18/DE

WP 254/rev.01

Artikel-29-Datenschutzgruppe

Referenzgrundlage für Angemessenheit

angenommen am 28. November 2017

zuletzt überarbeitet und angenommen am 6. Februar 2018

Einleitung

Die Arbeitsgruppe der EU-Datenschutzbehörden[1] (G29) veröffentlichte in der Vergangenheit eine Arbeitsunterlage zu Übermittlungen personenbezogener Daten an Drittländer (WP 12)[2]. Angesichts der Ablösung der Richtlinie durch die EU-Datenschutz-Grundverordnung (DSGVO)[3] überprüft die G29 die WP 12, ihre früheren Leitlinien, um sie vor dem Hintergrund der neuen Gesetzgebung und der jüngsten Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) zu aktualisieren[4].

Mit der vorliegenden Arbeitsunterlage soll das Kapitel 1 der WP 12 in Bezug auf die zentrale Frage des angemessenen Datenschutzniveaus in einem Drittland, in einem Gebiet oder in einem oder mehreren spezifischen Sektoren in diesem Drittland oder in einer internationalen Organisation (im Folgenden: „Drittländer oder internationale Organisationen“) aktualisiert werden. Die vorliegende Arbeitsunterlage unterliegt einer laufenden Überprüfung und wird in den kommenden Jahren auf der Grundlage der praktischen Erfahrung mit der Anwendung der DSGVO gegebenenfalls aktualisiert. Kapitel 2 (*Anwendung des Ansatzes auf Länder, die das Übereinkommen Nr. 108 ratifiziert haben*) und 3 (*Anwendung des Ansatzes auf die Selbstkontrolle der Wirtschaft*) der WP 12 sollten zu einem späteren Zeitpunkt aktualisiert werden.

Die vorliegende Arbeitsunterlage betrifft ausschließlich Angemessenheitsbeschlüsse nach Artikel 45 der DSGVO, bei denen es sich um Durchführungsrechtsakte[5] der Europäischen Kommission handelt. Sonstige Aspekte der Übermittlungen personenbezogener Daten an Drittländer und internationale Organisationen werden in nachfolgenden Arbeitsunterlagen behandelt, die gesondert veröffentlicht werden (verbindliche interne Datenschutzvorschriften, Ausnahmen).

Das vorliegende Dokument soll eine Orientierungshilfe für die Europäische Kommission und die Artikel-29-Datenschutzgruppe nach der DSGVO für die Beurteilung des Datenschutzniveaus in Drittländern und internationalen Organisationen darstellen. Es sollen darin die wichtigsten datenschutzrechtlichen Grundsätze dargelegt werden, die im Rechtsrahmen eines Drittlands oder einer internationalen Organisation gegeben sein müssen, damit sichergestellt werden kann, dass dieser Rechtsrahmen der Sache nach gleichwertig mit dem Rechtsrahmen der EU ist. Darüber hinaus kann das Dokument auch Drittländern und internationalen Organisationen als Richtschnur dienen, die ein Interesse daran haben, Angemessenheit zu erreichen. Die in dieser Arbeitsunterlage dargelegten Grundsätze richten sich aber nicht unmittelbar an Verantwortliche oder Auftragsverarbeiter.

Das vorliegende Dokument ist in vier Kapitel gegliedert:

Kapitel 1: Allgemeine Informationen zum Begriff der Angemessenheit

Kapitel 2: Verfahrensrechtliche Aspekte von Angemessenheitsfeststellungen gemäß DSGVO

Kapitel 3: Allgemeine Datenschutzgrundsätze. In diesem Kapitel werden die wichtigsten allgemeinen Datenschutzgrundsätze behandelt, mit denen sichergestellt wird, dass das Datenschutzniveau in einem Drittland oder in einer internationalen Organisation der Sache nach gleichwertig mit dem Datenschutzniveau laut EU-Vorschriften ist.

Kapitel 4: Wesentliche Garantien hinsichtlich des Zugangs der Rechtdurchsetzungsbehörden und nationaler Sicherheitsbehörden zur Begrenzung des Eingriffs in die Grundrechte. In diesem Kapitel werden die wesentlichen Garantien hinsichtlich des Zugangs der Rechtdurchsetzungsbehörden und nationaler Sicherheitsbehörden behandelt, die mit dem Schrems-Urteil des Gerichtshofs aus dem Jahr

---

[1] Eingerichtet nach Artikel 29 der Datenschutzrichtlinie 95/46/EG der EU.

2 WP 12, „Arbeitsunterlage: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“, von der Arbeitsgruppe am 24. Juli 1998 angenommen.

3 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) (Text von Bedeutung für den EWR).

4 Einschließlich Rechtssache C‑362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015.

[5] Für weitere Informationen über die Durchführungsrechtsakte siehe einschlägige Artikel 45 Absatz 3 und Artikel 93 Absatz 2 der DSGVO.

2015 und auf der Grundlage der 2016 angenommenen Arbeitsunterlage der Artikel-29-Datenschutzgruppe in Bezug auf wesentliche Garantien festgelegt wurden.

Kapitel 1: Allgemeine Informationen zum Begriff der Angemessenheit

In Artikel 45 Absatz 1 der DSGVO ist der Grundsatz aufgeführt, dass Datenübermittlungen an ein Drittland oder an eine internationale Organisation nur dann zulässig sind, wenn das betreffende Drittland, das Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bieten.

Der Begriff „angemessenes Schutzniveau", der bereits im Rahmen der Richtlinie 95/46 existierte, wurde vom EuGH weiterentwickelt. An dieser Stelle sei an den Standard erinnert, der vom EuGH im Schrems-Urteil festgelegt wurde und der besagt, dass das „*Schutzniveau*" im Drittland zwar „*der Sache nach gleichwertig*" mit dem in der EU gewährleisteten Schutzniveau sein muss, doch „*die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, [können sich] von denen unterscheiden..., die in der Union herangezogen werden*"[6]. Das Ziel ist also nicht, die europäischen Vorschriften Punkt für Punkt wiederzugeben, sondern vielmehr die wesentlichen Kernanforderungen dieser Vorschriften festzulegen.

Zweck der Angemessenheitsbeschlüsse der Europäischen Kommission ist es, gegenüber den Mitgliedstaaten verbindlich zu bestätigen[7], dass das Datenschutzniveau in einem Drittland oder in einer internationalen Organisation der Sache nach gleichwertig mit dem Datenschutzniveau in der Europäischen Union ist[8]. Angemessenheit kann durch eine Kombination von gegenüber den Betroffenen eingeräumten Rechten, bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt, und die Aufsicht durch unabhängige Behörden erreicht werden. Datenschutzvorschriften sind allerdings nur dann wirksam, wenn sie durchsetzbar sind und in der Praxis eingehalten werden. Daher sind nicht nur der Inhalt der geltenden Vorschriften für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation zu beachten, sondern auch das System, mit dem die Wirksamkeit der Regeln gesichert werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit von Datenschutzvorschriften von wesentlicher Bedeutung.

In Artikel 45 Absatz 2 der DSGVO werden die verschiedenen Elemente festgelegt, welche die Europäische Kommission bei der Beurteilung der Angemessenheit des Schutzniveaus in einem Drittland oder in einer internationalen Organisation berücksichtigen soll.

So berücksichtigt die Kommission zum Beispiel die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, relevante Gesetzesbestimmungen, das Bestehen und wirksames Funktionieren einer oder mehrerer unabhängiger Aufsichtsbehörden sowie internationale Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen sind.

Vor diesem Hintergrund wird deutlich, dass die Analyse des angemessenen Schutzniveaus ohne die Einbeziehung der beiden folgenden Grundelemente sinnlos ist: Inhalt der geltenden Vorschriften und Mittel zur Sicherung ihrer wirksamen Anwendung. Die Europäische Kommission ist dafür verantwortlich, regelmäßig zu überprüfen, ob die bestehenden Vorschriften in der Praxis wirksam sind.

Der „Kern" der datenschutzrechtlichen Grundsätze hinsichtlich des „Inhalts" der Vorschriften sowie die „verfahrensrechtlichen/durchsetzungsbezogenen" Anforderungen, die als Mindestanforderung für die Angemessenheit des Schutzniveaus betrachtet werden können, ergeben sich aus der Charta der Grundrechte der Europäischen Union sowie aus der DSGVO. Darüber hinaus sollten auch die internationalen Datenschutzabkommen wie zum Beispiel das Übereinkommen Nr. 108[9] berücksichtigt werden.

---

[6] Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015 (Rdnrn. 73 und 74).

[7] Artikel 288 Absatz 2 AEUV.

[8] Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015 (Rdnr. 52).

9 Erwägungsgrund 105 der DSGVO.

Ferner muss auch der Rechtsrahmen für den Zugang von Behörden zu personenbezogenen Daten beachtet werden. Eine weitere Orientierungshilfe dazu bietet das Arbeitspapier WP 237 (Papier über die wesentlichen Garantien)[10] in Bezug auf Garantien im Zusammenhang mit der Überwachung.

Allgemeine Bestimmungen zum Schutz von Daten und der Privatsphäre im Drittland sind nicht ausreichend. Der Rechtsrahmen des Drittlands bzw. der internationalen Organisation muss vielmehr spezifische Bestimmungen für konkrete Bedürfnisse beinhalten, die in Bezug auf praxisrelevante Aspekte des Rechts auf Datenschutz bestehen. Diese Bestimmungen müssen durchsetzbar sein.

Kapitel 2: Verfahrensrechtliche Aspekte von Angemessenheitsfeststellungen gemäß DSGVO

Damit der EDSA seine Aufgabe nach Artikel 70 Absatz 1 Buchstabe s der DSGVO, die Kommission zu beraten, erfüllen kann, sollten dem EDSA relevante Dokumente, darunter einschlägige Korrespondenz und die Feststellungen der Europäischen Kommission, vorgelegt werden. Bei komplexen Rechtsrahmen sollte auch ein Bericht über das Datenschutzniveau in dem Drittland oder in der internationalen Organisation beiliegen. In jedem Fall sollten die von der Europäischen Kommission bereitgestellten Informationen umfassend sein und es dem EDSA ermöglichen, das Datenschutzniveau im betreffenden Drittland selbst zu beurteilen. Der EDSA wird zu den Feststellungen der Europäischen Kommission rechtzeitig Stellung nehmen und auf etwaige Mängel am Angemessenheitsrahmen hinweisen. Darüber hinaus wird sich der EDSA bemühen, zur Behebung möglicher Mängel Änderungen oder Ergänzungen vorzuschlagen.

Nach Artikel 45 Absatz 4 der DSGVO ist die Europäische Kommission dafür verantwortlich, jegliche Entwicklungen, die die Wirkungsweise eines Angemessenheitsbeschlusses beeinträchtigen könnten, fortlaufend zu überwachen.

Artikel 45 Absatz 3 der DSGVO sieht eine regelmäßige Überprüfung vor, die mindestens alle vier Jahre erfolgt. Es handelt sich dabei allerdings um einen allgemeinen Zeitrahmen, der je nach Drittland oder internationaler Organisation, für die ein Angemessenheitsbeschluss vorliegt, anzupassen ist. Je nach den besonderen Umständen des Einzelfalls kann ein kürzerer Überprüfungszyklus gerechtfertigt sein. Zudem können einzelne Vorfälle oder andere Informationen über den Rechtsrahmen des betreffenden Drittlands bzw. der betreffenden internationalen Organisation oder diesbezügliche Änderungen eine vorzeitige Überprüfung erforderlich machen. Außerdem scheint es angebracht, bei gänzlich neuen Angemessenheitsbeschlüssen recht zeitnah eine erste Überprüfung durchzuführen und den Überprüfungszyklus dann ergebnisabhängig nach und nach anzupassen.

Angesichts seines Auftrags, gegenüber der Europäischen Kommission dazu Stellung zu nehmen, ob ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau mehr gewährleisten, ist der EDSA darauf angewiesen, rechtzeitig aussagekräftige Informationen über die von der Kommission durchgeführte Überwachung der relevanten Entwicklungen in dem betreffenden Drittland oder in der internationalen Organisation zu erhalten. Der EDSA sollte also über alle Überprüfungsverfahren und -missionen in einem betreffenden Drittland oder bei einer internationalen Organisation informiert werden. Eine Einladung zur Teilnahme an diesen Überprüfungsverfahren und -missionen würde der EDSA begrüßen.

Ferner sollte darauf hingewiesen werden, dass die Kommission nach Artikel 45 Absatz 5 der DSGVO berechtigt ist, bestehende Angemessenheitsbeschlüsse zu widerrufen, zu ändern oder auszusetzen. Durch Ersuchen um eine Stellungnahme nach Artikel 70 Absatz 1 Buchstabe s sollte der EDSA folglich an Verfahren zum Widerruf, zur Änderung oder zum Aussetzen von Angemessenheitsbeschlüssen beteiligt werden.

Wie inzwischen von Artikel 58 Absatz 5 der DSGVO und im Schrems-Urteil des EuGH bestätigt, müssen die Datenschutzbehörden außerdem in der Lage sein, sich an gerichtlichen Verfahren zu

[10] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP 237 (Arbeitsunterlage 01/2016 über die Rechtfertigung von Eingriffen in die Grundrechte auf den Schutz der Privatsphäre und auf den Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (wesentliche europäische Garantien)), 13. April 2016.

beteiligen, wenn sie die Beschwerde einer Person gegen einen Angemessenheitsbeschluss als begründet erachten: *„Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen.*“[11].

Kapitel 3: Allgemeine Datenschutzgrundsätze zur Sicherstellung, dass das Schutzniveau in einem Drittland, einem Gebiet oder einem oder mehreren spezifischen Sektoren in diesem Drittland oder in einer internationalen Organisation der Sache nach gleichwertig mit dem Schutzniveau gemäß den EU-Vorschriften ist

Das System eines Drittlands oder einer internationalen Organisation muss folgende inhaltliche, verfahrensrechtliche und durchsetzungsbezogene Datenschutzgrundsätze und -mechanismen vorsehen:

A. <u>Inhaltliche Grundsätze:</u>

1) Begriffe

Es sollten grundlegende Datenschutzbegriffe und/oder -grundsätze bestehen. Die in der DSGVO verwendete Terminologie muss dabei zwar nicht übernommen werden, doch sie sollten die Begriffe, die im europäischen Datenschutzrecht verankert sind, widerspiegeln und mit diesen im Einklang stehen. Die DSGVO enthält beispielsweise folgende wichtigen Begriffe: „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „Verantwortlicher“, „Auftragsverarbeiter“, „Empfänger“ und „sensible Daten“.

2) Gründe für die rechtmäßige und faire Verarbeitung für legitime Zwecke

Die Verarbeitung von Daten muss auf rechtmäßige, faire und legitime Weise erfolgen.

Die legitimen Grundlagen, nach denen die rechtmäßige, faire und legitime Verarbeitung personenbezogener Daten zulässig ist, sollten ausreichend klar dargelegt werden. Der europäische Rahmen erkennt mehrere solcher legitimen Gründe an, wie etwa Bestimmungen nach nationalem Recht, die Einwilligung der betroffenen Person, die Erfüllung eines Vertrags oder das berechtigte Interesse des Verantwortlichen oder eines Dritten, solange die Interessen der betroffenen Person vorrangig bleiben.

3) Grundsatz der Zweckbindung

Die Daten sollten für einen bestimmten Zweck verarbeitet werden und folglich nur insoweit verwendet werden, als das dem Zweck der Verarbeitung nicht entgegensteht.

4) Grundsatz der Datenqualität und der Verhältnismäßigkeit

Die Daten sollten sachlich richtig sein und erforderlichenfalls auf den neuesten Stand gebracht werden. Die Daten sollten angemessen, relevant und im Hinblick auf die Zwecke, für die sie verarbeitet werden, nicht exzessiv sein.

5) Grundsatz der Datenspeicherung

Die Daten sollten im Allgemeinen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

[11] Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015 (Rdnr. 65).

6) Grundsatz der Sicherheit und der Vertraulichkeit

Jede Stelle, die personenbezogene Daten verarbeitet, sollte sicherstellen, dass die Daten so verarbeitet werden, dass die Sicherheit der personenbezogenen Daten gewährleistet ist, wozu auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor versehentlichen Verluste, Zerstörung oder Beschädigung gehört, durch Anwendung geeigneter technischer und organisatorischer Maßnahmen. Der Stand der Technik und die verbundenen Kosten sollten beim Sicherheitsniveau berücksichtigt werden.

7) Grundsatz der Transparenz

Die betroffenen Personen sollten in einer klaren, leicht zugänglichen, präzisen, transparenten und verständlichen Form über die wichtigsten Elemente der Verarbeitung ihrer personenbezogenen Daten informiert werden. Diese Informationen sollten den Zweck der Verarbeitung, die Identität des Verantwortlichen, die Rechte der betroffenen Person und andere Informationen erhalten, die zur Sicherung der Verarbeitung nach Treu und Glauben erforderlich sind. Unter bestimmten Bedingungen können Ausnahmen von diesem Informationsrecht anwendbar sein, beispielsweise zum Schutz von Strafermittlungen, zur Wahrung der nationalen Sicherheit oder der richterlichen Unabhängigkeit oder aber zur Sicherung von Rechtsverfahren oder anderer wichtiger Ziele des allgemeinen öffentlichen Interesses, wie dies beispielsweise bei Artikel 23 der DSGVO der Fall ist.

8) Recht auf Auskunft zu und Berichtigung oder Löschung personenbezogener Daten sowie Recht auf Widerspruch

Die betroffene Person sollte ein Recht auf Auskunft darüber haben, ob sie betreffende Daten verarbeitet werden oder nicht, sowie zum Zugang zu ihren Daten berechtigt sein, was auch das Recht miteinschließt, eine Kopie aller sie betreffenden verarbeiteten Daten zu erhalten.

Unter bestimmten Umständen, beispielsweise bei nachweislich unrichtigen oder unvollständigen Daten, sollte die betreffende Person das Recht auf Berichtigung ihrer Daten haben sowie ferner berechtigt sein, die Löschung ihrer Daten zu verlangen, wenn deren Verarbeitung zum Beispiel nicht mehr erforderlich oder unrechtmäßig ist.

Darüber hinaus sollte die betroffene Person berechtigt sein, aus zwingenden berechtigten Gründen in Verbindung mit ihrer Situation und unter bestimmten Umständen, die im Rechtsrahmen des Drittlands festgelegt sind, der Verarbeitung ihrer Daten jederzeit zu widersprechen. Laut DSGVO umfassen solche Umstände beispielsweise auch Situationen, in denen die Verarbeitung zur Erfüllung einer Aufgabe im öffentlichen Interesse oder für die Ausübung einer hoheitlichen Befugnis des Verantwortlichen erforderlich ist oder in denen die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist.

Die Ausübung dieser Rechte sollte für die betroffene Person nicht übermäßig aufwendig sein. Mögliche Einschränkungen dieser Rechte könnten beispielsweise dann bestehen, wenn es um den Schutz von Strafermittlungen, um die Wahrung der nationalen Sicherheit oder der richterlichen Unabhängigkeit, um die Sicherung von Rechtsverfahren oder um die Wahrung anderer wichtiger Ziele des allgemeinen öffentlichen Interesses geht, wie dies etwa bei Artikel 23 der DSGVO der Fall ist.

9) Einschränkungen bei der Weiterleitung von Daten

Die Weiterleitung der personenbezogenen Daten des ursprünglichen Empfängers der ursprünglichen Datenübermittlung sollte nur zulässig sein, wenn der weitere Empfänger (d. h. der Empfänger der weitergeleiteten Daten) ebenfalls Vorschriften (einschließlich vertraglichen Bestimmungen) unterliegt und dadurch ein angemessenes Schutzniveau gewährleistet und die einschlägigen Anweisungen für die Verarbeitung von Daten im Namen des Verantwortlichen befolgt. Das Schutzniveau natürlicher Personen, deren Daten übermittelt werden, darf durch die Weiterleitung der Daten nicht untergraben werden. Der ursprüngliche Empfänger von aus der EU übermittelten Daten ist verpflichtet sicherzustellen, dass ohne Vorliegen eines Angemessenheitsbeschlusses geeignete Garantien für die Weiterleitung der Daten gegeben sind. Solche Weiterleitungen von Daten sollten nur für begrenzte und bestimmte Zwecke erfolgen und solange es eine Rechtsgrundlage für die Verarbeitung gibt.

B. Beispiele für zusätzliche inhaltliche Grundsätze für bestimmte Arten der Verarbeitung:

1) Besondere Kategorien personenbezogener Daten

Betrifft die Verarbeitung besondere Kategorien personenbezogener Daten, sollten besondere Garantien bestehen[12]. Diese Kategorien sollten die in Artikel 9 und 10 der DSGVO verankerten Kategorien abbilden. Dieser Schutz sollte durch die Anwendung anspruchsvollerer Anforderungen an die Datenverarbeitung gewährleistet werden, wie etwa die Forderung, dass die betroffene Person ausdrücklich in die Verarbeitung einwilligt, oder durch zusätzliche Sicherheitsmaßnahmen.

2) Direktwerbung

Werden Daten verarbeitet, um Direktwerbung zu betreiben, sollte es für die betroffene Person jederzeit möglich sein, kostenlos Widerspruch gegen die Verarbeitung ihrer Daten zu diesen Zwecken einzulegen.

3) Automatisierte Entscheidungen und Profiling

Entscheidungen, die allein auf der Grundlage der automatisierten Verarbeitung (automatisierte Entscheidungen im Einzelfall) einschließlich Profiling beruhen, die eine rechtliche Wirkung für die betroffene Person entfalten oder sie erheblich beeinträchtigen, sind nur unter bestimmten Bedingungen zulässig, die im Rechtsrahmen des Drittlands festzulegen sind. Im europäischen Rahmen umfassen diese Bedingungen zum Beispiel das Erfordernis, die ausdrückliche Einwilligung der betroffenen Person einzuholen, oder die Notwendigkeit einer solchen Entscheidung zum Abschluss eines Vertrags. Steht die Entscheidung nicht im Einklang mit den im Rechtsrahmen des Drittlands festgelegten Bedingungen, sollte die betroffene Person das Recht haben, ihr nicht zu unterliegen. In jedem Fall sollten nach dem Recht des Drittlands die erforderlichen Garantien gewährleistet werden, einschließlich des Rechts auf Unterrichtung über die besonderen Gründe, die der Entscheidung und der angewandten Logik zugrunde liegen, um unrichtige und unvollständige Angaben zu berichtigen und die Entscheidung anzufechten, falls sie auf der Grundlage einer falschen Sachlage getroffen wurde.

C. Verfahrens- und Durchsetzungsmechanismen:

Obwohl die Mittel, auf die ein Drittland zur Sicherstellung eines angemessenen Schutzniveaus zurückgreifen kann, von den Mitteln der Europäischen Union[13] abweichen können, muss ein System, das im Einklang mit dem europäischen System steht, folgende Elemente aufweisen:

1) Zuständige unabhängige Aufsichtsbehörden

Es sollte eine oder mehrere unabhängige Aufsichtsbehörden geben, die mit der Überwachung, Sicherstellung und Durchsetzung der Einhaltung von Datenschutz- und Bestimmungen zum Schutz der Privatsphäre im Drittland beauftragt sind. Die Aufsichtsbehörde hat bei der Erfüllung ihrer Pflichten und Ausübung ihrer Befugnisse völlig unabhängig zu handeln und darf dabei weder Anweisungen einholen noch entgegennehmen. In diesem Zusammenhang sollte die Aufsichtsbehörde über alle erforderlichen und verfügbaren Befugnisse und Aufträge verfügen, um die Achtung der Datenschutzrechte sicherzustellen und für ein größeres Bewusstsein zu sorgen. Darüber hinaus sind

[12] Diese besonderen Kategorien von Daten werden in Erwägungsgrund 10 der DSGVO auch als „sensible Daten" bezeichnet.

[13] Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015, Rdnr. 74.

auch das Personal und der Haushalt der Aufsichtsbehörde zu beachten. Ferner sollte die Aufsichtsbehörde in der Lage sein, auf eigene Initiative Untersuchungen durchzuführen.

2) Das Datenschutzsystem muss ein hohes Maß an Konformität gewährleisten

Das System eines Drittlands sollte ein hohes Maß an Rechenschaftspflicht und Bewusstsein seitens der Verantwortlichen und derjenigen, die in ihrem Namen personenbezogene Daten verarbeiten, über deren Pflichten, Aufgaben und Verantwortlichkeiten sowie seitens der betroffenen Personen über deren Rechte und Mittel zu deren Ausübung sicherstellen. Das Bestehen wirksamer und abschreckender Sanktionen kann eine wichtige Rolle dabei spielen, die Einhaltung von Vorschriften sicherzustellen, was natürlich auch durch unmittelbare Überprüfungen durch Behörden, Prüfer oder unabhängige Datenschutzbeauftragte erreicht werden kann.

3) Rechenschaftspflicht

Der Datenschutzrahmen eines Drittlands sollte die Verantwortlichen und/oder diejenigen, die in ihrem Namen personenbezogene Daten verarbeiten, zu dessen Einhaltung und dazu verpflichten, diese Einhaltung insbesondere gegenüber der zuständigen Aufsichtsbehörde nachzuweisen. Solche Maßnahmen können beispielsweise Datenschutz-Folgenabschätzungen, das Führen von Aufzeichnungen oder Protokolldateien der Datenverarbeitungstätigkeiten für einen angemessenen Zeitraum, die Benennung eines Datenschutzbeauftragten oder Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen umfassen.

4) Das Datenschutzsystem muss betroffenen Einzelpersonen bei der Ausübung ihrer Rechte Unterstützung und Hilfe sowie angemessene Rechtsschutzverfahren bieten

Die betroffene Person sollte in der Lage sein, zur Durchsetzung ihrer Rechte sowie zur Sicherstellung der Einhaltung der Vorschriften schnell und wirksam sowie ohne prohibitive Kosten Rechtsbehelfe in Anspruch zu nehmen. Dazu sind Überwachungsmechanismen erforderlich, die eine unabhängige Untersuchung von Beschwerden ermöglichen und dafür sorgen, dass Verletzungen des Rechts auf Datenschutz und auf die Achtung der Privatsphäre identifiziert und praktisch bestraft werden.

Bei mangelnder Einhaltung von Vorschriften sollten der betroffenen Person auch wirksame administrative und gerichtliche Abhilfen zur Verfügung stehen, einschließlich zur Forderung von Schadensersatz wegen unrechtmäßiger Verarbeitung ihrer personenbezogenen Daten. Es handelt sich dabei um ein Schlüsselelement, bei dem zwingend ein System der unabhängigen Entscheidungsfindung oder ein System unabhängiger Schiedsverfahren vorzusehen ist, in dem gegebenenfalls die Zahlung von Schadensersatz sowie die Auferlegung von Sanktionen möglich sind.

Kapitel 4: Wesentliche Garantien in Drittländern hinsichtlich der Rechtsdurchsetzung und hinsichtlich des Zugangs nationaler Sicherheitsbehörden zur Begrenzung des Eingriffs in Grundrechte

Bei der Beurteilung der Angemessenheit des Schutzniveaus ist die Kommission laut Artikel 45 Absatz 2 Buchstabe a verpflichtet, die „*geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften...*“ zu berücksichtigen.

In seinem Schrems-Urteil wies der EuGH darauf hin, dass „*der Ausdruck ‚angemessenes Schutzniveau‘ jedoch so zu verstehen [ist], dass verlangt wird, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist*.“ Auch wenn sich die Mittel, auf die dieses Drittland insoweit zurückgreift, von denen unterscheiden können, die in der Union herangezogen werden, müssen sich diese Mittel in der Praxis gleichwohl als wirksam erweisen.[14]

[14] Rs. C-362/14, Maximilian Schrems/Data Protection Commissioner, 6. Oktober 2015, Rdnr. 74.

In diesem Zusammenhang hat das Gericht außerdem entscheidend darauf hingewiesen, dass die frühere Safe-Harbor-Entscheidung „*keine Feststellung dazu [enthielt], ob es in den Vereinigten Staaten staatliche Regeln gibt, die dazu dienen, etwaige Eingriffe – zu denen die staatlichen Stellen dieses Landes in Verfolgung berechtigter Ziele wie der nationalen Sicherheit berechtigt wären – in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen.*“

Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme WP 237, die am 13. April 2016 angenommen wurde, wesentliche Garantien aufgeführt, die die Rechtsprechung des EuGH und des EGMR im Bereich der Überwachung widerspiegeln. Die Empfehlungen der WP 237 bleiben zwar gültig und sollten bei der Beurteilung der Angemessenheit eines Drittlands in Bezug auf die Überwachung zwar berücksichtigt werden, doch die Anwendung dieser Garantien darf in den Bereichen des Zugangs der Rechtdurchsetzungsbehörden und nationaler Sicherheitsbehörden zu Daten abweichen. In Bezug auf den Zugang zu Daten – ob zur Wahrung der nationalen Sicherheit oder zum Zwecke der Rechtsdurchsetzung – müssen dennoch alle Drittländer, die als angemessen gelten wollen, diese vier Garantien einhalten:

1) **Die Verarbeitung sollte auf der Grundlage von klaren, präzisen und zugänglichen Vorschriften erfolgen (Rechtsgrundlage).**

2) **Die Erforderlichkeit und Verhältnismäßigkeit in Bezug auf die berechtigten Ziele muss nachgewiesen werden.**

3) **Die Verarbeitung muss einer unabhängigen Aufsicht unterliegen.**

4) **Den betroffenen Personen müssen wirksame Rechtsbehelfe zur Verfügung stehen.**