen Garantien sind als Kernelemente zu betrachten, die bei der Beurteilung des Grades der Beeinträchtigung der Grundrechte auf Privatsphäre und Datenschutz zu finden sind. Sie sollten nicht unabhängig bewertet werden, da sie eng miteinander verknüpft sind, sondern auf einer allgemeinen Grundlage, bei der die einschlägigen Rechtsvorschriften in Bezug auf Überwachungsmaßnahmen, das Mindestniveau der Garantien für den Schutz der Rechte der betroffenen Personen und die nach dem nationalen Recht des Drittlandes vorgesehenen Rechtsbehelfe überprüft werden.
2. Diese Garantien erfordern ein gewisses Maß an Interpretation, zumal die Gesetzgebung des Drittlandes nicht mit dem EU-Rechtsrahmen identisch sein muss.
3. Wie der EGMR in Kennedy feststellte, "hängt eine Beurteilung von allen Umständen des Falles ab, wie z.B. von Art, Umfang und Dauer der möglichen Maßnahmen, den für ihre Anordnung erforderlichen Gründen, den für ihre Genehmigung, Durchführung und Überwachung zuständigen Behörden und der Art der im nationalen Recht vorgesehenen Rechtsmittel". 71
4. Folglich kann die Bewertung der Überwachungsmassnahmen der Drittländer gegen das EEG zu zwei Schlussfolgerungen führen:
	* Die fragliche Drittlandsgesetzgebung stellt die Anforderungen des EEG nicht sicher: In diesem Fall würde die Drittlandsgesetzgebung kein Schutzniveau bieten, das dem innerhalb der EU garantierten im Wesentlichen gleichwertig ist.
	* Die fragliche Drittlandsgesetzgebung genügt dem EEG.
5. Bei der Beurteilung der Angemessenheit des Schutzniveaus gemäß Artikel 45 GDPR wird die Kommission zu bewerten haben, ob das EEG als Teil der Elemente erfüllt ist, die zu berücksichtigen sind, um zu gewährleisten, dass die Gesetzgebung des Drittlandes insgesamt ein Schutzniveau bietet, das dem innerhalb der EU garantierten Schutzniveau im Wesentlichen gleichwertig ist.
6. Wenn sich die Datenexporteure zusammen mit den Datenimporteuren auf geeignete Schutzmaßnahmen nach Artikel 46 des GDPR stützen, müssten sie angesichts der Anforderungen der speziell für die übermittelten Daten geltenden Drittlandsgesetze sicherstellen, dass ein im Wesentlichen gleichwertiges Schutzniveau tatsächlich erreicht wird. Insbesondere in Fällen, in denen das Recht des Drittlandes nicht mit den Anforderungen des EEG übereinstimmt, würde dies bedeuten, dass sichergestellt werden müsste, dass das fragliche Recht die Garantien und Schutzvorkehrungen im Zusammenhang mit der Übermittlung nicht beeinträchtigt, damit weiterhin ein im Wesentlichen gleichwertiges Schutzniveau wie das innerhalb der EU garantierte gewährleistet ist.

69 Siehe §197 Schrems II, in dem der Gerichtshof dieses Wort ausdrücklich verwendet.

70 Siehe § 196 Schrems II.

71 EGMR, Kennedy §153.

1. Das EDPB hat weitere Leitlinien und Empfehlungen herausgegeben, die bei der weiteren Beurteilung zu berücksichtigen sind, je nach dem zu verwendenden Transferinstrument und der Notwendigkeit, geeignete Schutzmaßnahmen, gegebenenfalls einschließlich ergänzender Maßnahmen, vorzusehen. 72
2. Darüber hinaus ist anzumerken, dass die Europäischen Grundlegenden Garantien auf dem basieren, was gesetzlich vorgeschrieben ist. Das EDPB betont, dass die Europäischen Grundlegenden Garantien auf den Grundrechten basieren, die für alle Menschen unabhängig von ihrer Nationalität gelten.
3. Das EDPB weist erneut darauf hin, dass die Europäischen Grundlegenden Garantien ein Referenzstandard bei der Beurteilung von Eingriffen durch Überwachungsmaßnahmen von Drittländern im Zusammenhang mit internationalen Datentransfers sind. Diese Standards ergeben sich aus dem EU-Recht und der Rechtsprechung des EuGH und des EGMR, die für die Mitgliedstaaten verbindlich ist.

72 Adequacy Referential WP 254 rev.01, überarbeitet und angenommen am 6. Februar 2018; EDPB-Empfehlungen 01/2020 zu Maßnahmen, die die Transferinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten, 10. November 2020.