Stellungnahme 32/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Datenschutzniveaus in der Republik Korea

Version 1.0

Angenommen am 24. September 2021

INHALT

1. ZUSAMMENFASSUNG 4
1.1. Bereiche möglicher Konvergenz 5
1.2. Herausforderungen 5
1.2.1. Allgemeines 5
1.2.2. Allgemeine Datenschutzaspekte 6
1.2.3. Über den Zugang von Behörden zu an die Republik Korea übermittelten Daten 7
1.3. Schlussfolgerung 8
2. EINLEITUNG 8
2.1. Der koreanische Datenschutzrahmen 8
2.2. Umfang der Beurteilung durch den EDSA 10
2.3. Allgemeine Bemerkungen und Bedenken 11
2.3.1. Von der Republik Korea eingegangene internationale Verpflichtungen 11
2.3.2. Anwendungsbereich des Angemessenheitsbeschlusses 11
3. ALLGEMEINE ASPEKTE DES DATENSCHUTZES 12
3.1. Inhaltliche Grundsätze 12
3.1.1. Begriffe 13
3.1.2. Im PIPA vorgesehene teilweise Ausnahmen 15
3.1.3. Voraussetzungen für eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu legitimen Zwecken 17
3.1.4. Grundsatz der Zweckbindung 18
3.1.5. Grundsatz der Datenqualität und der Verhältnismäßigkeit 19
3.1.6. Grundsatz der Datenspeicherung 19
3.1.7. Grundsatz der Sicherheit und Vertraulichkeit 20
3.1.8. Grundsatz der Transparenz 20
3.1.9. Besondere Kategorien personenbezogener Daten 21
3.1.10. Recht auf Auskunft, Berichtigung, Löschung und Widerspruch 22
3.1.11. Beschränkungen für Weiterübermittlungen 25
3.1.12. Direktwerbung 27
3.1.13. Automatisierte Entscheidungsfindung und Profiling 27
3.1.14. Rechenschaftspflicht 28
3.2. Verfahrens- und Durchsetzungsmechanismen 29
3.2.1. Zuständige unabhängige Aufsichtsbehörde 29

3.2.2. Vorhandensein eines Datenschutzsystems, das ein gutes Maß an Einhaltung der Vorschriften gewährleistet 30

3.2.3. Das Datenschutzsystem muss betroffenen Personen bei der Ausübung ihrer Rechte Unterstützung und Hilfe sowie angemessene Rechtsbehelfsverfahren bieten 31

4. ZUGANG ZU PERSONENBEZOGENEN DATEN UND VERWENDUNG VON PERSONENBEZOGENEN DATEN, DIE AUS DER EUROPÄISCHEN UNION AN BEHÖRDEN IN SÜDKOREA ÜBERMITTELT WERDEN 32

4.1. Allgemeiner Datenschutzrahmen im Zusammenhang mit dem Zugang staatlicher Stellen 32

4.2. Schutz und Garantien für Kommunikationsbestätigungsdaten im Zusammenhang mit dem Zugang staatlicher Stellen zu Strafverfolgungszwecken 33

4.3. Zugang koreanischer Behörden zu Kommunikationsdaten für Zwecke der nationalen Sicherheit 34

4.3.1. Keine Verpflichtung, Personen über den Zugang staatlicher Stellen zur Kommunikation zwischen ausländischen Staatsangehörigen zu unterrichten 35

4.3.2. Keine vorherige unabhängige Genehmigung für die Erhebung von Daten über die Kommunikation zwischen Ausländern 36

4.4. Freiwillige Offenlegung 38

4.5. Weiterverwendung von Daten 38

4.5. Weiterübermittlungen und Austausch nachrichtendienstlicher Erkenntnisse 39

4.6.1. Geltender Rechtsrahmen für Weiterübermittlungen durch Strafverfolgungsbehörden 40

4.6.2. Geltender Rechtsrahmen für Weiterübermittlungen für Zwecke der nationalen Sicherheit 41

4.6.3. Internationale Abkommen 42

4.7. Aufsicht 42

4.8. Gerichtlicher Rechtsbehelf und Rechtsmittel 43

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 („**DSGVO**“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum („**EWR**“), 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[1],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. ZUSAMMENFASSUNG

1. Die Europäische Kommission hat das förmliche Verfahren zur Annahme ihres Entwurfs eines Durchführungsbeschlusses („**Beschlussentwurf**“) über den angemessenen Schutz personenbezogener Daten in der Republik Korea nach dem Gesetz über den Schutz personenbezogener Daten gemäß der DSGVO am 16. Juni 2021 eingeleitet.[2]

2. Am gleichen Tag ersuchte die Europäische Kommission den Europäischen Datenschutzausschuss („**EDSA**“) um eine Stellungnahme.[3] Der EDSA stützte seine Bewertung der Angemessenheit des in der Republik Korea gewährten Schutzniveaus auf eine Prüfung des Beschlussentwurfs selbst sowie auf eine Auswertung der von der Europäischen Kommission bereitgestellten Unterlagen[4].

3. In den Mittelpunkt seiner Beurteilung stellte der EDSA sowohl die allgemeinen auf die DSGVO bezogenen Aspekte des Beschlussentwurfs als auch den Zugriff von Behörden auf personenbezogene Daten, die aus dem EWR für Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt werden, einschließlich der Rechtsbehelfe, die Personen im EWR zur Verfügung stehen. Der EDSA prüfte ferner, ob die im koreanischen Rechtsrahmen vorgesehenen Garantien tatsächlich vorhanden und wirksam sind.

4. Als Maßstab für diese Prüfungsarbeit hat der EDSA seine im Februar 2018 angenommene Referenzgrundlage für die Angemessenheit im Sinne der DSGVO[5] („**DSGVO-Referenzgrundlage für Angemessenheit**“) sowie die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen[6] verwendet.

[1] Soweit in dieser Stellungnahme von „**Mitgliedstaaten**“ die Rede ist, sind damit die Mitgliedstaaten des EWR gemeint.
[2] Siehe die Pressemitteilung https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ebenda.
[4] Der EDSA stützte seine Analyse auf offizielle Übersetzungen der koreanischen Regierung.
[5] WP 254, Referenzgrundlage für Angemessenheit, 6. Februar 2018 (vom EDSA gebilligt, siehe https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Siehe EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Konvergenzbereiche

5. Hauptziel des EDSA ist es, der Europäischen Kommission eine Stellungnahme zur Angemessenheit des Schutzniveaus für Personen vorzulegen, deren personenbezogene Daten an die Republik Korea übermittelt werden. Natürlich erwartet der EDSA nicht, dass der koreanische Rechtsrahmen das europäische Datenschutzrecht nachbildet.

6. Der EDSA weist jedoch darauf hin, dass nach Artikel 45 DSGVO und nach der Rechtsprechung des Gerichtshofs der Europäischen Union („**EuGH**“) die Rechtsvorschriften des Drittlandes an die in der DSGVO verankerten Grundsätze im Wesentlichen angeglichen sein müssen, damit davon ausgegangen werden kann, dass sie ein angemessenes Schutzniveau bieten. Diesbezüglich weist der koreanische Datenschutzrahmen zahlreiche Ähnlichkeiten mit dem europäischen Datenschutzrahmen auf – so besteht dieser aus einer allgemeinen Gesetzgebung, die sowohl für den öffentlichen als auch für den nichtöffentlichen Bereich gilt, und welche durch bereichsspezifische Gesetze ergänzt wird,.

7. Inhaltlich stellt der EDSA fest, dass es Schlüsselbereiche der Angleichung zwischen dem von der DSGVO gebotenen Rahmen und dem koreanischen Datenschutzrahmen in Bezug auf wesentliche Bestimmungen gibt, beispielsweise bei den Begriffen (z. B. „personenbezogene Informationen“, „Verarbeitung“, „betroffene Person“); Grundlagen für eine rechtmäßige Verarbeitung nach Treu und Glauben für legitime Zwecke; Zweckbindung: Datenqualität und Verhältnismäßigkeit; Datenspeicherung, Datensicherheit und Vertraulichkeit; Transparenz und besondere Kategorien von Daten.

8. Darüber hinaus begrüßt der EDSA die Bemühungen der Europäischen Kommission und der koreanischen Behörden, dafür zu sorgen, dass die Republik Korea ein der DSGVO angemessenes Schutzniveau bietet, bspw. durch die Verabschiedung von Notifizierungen seitens der koreanischen Aufsichtsbehörde – die in ihrem Anwendungsbereich nicht nur auf vom EWR nach Korea übermittelte personenbezogene Daten, beschränkt ist – mit dem Ziel, die Lücken zwischen der DSGVO und dem koreanischen Datenschutzrahmen zu schließen. In diesem Zusammenhang möchte der EDSA die Relevanz dieser Notifizierungen für die Bewertung der Angemessenheit der Republik Korea unterstreichen und beispielsweise darauf hinweisen, dass sie wichtige Klarstellungen zu einigen wichtigen Garantien enthalten, unter anderem in Bezug auf den Anwendungsbereich der Ausnahmen vom PIPA für die Verarbeitung pseudonymisierter personenbezogener Informationen für wissenschaftliche, Forschungs- und statistische Zwecke, Weiterübermittlungen und die im Zusammenhang mit dem Zugriff auf Daten durch Behörden anwendbaren Vorschriften.

1.2. Herausforderungen

9. Der EDSA hat zwar festgestellt, dass viele Aspekte des koreanischen Datenschutzrahmens im Wesentlichen dem europäischen Datenschutzrahmen gleichwertig sind, er kam aber auch zu dem Schluss, dass bestimmte Aspekte einer genaueren Betrachtung und Klärung bedürfen. Nach Auffassung des EDSA sollten im Einzelnen folgende Punkte weiter geprüft werden, um sicherzustellen, dass ein der Sache nach gleichwertiges Schutzniveau erreicht wird, und die Europäische Kommission diese Punkte genau überwachen sollte.

1.2.1. Allgemeines

10. Der EDSA nimmt zur Kenntnis, dass die Notifizierung Nr. 2021-1 *den Status einer rechtsverbindlichen Verwaltungsvorschrift für den für die Verarbeitung personenbezogener Informationen Verantwortlichen in dem Sinne hat, dass jeder Verstoß gegen die Notifizierung als Verstoß gegen die einschlägigen Bestimmungen des PIPA betrachtet werden kann.*[7] In Anbetracht der Tatsache, dass die Notifizierung an sich keine zusätzlichen Vorschriften enthält, sondern vielmehr Klarstellungen

[7] Siehe Anhang I Abschnitt I des Beschlussentwurfs.

darüber, wie der Gesetzestext des PIPA anzuwenden ist, und angesichts ihrer Bedeutung im Allgemeinen, insbesondere im Hinblick auf die Pseudonymisierungsbestimmungen des PIPA, die nach Verständnis des EDSA Gegenstand laufender Gerichtsverfahren sind, ersucht der EDSA die Europäische Kommission um weitere Informationen über den verbindlichen Charakter, die Durchsetzbarkeit und die Gültigkeit der Notifizierung Nr. 2021-1 und empfiehlt eine aufmerksame Überwachung dieser Aspekte in der Praxis, insbesondere im Hinblick auf ihre Anwendung nicht nur durch die koreanische Aufsichtsbehörde, sondern auch durch Gerichte, vor allem in Fällen, in denen sich das vom koreanischen Rechtsrahmen gebotene gleichwertige Schutzniveau auf die darin enthaltenen Klarstellungen stützt.

1.2.2. Allgemeine Aspekte des Datenschutzes

11. In Bezug auf den Anwendungsbereich des Angemessenheitsbeschlusses stellt der EDSA fest, dass er Übermittlungen aus dem EWR-Rechtsrahmen sowohl an öffentliche als auch an nichtöffentliche „für die Verarbeitung personenbezogener Informationen Verantwortliche“, die in den Anwendungsbereich des PIPA fallen, erfassen wird. Der EDSA geht davon aus, dass Stellen, die als Auftragsverarbeiter im Sinne der DSGVO fungieren, ebenfalls unter diesen Begriff fallen. Um jedoch Missverständnisse zu vermeiden, fordert er die Europäische Kommission auf, deutlicher zu machen, dass der Angemessenheitsbeschluss auch Datenübermittlungen an „Auftragsverarbeiter“ in Korea abdeckt.

12. Ein wichtiger Aspekt, auf den der EDSA aufmerksam machen möchte, ist das Konzept der pseudonymisierten Informationen im koreanischen Datenschutzrahmen. Nach koreanischem Recht gelten für die Verarbeitung pseudonymisierter personenbezogener Informationen Ausnahmen von einer Reihe einschlägiger Bestimmungen, einschließlich der Bestimmungen über die Rechte der betroffenen Person und die Datenspeicherung. Nach Ansicht der Europäischen Kommission trifft dies nur zu, wenn pseudonymisierte personenbezogene Informationen zu im öffentlichen Interesse liegenden statistischen Zwecken, wissenschaftlichen Forschungszwecken oder Archivzwecken verarbeitet werden. Diese Annahme wird jedoch hauptsächlich durch die Notifizierung Nr. 2021-1 gestützt, die die bereits erwähnte Notwendigkeit zusätzlicher Informationen und der Überwachung der Verbindlichkeit, Durchsetzbarkeit und Gültigkeit dieser Notifizierung in diesem Zusammenhang äußerst relevant macht. Darüber hinaus ersucht der EDSA die Europäische Kommission, näher zu prüfen, wie sich die Pseudonymisierung nach koreanischem Recht auswirkt und vor allem wie sie sich auf die Grundrechte und Grundfreiheiten der betroffenen Personen auswirken kann, deren personenbezogene Daten im Rahmen des Angemessenheitsbeschlusses an die Republik Korea übermittelt werden. Insbesondere fordert der EDSA die Europäische Kommission auf, die in Artikel 28 Absatz 7 PIPA und Artikel 40 Absatz 3 CIA vorgesehenen Ausnahmen weiter zu prüfen und ihre Anwendung und die einschlägige Rechtsprechung aufmerksam zu überwachen, um sicherzustellen, dass die Rechte der betroffenen Person nicht ungebührlich eingeschränkt werden, wenn auf Grundlage des Angemessenheitsbeschlusses übermittelte personenbezogene Daten für diese Zwecke verarbeitet werden.

13. Darüber hinaus stellt der EDSA fest, dass nach koreanischem Recht ein Recht auf Widerruf der Einwilligung nur unter bestimmten Umständen besteht, und fordert die Europäische Kommission daher auf, die Auswirkungen des Fehlens eines allgemeinen Rechts auf Widerruf der Einwilligung weiter zu prüfen und weitere Zusicherungen zu geben, um sicherzustellen, dass jederzeit ein wesentliches Datenschutzniveau gewährleistet ist, erforderlichenfalls auch, indem die Rolle des Rechts auf Aussetzung nach dem PIPA in Ermangelung eines allgemeinen Rechts auf Widerruf der Einwilligung klargestellt wird.

14. In Bezug auf Weiterübermittlungen erkennt der EDSA an, dass die informierte Einwilligung der betroffenen Person in der Regel als Grundlage für Datenübermittlungen von einem in Korea niedergelassenen für die Verarbeitung personenbezogener Informationen Verantwortlichen an einen

in einem Drittland niedergelassenen Empfänger verwendet wird und dass gemäß der Notifizierung Nr. 2021-1 Personen über das Drittland unterrichtet werden müssen, an das ihre Daten übermittelt werden. Der EDSA fordert die Europäische Kommission jedoch auf, dafür zu sorgen, dass die der betroffenen Person bereitzustellenden Angaben auch Informationen über solche möglichen Risiken von Datenübermittlungen enthalten, die sich aus dem Fehlen eines angemessenen Schutzes in dem Drittland ergeben, sowie über das Fehlen geeigneter Garantien. Darüber hinaus würde der EDSA im Angemessenheitsbeschluss enthaltene Zusicherungen dahingehend begrüßen, dass personenbezogene Daten nicht von koreanischen Verantwortlichen an ein Drittland übermittelt werden, wenn keine nach der DSGVO gültige Einwilligung erteilt werden könnte, z. B. wegen eines Machtungleichgewichts.

15. Was die Ernennung der Mitglieder der koreanischen Aufsichtsbehörde betrifft, so würde das formelle Verfahren zwar im Einklang mit der DSGVO stehen und daher den Gleichwertigkeitstest mit dem EWR-Rechtsrahmen bestehen, doch würde der EDSA es begrüßen, wenn die Europäische Kommission alle Entwicklungen im Auge behalten würde, die die Unabhängigkeit der Mitglieder der südkoreanischen Aufsichtsbehörde beeinträchtigen könnten.

16. Betreffend den Haushalt wird, wiederum nach den von der Europäischen Kommission vorgelegten Informationen, weder auf die Besonderheiten des der PIPC zugewiesenen Personals noch auf die ihr zur Verfügung gestellten Finanzmittel Bezug genommen. Der EDSA würde daher zusätzliche Informationen im Beschlussentwurf zu diesen beiden wichtigen Themen begrüßen.

1.2.3. Über den Zugriff von Behörden auf an die Republik Korea übermittelte Daten

17. Der EDSA hat den koreanischen Rechtsrahmen auch in Bezug auf den Zugriff staatlicher Stellen auf aus dem EWR nach Korea übermittelte personenbezogenen Daten für Zwecke der Strafverfolgung und der nationalen Sicherheit analysiert. Der EDSA nimmt die in Anhang II des Beschlussentwurfs dargelegten Erklärungen und Zusicherungen der koreanischen Regierung zur Kenntnis, sieht aber dennoch eine Reihe von Aspekten, die einer Klärung bedürfen oder Bedenken aufwerfen.

18. Der EDSA stellt fest, dass die Bestimmungen des PIPA für den Bereich der Strafverfolgung uneingeschränkt gelten. Der EDSA stellt ferner fest, dass die Datenverarbeitung im Bereich der nationalen Sicherheit einem begrenzteren Katalog von Bestimmungen des PIPA unterliegt.

19. In Bezug auf die freiwillige Offenlegung personenbezogener Informationen durch Telekommunikationsanbieter gegenüber nationalen Sicherheitsbehörden hat der EDSA Bedenken darüber, dass das Verhältnis zwischen Anhang I Abschnitt 3 des Beschlussentwurfs, in dem festgelegt ist, dass Anbieter grundsätzlich die betroffene Person unterrichten müssen, wenn sie einem entsprechenden Ersuchen freiwillig nachkommen, und Artikel 58 Absatz 1 Ziffer 2 PIPA über die teilweise Befreiung von dieser Pflicht aus Gründen der nationalen Sicherheit unklar ist. Dadurch könnten Informationspflichten wirkungslos werden, sodass es betroffenen Personen erheblich erschwert wäre, ihre Datenschutzrechte und insbesondere Rechtsschutzmöglichkeiten geltend zu machen.

20. Obwohl dies im Beschlussentwurf nicht ausdrücklich vorgesehen ist, entnimmt der EDSA den Erläuterungen der Europäischen Kommission, dass der koreanische Rechtsrahmen die Massenerhebung von Telekommunikationsdaten nicht zulässt. Daher wäre die jüngste Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte („**EGMR**“) zu massenweisen Datenerhebung für die Beurteilung des Datenschutzniveaus in Korea nicht unmittelbar relevant.

21. Zum Rechtsrahmen für Weiterübermittlungen im Bereich der nationalen Sicherheit enthält der Beschlussentwurf keine Informationen. Der EDSA geht zwar davon aus, dass nach Ansicht der Europäischen Kommission Weiterübermittlungen für Zwecke der nationalen Sicherheit durch die allgemeinen Garantien und Grundsätze, die sich aus dem verfassungsrechtlichen Rahmen und dem

PIPA ergeben, ausreichend geregelt sind, hat jedoch Bedenken, ob dies den Anforderungen der Normenklarheit entspricht sowie wirksame und durchsetzbare Garantien vorsieht. Die Garantien, auf die sich die Europäische Kommission bezieht, sind sehr allgemein gehalten und regeln nicht als Rechtsgrundlage die besonderen Umstände und Bedingungen, unter denen Weiterübermittlungen für Zwecke der nationalen Sicherheit erfolgen dürfen. In diesem Zusammenhang stellt der EDSA auch fest, dass die Europäische Kommission das Bestehen internationaler Abkommen zwischen der Republik Korea und Drittländern oder internationalen Organisationen, die spezifische Bestimmungen für die internationale Übermittlung personenbezogener Daten durch Strafverfolgungsbehörden und/oder Nachrichtendienste an Drittländer enthalten könnten, nicht berücksichtigt hat. Nach Auffassung des EDSA könnte sich der Abschluss bilateraler oder multilateraler Abkommen mit Drittländern für Zwecke der Strafverfolgung oder der nachrichtendienstlichen Zusammenarbeit auf den koreanischen Datenschutzrechtsrahmen in der beurteilten Fassung auswirken.

22. Der EDSA stellt fest, dass die Aufsicht über Strafverfolgungsbehörden und nationale Sicherheitsbehörden durch eine Kombination verschiedener interner und externer Stellen gewährleistet wird, insbesondere durch die PIPC, die mit ausreichenden Exekutivbefugnissen ausgestattet ist.

23. Wirksame Rechtsbehelfe und Rechtsmittel setzen voraus, dass sich betroffene Personen an eine zuständige Stelle wenden können, die die Anforderungen von Artikel 47 der Charta der Grundrechte der Europäischen Union („**Charta**“) erfüllt. D.h. eine Stelle, die dafür zuständig ist, festzustellen, dass eine Datenverarbeitung stattfindet, die Rechtmäßigkeit der Verarbeitung zu überprüfen, und die über durchsetzbare Abhilfebefugnisse verfügt, wenn die Datenverarbeitung unrechtmäßig ist. Vor diesem Hintergrund ersucht der EDSA die Europäische Kommission um Klarstellung, ob eine Beschwerde bei der PIPC oder eine Klage vor einem Gericht materiell- und/oder verfahrensrechtlichen Anforderungen, wie etwa einer Beweislastregelung, unterliegt und ob Personen im EWR in der Lage wären, diese Voraussetzung zu erfüllen.

1.3. Schlussfolgerung

24. Der EDSA ist der Auffassung, dass dieser Angemessenheitsbeschluss von allergrößter Bedeutung ist, auch unter Berücksichtigung der Tatsache, dass er – abgesehen von den in der Stellungnahme hervorgehobenen Ausnahmen – Übermittlungen sowohl im öffentlichen als auch im nichtöffentlichen Bereich abdecken wird.

25. Der EDSA begrüßt die Bemühungen der Europäischen Kommission und der koreanischen Behörden, den koreanischen Rechtsrahmen an den europäischen Rechtsrahmen anzugleichen. Die mit der Notifizierung Nr. 2021-1 angestrebten Verbesserungen zur Überbrückung einiger der Unterschiede zwischen den beiden Regelwerken sind äußerst wichtig und begrüßenswert. Der EDSA stellt jedoch fest, dass eine Reihe von Bedenken, auch in Bezug auf die Notifizierung Nr. 2021-1, in Verbindung mit der Notwendigkeit weiterer Klarstellungen zu anderen Fragen bestehen bleibt und empfiehlt der Europäischen Kommission, auf die vom EDSA geäußerten Bedenken und Bitten um Klarstellung einzugehen und weitere Informationen und Erläuterungen zu den in dieser Stellungnahme aufgeworfenen Fragen vorzulegen.

2. EINLEITUNG

2.1. Der koreanische Datenschutzrahmen

26. Das wichtigste Gesetz für den Datenschutz in der Republik Korea ist das Gesetz über den Schutz personenbezogener Informationen (Gesetz Nr. 10465 vom 29. März 2011, zuletzt geändert durch das Gesetz Nr. 16930 vom 4. Februar 2020, auf Englisch: *Personal Information Protection Act*, „**PIPA**“). Ergänzt wird das Gesetz durch einen Durchführungserlass (Präsidentialerlass Nr. 23169 vom

29. September 2011, zuletzt geändert durch Präsidentialerlass Nr. 30892 vom 4. August 2020, „PIPA-Durchführungserlass“), der rechtsverbindlich und durchsetzbar ist.

27. Neben dem PIPA umfasst der koreanische Datenschutzrahmen auch behördliche „Notifizierungen“ der koreanischen Aufsichtsbehörde, der Kommission für den Schutz personenbezogener Informationen (auf Englisch: *Personal Information Protection Commission*, „**PIPC**“), die weitere Bestimmungen für die Auslegung und Anwendung des PIPA enthalten. Vor kurzem verabschiedete die PIPC die Notifizierung Nr. 2021-1 vom 21. Januar 2021 (mit der die vorherige Notifizierung Nr. 2020-10 vom 1. September 2020 geändert wurde) („**Notifizierung Nr. 2021-1**“) über die Auslegung, Anwendung und Durchsetzung bestimmter Bestimmungen des PIPA. Diese Notifizierung war das Ergebnis insbesondere der Angemessenheitsgespräche zwischen den koreanischen Behörden und der Europäischen Kommission. Sie enthält Klarstellungen zur Anwendung spezifischer Bestimmungen des PIPA, unter anderem in Bezug auf die Verarbeitung personenbezogener Daten, die nach Korea auf der Grundlage des geplanten Angemessenheitsbeschlusses übermittelt werden[8], und *hat den Status einer rechtsverbindlichen Verwaltungsvorschrift für den für die Verarbeitung personenbezogener Informationen Verantwortlichen in dem Sinne, dass jeder Verstoß gegen die Notifizierung als Verstoß gegen die einschlägigen Bestimmungen des PIPA betrachtet werden kann*[9]. In diesem Zusammenhang möchte der EDSA darauf hinweisen, dass die Notifizierung, obwohl sie im Beschlussentwurf als „Ergänzende Vorschriften“ bezeichnet wird, an sich keine zusätzlichen Vorschriften enthält, sondern eher Erläuterungen, mit denen klargestellt werden soll, wie der Gesetzestext des PIPA zu verstehen ist, insbesondere in Bezug auf Daten, die aus dem EWR übermittelt werden. Vor diesem Hintergrund empfiehlt der EDSA eine aufmerksame Überwachung der Einhaltung der Notifizierung Nr. 2021-1 in der Praxis, insbesondere im Hinblick auf ihre Anwendung nicht nur durch die PIPC, sondern auch durch Gerichte, vor allem in Fällen, in denen sich das vom koreanischen Rechtsrahmen gebotene gleichwertige Schutzniveau auf die in der Notifizierung Nr. 2021-1 enthaltenen Klarstellungen stützt.

28. Andere einschlägige Datenschutzgesetze im koreanischen Rechtsrahmen enthalten Bestimmungen für die Verarbeitung personenbezogener Daten in bestimmten Wirtschaftszweigen, wie z. B.

- das Gesetz über die Nutzung und den Schutz von Kreditinformationen (auf Englisch: *Act on the Use and Protection of Credit Information*,„**CIA**“) einschließlich seines Durchführungserlasses („**CIA-Durchführungserlass**“), in dem besondere Vorschriften für gewerbliche Betreiber und spezialisierte Unternehmen (wie Ratingagenturen, Finanzinstitute) festgelegt sind, wenn diese personenbezogene Kreditinformationen verarbeiten, die zur Feststellung der Kreditwürdigkeit der Parteien von Finanz- oder Handelsgeschäften erforderlich sind;
- das Gesetz über die Förderung der Nutzung von Informations- und Kommunikationsnetzen und des entsprechenden Datenschutzes („**Netzwerkgesetz**“) und
- das Gesetz über den Schutz der Privatsphäre in der Kommunikation (auf Englisch: *Communications Privacy Protection Act*, „**CPPA**“)

29. Im Bereich des Zugriffs staatlicher Stellen hat der EDSA neben den einschlägigen Bestimmungen des PIPA und des CPPA einige andere Rechtsvorschriften geprüft, z. B. die Strafprozessordnung (auf Englisch: *Criminal Procedure Act*, „**CPA**“), das Gesetz über Telekommunikationsunternehmen (auf Englisch: *Telecommunications Business Act*, „**TBA**“), das Gesetz über die Meldung und Nutzung bestimmter Informationen über finanzielle Transaktionen (auf Englisch: *Act on Reporting and Using Specified Financial Transaction Information*, „**ARUSFTI**“) und das Gesetz über den Nationalen Nachrichtendienst (auf Englisch: *National Intelligence Service Act*, „**NISA**“).

[8] Siehe Anhang I Abschnitt I des Beschlussentwurfs.
[9] Ebenda.

2.2. Umfang der Bewertung durch den EDSA

30. Der Beschlussentwurf der Europäischen Kommission ist das Ergebnis einer Prüfung des koreanischen Datenschutzrahmens und anschließender Gespräche mit der koreanischen Regierung. Gemäß Artikel 70 Absatz 1 Buchstabe s DSGVO wird vom EDSA erwartet, dass er eine unabhängige Stellungnahme zu den Feststellungen der Europäischen Kommission abgibt, etwaige Unzulänglichkeiten des Angemessenheitsrahmens ermittelt feststellt und entsprechende Vorschläge zu deren Beseitigung unterbreitet.

31. Um Wiederholungen zu vermeiden und bei der Bewertung des koreanischen Rechtsrahmens behilflich zu sein, hat sich der EDSA dafür entschieden, sich auf einige spezifische Punkte des Beschlussentwurfs zu konzentrieren und seine Analyse und Stellungnahme hierzu abzugeben, wobei er meist davon absieht, die Sachverhaltsfeststellungen und Bewertungen wiederzugeben, bei denen der EDSA keinen Anhaltspunkt dafür hat, dass das Recht der Republik Korea dem Recht im EWR der Sache nach nicht gleichwertig wäre. Darüber hinaus – im Einklang mit der Rechtsprechung des EuGH – umfasst ein sehr wichtiger Teil der Analyse den Rechtsrahmen betreffend den mit der nationalen Sicherheit im Zusammenhang stehenden Zugriff auf die an die Republik Korea übermittelten personenbezogenen Daten und die Praxis ihres nationalen Sicherheitsapparats.

32. Bei seiner Prüfung berücksichtigte der EDSA den geltenden europäischen Datenschutzrahmen, einschließlich der Artikel 7, 8 und 47 der Charta, betreffend jeweils den Schutz des Rechts auf Privat- und Familienleben, das Recht auf Schutz personenbezogener Daten bzw. das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, sowie Artikel 8 EMRK zum Schutz des Privat- und Familienlebens. Darüber hinaus hat der EDSA den Anforderungen der DSGVO Rechnung getragen und sich mit der einschlägigen Rechtsprechung befasst.

33. Ziel dieser Übung ist es, der Europäischen Kommission eine Stellungnahme zur Beurteilung der Angemessenheit des Schutzniveaus in der Republik Korea vorzulegen. Der Begriff des „angemessenen Schutzniveaus“, der bereits in der Richtlinie 95/46 existierte, wurde vom EuGH weiterentwickelt. Es ist wichtig, sich den Standard zu vergegenwärtigen, den der EuGH in seinem Urteil in der Rechtssache *Schrems I* festgelegt hat; dieser besagt, dass das „*Schutzniveau*“ in dem Drittland zwar „*der Sache nach gleichwertig*“ mit dem in der EU gewährleisteten Schutzniveau sein muss, dass sich aber „*die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden*“.[10] Das Ziel ist also nicht, die europäischen Rechtsvorschriften Punkt für Punkt zu übernehmen, sondern vielmehr, die wesentlichen Kernanforderungen dieser Vorschriften festzustellen. Angemessenheit kann durch eine Kombination aus Rechten für betroffene Personen, Pflichten für Daten verarbeitende oder die Datenverarbeitende kontrollierende Stellen und die Aufsicht durch unabhängige Gremien 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 bestehende System, mit dem die Wirksamkeit der Regeln gesichert werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit der Datenschutzvorschriften von wesentlicher Bedeutung.[11]

[10] C-362/14, *Maximillian Schrems gegen Data Protection Commissioner*, 6. Oktober 2015, ECLI:EU:C:2015:650, Rn. 73-74.
[11] WP 254, S. 3.

2.3. Allgemeine Bemerkungen und Bedenken

2.3.1. Von der Republik Korea eingegangene internationale Verpflichtungen

34. Gemäß Artikel 45 Absatz 2 Buchstabe c DSGVO und der DSGVO-Referenzgrundlage für Angemessenheit[12] berücksichtigt die Europäische Kommission bei der Bewertung der Angemessenheit des Schutzniveaus eines Drittlands unter anderem die von dem betreffenden Drittland eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen, insbesondere in Bezug auf den Schutz personenbezogener Daten sowie die Umsetzung derartiger Verpflichtungen.

35. Korea ist Vertragspartei mehrerer internationaler Übereinkünfte, die das Recht auf Privatsphäre garantieren, wie dem Internationalen Pakt über bürgerliche und politische Rechte (Artikel 17), dem Übereinkommen über die Rechte von Menschen mit Behinderungen (Artikel 22) und dem Übereinkommen über die Rechte des Kindes (Artikel 16). Darüber hinaus hält Korea als Mitglied der OECD den Datenschutzrahmen der OECD, insbesondere die Leitlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Austausch personenbezogener Daten, ein.

36. Der EDSA nimmt ferner zur Kenntnis, dass Korea als Beobachterstaat an der Arbeit des Beratenden Ausschusses des Übereinkommens Nr. 108(+) des Europarats teilnimmt, obwohl es über den Beitritt noch nicht entschieden hat.

2.3.2. Anwendungsbereich des Angemessenheitsbeschlusses

37. Gemäß Erwägungsgrund 5 des Beschlussentwurfs kommt die Europäische Kommission zu dem Schluss, dass die Republik Korea ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die von einem in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter an für die Verarbeitung personenbezogener Informationen Verantwortliche (z. B. natürliche oder juristische Personen, Organisationen, öffentliche Einrichtungen), die in den Anwendungsbereich des PIPA fallen, übermittelt werden, mit Ausnahme der Verarbeitung personenbezogener Daten betreffend die Missionstätigkeit religiöser Organisationen und die Nominierung von Kandidaten durch politische Parteien[13] oder der Verarbeitung personenbezogener Kreditinformationen nach dem CIA durch Verantwortliche, die der Aufsicht durch die Aufsichtsbehörde für Finanzdienstleistungen unterliegen.

38. Der EDSA stellt fest, dass der Angemessenheitsbeschluss Übermittlungen aus dem Anwendungsbereich des EWR-Rechtsrahmens sowohl an öffentliche als auch an nichtöffentliche „für die Verarbeitung personenbezogener Informationen Verantwortliche“, die in den Anwendungsbereich des PIPA fallen, abdecken wird. Der EDSA geht davon aus, dass Einrichtungen, die als Auftragsverarbeiter im Sinne der DSGVO fungieren, ebenfalls unter den Begriff „für die Verarbeitung personenbezogener Informationen Verantwortlicher“ fallen, da das PIPA gleichermaßen für sie gelten wird, und dass besondere Verpflichtungen gelten, wenn ein für die Verarbeitung personenbezogener Informationen Verantwortlicher („Auftraggeber“) einen Dritten mit der Verarbeitung personenbezogener Informationen beauftragt („Auftragnehmer“); um Missverständnisse zu vermeiden, fordert der EDSA die Europäische Kommission jedoch auf, deutlicher zu machen, dass der Angemessenheitsbeschluss auch für „Auftragsverarbeiter“ in Korea gilt und dass das Schutzniveau für aus dem EWR übermittelte personenbezogene Daten auch in diesen Fällen nicht untergraben wird.

39. Da der Angemessenheitsbeschluss auch für die Übermittlung personenbezogener Daten zwischen öffentlichen Stellen gilt, geht der EDSA ferner davon aus, dass damit auch Übermittlungen zwischen

[12] WP 254, S. 3.

[13] Für weitere Informationen zum Kontext siehe Abschnitt 3.1.2 dieser Stellungnahme.

Datenschutzaufsichtsbehörden umfasst sind und fordert die Europäische Kommission im Interesse der Klarheit auf, sich speziell mit dieser Frage zu befassen.

40. Darüber hinaus möchte der EDSA mit Blick auf die vom Anwendungsbereich des Angemessenheitsbeschlusses ausgenommenen Einrichtungen betonen, dass der Angemessenheitsbeschluss von einer klareren Definition „gewerblicher Organisationen" profitieren könnte, die der Aufsicht durch die PIPC unterliegen (Artikel 45 Absatz 3 CIA), damit im EWR niedergelassene Verantwortliche und Auftragsverarbeiter ohne größere Umstände beurteilen können, ob der Datenimporteur auch in den Anwendungsbereich des Angemessenheitsbeschlusses fällt, bevor sie Daten an Einrichtungen übermitteln, die in den Anwendungsbereich des CIA fallen, oder zumindest darauf hingewiesen werden können, dass dieser Aspekt zu prüfen ist.

41. Bezüglich des Anwendungsbereichs des Angemessenheitsbeschlusses hat der EDSA den zusätzlichen Erläuterungen der Europäischen Kommission entnommen, dass die koreanische Finanznachrichtendienst (auf Englisch: *Korea Financial Intelligence Unit*, „**KOFIU**"), die von der Kommission für Finanzdienstleistungen eingerichtet wurde und die Verhinderung von Geldwäsche und Terrorismusfinanzierung gemäß ARUSFTI[14] beaufsichtigt, ebenfalls vom Anwendungsbereich ausgenommen ist, da sie nur für Finanzinstitute zuständig ist, die selbst nicht unter den Beschlussentwurf fallen. Nach Artikel 1 Absatz 2 Buchstabe c des Beschlussentwurfs sind jedoch nur die für die Verarbeitung personenbezogener Informationen Verantwortlichen, die der Aufsicht der Kommission für Finanzdienstleistungen unterliegen und personenbezogene Kreditinformationen im Rahmen des CIA verarbeiten, von seinem Anwendungsbereich ausgenommen. Vor diesem Hintergrund ersucht der EDSA die Europäische Kommission um Klarstellung, ob die KOFIU und die von der KOFIU selbst durchgeführten Datenverarbeitungstätigkeiten unter den Beschlussentwurf fallen.

3. ALLGEMEINE ASPEKTE DES DATENSCHUTZES

3.1. Grundsätze

42. Kapitel 3 der DSGVO-Referenzgrundlage für Angemessenheit befasst sich mit den „inhaltlichen Grundsätzen". Diese müssen im System eines Drittlandes enthalten sein, damit dessen Schutzniveau dem innerhalb der EU garantierten Schutzniveau als der Sache nach gleichwertig betrachtet werden kann.

43. Auch wenn das Recht auf den Schutz personenbezogener Daten an sich nicht ausdrücklich in der koreanischen Verfassung verankert ist, wird es als Grundrecht anerkannt, indem es aus den verfassungsmäßigen Rechten auf Menschenwürde und das Streben nach Glück (Artikel 10), Privatleben (Artikel 17) und Privatsphäre in der Kommunikation (Artikel 18) herleitet wird. Wie im Beschlussentwurf der Europäischen Kommission ausgeführt, wurde dies sowohl vom Obersten Gerichtshof als auch vom Verfassungsgericht bestätigt.[15] Der EDSA nimmt diese Anerkennung zur Kenntnis, da er daraus ableitet, dass der Datenschutz als Grundrecht gemäß Artikel 37 der koreanischen Verfassung „*nur per Gesetz beschränkt werden darf und wenn dies für die nationale Sicherheit, die Aufrechterhaltung der öffentlichen Ordnung oder das Gemeinwohl erforderlich ist*", und dass „*selbst wenn solche Beschränkungen auferlegt werden, sie den Wesensgehalt der Freiheit oder des Rechts nicht beeinträchtigen dürfen*".

44. Laut der Europäischen Kommission[16] hat das Verfassungsgericht entschieden, dass Grundrechte auch für Ausländer gelten. Den offiziellen Erklärungen der koreanischen Regierung zufolge[17] hat sich die

[14] Siehe Anhang II, Abschnitt 2.2.3.1.
[15] Siehe Erwägungsgrund 8 des Beschlussentwurfs sowie die einschlägige Rechtsprechung, auf die in Fußnote 10 des Beschlussentwurfs Bezug genommen wird, von der lediglich englische Zusammenfassungen vorliegen.
[16] Siehe Erwägungsgrund 9 des Beschlussentwurfs.
[17] Anhang II Abschnitt 1.1 des Beschlussentwurfs.

Rechtsprechung zwar bisher nicht speziell mit dem Recht nichtkoreanischer Staatsangehöriger auf Privatsphäre befasst, doch wird in Wissenschaftlerkreisen weithin anerkannt, dass in den Artikeln 12 bis 22 der Verfassung „Menschenrechte“ festgelegt sind. Darüber hinaus hat die Republik Korea eine Reihe von Gesetzen im Bereich des Datenschutzes erlassen, die Garantien für alle Personen unabhängig von ihrer Staatsangehörigkeit vorsehen, wie das PIPA. Diesbezüglich nimmt der EDSA zur Kenntnis, dass gemäß Artikel 6 Absatz 2 der Verfassung vorsieht, dass der Status von Ausländern nach Maßgabe des Völkerrechts und der völkerrechtlichen Verträge sowie der im Beschlussentwurf erwähnten Rechtsprechung gewährleistet ist, wonach ein „Ausländer“ Träger von „Grundrechten“ sein kann. Angesichts der Bedeutung der Anerkennung des Rechts auf Datenschutz für „ausländische Staatsangehörige“ weist der EDSA die Europäische Kommission darauf hin, dass die Rechtsprechung zum Datenschutz als Grundrecht, das nicht nur koreanischen Bürgern, sondern allen betroffenen Personen zuerkannt wird, weiterhin beobachtet werden muss, um sicherzustellen, dass das durch die DSGVO garantierte Schutzniveau für natürliche Personen nicht untergraben wird, wenn personenbezogene Daten auf Grundlage des Angemessenheitsbeschlusses an Korea übermittelt werden.

3.1.1. Begriffe

45. Auf der Grundlage der DSGVO-Referenzgrundlage für Angemessenheit sollten in dem System eines Drittlands grundlegende Datenschutzkonzepte und/oder -grundsätze gegeben sein. Die in der DSGVO verwendete Terminologie muss dabei zwar nicht übernommen werden, doch sollten sie die Begriffe, die im europäischen Datenschutzrecht verankert sind, widerspiegeln und mit diesen im Einklang stehen. Die DSGVO enthält beispielsweise folgende wichtige Begriffe: „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „Verantwortlicher“, „Auftragsverarbeiter“, „Empfänger“ und „sensible Daten“.[18]

46. Das PIPA enthält eine Reihe von Definitionen wie unter anderem der Begriffe „personenbezogene Informationen“, „Verarbeitung“ und „betroffene Person“, die den entsprechenden Begriffen der DSGVO sehr ähnlich sind.

3.1.1.1. *Der Begriff „pseudonymisierte Daten“*

47. Zu den Begriffsbestimmungen im PIPA gehört die in Artikel 2 Absatz 1 enthaltene, der zufolge als personenbezogene Informationen insbesondere folgende Informationen gelten, die sich auf eine lebende Person beziehen: a) Informationen, mit denen eine bestimmte Person anhand ihres vollständigen Namens, ihrer Personenkennzahl, ihres Bildes usw. identifiziert wird, und b) Informationen, die selbst dann, wenn sie für sich alleine eine bestimmte Person nicht identifizieren, leicht mit anderen Informationen kombiniert werden können, um eine bestimmte Person zu identifizieren. In den letzteren Fällen wird die Frage, ob eine Kombination einfach ist, unter angemessener Berücksichtigung des Zeitaufwands, der Kosten, der Technologie usw. ermittelt, die zur Identifizierung der Person verwendet wird, z. B. die Wahrscheinlichkeit, dass die anderen Informationen beschafft werden können.

48. Darüber hinaus gelten nach Artikel 2 Absatz 1 Buchstabe c PIPA auch „pseudonymisierte Informationen“ als personenbezogene Informationen. Pseudonymisierte Informationen sind definiert als Informationen nach den genannten Buchstaben a oder b, die gemäß Unterabsatz 1-2 pseudonymisiert sind, und mit denen daher ohne die Verwendung oder Kombination von Informationen zur Wiederherstellung des ursprünglichen Zustands eine bestimmte Person nicht identifiziert werden kann. Vollständig anonymisierte Informationen sind vom Anwendungsbereich des PIPA ausgenommen. Nach Artikel 58 Absatz 2 PIPA gilt das Gesetz nicht für Informationen, mit denen

[18] WP 254, S. 4.

in Kombination mit anderen Informationen eine bestimmte Person nicht mehr identifiziert werden kann, wobei der Zeitaufwand, die Kosten, die Technologie usw. angemessen berücksichtigt werden.

49. Die Europäische Kommission stellt in Erwägungsgrund 17 ihres Beschlussentwurfs fest, dass dies dem sachlichen Anwendungsbereich der DSGVO und ihren Begriffen „personenbezogene Daten", „Pseudonymisierung" und „anonymisierte Daten" entspricht.

50. Nach Artikel 28 Absatz 7 PIPA gelten jedoch die Artikel 20, 21, 27, 34 Absatz 1, Artikel 35 bis 37, Artikel 39 Absatz 3, Artikel 39 Absatz 4, Artikel 39 Absätze 6 bis 8 nicht für pseudonymisierte personenbezogene Informationen.

51. In ihrem Beschlussentwurf führt die Europäische Kommission aus, dass Artikel 28 Absatz 7 PIPA nur dann auf pseudonymisierte personenbezogene Informationen anwendbar ist, wenn diese zu im öffentlichen Interesse liegenden statistischen Zwecken, zu wissenschaftlichen Forschungszwecken oder zu Archivzwecken verarbeitet werden.[19] Dies folgt jedoch nicht unmittelbar aus dem Gesetzestext, sondern aus den Erläuterungen in der Notifizierung Nr. 2021-1.[20] Der EDSA räumt zwar ein, dass aufgrund der Struktur und der Logik des PIPA argumentiert werden kann, dass Artikel 28 Absatz 2 PIPA so verstanden und logischerweise so ausgelegt werden sollte, dass er auch für Artikel 28 Absatz 7 PIPA gilt, doch angesichts der Bedeutung der Notifizierung Nr. 2021-1 für die Beurteilung der Angemessenheit des Schutzniveaus personenbezogener Daten in der Republik Korea durch die Europäische Kommission und zur Vermeidung von Zweifeln ersucht der EDSA die Europäische Kommission, weitere Informationen über den verbindlichen Charakter, die Durchsetzbarkeit und die Gültigkeit der Notifizierung Nr. 2021-1 vorzulegen und ihre Anwendung in diesem konkreten Zusammenhang zu überwachen.

52. In diesem Zusammenhang möchte der EDSA daran erinnern, dass die Pseudonymisierung gemäß DSGVO als eine empfohlene Sicherheitsmaßnahme zu verstehen ist. Mit anderen Worten: Nach der DSGVO bleiben pseudonymisierte Daten personenbezogene Daten, für die die DSGVO uneingeschränkt gilt. In Anbetracht dessen hat der EDSA Bedenken, dass das Schutzniveau der DSGVO für pseudonymisierte personenbezogene Daten untergraben werden könnte, wenn personenbezogene Daten nach Korea übermittelt werden. Der EDSA ersucht daher die Europäische Kommission, die Auswirkungen der Pseudonymisierung im Rahmen des PIPA und vor allem die Frage näher zu prüfen, wie sie sich auf die Grundrechte und Grundfreiheiten der betroffenen Personen auswirken könnte, deren personenbezogene Daten auf der Grundlage des Angemessenheitsbeschlusses an die Republik Korea übermittelt würden. Daher fordert der EDSA die Europäische Kommission auf, Zusicherungen zu geben, dass der Schutz personenbezogener Daten von betroffenen Personen im EWR nach der Übermittlung an die Republik Korea auch dann nicht gesenkt wird, wenn die übermittelten personenbezogenen Daten pseudonymisiert sind.

3.1.1.2. *Begriff des für die Verarbeitung personenbezogener Informationen Verantwortlichen*

53. Artikel 2 Absatz 5 PIPA enthält eine Definition des Begriffs „für die Verarbeitung personenbezogener Informationen Verantwortlicher"; dabei handelt es sich um eine öffentliche Einrichtung, juristische Person, Organisation oder natürliche Person usw., die personenbezogene Informationen direkt oder indirekt verarbeitet, um „*im Rahmen ihrer Tätigkeiten*" Dateien mit personenbezogene Informationen zu führen. Allerdings wird der Begriff „für die Verarbeitung personenbezogener Informationen Verantwortlicher" in den zusätzlichen Garantien in der Notifizierung Nr. 2021-1 als öffentliche Einrichtung, juristische Person, Organisation, natürliche Person usw. definiert, die personenbezogene

[19] Siehe u. a. Erwägungsgrund 82 des Beschlussentwurfs.
[20] Anhang I Abschnitt 4 des Beschlussentwurfs.

Informationen direkt oder indirekt verarbeitet, um Dateien „*für geschäftliche Zwecke*“ zu führen. Dagegen heißt es in Fußnote 272 des Beschlussentwurfs zum Begriff des für die Verarbeitung personenbezogener Informationen Verantwortlichen: „*Wie in Artikel 2 PIPA definiert, handelt es sich um eine öffentliche Einrichtung, eine juristische Person, eine Organisation, eine natürliche Person usw., die personenbezogene Informationen direkt oder indirekt verarbeitet, um Dateien mit personenbezogenen Informationen ‚für amtliche oder geschäftliche Zwecke zu führen‘.*“

54. Der EDSA räumt ein, dass diese Unstimmigkeiten möglicherweise auf die von den koreanischen Behörden bereitgestellten Übersetzungen des Originaltextes zurückzuführen sind, und fordert die Europäische Kommission auf, die Qualität und Zuverlässigkeit der Übersetzungen regelmäßig zu überprüfen. Der EDSA betont jedoch, dass für die Beurteilung der in der Sache bestehenden Gleichwertigkeit des Datenschutzniveaus des koreanischen Rechtsrahmens ein klares Verständnis der Verarbeitungszwecke erforderlich ist, die in den sachlichen Anwendungsbereich des PIPA fallen. Ferner stellt der EDSA in diesem Zusammenhang fest, dass das PIPA in Bezug auf die Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ nicht dieselbe Terminologie wie die DSGVO verwendet, und fordert die Europäische Kommission auf, die korrekte Definition und den Anwendungsbereich des Begriffs „für die Verarbeitung personenbezogener Informationen Verantwortlicher“ klarzustellen und konkret der Frage nachzugehen, ob dieser Begriff auch Auftragsverarbeiter im Sinne der DSGVO umfasst, da sich dies unmittelbar auf den Anwendungsbereich des Angemessenheitsbeschlusses auswirkt.[21]

3.1.2. Im PIPA vorgesehene teilweise Ausnahmen

55. Artikel 58 Absatz 1 PIPA schließt die Anwendung von Teilen des PIPA (nämlich Artikel 15 bis 57) in Bezug auf die Verarbeitung von vier Kategorien personenbezogener Daten aus, wie nachstehend beschrieben. Die Ausnahmen betreffen insbesondere die Bestimmungen des PIPA zu spezifischen Grundlagen für die Verarbeitung, bestimmten Datenschutzpflichten, den detaillierten Regeln für die Ausübung der Rechte des Einzelnen sowie den Regeln für die Streitbeilegung. Der EDSA nimmt jedoch zur Kenntnis, dass einige allgemeine Bestimmungen des PIPA weiterhin gelten, wie etwa die Bestimmungen über die Datenschutzgrundsätze (Artikel 3 PIPA) und die Betroffenenrechte(Artikel 4 PIPA). Darüber hinaus sind in Artikel 58 Absatz 4 PIPA spezifische Verpflichtungen für diese vier Datenverarbeitungskategorien festgelegt.

56. Erstens bezieht sich die teilweise Ausnahme auf personenbezogene Informationen, die gemäß dem Statistikgesetz für die Verarbeitung durch öffentliche Einrichtungen erhoben werden. Die Europäische Kommission stellt in Erwägungsgrund 27 ihres Beschlussentwurfs fest, dass den Erläuterungen der koreanischen Regierung zufolge personenbezogene Daten, die in diesem Zusammenhang verarbeitet werden, normalerweise koreanische Staatsangehörige betreffen und nur ausnahmsweise Informationen über Ausländer enthalten, nämlich im Falle von Statistiken über die Einreise in das und die Ausreise aus dem Hoheitsgebiet oder über ausländische Investitionen. Dem Beschlussentwurf zufolge werden solche Daten jedoch selbst in diesen Fällen normalerweise nicht von Verantwortlichen/Auftragsverarbeitern im EWR übermittelt, sondern würden vielmehr direkt von Behörden in Korea erhoben.

57. Der EDSA erkennt die Argumente der Europäischen Kommission betreffend den Ausnahmecharakter der Anwendung des Statistikgesetzes auf die Verarbeitung von auf Grundlage des Angemessenheitsbeschlusses übermittelten personenbezogenen Daten an; er würde jedoch weitere Informationen und Zusicherungen zu den spezifischen Garantien begrüßen, die für den Fall gelten würden, dass aus dem EWR übermittelte personenbezogene Daten gemäß dem Statistikgesetz für die Verarbeitung durch öffentliche Einrichtungen weiter erhoben werden, insbesondere in Bezug auf die Ausübung der Betroffenenrechte im Einklang mit Artikel 89 Absatz 2 DSGVO, sofern diese Rechte die

[21] Siehe auch weiter oben Rn. 38.

Verwirklichung der spezifischen Zwecke voraussichtlich nicht unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke nicht erforderlich sind.

58. In dieser Hinsicht scheint die Anwendung von Artikel 4 PIPA auch auf diese Art von Verarbeitung Zusicherungen zu bieten, doch würde der EDSA zusätzliche Informationen und Klarstellungen im Angemessenheitsbeschluss zu den spezifischen Verpflichtungen begrüßen, die gemäß Artikel 58 Absatz 4 PIPA für diese Verarbeitungstätigkeiten gelten, insbesondere in Bezug auf die Datenminimierung, die begrenzte Datenspeicherung, Sicherheitsmaßnahmen und die Bearbeitung von Beschwerden.

59. Zweitens gilt die teilweise Ausnahme für personenbezogene Informationen, die für die Analyse von Informationen im Zusammenhang mit der nationalen Sicherheit erhoben oder angefordert werden. Dem EDSA ist bewusst, dass die Staaten im Bereich der nationalen Sicherheit über einen vom EGMR anerkannten breiten Ermessensspielraum verfügen. Der EDSA stellt ferner fest, dass gemäß Artikel 37 Absatz 2 der koreanischen Verfassung jede Einschränkung der Freiheiten und Rechte, beispielsweise wenn dies zum Schutz der nationalen Sicherheit erforderlich ist, nicht gegen den Wesensgehalt dieser Freiheit oder dieses Rechts verstoßen darf. Darüber hinaus nimmt der EDSA die Garantien in Abschnitt 6 der Notifizierung Nr. 2021-1 hinsichtlich der Verarbeitung personenbezogener Daten für Zwecke der nationalen Sicherheit, einschließlich der Untersuchung von Verstößen und der Durchsetzung, zur Kenntnis. In diesem Zusammenhang fordert der EDSA die Europäische Kommission jedoch auf, den Anwendungsbereich der Ausnahmen weiter klarzustellen, da er sich fragt, ob alle in Artikel 58 Absatz 1 Ziffer 2 PIPA vorgesehenen Ausnahmen (Kapitel III bis VII) für die Arbeit der Nachrichtendienste von Bedeutung sind und ob sie die Gleichwertigkeit mit den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit gewährleisten. Der EDSA fordert die Europäische Kommission insbesondere auf, näher zu erläutern, unter welchen Umständen ein Nachrichtendienst auf die Ausnahmen zurückgreifen könnte. Der EDSA hält es für erforderlich, die Auswirkungen dieser Beschränkungen insbesondere auf die wirksame Ausübung und Durchsetzung der Betroffenenrechte in der Praxis genau zu überwachen.

60. Drittens gilt die teilweise Ausnahme für „*personenbezogene Informationen, die vorübergehend verarbeitet werden, wenn dies aus Gründen der öffentlichen Sicherheit, der öffentlichen Gesundheit usw. dringend erforderlich ist*“. Gemäß Erwägungsgrund 29 des Beschlussentwurfs der Europäischen Kommission wird diese Kategorie von der PIPC eng ausgelegt und gilt nur für Notfälle, die dringende Maßnahmen erfordern, beispielsweise zur Verfolgung von Infektionserregern oder zur Rettung und Unterstützung von Opfern von Naturkatastrophen.

61. Der EDSA betont ferner, dass Ausnahmen vom Schutzniveau für personenbezogene Daten eng auszulegen sind. Gleichzeitig stellt der EDSA fest, dass die Bestimmung nicht präzise ist und keine abschließende Liste von Beispielen für Situationen enthält, in denen die Verarbeitung personenbezogener Daten als „*dringend erforderlich*“ angesehen werden könnte. So gibt der EDSA beispielsweise zu bedenken, ob internationale Übermittlungen von Gesundheitsdaten während der anhaltenden COVID-19-Pandemie ebenfalls in den Anwendungsbereich dieser Ausnahme fallen würde. Vor diesem Hintergrund fordert der EDSA die Europäische Kommission auf, weitere Klarstellungen zum Anwendungsbereich dieser Ausnahme vorzulegen und ihre Anwendung und ihren Geltungsbereich umfassend zu überwachen, um sicherzustellen, dass der Schutz personenbezogener Daten aus dem EWR nach der Übermittlung an Korea auf der Grundlage des Angemessenheitsbeschlusses nicht verringert wird.

62. Schließlich gilt die teilweise Ausnahme für personenbezogene Informationen, die für die Berichterstattung durch die Presse, für die Missionstätigkeit religiöser Organisationen und für die

Nominierung von Kandidaten durch politische Parteien erhoben oder verwendet werden.[22] In Bezug auf die Verarbeitung personenbezogener Informationen durch die Presse für journalistische Zwecke trägt die Europäische Kommission in Erwägungsgrund 31 ihres Beschlussentwurfs vor, dass die Abwägung zwischen dem Recht auf freie Meinungsäußerung und anderen Rechten, einschließlich des Rechts auf Privatsphäre, im Gesetz über Schiedssprüche und Rechtsbehelfe usw. für Schäden durch Presseberichte (im Folgenden „**Pressegesetz**“) geregelt ist, und spezifische Garantien aufführt, die sich aus dem Pressegesetz ergeben. Der EDSA fordert die Kommission jedoch auf, diese Ausnahme und die einschlägige Rechtsprechung umfassend zu überwachen, um sicherzustellen, dass ein gleichwertiges Datenschutzniveau auch in der Praxis im koreanischen Rechtsrahmen gewährleistet ist.

3.1.3. Grundlagen für eine rechtmäßige Verarbeitung zu legitimen Zwecken nach Treu und Glauben

63. Gemäß der DSGVO-Referenzgrundlage für Angemessenheit und im Einklang mit der DSGVO muss die Verarbeitung von Daten auf rechtmäßige Weise und nach Treu und Glauben für legitime Zwecke erfolgen. Die Rechtsgrundlage, auf der personenbezogene Daten rechtmäßig, nach Treu und Glauben und auf legitime Weise verarbeitet werden dürfen, sollten hinreichend klar dargelegt werden. Im europäischen Rahmen werden mehrere solche rechtlichen Grundlagen anerkannt, darunter Bestimmungen des nationalen Rechts, die Einwilligung der betroffenen Person, die Erfüllung eines Vertrags oder das berechtigte Interesse des Verantwortlichen oder eines Dritten, das keinen Vorrang vor den Interessen des Einzelnen hat.

64. Dem Aufbau der DSGVO folgend führt das PIPA zunächst den Grundsatz der Rechtmäßigkeit, Fairness und Transparenz ein (Artikel 3 Absätze 1 und 2 PIPA) und legt die spezifischen Regeln für seine Anwendung anschließend fest (Artikel 15 bis 19 PIPA). Insbesondere Artikel 15 PIPA enthält einen Katalog der Rechtsgrundlagen, auf die die für die Verarbeitung personenbezogener Informationen Verantwortlichen die Erhebung personenbezogener Daten stützen und diese im Rahmen des Erhebungszwecks verwenden können. Bei diesen Rechtsgrundlagen handelt es sich um 1) die informierte Einwilligung der betroffenen Person; 2) eine gesetzliche Erlaubnis oder die Erforderlichkeit für die Erfüllung einer gesetzlichen Pflicht; 3) die Erforderlichkeit für die Wahrnehmung der Aufgaben einer öffentlichen Einrichtung; 4) die Erforderlichkeit für die Erfüllung eines Vertrags mit einer betroffenen Person; 5) die Erforderlichkeit zum Zwecke des Schutzes von Leben, körperlicher Unversehrtheit oder Eigentumsinteressen der betroffenen Person oder eines Dritten vor unmittelbarer Gefahr (wenn eine vorherige Einwilligung nicht eingeholt werden kann); 6) die Erforderlichkeit zur Wahrung von einem gerechtfertigten Interesse eines für die Verarbeitung personenbezogener Informationen Verantwortlichen, das höher als die der betroffenen Person eingestuft wird.

65. Zusätzlich dazu sind in Artikel 17 PIPA die Rechtsgrundlagen für die Weitergabe personenbezogener Informationen an einen Dritten aufgeführt, darunter 1) die informierte Einwilligung der betroffenen Person; 2) eine gesetzliche Erlaubnis oder die Erforderlichkeit für die Erfüllung einer gesetzlichen Pflicht; 3) die Erforderlichkeit für die Wahrnehmung der Aufgaben einer öffentlichen Einrichtung; 4) die Erforderlichkeit zum Zwecke des Schutzes von Leben, körperlicher Unversehrtheit oder Eigentumsinteressen der betroffenen Person oder eines Dritten vor unmittelbarer Gefahr (wenn eine vorherige Einwilligung nicht eingeholt werden kann). Auch ohne Einwilligung der betroffenen Person ist die Weitergabe personenbezogener Informationen zulässig, wenn dies in einem Umfang geschieht,

[22] Dementsprechend sind auch die Verarbeitung personenbezogener Daten durch religiöse Organisationen für ihre Missionstätigkeit und die Verarbeitung personenbezogener Daten durch politische Parteien im Zusammenhang mit der Nominierung von Kandidaten vom Geltungsbereich des Angemessenheitsbeschlusses ausgenommen. Siehe auch Rn. 37 weiter oben in Abschnitt 2.3.2.

der in angemessenem Zusammenhang mit den Zwecken steht, für die die personenbezogenen Informationen ursprünglich erhoben wurden (Artikel 17 Absatz 4 PIPA).

66. Artikel 18 PIPA enthält spezifische Vorschriften für die Verwendung und die Weitergabe personenbezogener Informationen, wenn dies außerhalb des ursprünglichen Zwecks der Erhebung oder Bereitstellung geschieht. Auch hier ist unter anderem die Einwilligung ein Erlaubnistatbestand.

67. Der EDSA erkennt zwar an, dass das koreanische Recht im Hinblick auf den Grundsatz der Rechtmäßigkeit mit der DSGVO im Wesentlichen vergleichbar ist . Auch erkennt der EDSA das Bestehen eines allgemeinen Rechts auf Aussetzung (Artikel 37 PIPA) an, das auch dann geltend gemacht werden kann, wenn personenbezogene Daten auf der Grundlage einer Einwilligung verarbeitet werden. Nichtsdestotrotz weist er darauf hin, dass das PIPA kein allgemeines Recht auf Widerruf der Einwilligung vorsieht.[23] Angesichts der Bedeutung der Einwilligung als Rechtsgrundlage in allen oben beschriebenen Szenarien und unter Berücksichtigung der Rolle der Betroffenenrechte in einem Datenschutzrechtsystem für die Zwecke der Wahrung der Grundrechte und Grundfreiheiten der betroffenen Personen ersucht der EDSA die Europäische Kommission, die Auswirkungen des Fehlens eines allgemeinen Rechts auf Widerruf der Einwilligung nach koreanischem Recht weiter zu prüfen und weitere Zusicherungen zu geben, um sicherzustellen, dass ein wesentliches Datenschutzniveau, wie es in der DSGVO vorgesehen ist, jederzeit gewährleistet ist, erforderlichenfalls durch Klarstellung der Rolle des Rechts auf Aussetzung in diesem Zusammenhang.

3.1.4. Grundsatz der Zweckbindung

68. Im Einklang mit der DSGVO sieht die DSGVO-Referenzgrundlage für Angemessenheit vor, dass personenbezogene Daten für einen bestimmten Zweck verarbeitet und anschließend nur insoweit verwendet werden sollten, als dies nicht mit dem Zweck der Verarbeitung unvereinbar ist.

69. Gemäß Artikel 3 Absätze 1 und 2 PIPA legen die für die Verarbeitung personenbezogener Informationen Verantwortlichen die Zwecke der Verarbeitung genau und ausführlich fest und stellen sicher, dass die Verarbeitung mit diesen Zwecken vereinbar ist. Dieser Grundsatz wird zwar in anderen Bestimmungen (nämlich Artikel 15 Absatz 1, Artikel 18 Absatz 1 und Artikel 19 Absatz 1 PIPA) bekräftigt, doch ist die Verarbeitung für „in einem angemessenen Verhältnis stehende“ Zwecke unter bestimmten Umständen zulässig (siehe Artikel 17 Absatz 4 PIPA)[24], ebenso die zweckfremde Verwendung und Bereitstellung personenbezogener Informationen (siehe Artikel 18 und 19 PIPA)[25].

70. Der EDSA geht davon aus, dass bei Übermittlungen personenbezogener Daten aus dem EWR an die Republik Korea auf der Grundlage des Angemessenheitsbeschlusses der Zweck der Erhebung durch den im EWR niedergelassenen Verantwortlichen der Zweck der Datenübermittlung ist, der auch für die Verarbeitung durch den empfangenden koreanischen Verantwortlichen gilt. Eine Zweckänderung durch den in Korea niedergelassenen Verantwortlichen wäre nur gemäß Artikel 18 Absatz 2 Ziffer 1-3

[23] Auch wenn betroffene Personen unter bestimmten Umständen die Einwilligung verweigern können, siehe beispielsweise Artikel 18 Absatz 3 Ziffer 5 PIPA. Das Recht auf Widerruf der Einwilligung scheint hingegen nur in besonderen Fällen zu bestehen; nach Artikel 27 Absatz 1 Ziffer 2 PIPA haben betroffene Personen das Recht, ihre Einwilligung zu widerrufen, wenn sie nicht möchten, dass ihre personenbezogenen Informationen an einen Dritten in Folge einer Unternehmenstransaktion des Verantwortlichen, eines Zusammenschlusses, usw., übermittelt werden; nach Artikel 39 Absatz 7 PIPA können Nutzer jederzeit bei Anbietern von Informations- und Kommunikationsdiensten usw. ihre Einwilligung in die Erhebung, Verwendung und Bereitstellung ihrer personenbezogenen Informationen widerrufen; und nach Artikel 37 CIA kann eine Person, über die Kreditinformationen erhoben wurden, gegenüber einem Anbieter/Nutzer von Kreditinformationen widerrufen.

[24] Wobei die Vereinbarkeit mit dem Zweck vorab anhand der Kriterien von Artikel 14-2 des PIPA-Durchführungserlasses zu ermitteln ist.

[25] Siehe auch weiter oben unter Rn. 66.

PIPA zulässig, „*sofern dadurch nicht die Interessen einer betroffenen Person oder eines Dritten in unlauterer Weise verletzt werden*“.[26] In diesem Zusammenhang nimmt der EDSA die Ausführungen der Europäischen Kommission in Erwägungsgrund 55 des Beschlussentwurfs zur Kenntnis, dass in Fällen, in denen Zweckänderungen gesetzlich zulässig sind, die entsprechenden Gesetze das Grundrecht auf Privatsphäre und Datenschutz achten müssen. Der EDSA stellt jedoch fest, dass keine konkreten Informationen zur Untermauerung gerade dieser Aussage vorgelegt wurden; so wurde beispielsweise nicht auf Artikel 37 der (koreanischen) Verfassung Bezug genommen. Daher fordert der EDSA die Europäische Kommission auf, im Beschlussentwurf weitere Zusicherungen und Garantien zu geben, um sicherzustellen, dass Gesetze, die eine Änderung des Verarbeitungszwecks gestatten, die Grundrechte und Grundfreiheiten der betroffenen Personen in Bezug auf den Schutz der Privatsphäre und den Datenschutz wahren müssen.

3.1.5. Grundsatz der Datenqualität und der Verhältnismäßigkeit

71. In der DSGVO-Referenzgrundlage für Angemessenheit heißt es, dass Daten sachlich richtig sein und erforderlichenfalls auf dem neuesten Stand gehalten werden sollten. Die Daten sollten angemessen, relevant und im Hinblick auf die Zwecke, für die sie verarbeitet werden, nicht exzessiv sein.

72. Gemäß dem PIPA müssen für die Verarbeitung personenbezogener Informationen Verantwortliche sicherstellen, dass personenbezogene Informationen richtig, vollständig und auf dem neuesten Stand sind, soweit dies für die Zwecke, für die die personenbezogenen Informationen verarbeitet werden, erforderlich ist (Artikel 3 Absatz 3 PIPA). Für die Verarbeitung personenbezogener Informationen Verantwortliche sind verpflichtet, nur die zur Erreichung eines bestimmten Zwecks erforderlichen personenbezogenen Informationen zu erheben. Sie tragen diesbezüglich die Beweislast (Artikel 16 Absatz 1 PIPA).

73. Vor diesem Hintergrund teilt der EDSA die Einschätzung der Europäischen Kommission in Bezug auf die der Sache nach bestehende Gleichwertigkeit des Schutzniveaus im Rahmen des PIPA mit dem der DSGVO in dieser Hinsicht.

3.1.6. Grundsatz der Datenspeicherung

74. Gemäß der DSGVO-Referenzgrundlage für Angemessenheit sollten Daten im Allgemeinen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Gemäß Artikel 21 Absatz 1 PIPA besteht dieser Grundsatz auch im koreanischen Recht. Nach dem PIPA sind für die Verarbeitung personenbezogener Informationen Verantwortliche verpflichtet, personenbezogene Informationen unverzüglich zu vernichten, wenn die personenbezogenen Informationen nach Ablauf der Speicherfrist oder nach Erreichen des beabsichtigten Verarbeitungszweck nicht mehr erforderlich sind, es sei denn, es gelten gesetzliche Aufbewahrungsfristen.

75. Der EDSA ist jedoch besorgt darüber, dass Artikel 21 Absatz 1 PIPA auf pseudonymisierte personenbezogene Informationen nicht anwendbar ist. Der EDSA nimmt zur Kenntnis, dass gemäß Abschnitt 4 Ziffer iii der Notifizierung Nr. 2021-1 „[w]*enn ein für die Verarbeitung personenbezogener Informationen Verantwortlicher pseudonymisierte Informationen für die Zwecke der Erstellung von Statistiken, der wissenschaftlichen Forschung, der Aufbewahrung öffentlicher Aufzeichnungen usw. verarbeitet, und wenn die pseudonymisierten Informationen im Einklang mit Artikel 37 der Verfassung und Artikel 3 (Grundsätze für den Schutz personenbezogener Daten) des Gesetzes nicht vernichtet wurde* [sic]*, nachdem der spezifische Zweck der Verarbeitung erreicht worden ist, er die Informationen anonymisiert, um sicherzustellen, dass allein mit diesen Informationen oder in Kombination mit anderen Informationen eine bestimmte Person nicht länger identifiziert werden kann, wobei im Einklang mit Artikel 58 Absatz 2 PIPA der Zeitaufwand, die Kosten, die Technologie usw. angemessen*

[26] Artikel 18 Absatz 2 PIPA.

berücksichtigt werden." In Anbetracht, auch in diesem Fall, der Bedeutung der Notifizierung Nr. 2021-1 und im Interesse der Rechtssicherheit bezüglich der Gleichwertigkeit des Schutzniveaus für auf Grundlage des Angemessenheitsbeschlusses an die Republik Korea übermittelte personenbezogene Daten, fordert der EDSA die Europäische Kommission erneut auf, nähere Informationen dazu vorzulegen, wie die Notifizierung Nr. 2021-1 rechtsverbindlich gemacht und ihre Durchsetzbarkeit und Gültigkeit gewährleistet wird.[27]

3.1.7. Grundsatz der Sicherheit und Vertraulichkeit

76. Wie in der DSGVO-Referenzgrundlage für Angemessenheit beschrieben, müssen Stellen, die personenbezogene Daten verarbeiten, nach dem Grundsatz der Sicherheit und Vertraulichkeit sicherstellen, dass die Sicherheit der personenbezogenen Daten gewährleistet ist, wozu auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor versehentlichem Verlust, versehentlicher Zerstörung oder versehentlicher Beschädigung durch geeignete technische oder organisatorische Maßnahmen gehört. Der Stand der Technik und die damit verbundenen Kosten sollten beim Sicherheitsniveau berücksichtigt werden.

77. Die Europäische Kommission hat in Artikel 3 Absatz 4 PIPA einen ähnlichen Grundsatz der Datensicherheit festgestellt, der in Artikel 29 PIPA näher ausgeführt wird. Darüber hinaus gelten die Datensicherheitsbestimmungen, wenn der für die Verarbeitung personenbezogener Informationen Verantwortliche einen „Auftragnehmer" einsetzt. Die Sicherheit der Verarbeitung muss durch technische und administrative Sicherheitsvorkehrungen gewährleistet werden, die auch in die verbindliche Auftragsdatenverarbeitungsvereinbarung aufgenommen werden müssen (Artikel 26 PIPA und Artikel 28 PIPA-Durchführungserlass). Darüber hinaus gelten im Rahmen des PIPA im Falle einer Verletzung des Schutzes personenbezogener Daten spezifische Pflichten, einschließlich Meldepflichten gegenüber betroffenen Personen und der Aufsichtsbehörde, wenn die Zahl der betroffenen Personen den geltenden Schwellenwert überschreitet (Artikel 34 PIPA in Verbindung mit Artikel 39 des PIPA-Präsidialerlasses), es sei denn, es handelt sich um pseudonymisierte personenbezogene Informationen, die zu im öffentlichen Interesse liegenden statistischen Zwecken, zu wissenschaftlichen Forschungszwecken oder zu Archivzwecken verarbeitet werden (Artikel 28 Absatz 7 PIPA). Auch hier[28] hegt der EDSA Bedenken bezüglich der weit reichenden Ausnahmen für pseudonymisierte Informationen und wiederholt seine Aufforderung an die Europäische Kommission, diesen Aspekt weiter zu prüfen, um sicherzustellen, dass im koreanischen Recht ein der Sache nach gleichwertiges Schutzniveau gegeben ist.[29]

78. Dessen ungeachtet ist der EDSA insgesamt mit der Beurteilung und Schlussfolgerung der Europäischen Kommission bezüglich der der Sache nach bestehenden Gleichwertigkeit des koreanischen Rechts in Bezug auf den Grundsatz der Sicherheit und Vertraulichkeit zufrieden.

3.1.8. Grundsatz der Transparenz

79. Gemäß Artikel 5 DSGVO ist Transparenz ein tragender Grundsatz des EU-Datenschutzsystems. In Erwägungsgrund 39 der DSGVO wird die entscheidende Funktion dieses Grundsatzes folgendermaßen dargelegt: „*Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeiten werden. (...) Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im*

[27] Siehe weiter oben Rn. 51 in Abschnitt 3.1.1.1 dieser Stellungnahme sowie Rn. 52 zu den allgemeinen Bedenken des EDSA hinsichtlich der Auswirkungen der Pseudonymisierung nach koreanischem Recht.
[28] Wie bereits weiter oben in den Rn. 51-52 und in Abschnitt 3.1.1.1 dieser Stellungnahme ausgeführt.
[29] Siehe auch die Abschnitte 3.1.6 und 3.1.10 dieser Stellungnahme.

Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können."

80. In der DSGVO-Referenzgrundlage für Angemessenheit wird „Transparenz" ausdrücklich als einer der Grundsätze genannt, die bei der Beantwortung der Frage zu berücksichtigen sind, ob das von einem Drittland gebotene Schutzniveau der Sache nach gleichwertig ist. Konkret heißt es darin: „*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 enthalten, die zur Sicherung der Verarbeitung nach Treu und Glauben erforderlich sind. Unter bestimmten Voraussetzungen 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 allgemeinem öffentlichen Interesses, wie dies beispielsweise bei Artikel 23 der DSGVO der Fall ist.*"

81. Ähnlich wie in der DSGVO gibt es auch im PIPA einen allgemeinen Transparenzgrundsatz, der von den für die Verarbeitung personenbezogener Informationen Verantwortlichen verlangt, ihre Datenschutzrichtlinie und andere Unterlagen im Zusammenhang mit der Verarbeitung personenbezogener Informationen zu veröffentlichen (Artikel 3 Absatz 5 PIPA). Besondere Informationspflichten gelten, wenn für die Verarbeitung personenbezogener Informationen Verantwortliche die Einwilligung der betroffenen Personen in die Erhebung und Verarbeitung personenbezogener Informationen (Artikel 15 Absatz 2 PIPA), in die Weitergabe personenbezogener Informationen an Dritte (Artikel 17 Absatz 2 PIPA) und für eine zweckfremde Verarbeitung (Artikel 18 Absatz 3 PIPA) einholen wollen. Es ist nennenswert, dass diese Informationspflichten sinngemäß auch für den Auftragnehmer gelten (Artikel 26 Absatz 7 PIPA).

82. Der EDSA erkennt an und begrüßt die zusätzlichen Garantien in Abschnitt 3 Ziffern i und ii der Notifizierung Nr. 2021-1[30] in Bezug auf Informationen, die betroffenen Personen bei der Übermittlung ihrer Daten durch im EWR niedergelassenen Stelle bereitzustellen sind, wobei zu berücksichtigen ist, dass gemäß Artikel 20 Absatz 1 PIPA betroffene Personen, wenn die Daten nicht bei der betroffenen Person erhoben wurden, nur auf Antrag informiert werden, während ein allgemeines Recht auf Unterrichtung gemäß Artikel 20 Absatz 2 PIPA nur dann gilt, wenn bestimmte Verarbeitungsvorgänge die im PIPA-Durchführungserlass (Artikel 15 Absatz 2) festgelegten Schwellenwerte überschreiten.

83. Insgesamt ist der EDSA damit zufrieden, dass das Schutzniveau nach koreanischem Recht in Bezug auf den Transparenzgrundsatz dem in der DSGVO vorgesehenen der Sache nach gleichwertig ist.

3.1.9. Besondere Kategorien personenbezogener Daten

84. Damit das Datenschutzsystem eines Drittlands als ein dem der DSGVO der Sache nach gleichwertiges Schutzniveau für personenbezogene Daten bietend anerkannt wird, sollten besondere Garantien vorhanden sein, wenn es sich um besondere Kategorien personenbezogener Daten im Sinne der Artikel 9 und 10 DSGVO handelt.

85. Nach dem PIPA gelten besondere Bestimmungen für die Verarbeitung so genannter sensibler Informationen, zu denen personenbezogene Informationen gehören, die Auskunft geben über weltanschauliche oder religiöse Überzeugungen, die Aufnahme in eine Gewerkschaft oder eine politische Partei oder den Austritt aus einer Gewerkschaft oder politischen Partei, politische Meinungen, Gesundheit und Sexualleben, sowie andere personenbezogene Informationen, die eine erhebliche Beeinträchtigung der Privatsphäre einer betroffenen Person darstellen können, ferner – gemäß dem PIPA-Durchführungserlass – DNA-Informationen, die aus Gentests gewonnen wurden,

[30] Anhang I des Beschlussentwurfs.

Informationen, die in einem Strafregisterauszug zu finden sind, sowie personenbezogene Informationen, die aus einer besonderen technischen Verarbeitung von Daten über die physischen, physiologischen oder verhaltensbezogenen Merkmale einer Person zum Zwecke der eindeutigen Identifizierung dieser Person resultieren, und personenbezogene Informationen, aus denen die rassische oder ethnische Herkunft hervorgeht.

86. Ähnlich wie die DSGVO verbietet auch das koreanische Datenschutzrecht die Verarbeitung sensibler Daten, es sei denn, es gelten spezifische Ausnahmen, die darin bestehen, 1) die betroffene Person zu informieren und eine spezifische Einwilligung einzuholen ist, und 2) es Rechtsvorschriften gibt, die die Verarbeitung gestatten (Artikel 23 Absatz 2 PIPA).

87. Auf dieser Grundlage stimmt der EDSA grundsätzlich der Schlussfolgerung der Europäischen Kommission zu, dass das koreanische Recht in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten der Sache nach gleichwertig ist. Der EDSA weist jedoch darauf hin, dass ihm weder das PIPA-Handbuch noch Klarstellungen der PIPC zum Begriff „Sexualleben" dahingehend übermittelt wurden, dass er auch die sexuelle Ausrichtung oder die sexuellen Präferenzen einer Person abdeckt, die beide nicht in der Notifizierung Nr. 2021-1 erwähnt werden. Der EDSA fordert die Europäische Kommission daher auf, diese Informationen zur Verfügung zu stellen, um eine abhängige Prüfung derselben zu ermöglichen. Darüber hinaus fordert der EDSA die Europäische Kommission auf, konkret die Dokumente zu nennen, in denen die von ihr genannten Informationen zu diesem Thema zu finden sind.

3.1.10. Recht auf Auskunft, Berichtigung, Löschung und Widerspruch

88. Im koreanischen Rechtsrahmen werden die Rechte betroffener Personen in Artikel 3 Absatz 5 PIPA anerkannt. Danach gewährleitet der für die Verarbeitung der personenbezogenen Informationen Verantwortliche die in Artikel 4 PIPA aufgeführten und in den Artikeln 35 bis 37, 39 und 39 Absatz 2 PIPA näher spezifizierten Rechte der betroffenen Person sowie in Bezug auf „personenbezogene Kreditinformationen" (d. h. Kreditinformationen, also Daten, die zur Feststellung der Kreditwürdigkeit von Parteien finanzieller oder kommerzieller Transaktionen erforderlich sind – siehe Erwägungsgrund 3 des Beschlussentwurfs), in den Artikeln 37, 38 und 38 Absatz 3 CIA.

89. Der EDSA stellt fest, dass das Recht auf Auskunft (sowie auf Berichtigung und Löschung, die von einer *„betroffenen Person, die gemäß Artikel 35 PIPA Auskunft über ihre personenbezogenen Informationen erhalten hat",* ausgeübt werden kann), eingeschränkt oder verweigert werden kann, *„wenn die Auskunft durch Gesetz untersagt oder eingeschränkt ist*", *„wenn die Auskunft das Leben oder die körperliche Unversehrtheit eines Dritten schädigen oder eine ungerechtfertigte Verletzung von Eigentum oder sonstigen Interessen einer anderen Person verursachen kann*", und außerdem für öffentliche Einrichtungen, wenn die Auskunft bei der Wahrnehmung bestimmter Aufgaben nach Artikel 35 Absatz 4 PIPA[31] *„erhebliche Schwierigkeiten verursachen würde*". Ähnliche Bestimmungen finden sich auch in Artikel 37 PIPA über das Recht auf Aussetzung der Verarbeitung personenbezogener Informationen.

90. Artikel 23 DSGVO eröffnet die Möglichkeit, durch Rechtsvorschriften der Union oder der Mitgliedstaaten die Rechte des Einzelnen zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt und solche Beschränkungen vorsieht, um unter anderem den Schutz der betroffenen Person oder die Rechte und Freiheiten anderer sowie *„Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung*

[31] Die gleichen Bedingungen und Ausnahmen von den im PIPA vorgesehenen Auskunfts- und Berichtigungsrechten gelten auch in Bezug auf das im CIA für personenbezogene Kreditinformationen vorgesehene Recht auf Auskunft und Berichtigung (Fußnote 135 des Beschlussentwurfs).

öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecken verbunden sind“, zu schützen.

91. Vor diesem Hintergrund würde der EDSA allgemeine Zusicherungen im Beschlussentwurf begrüßen, wonach es zur Einschränkung der Betroffenenrechte eines Gesetzes oder einer Vorschrift bedarf, welche die Anforderungen der koreanischen Verfassung einhält, wonach ein Grundrecht nur eingeschränkt werden darf, wenn dies für die nationale Sicherheit oder die Aufrechterhaltung der öffentlichen Ordnung erforderlich ist, und dass diese Einschränkung den Wesensgehalt der betreffenden Freiheit oder des betreffenden Rechts nicht beeinträchtigen darf (Artikel 37 Absatz 2 der koreanischen Verfassung).

92. Mit Blick auf die Ausnahme betreffend „*eine ungerechtfertigte Verletzung von Eigentums- oder sonstigen Interessen anderer Personen*“ erkennt der EDSA an, dass dies „*impliziert, dass ein Ausgleich zwischen den verfassungsrechtlich geschützten Rechten und Freiheiten des Einzelnen einerseits und denen anderer Personen andererseits vorgenommen werden sollte*“[32]; er fordert die Europäische Kommission jedoch auf, die Anwendung dieser Ausnahme und der einschlägigen Rechtsprechung umfassend zu überwachen, um sicherzustellen, dass ein gleichwertiges Schutzniveau für die Rechte der betroffenen Personen auch in der Praxis gewährleistet ist.

93. Desgleichen würde der EDSA eine aufmerksame Überwachung der Anwendung der Ausnahmeregelung für öffentliche Einrichtungen begrüßen, insbesondere in Bezug auf die Fälle, in denen die Erteilung von Auskünften als „*erhebliche Schwierigkeiten bereitend*“ bei der Erfüllung ihrer Aufgaben angesehen würde, da dieser Begriff weiter gefasst zu sein scheint als in anderen Bestimmungen des PIPA, z. B. in Artikel 18 Absatz 2 Ziffer 5[33] und restriktiv ausgelegt werden sollte, um ungerechtfertigte Einschränkungen der Rechte betroffener Personen zu vermeiden.

94. Darüber hinaus hat der EDSA Bedenken dahingehend, ob die Ausnahmen, nach denen die Bestimmungen über Transparenz auf Antrag (Artikel 20 PIPA) und die Betroffenenrechte (Artikel 35 bis 37 PIPA) – sowie ähnliche Bestimmungen über die Anforderungen an Anbieter von Informations- und Kommunikationsdiensten (Artikel 39 Absatz 2, Artikel 39 Absätze 6 bis 8 PIPA) und die im CIA enthaltenen Bestimmungen (siehe Ausnahmen nach Artikel 40 Absatz 3 CIA) – in Bezug auf pseudonymisierte Informationen nicht gelten, wenn diese zu im öffentlichen Interesse liegenden statistischen Zwecken, wissenschaftlichen Zwecken oder Archivzwecken verarbeitet werden (Artikel 28 Absatz 7 PIPA), und dies im Einklang mit den Garantien im europäischen Rechtsrahmen steht.

95. Diese Bestimmungen scheinen eine allgemeine Ausnahmeregelung für diese Art der Verarbeitung einzuführen, während in der DSGVO vorgesehen ist, dass in Fällen, in denen personenbezogene Daten (einschließlich pseudonymisierter personenbezogener Daten) zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden, im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Betroffenenrechte vorgesehen werden können, „*als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind*“, wobei die Pseudonymisierung nur eine der technischen und organisatorischen Maßnahmen ist, mit der die Einhaltung von Artikel 89 Absatz 1 DSGVO gewährleistet werden kann.

96. Die Europäische Kommission hält die in Artikel 28 Absatz 7 PIPA vorgesehene Ausnahmeregelung auch mit Blick auf Artikel 28 Absatz 5 PIPA für gerechtfertigt, wonach es dem für die Verarbeitung

[32] Erwägungsgrund 76 des Beschlussentwurfs.

[33] In Bezug auf Ausnahmen von der Beschränkung der zweckfremden Verwendung und Bereitstellung personenbezogener Informationen, spricht Artikel 18 Absatz 2 Ziffer 5 PIPA von Situationen, in denen es öffentlichen Einrichtungen *unmöglich ist*, die Aufgaben wahrzunehmen.

personenbezogener Informationen Verantwortlichen ausdrücklich untersagt ist, pseudonymisierte Informationen zum Zwecke der Identifizierung einer bestimmten Person zu verarbeiten, und verweist auf den Ansatz von Artikel 11 Absatz 2 DSGVO (in Verbindung mit Erwägungsgrund 57 DSGVO) in Bezug auf Verarbeitungen, für die eine Identifizierung nicht erforderlich ist.[34]

97. Nach Artikel 11 DSGVO ist der Verantwortliche nämlich nicht verpflichtet, zur bloßen Einhaltung der DSGVO *„zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten*, *um die betroffene Person zu identifizieren"*, wenn er für die beabsichtigten Zwecke personenbezogene Daten verarbeiten darf, die die Identifizierung einer betroffenen Person nicht oder nicht mehr erfordern; kann der Verantwortliche in solchen Fällen nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, finden die Betroffenenrechte keine Anwendung. Wie von der Europäischen Kommission festgestellt[35], schreibt die DSGVO daher in solchen Fällen eine „praktische" Unmöglichkeit für den Verantwortlichen vor und erkennt im Einklang mit dem Grundsatz der Datenminimierung an, dass keine zusätzlichen Daten „aufgrund" der DSGVO verarbeitet werden müssen.

98. Der EDSA ist jedoch der Auffassung, dass sich diese Situation von derjenigen unterscheidet, in der ein Verantwortlicher praktisch in der Lage ist, die betroffene Person zu identifizieren, dies aber aufgrund einer gesetzlichen Bestimmung wie der in Artikel 28 Absatz 5 PIPA nicht tun darf. In diesem Zusammenhang begrüßt der EDSA die Klarstellungen der PIPC in der Notifizierung Nr. 2021-1[36], in der bestätigt wird, dass Abschnitt 3 PIPA (einschließlich Artikel 28 Absatz 7) und die Ausnahme nach Artikel 40 Absatz 3 CIA nur dann Anwendung finden, wenn pseudonymisierte Informationen zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken, statistischen Zwecken oder Archivzwecken verarbeitet werden. Allerdings fragt sich der EDSA, abgesehen von den bereits erwähnten Bedenken hinsichtlich desverbindlichen Charakters der Notifizierung Nr. 2021-1[37], nach wie vor, ob die in Artikel 28 Absatz 7 PIPA und Artikel 40 Absatz 3 CIA vorgesehenen Ausnahmen in einer demokratischen Gesellschaft als erforderlich und verhältnismäßig angesehen werden könnten, da sie die Rechte der betroffenen Personen in allen Fällen einschränken, in denen pseudonymisierte Informationen für solche Zwecke verarbeitet werden, d. h. auch dann, wenn der für die Verarbeitung personenbezogener Informationen Verantwortliche praktisch in der Lage ist, die betroffene Person zu identifizieren, und die Rechte das Erreichen der spezifischen Zwecke voraussichtlich nicht unmöglich machen oder ernsthaft behindern.

99. Der EDSA befürchtet insbesondere, dass diese Ausnahmeregelungen nicht gerechtfertigt wären und weiter geprüft werden müssten, vor allem wenn sie von dem für die Verarbeitung personenbezogener Informationen Verantwortlichen angewandt werden, der die Daten *„im öffentlichen Interesse zu statistischen Zwecken, wissenschaftlichen Forschungszwecken und Archivzwecken usw.*" pseudonymisiert, gemäß Artikel 28 Absatz 2PIPA *„ohne Einwilligung der betroffenen Personen*" (und ohne die in Artikel 20 PIPA vorgesehenen Informationen bereitzustellen)[38], sofern dieser Verantwortliche die Informationen aufbewahrt, die eine erneute Identifizierung ermöglichen. Nach

[34] Es sei darauf hingewiesen, dass diese Argumentation als solche nicht für die in Artikel 40 Absatz 3 CIA vorgesehene Ausnahme für die Verarbeitung pseudonymisierter Kreditinformationen gelten würde, da Artikel 40 Absatz 2 Satz 6 Folgendes vorsieht: *„Ein Kreditinformationsunternehmen usw. verarbeitet pseudonymisierte Informationen nicht auf eine Weise, die die Identifizierung einer bestimmten Person für Gewinnerzielungsabsicht oder unlautere Zwecke ermöglicht*" und könnte daher eine erneute Identifizierung zu einem lauteren Zweck wie dem ermöglichen, einem Antrag der betroffenen Person nachzukommen.

[35] Siehe Erwägungsgrund 82 des Beschlussentwurfs.

[36] Anhang I Abschnitt 4 des Beschlussentwurfs.

[37] Siehe weiter oben Abschnitt 3.1.1.1.

[38] Siehe Artikel 28 Absatz 7 PIPA, wie in der Notifizierung Nr. 2021-1 erläutert, wonach bestimmte Garantien des PIPA, nämlich *„Artikel 20, Artikel 21, Artikel 27, Artikel 34 Absatz 1, Artikel 35 bis 37, Artikel 39 Absatz 3, Artikel 39 Absatz 4, Artikel 39 Absätze 6 bis 8* ", nicht für pseudonymisierte Informationen gelten, die zum Zweck der Erstellung von Statistiken, der wissenschaftlichen Forschung, der Aufbewahrung öffentlicher Register usw. verarbeitet werden.

der DSGVO sollten Personen in der Lage sein, ihre Rechte in Bezug auf alle Daten auszuüben, mit denen sie identifiziert oder ausgesondert werden können, selbst wenn die Daten als „pseudonymisiert“ gelten, sofern nicht der bereits erwähnte Artikel 11 DSGVO Anwendung findet. In diesem Zusammenhang stellt der EDSA fest, dass nur dann, wenn diese Daten einem Dritten für dieselben statistischen Zwecke, wissenschaftlichen Forschungszwecke und Archivzwecke zur Verfügung gestellt werden, Daten, die zur Identifizierung einer bestimmten Person verwendet werden können, nicht aufgenommen werden sollten, und dass daher nur der für die Verarbeitung personenbezogener Informationen Verantwortliche, dem pseudonymisierte Daten gemäß Artikel 28 Absatz 2 Satz 2 PIPA bereitgestellt werden, wahrscheinlich „praktisch“ nicht in der Lage wäre, die betroffene Person ohne zusätzliche Informationen zu identifizieren.

100. Kurz zusammengefasst: In der Erwägung, dass das PIPA, wie von der Europäischen Kommission anerkannt, „*nicht auf die Pseudonymisierung als mögliche Schutzmaßnahme setzt, sondern sie als Vorbedingung für die Durchführung bestimmter Verarbeitungstätigkeiten zu im öffentlichen Interesse liegenden statistischen Zwecken, zu wissenschaftlichen Forschungszwecken und zu Archivzwecken vorschreibt (z. B. um die Daten ohne Einwilligung verarbeiten zu können oder verschiedene Datensätze zu kombinieren)*“[39], sondern für derartige Fälle erhebliche Einschränkungen der Rechte der betroffenen Personen vorsieht, fordert der EDSA die Europäische Kommission auf, die Ausnahmen in Artikel 28 Absatz 7 PIPA und Artikel 40 Absatz 3 CUA näher zu prüfen und ihre Anwendung und die einschlägige Rechtsprechung[40] aufmerksam zu überwachen, um sicherzustellen, dass die Rechte der betroffenen Personen nicht über Gebühr eingeschränkt werden, wenn auf Grundlage dieses Angemessenheitsbeschlusses übermittelte personenbezogene Daten zu diesen Zwecken verarbeitet werden, wobei in vielen Fällen diese Rechte auch dem Verantwortlichen helfen, die Qualität der verarbeiteten Daten zu gewährleisten.

3.1.11. Beschränkungen für Weiterübermittlungen

101. In der DSGVO-Referenzgrundlage für Angemessenheit wird klargestellt, dass das Schutzniveau für natürliche Personen, deren personenbezogene Daten im Rahmen eines Angemessenheitsbeschlusses übermittelt werden, durch die Weiterübermittlung nicht untergraben werden darf und daher jede Weiterübermittlung „*nur dann zulässig sein [sollte], 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*“.

102. Was die Weiterübermittlung an Auftragnehmer (d. h. „Auftragsverarbeiter“) in anderen Drittländern anbelangt, so stellt der EDSA fest, dass der koreanische Rechtsrahmen keine besonderen Vorschriften für diese Fälle enthält und dass ein koreanischer für die Verarbeitung personenbezogener Informationen Verantwortlicher nach Auffassung der Europäischen Kommission[41] die Einhaltung der Bestimmungen des PIPA über die Auslagerung (Artikel 26 PIPA) durch ein rechtsverbindliches Instrument sicherstellen muss und er für die ausgelagerten personenbezogenen Informationen verantwortlich ist (Artikel 26 PIPA).

103. In Bezug auf die Weiterübermittlung an Dritte (d. h. andere für die Verarbeitung personenbezogener Informationen Verantwortliche) muss ein koreanischer für die Verarbeitung personenbezogener Informationen Verantwortlicher gemäß Artikel 17 Absatz 3 PIPA die betroffenen Personen über die Übermittlungen ins Ausland informieren und deren Einwilligung einholen und „[er] *darf keinen*

[39] Erwägungsgrund 42 des Beschlussentwurfs.
[40] Siehe beispielsweise die verfassungsrechtliche Problematik des Open Net (Informationen unter https://opennet.or.kr/19909, nur in koreanischer Sprache verfügbar).
[41] Erwägungsgrund 87 des Beschlussentwurfs.

Vertrag über die grenzüberschreitende Übermittlung personenbezogener Daten schließen, der gegen das PIPA verstößt". Der EDSA stellt fest, dass mit dieser letzten Bestimmung – nach Auffassung der Europäischen Kommission[42] – sichergestellt wird, dass kein Vertrag über grenzüberschreitende Datenübermittlungen Pflichten enthalten kann, die im Widerspruch zu den Anforderungen stehen, die das PIPA dem für die Verarbeitung personenbezogener Informationen Verantwortlichen auferlegt, und dass sie daher als Garantie betrachtet werden könnte; sie enthält jedoch keine Verpflichtung zur Einführung von Sicherheitsvorkehrungen, um sicherzustellen, dass der Empfänger das gleiche Schutzniveau wie das PIPA bietet. Daher geht der EDSA davon aus, dass die informierte Einwilligung der betroffenen Person in der Regel als Grundlage für Datenübermittlungen von einem koreanischen für die Verarbeitung personenbezogener Informationen Verantwortlichen an einen Empfänger mit Sitz in einem Drittland herangezogen wird.

104. In diesem Zusammenhang begrüßt er die zusätzlichen Klarstellungen der PIPC in der Notifizierung Nr. 2021-1 in Bezug auf die Verpflichtung zur Unterrichtung von Personen über das Drittland, in das ihre Daten übermittelt werden[43], da dies – wie von der Europäischen Kommission unterstrichen[44] – betroffenen Personen im EWR dabei helfen würde, in voller Kenntnis der Sachlage zu entscheiden, ob sie einer Übermittlung in das Ausland zustimmen oder nicht.

105. Wie auch in der Stellungnahme 28/2018 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten in Japan dargelegt, ist jedoch hervorzuheben, dass betroffene Personen gemäß der DSGVO ausdrücklich über die möglichen Risiken solcher Übermittlungen informiert werden müssen, die sich aus dem Fehlen eines angemessenen Schutzes in dem Drittland und dem Fehlen geeigneter Garantien ergeben, bevor eine Einwilligung erteilt wird. Eine solche Erklärung sollte beispielsweise die Information enthalten, dass es in dem Drittland möglicherweise keine Aufsichtsbehörde gibt und/oder keine Datenverarbeitungsgrundsätze bestehen und/oder dass den betroffenen Personen in dem Drittland möglicherweise keine Betroffenenrechte zustehen.[45] Für den EDSA ist die Erteilung dieser Informationen von wesentlicher Bedeutung, damit die betroffene Person eine informierte Einwilligung in voller Kenntnis der konkreten Umstände der Übermittlung erteilen kann.[46] Der EDSA hat daher Bedenken hinsichtlich der Feststellungen der Europäischen Kommission im Entwurf des Angemessenheitsbeschlusses in Bezug auf diese spezifische Art von Übermittlungen. Betroffene Personen sind in der Regel nicht mit dem Datenschutzrahmen in Drittländern vertraut. Daher kann nicht geschlossen werden, dass eine betroffene Person das Risiko einer Datenübermittlung beurteilen könnte, wenn sie nur das jeweilige Bestimmungsland kennt. Vielmehr müssen vor der Einwilligung der betroffenen Person klare Informationen über die spezifischen Risiken einer solchen Übermittlung personenbezogener Daten an ein Land außerhalb des Hoheitsgebiets der Republik Korea zur Verfügung gestellt werden.

106. Daher fordert der EDSA die Europäische Kommission auf, dafür zu sorgen, dass die Informationen, die der betroffenen Person „*über die Umstände der Übermittlung*" erteilt werden, Informationen über die möglichen Risiken der Übermittlung enthalten, die sich aus dem Fehlen eines angemessenen Schutzes und angemessener Garantien in dem Drittland ergeben. Dies ist für den EDSA wichtig, um beurteilen zu können, ob die Anforderungen an die Einwilligung der Sache nach denen der DSGVO gleichwertig sind.

107. Darüber hinaus würde der EDSA angesichts der Tatsache, dass die Einwilligung freiwillig, in Kenntnis der Sachlage, für den bestimmten Fall und unmissverständlich erfolgen muss, die Zusicherung in dem

[42] Erwägungsgrund 88 des Beschlussentwurfs.
[43] Ebenda.
[44] Ebenda.
[45] Leitlinien des EDSA 2/2018 über Ausnahmen von Artikel 49 der Verordnung (EU) 2016/679, 25. Mai 2018, S. 9.
[46] Leitlinien des EDSA 2/2018 über Ausnahmen von Artikel 49 der Verordnung (EU) 2016/679, 25. Mai 2018, S. 9.

Angemessenheitsbeschluss begrüßen, dass personenbezogene Daten nicht von koreanischen für die Verarbeitung personenbezogener Informationen Verantwortlichen an einen Dritten in einem Drittland übermittelt werden, wenn nach der DSGVO keine rechtswirksame Einwilligung erteilt werden konnte, z. B. wegen eines Machtungleichgewichts.

108. Mit Blick auf Fälle, in denen der für die Verarbeitung personenbezogener Informationen Verantwortliche personenbezogene Informationen einem Dritten im Ausland ohne die Einwilligung der betroffenen Person zur Verfügung stellen darf – wenn also 1) personenbezogene Informationen zu einem Zweck, der mit dem ursprünglichen Zweck der Erhebung gemäß Artikel 17 Absatz 4 PIPA in einem angemessenen Zusammenhang steht, bereitgestellt werden, und wenn 2) personenbezogene Informationen in den in Artikel 18 Absatz 2 PIPA genannten Ausnahmefällen Dritten bereitgestellt werden können –, nimmt der EDSA die Klarstellungen der PIPC in Abschnitt 2 der Notifizierung Nr. 2021-1 zur Kenntnis (und begrüßt die vorgesehene Pflicht des koreanischen Verantwortlichen und des Empfängers im Ausland, durch ein rechtsverbindliches Instrument (wie einen Vertrag) ein Schutzniveau zu gewährleisten, das dem PIPA gleichwertig ist, auch in Bezug auf die Rechte der betroffenen Person).

3.1.12. Direktwerbung

109. Gemäß Artikel 21 Absatz 2 und Artikel 21 Absatz 3 DSGVO und der DSGVO-Referenzgrundlage für Angemessenheit muss es für die betroffene Person jederzeit möglich sein, unentgeltlich der Datenverarbeitung zum Zwecke des Profiling und der Direktwerbung zu widersprechen.

110. In Bezug auf das in Artikel 37 PIPA vorgesehene Recht auf Aussetzung nimmt der EDSA zur Kenntnis, dass nach Auffassung der Europäischen Kommission dieses Recht auch dann gilt, wenn Daten für Zwecke der Direktwerbung verwendet werden.[47] Der EDSA würde jedoch zusätzliche Informationen und Klarstellungen im Beschlussentwurf zu dieser Einschätzung und insbesondere zur praktischen Anwendung des Rechts auf Aussetzung im Zusammenhang mit Direktwerbung begrüßen (z. B. Verweise auf die einschlägige Rechtsprechung usw.). In diesem Zusammenhang weist der EDSA auch darauf hin, dass das Recht, von einem Kreditinformationsanbieter/-nutzer zu verlangen, eine Person nicht mehr zu kontaktieren, um ihr Waren oder Dienstleistungen vorzustellen und zu deren Kauf aufzufordern, im CIA eindeutig geregelt ist (Artikel 37 Absatz 2).

111. Wie von der Europäischen Kommission anerkannt[48], erfordert eine solche Verarbeitung im koreanischen Rechtsrahmen im Allgemeinen die konkrete (zusätzliche) Einwilligung der betroffenen Person (siehe Artikel 15 Absatz 1 Ziffer 1, Artikel 17 Absatz 2 Ziffer 1 PIPA).

112. Da nicht ausgeschlossen werden kann, dass aus dem EWR übermittelte personenbezogene Daten in Korea möglicherweise für solche Zwecke verarbeitet werden, würde der EDSA auch Klarstellungen im Angemessenheitsbeschluss begrüßen, die das Recht der betroffenen Person auf Widerruf ihrer Einwilligung[49] und das Recht auf Löschung und Einstellung der weiteren Verarbeitung ihrer personenbezogenen Daten betreffen, wenn sich die Verarbeitung auf ihre Einwilligung stützt (z. B. bei einer Verarbeitung zu Marketingzwecken) und die betroffene Person diese widerrufen hat.

3.1.13. Automatisierte Entscheidungsfindung und Profiling

113. Wie die Europäische Kommission in ihrem Beschlussentwurf ausführt[50], enthalten das PIPA und der entsprechende Durchführungserlass keine allgemeinen Bestimmungen, die sich mit Entscheidungen

[47] Erwägungsgrund 79 des Beschlussentwurfs.
[48] Ebenda.
[49] Siehe auch oben Rn. 67: Während die Möglichkeit, die Einwilligung zu widerrufen, in Artikel 37 Absatz 1 CIA eindeutig vorgesehen ist, wird dieses Recht im PIPA nur zweimal, nämlich in Artikel 27 Absatz 1 Ziffer 2 und Artikel 39 Absatz 7, für besondere Umstände erwähnt.
[50] Siehe Erwägungsgrund 81 des Beschlussentwurfs.

befassen, die die betroffene Person betreffen und ausschließlich auf der automatisierten Verarbeitung personenbezogener Daten beruhen. Dennoch sieht die koreanische Rechtsordnung ein solches Recht im CIA vor, das Vorschriften über automatisierte Entscheidungen (Artikel 36 Absatz 2) enthält, auch wenn ihre Anwendung offenbar nicht unter die Aufsicht durch die PIPC fällt (und somit nicht in den Anwendungsbereich dieses Beschlussentwurfs fällt – siehe weiter oben Abschnitt 2.3.2 zum Anwendungsbereich des Beschlussentwurfs).

114. Wie bereits von der Artikel 29-Datenschutzgruppe[51] in ihrer Stellungnahme 1/2016 zum Datenschutzschild und vom EDSA in seiner früheren Stellungnahme zum Angemessenheitsbeschluss in Bezug auf Japan[52] erwogen, würde die zunehmende Bedeutung der automatisierten Entscheidungsfindung, der Erstellung von Profilen und von KI in dieser Hinsicht auf einen stärker schützenden Ansatz hindeuten. Entgegen dem Vorbringen der Europäischen Kommission[53], dass das Fehlen spezifischer Vorschriften für die automatisierte Entscheidungsfindung im PIPA das Schutzniveau für in der Union erhobene personenbezogene Daten nicht beeinträchtigen dürfte (da jede Entscheidung auf der Grundlage einer automatisierten Verarbeitung in der Regel vom Verantwortlichen in der Union getroffen würde, der in direktem Zusammenhang mit der betroffenen Person steht), kann nach Auffassung des EDSA nicht ausgeschlossen werden, dass automatisierte Entscheidungen von einem koreanischen für die Verarbeitung personenbezogener Informationen Verantwortlichen getroffen werden können, wenn Daten auf Grundlage des Angemessenheitsbeschlusses übermittelt werden (z. B. im Beschäftigungskontext, bei der Beurteilung der Leistung bei der Arbeit, der Zuverlässigkeit, des Verhaltens usw.).

115. Die Entwicklung neuer Technologien ermöglicht es den Unternehmen, automatisierte Entscheidungssysteme leichter umzusetzen oder in Erwägung zu ziehen, was zu einer Schwächung der Stellung von Personen führen kann. Wenn Entscheidungen, die ausschließlich von diesen automatisierten Systemen getroffen werden, Auswirkungen auf die Rechtsstellung von Personen haben oder sie erheblich beeinträchtigen (z. B. durch die Erstellung von schwarzen Listen, wodurch Personen ihrer Rechte beraubt werden), ist es von entscheidender Bedeutung, ausreichende Garantien vorzusehen, einschließlich des Rechts auf Unterrichtung über die besonderen Gründe, die der Entscheidung und der angewandten Logik zugrunde liegen, um unrichtige oder unvollständige Angaben zu berichtigen und die Entscheidung anzufechten, wenn sie auf der Grundlage einer falschen Sachlage getroffen wurde[54].

116. In diesem Zusammenhang hat der EDSA Bedenken hinsichtlich des Fehlens von Rechtsvorschriften über die automatisierte Entscheidungsfindung im PIPA und fordert die Europäische Kommission daher auf, sich mit diesen Bedenken auseinanderzusetzen und die Entwicklung des koreanischen Rechtsrahmens in dieser Hinsicht weiterhin zu überwachen.

3.1.14. Rechenschaftspflicht

117. Der koreanische Rechtsrahmen enthält mehrere Vorschriften, mit denen sichergestellt werden soll, dass die für die Verarbeitung personenbezogener Informationen Verantwortlichen geeignete technische und organisatorische Maßnahmen ergreifen, um ihren Datenschutzpflichten wirksam nachzukommen und diese Einhaltung unter anderem gegenüber der zuständigen Aufsichtsbehörde nachzuweisen. Der EDSA begrüßt insbesondere die Existenz von Vorschriften über die

[51] Diese Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie war ein unabhängiges europäisches Beratungsgremium für den Datenschutz und den Schutz der Privatsphäre. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG beschrieben. Aus der Artikel 29-Datenschutzgruppe (WP29) ist nunmehr der EDSA geworden.

[52] Stellungnahme 28/2018 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten in Japan, angenommen am 5. Dezember 2018.

[53] Erwägungsgrund 81 des Beschlussentwurfs.

[54] WP 254, S. 7.

Implementierung eines internen Managementplans (Artikel 29 PIPA), die Verpflichtung zur Durchführung einer so genannten Folgenabschätzung hinsichtlich der Auswirkungen auf die Privatsphäre (auf Englisch: *privacy impact assessment*, „**PIA**“) für Fälle, in denen die Verarbeitung ein höheres Risiko möglicher Verletzungen der Privatsphäre birgt (Artikel 33 Absatz 1 PIPA und Artikel 35 PIPA-Durchführungserlass), Vorschriften für die Schulung und Überwachung des Personals (Artikel 28 PIPA) sowie die Pflicht zur Benennung eines Datenschutzbeauftragten (Artikel 31 PIPA in Verbindung mit Artikel 32 PIPA-Durchführungserlass).

118. Der EDSA teilt die Auffassung der Europäischen Kommission in Bezug auf den von ihnen gewährleisteten der Sache nach gleichwertigen Schutz – selbst in Fällen, in denen die Vorschriften offenbar ziemlich von denen der DSGVO abweichen; so gibt es z. B. keine Bestimmung, wonach der Datenschutzbeauftragte unabhängig sein muss, doch ist eindeutig festgelegt, dass er dem Management des für die Verarbeitung der personenbezogenen Informationen Verantwortlichen Bericht erstatten muss (Artikel 31 Absatz 4 PIPA) und dass er/sie bei der Wahrnehmung dieser Aufgaben keine ungerechtfertigten Nachteile erleiden darf (Artikel 31 Absatz 5 PIPA) - und würde der Europäischen Kommission vorschlagen, bei der Überprüfung des Angemessenheitsbeschlusses die tatsächliche Anwendung dieser Bestimmungen zu überwachen, um sicherzustellen, dass sie wirksam angewandt werden.

3.2. Verfahrens- und Durchsetzungsmechanismen

119. Ausgehend von den in der DSGVO-Referenzgrundlage für Angemessenheit festgelegten Kriterien hat der EDSA folgende Aspekte des koreanischen Datenschutzrechtsrahmens analysiert, die vom Beschlussentwurfs umfasst sind: das Bestehen und wirksame Funktionieren einer unabhängigen Aufsichtsbehörde; das Vorhandensein eines Systems, das ein hohes Maß an Konformität gewährleistet, sowie das Bestehen eines Systems für den Zugang zu geeigneten Rechtsschutzverfahren, die natürlichen Personen in der EU die Möglichkeit bieten, ihre Rechte wahrzunehmen und Rechtsbehelfe einzulegen, ohne dabei auf große Hürden zu stoßen.

120. Gemäß Kapitel VI der DSGVO und Kapitel 3 der DSGVO-Referenzgrundlage für Angemessenheit muss es eine oder mehrere unabhängige Aufsichtsbehörde(n) geben, deren Aufgabe die Überwachung, Sicherstellung und Durchsetzung der Einhaltung der Bestimmungen über den Datenschutz und den Schutz der Privatsphäre in einem Drittland ist, um ein dem Schutzniveau im EWR gleichwertiges Schutzniveau zu gewährleisten.

121. In diesem Zusammenhang muss die Aufsichtsbehörde des Drittlands bei der Wahrnehmung ihrer Aufgaben und Befugnisse völlig unabhängig und unparteiisch handeln und darf dabei weder Weisungen anfordern noch entgegennehmen. Darüber hinaus sollte die Aufsichtsbehörde über alle erforderlichen Befugnisse und Aufgaben verfügen, um die Einhaltung der Datenschutzrechte zu gewährleisten und das Bewusstsein für den Datenschutz zu fördern. Ferner ist die Aufsichtsbehörde angemessen mit Personal und Haushaltsmitteln auszustatten. Die Aufsichtsbehörde sollte darüber hinaus von sich aus Verfahren einleiten können.

3.2.1. Zuständige unabhängige Aufsichtsbehörde

122. In der Republik Korea ist die PIPC die unabhängige Behörde für die Überwachung und Durchsetzung des PIPA. Die PIPC besteht aus einem Vorsitzenden, einem stellvertretenden Vorsitzenden und sieben Kommissionsmitgliedern. Der Vorsitzende und der stellvertretende Vorsitzende werden vom Präsidenten auf Empfehlung des Premierministers ernannt. Zwei der Kommissionsmitglieder werden auf Empfehlung des Vorsitzenden ernannt, zwei auf Empfehlung von Vertretern der politischen Partei, der der Präsident angehört, und die drei übrigen auf Empfehlung von Vertretern anderer politischer Parteien (Artikel 7 Absatz 2 Satz 2 PIPA). Die PIPC wird von einem Sekretariat unterstützt (Artikel 7 Absatz 13) und kann Unterausschüsse (bestehend aus drei Kommissionsmitgliedern) einsetzen, die

sich mit geringfügigen Verstößen und wiederkehrenden Angelegenheiten befassen (Artikel 7 Absatz 12 PIPA).

123. In diesem Sinne erkennt der EDSA an, dass die PIPC trotz ihrer jüngsten Umstrukturierung, durch die ihr Status und ihre Befugnisse grundlegend verändert wurden, erhebliche Anstrengungen unternommen hat, um die erforderliche Infrastruktur für die Umsetzung des PIPA und seiner jüngsten Änderungen aufzubauen. Zu diesen Bemühungen zählen die Ausarbeitung der Geschäftsordnung der PIPC, die Ausarbeitung von Leitlinien für die Auslegung des PIPA und die Einrichtung einer Hotline für die Beratung von Unternehmern und Einzelpersonen zu Datenschutzbestimmungen sowie einer Schlichtungsstelle für die Bearbeitung von Beschwerden. Zu den Aufgaben der PIPC gehören insbesondere die Beratung in Bezug auf Gesetze und Vorschriften im Bereich des Datenschutzes, die Entwicklung von Datenschutzrichtlinien und -leitlinien, die Untersuchung von Verletzungen der Betroffenenrechte, die Bearbeitung von Beschwerden und die Schlichtung von Streitigkeiten, die Durchsetzung des PIPA, die Gewährleistung von Schulung und Aufklärung im Bereich des Datenschutzes sowie der Austausch und die Zusammenarbeit mit Datenschutzbehörden von Drittländern.[55]

124. Die Ernennung der Mitglieder und die Zusammensetzung der PIPC sind in Artikel 7 Absatz 2 PIPA geregelt. Obwohl die PIPC in die Zuständigkeit des Premierministers fällt (und der Vorsitzende und der stellvertretende Vorsitzende vom Präsidenten auf Empfehlung des Premierministers ernannt werden), ist den Kommissionsmitgliedern durch den Rechtsrahmen vorgeschrieben, dass sie ihre Aufgaben unabhängig nach dem Gesetz und ihrem Gewissen wahrzunehmen haben. Der EDSA erkennt die institutionellen und verfahrensrechtlichen Garantien an, die im PIPA und insbesondere in Artikel 7 Absätze 4 bis 7 enthalten sind. Dennoch würde der EDSA es begrüßen, wenn die Europäische Kommission alle Entwicklungen überwachen würde, die die Unabhängigkeit der Mitglieder der südkoreanischen Aufsichtsbehörde beeinträchtigen könnten.

125. Darüber hinaus enthält der Beschlussentwurf noch keine Analyse des Haushalts der PIPC, einschließlich der Finanzierungsquellen und der Haushaltstransparenz. Nach Auffassung des EDSA muss dieser Aspekt, der sowohl in Artikel 56 Absatz 1 DSGVO als auch in den Verfahrens- und Durchsetzungsmechanismen genannt wird, die bei der Beurteilung des Systems eines Landes oder einer internationalen Organisation nach der DSGVO-Referenzgrundlage für Angemessenheit zu prüfen sind, eingehend berücksichtigt werden, da es sich dabei um einen Indikator für die wirtschaftlichen und personellen Ressourcen handelt, die der Aufsichtsbehörde für die unabhängige Erfüllung ihrer gesetzlichen Datenschutzpflichten und -aufgaben zur Verfügung stehen, und er empfiehlt daher der Europäischen Kommission, dies im Beschlussentwurf eingehender zu berücksichtigen.

3.2.2. Vorhandensein eines Datenschutzsystems, das ein hohes Maß an Einhaltung der Vorschriften gewährleistet

126. Im Bereich der Durchsetzung erkennt der EDSA die Bandbreite der Durchsetzungsbefugnisse und Sanktionen der PIPC an, wie sie im PIPA und im CIA vorgesehen sind, und nimmt die in der Notifizierung Nr. 2021-1 enthaltenen Klarstellungen zur Kenntnis, wonach die in Artikel 64 Absatz 1 PIPA und Artikel 45 Absatz 4 CIA[56] genannten Bedingungen bei Verstößen gegen Grundsätze, Rechte und Pflichten, die im Gesetz zum Schutz personenbezogener Informationen enthalten sind, anzuwenden sind. Er empfiehlt der Europäischen Kommission jedoch, die praktische Anwendung der Befugnisse der PIPC genau zu überwachen, den Zuwiderhandelnden anzuweisen, die von ihr nach

[55] Die Aufgaben und Befugnisse der PIPC sind im Wesentlichen in Artikel 7 Absätze 8 und 9 sowie in den Artikeln 61 bis 66 PIPA festgelegt.

[56] D. h., *„es wird davon ausgegangen, dass ein Verstoß gegen das Gesetz wahrscheinlich die Rechte und Freiheiten des Einzelnen in Bezug auf personenbezogene Informationen verletzt, und dass Untätigkeit einen schwer zu behebenden Schaden verursachen kann*“.

Artikel 64 Absatz 1 PIPA oder Artikel 45 Absatz 4 CIA als angemessen erachtete Maßnahme zu ergreifen.

127. Darüber hinaus ist die PIPC in Bezug auf die in Artikel 64 Absatz 1 PIPA vorgesehenen Korrekturmaßnahmen befugt, im Falle der Nichtergreifung einer Abhilfemaßnahme eine Geldbuße in Höhe von höchstens 50 Mio. koreanischen Won zu verhängen (Artikel 75 Absatz 2 Ziffer 13 PIPA). Dieser Betrag entspricht 36 564 EUR. Der EDSA ist der Auffassung und befürchtet, dass ein derart begrenztes Spektrum von Geldbußen keine besonders stark abschreckende Wirkung auf die Zuwiderhandelnden haben könnte, wie sie im Gesetz vorgesehen ist, um die Durchsetzung der Datenschutzvorschriften zu gewährleisten, da es nicht ausreichend scheint, um abschreckend zu wirken, insbesondere im Falle großer Organisationen oder Unternehmen, die über beträchtliche finanzielle Mittel verfügen.

128. In Bezug auf die Möglichkeit, dass die PIPC den Leiter einer zentralen Verwaltungsstelle auffordern kann, eine Untersuchung gegen den für die Verarbeitung personenbezogener Informationen Verantwortlichen einzuleiten oder gemeinsam eine Untersuchung wegen Verstößen gegen das PIPA einzuleiten und sogar Korrekturmaßnahmen gegen in ihre Zuständigkeit fallende für die Verarbeitung personenbezogener Informationen Verantwortliche zu verhängen (Artikel 63 Absätze 4 und 5 PIPA), stellt der EDSA fest, dass die Natur dieser anderen Stellen und ihre rechtlichen Beziehungen zur PIPC insgesamt eher unklar sind, auch wenn Erwägungsgrund 122 des Beschlussentwurfs einige Informationen hierzu enthält. Darüber hinaus werden in Artikel 68 Absatz 1 PIPA viele Einrichtungen genannt, an die die Befugnisse der PIPC übertragen werden könnten. Selbst wenn diese Bestimmung offenbar nur in Bezug auf die koreanische Internet- und Sicherheitsagentur angewandt wurde[57], würde der EDSA Klarstellungen hinsichtlich der Art möglicher Interaktionen zwischen diesen Stellen und eine aufmerksame Überwachung der künftigen Anwendung dieser Bestimmung begrüßen, um die Unabhängigkeit der mit der Anwendung der Datenschutzvorschriften betrauten Stellen zu gewährleisten.

129. Bei Sanktionen scheint das koreanische System verschiedene Arten von Sanktionen zu kombinieren, von Korrekturmaßnahmen und Bußgeldern bis hin zu strafrechtlichen Sanktionen, die wahrscheinlich eine stark abschreckende Wirkung haben, und die koreanischen Behörden haben mehrere Beispiele für Geldbußen vorgelegt, die kürzlich von der PIPC verhängt wurden, unter anderem eine von 6,7 Milliarden koreanischen Won, verhängt im Dezember 2020 gegen ein Unternehmen wegen Verstoßes gegen verschiedene Bestimmungen des PIPA, und eine weitere Geldbuße von 103,3 Millionen koreanischer Won, die am 28. April 2021 gegen ein KI-Technologieunternehmen wegen Verstoßes gegen die Vorschriften über die Rechtmäßigkeit der Verarbeitung, insbesondere der Verarbeitung pseudonymisierter Informationen, verhängt wurde.

130. Auch wenn die oben genannten Beträge eine abschreckende Wirkung haben können, würde der EDSA zusätzliche Informationen über die Methode der PIPC zur Berechnung der Höhe der Geldbußen begrüßen, beispielsweise in Bezug auf Geldbußen, die verhängt werden, wenn eine gemäß Artikel 64 Absatz 1 PIPA erlassene Abhilfemaßnahme nicht erfolgt (siehe Artikel 75 Absatz 2 Ziffer 13 PIPA). Dies gilt insbesondere für strafrechtliche Sanktionen und die Anwendung des (koreanischen) Strafgesetzbuchs.

3.2.3. Das Datenschutzsystem muss betroffenen Personen bei der Ausübung ihrer Rechte Unterstützung und Hilfe sowie angemessene Rechtsschutzverfahren bieten

131. Was Rechtsbehelfe anbelangt, scheint das koreanische System verschiedene Wege zu bieten, um einen angemessenen Schutz zu gewährleisten, insbesondere die Durchsetzung der Rechte der

[57] Siehe Erwägungsgrund 117 des Beschlussentwurfs und Artikel 62 des Durchführungserlasses.

Betroffenen mit einem wirksamen verwaltungsrechtlichen und gerichtlichen Rechtsschutz, einschließlich Schadensersatz.

132. Das koreanische System bietet neben verwaltungsrechtlichen und gerichtlichen Wegen, wie in den Erwägungsgründen 132 und 133 des Beschlussentwurfs jeweils in Bezug auf das „Privacy Call Centre“ bzw. „Dispute Mediation Committee“ erläutert wird, auch alternative Mechanismen, auf die Personen bei der Einlegung von Rechtsbehelfen zurückgreifen können. Da es sich hierbei um zusätzliche Rechtsschutzmöglichkeiten handelt, würde der EDSA ausführlichere Erläuterungen dazu begrüßen, in welcher Form sie die Rechtsschutzmöglichkeiten vor der PIPC und den Gerichten für betroffene Personen, deren personenbezogene Daten auf Grundlage des Angemessenheitsbeschlusses an Korea übermittelt werden, ergänzen.

4. ZUGRIFF AUF UND NUTZUNG VON AUS DER EUROPÄISCHEN UNION ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IN SÜDKOREA

133. Zur Beurteilung des Datenschutzniveaus in den Bereichen Strafverfolgung und nationale Sicherheit hat die Europäische Kommission in ihrem Beschlussentwurf und den zur Verfügung gestellten Anhängen umfassende Informationen vorgelegt. Daher verzichtet der EDSA darauf, den Großteil der Sachverhaltsfeststellungen und Bewertungen in dieser Stellungnahme wiederzugeben.

134. Die Europäische Kommission kommt zu dem Schluss, dass in den genannten Bereichen ein Datenschutzniveau besteht, das den Anforderungen der Rechtsprechung des EuGH entspricht und daher dem der Europäischen Union als in der Sache gleichwertig angesehen werden kann.

135. Generell möchte der EDSA betonen, dass selbst in Fällen, in denen es den Anschein hat oder die Europäische Kommission anführt, dass aus der EU nach Südkorea übermittelte Daten wahrscheinlich nicht von den einschlägigen koreanischen Rechtsvorschriften betroffen sein dürften, nach wie vor geprüft werden muss, ob das koreanische Datenschutzniveau in Bezug auf solche Fälle angemessen ist. Die Relevanz solcher Fälle zeigt sich auch darin, dass die Europäische Kommission sie in ihrem Beschlussentwurf selbst aufgegriffen hat.

4.1. Allgemeiner Datenschutzrahmen im Zusammenhang mit dem Zugriff staatlicher Stellen

136. Im Hinblick auf den Zugriff von Behörden auf personenbezogene Daten müssen verschiedene koreanische Gesetze geprüft werden, um das Schutzniveau des Rechts auf Privatsphäre und Datenschutz zu beurteilen. Zunächst stellt der EDSA fest, dass das PIPA als zentrales Datenschutzgesetz weitgehend anzuwenden ist. Während das PIPA im Bereich der Strafverfolgung uneingeschränkt anwendbar ist, ist seine Anwendung auf die Datenverarbeitung für Zwecke der nationalen Sicherheit begrenzt. Gemäß Artikel 58 Absatz 1 Ziffer 2 PIPA gelten die Kapitel III bis VII nicht für die Verarbeitung personenbezogener Daten für Zwecke der nationalen Sicherheit. Hingegen sind die Kapitel I, II, IX und X durchaus auf den Bereich der nationalen Sicherheit anwendbar. Somit gelten die Grundprinzipien des PIPA sowie die grundlegenden Garantien für die Rechte betroffener Personen und die Bestimmungen über Aufsicht, Durchsetzung und Rechtsbehelfe für den Zugriff auf und die Nutzung von personenbezogenen Daten durch nationale Sicherheitsbehörden.

137. Auch in der südkoreanischen Verfassung sind wesentliche Datenschutzgrundsätze verankert, nämlich die Grundsätze der Rechtmäßigkeit, der Erforderlichkeit und der Verhältnismäßigkeit. Diese

Grundsätze gelten auch für den Zugriff südkoreanischer Behörden auf personenbezogene Daten in den Bereichen Strafverfolgung und nationale Sicherheit.[58]

138. Im Bereich der Strafverfolgung können Polizei, Staatsanwälte, Gerichte und andere öffentliche Stellen personenbezogene Daten auf der Grundlage spezifischer Rechtsvorschriften erheben, z. B. auf der Grundlage der Strafprozessordnung (auf Englisch: *Criminal Procedure Act*, „**CPA**"), des Gesetzes zum Schutz der Privatsphäre in der Kommunikation (auf Englisch: *Communications Privacy Protection Act*, „**CPPA**"), des Gesetzes über Telekommunikationsunternehmen (auf Englisch: *Telecommunications Business Act*, „**TBA**") und des Gesetzes über die Meldung und Verwendung spezifischer Informationen über Finanztransaktionen (auf Englisch: *Act on Reporting and Using Specified Financial Transaction Information*, „**ARUSFTI**"), das für die Verfolgung und Verhütung von Geldwäsche und Terrorismusfinanzierung gilt. Diese besonderen Gesetze enthalten weitere Beschränkungen, Garantien und Ausnahmen.

139. Im Bereich der nationalen Sicherheit kann der nationale Nachrichtendienst (auf Englisch: *National Intelligence Service*, „**NIS**") auf der Grundlage des Gesetzes über den nationalen Nachrichtendienst (auf Englisch: *National Intelligence Service Act*, „**NISA**") und weiterer „nationaler Sicherheitsgesetze"[59] personenbezogene Daten erheben und Kommunikation überwachen. Der EDSA geht davon aus, dass der NIS bei der Ausübung seiner Befugnisse die genannten Rechtsvorschriften sowie das PIPA einhalten muss.

140. Der EDSA ersucht die Kommission um Klarstellung, ob es neben dem NIS noch andere Behörden in Korea gibt, die für den Bereich der nationalen Sicherheit zuständig sind, da in Anhang I Abschnitt 6 die Europäische Kommission den Eindruck erweckt, dass der NIS nur ein Beispiel für nationale Sicherheitsbehörden ist.

4.2. Schutz und Garantien für „Kommunikationsbestätigungsdaten" im Rahmen staatlicher Zugriffsbefugnisse für Strafverfolgungszwecke

141. Auf der Grundlage des einschlägigen Gesetzes, des CPPA, können Strafverfolgungsbehörden zwei Arten von Maßnahmen für den Zugriff auf Kommunikationsdaten ergreifen. Das CPPA unterscheidet zwischen kommunikationsbeschränkenden Maßnahmen, die sowohl die Erfassung des Inhalts gewöhnlicher Post als auch das direkte Abfangen von Telekommunikationsinhalten umfassen[60], und die Erhebung so genannter Kommunikationsbestätigungsdaten. Letztere umfassen das Datum der Telekommunikation, ihre Start- und Endzeit, die Zahl der abgehenden und eingehenden Anrufe sowie die Teilnehmernummer der anderen Partei, die Häufigkeit der Nutzung, Protokolldateien zur Nutzung von Telekommunikationsdiensten und Standortdaten.[61]

142. Der EDSA stellt fest, dass für Kommunikationsbestätigungsdaten offenbar nicht dieselben Garantien gelten wie für Daten, die durch kommunikationsbeschränkende Maßnahmen erhoben werden, d. h. Inhaltsdaten. Der EDSA stellt fest, dass für die Erhebung von Inhaltsdaten mehr Schutzmaßnahmen bestehen als für die Erhebung von Kommunikationsbestätigungsdaten zu Strafverfolgungszwecken: Erstens ist die Erhebung von Kommunikationsbestätigungsdaten anders als die Erhebung von Inhaltsdaten nicht auf die Untersuchung bestimmter schwerer Straftaten beschränkt, sondern kann durchgeführt werden, wenn dies für die Durchführung von „Ermittlungen oder die Vollstreckung einer Strafe" als erforderlich erachtet wird (Artikel 13 Absatz 1 CPPA). Zweitens ist die Erhebung von

[58] Siehe Erwägungsgrund 145 des Beschlussentwurfs.
[59] Zu den nationalen Sicherheitsgesetzen gehören beispielsweise das Gesetz zum Schutz der Privatsphäre in der Kommunikation, das Gesetz zur Terrorismusbekämpfung zum Schutz der Bürger und der öffentlichen Sicherheit oder das Gesetz über Telekommunikationsunternehmen.
[60] Artikel 3 Absatz 2, Artikel 2 Absatz 6 und Artikel 2 Absatz 7 CPPA.
[61] Artikel 2 Absatz 11 CPPA.

Kommunikationsbestätigungsdaten grundsätzlich nicht als letztes Mittel vorgesehen, das nur dann eingesetzt werden darf, wenn mit anderen Mitteln nur schwer die Begehung einer Straftat verhindert, der Straftäter festgenommen oder Beweise erhoben werden können.[62] Kommunikationsbestätigungsdaten können erhoben werden, wenn ein Staatsanwalt oder ein Polizeibeamter es für die Ermittlungen in einer Straftat oder die Vollstreckung einer Strafe „für erforderlich hält". In diesem Zusammenhang gibt es jedoch gemäß Artikel 13 Absatz 2 CPPA eine Ausnahme für Echtzeit-Ortungsdaten und Kommunikationsbestätigungsdaten für eine bestimmte Basisstation. Drittens müssen Strafverfolgungsbehörden, die den Inhalt von Kommunikation erheben, dies unverzüglich einstellen, sobald ein fortdauernder Zugriff nicht mehr erforderlich ist.[63] Für Kommunikationsbestätigungsdaten ist dies zumindest im CPPA oder seinem Durchführungserlass nicht ausdrücklich vorgesehen.

143. Der EDSA stellt fest, dass die Erhebung von Kommunikationsbestätigungsdaten nur auf der Grundlage einer gerichtlichen Anordnung erfolgen darf. Darüber hinaus verlangt das CPPA detaillierte Angaben sowohl im Antrag auf Erlass der Anordnung als auch in der Anordnung selbst.[64] Eine solche vorherige richterliche Genehmigung dient dazu, das Ermessen der Strafverfolgungsbehörden bei der Rechtsanwendung einzuschränken und zu prüfen, ob in jedem Fall hinreichende Gründe für die Erhebung von Kommunikationsbestätigungsdaten vorliegen. Der EDSA nimmt außerdem zur Kenntnis, dass das Recht der Republik Korea offenbar keine allgemeine und unterschiedslose Vorratsdatenspeicherung von Kommunikationsbestätigungsdaten vorsieht. Der Zugriff staatlicher Stellen auf solche Daten bezieht sich daher immer auf Daten, die für die Zwecke der Abrechnung und der Bereitstellung der Kommunikationsdienste selbst noch gespeichert werden.

144. Der EDSA betont jedoch, dass der EuGH in Frage gestellt hat, dass Verkehrsdaten weniger schützenswert sind als andere, insbesondere Inhaltsdaten.[65] Angesichts der Tatsache, dass Kommunikationsbestätigungsdaten in mehrfacher Hinsicht ein geringeres Schutzniveau genießen als Inhaltsdaten, ersucht der EDSA die Europäische Kommission, genau zu überwachen, ob die nach koreanischem Recht für diese Kategorie personenbezogener Daten vorgesehenen Garantien ein in der Sache dem in der EU gewährten Schutzniveau gleichwertiges Schutzniveau gewährleisten, insbesondere im Hinblick auf die Verhältnismäßigkeit und Vorhersehbarkeit des Gesetzes.

1.3. Zugriff koreanischer Behörden auf Kommunikationsdaten für Zwecke der nationalen Sicherheit

145. In Bezug auf den Rechtsrahmen für den Zugriff nationaler Sicherheitsbehörden auf Kommunikationsdaten, die aus dem EWR nach Korea übermittelt werden, hat der EDSA zwei Aspekte identifiziert, die Anlass zur Besorgnis geben. Beide betreffen die Regelung des Zugriffs auf Kommunikationsvorgängen zwischen nicht koreanischen Staatsangehörigen, die unter eine bestimmte Reihe von Anwendungsfällen fallen (siehe Ziffer 29). In diesen Fällen gelten sowohl in Bezug auf Kommunikationsbestätigungsdaten als auch Inhaltsdaten bestimmte anderweitig

[62] Dies gilt für Inhaltsdaten gemäß Artikel 3 Absatz 2 und Artikel 5 Absatz 1 CPPA.
[63] Artikel 2 des CPPA-Durchführungserlasses.
[64] Siehe Erwägungsgrund 156 des Beschlussentwurfs.
[65] Siehe EuGH, C-623/17, *Privacy International*, 6. Oktober 2020, ECLI:EU:C:2020:790, Rn. 71: „*Der mit der Übermittlung von Verkehrs- und Standortdaten an die Sicherheits- und Nachrichtendienste verbundene Eingriff in das in Art. 7 der Charta verankerte Recht ist insbesondere angesichts des sensiblen Charakters der Informationen, die diese Daten liefern können, und vor allem angesichts der Möglichkeit, anhand von ihnen ein Profil der Betroffenen zu erstellen, als besonders schwer anzusehen, da eine solche Information ebenso sensibel ist wie der Inhalt der Kommunikationen selbst. Überdies ist er geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend Urteile vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 27 und 37, sowie vom 21. Dezember 2016, Tele2, C-203/15 und C-698/15, EU:C:2016:970, Rn. 99 und 100)*."

vorgesehene Garantien nicht. Mit anderen Worten: In diesen spezifischen Fällen unterliegen diese Daten nicht den gleichen Garantien wie die übermittelten Daten in Fällen, in denen mindestens ein koreanischer Staatsangehöriger an der Kommunikation beteiligt ist.

4.3.1. Keine Verpflichtung, Personen über den Zugriff staatlicher Stellen auf die Kommunikation zwischen ausländischen Staatsangehörigen zu unterrichten

146. In einem Szenario wie dem oben beschriebenen, wenn also keine der Parteien einer Kommunikation koreanischer Staatsangehöriger ist, sind die nationalen Sicherheitsbehörden nicht verpflichtet, Personen über die Erhebung und Verarbeitung ihrer Daten zu unterrichten. Der EDSA räumt ein, dass dieses Problem nur bestimmte Fälle betrifft. Erstens gelten, wie bereits erwähnt, immer dann, wenn mindestens ein koreanischer Staatsangehöriger an einer Kommunikation beteiligt ist, die Unterrichtungspflichten nach dem CPPA für alle an der Kommunikation beteiligten Parteien unabhängig von ihrer Staatsangehörigkeit.[66] Zweitens unterliegt die Erhebung personenbezogener Daten, die sich ausschließlich aus der Kommunikation zwischen Ausländern ergeben, bestimmten Anwendungsfällen. Das Zugriffsrecht erstreckt sich in solchen Fällen insbesondere auf die Kommunikation von a) Ländern, die der Republik Korea gegenüber feindlich eingestellt sind, b) ausländischen Einrichtungen, Gruppen oder Staatsangehörigen, die verdächtigt werden, anti-koreanischen Aktivitäten nachzugehen[67], oder c) Mitgliedern von Gruppen, die auf der koreanischen Halbinsel, aber faktisch über die Souveränität der Republik Korea hinaus tätig sind, und ihrer Dachorganisationen mit Sitz in anderen Ländern. Daten der Kommunikation zwischen Personen in der EU, die nach Korea übermittelt werden, können daher nur für Zwecke der nationalen Sicherheit erhoben werden, wenn sie unter eine der drei oben genannten Kategorien fallen.[68] Als weiteren einschränkenden Faktor hat der EDSA den zusätzlichen Erläuterungen der Europäischen Kommission entnommen, dass der geltende Rechtsrahmen keine Überwachung von Daten während ihrer Übermittlung außerhalb Koreas vorsieht.

147. Daher könnte das Fehlen einer Mitteilungspflicht im Hinblick auf die praktischen Auswirkungen als begrenzt kritisch angesehen werden. Der EDSA betont jedoch, wie wichtig die (spätere) Benachrichtigung über den staatlichen Zugriff ist, insbesondere im Hinblick auf die Gewährleistung wirksamer Rechtsbehelfe. Der EuGH befand Folgendes: „*Diese Unterrichtung ist nämlich der Sache nach erforderlich, damit die betroffenen Personen ihre Rechte aus den Artikeln 7 und 8 der Charta ausüben, Zugang zu ihren personenbezogenen Daten, die Gegenstand dieser Maßnahmen sind, beantragen und gegebenenfalls die Berichtigung oder Löschung dieser Daten verlangen sowie gemäß Artikel 47 Absatz 1 der Charta einen wirksamen Rechtsbehelf bei einem Gericht einlegen können*“.[69] Der Zugriff staatlicher Stellen für Zwecke der nationalen Sicherheit umfasst häufig geheime Überwachungsmaßnahmen, was bedeutet, dass die Überwachten, d. h. die betroffenen Personen, keine Kenntnis von der Verarbeitung ihrer Daten haben. Somit „*hat die betroffene Person grundsätzlich kaum Möglichkeiten, den Rechtsweg zu beschreiten, es sei denn, sie wird über die ohne ihr Wissen durchgeführten Maßnahmen in Kenntnis gesetzt und kann so deren Rechtmäßigkeit im Nachhinein anfechten, oder sie kann, wenn sie den Verdacht hat, dass ihre Kommunikation überwacht wurde oder wird, die Gerichte anrufen, sodass die Zuständigkeit der Gerichte nicht von der*

[66] Siehe Erwägungsgrund 192 des Beschlussentwurfs.
[67] Siehe Anhang II, Fußnote 244, wonach der Begriff „anti-koreanische Aktivitäten“ Aktivitäten bezeichnet, die die Existenz und Sicherheit der Nation, die demokratische Ordnung oder das Überleben und die Freiheit des Volkes bedrohen.
[68] Siehe Erwägungsgrund 187 des Beschlussentwurfs.
[69] EuGH, verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, *La Quadrature du Net* u. a., 6. Oktober 2020, ECLI:EU:C:2020:791, Rn. 190.

Benachrichtigung der überwachten Person über die Überwachung ihrer Kommunikation abhängt“.[70] In diesem Zusammenhang und im Einklang damit hat der EDSA mehrfach seine Besorgnis im Hinblick auf wirksame Rechtsbehelfe in solchen Fällen zum Ausdruck gebracht. Der EDSA betont, dass die Geheimhaltung staatlicher Maßnahmen nicht dazu führen darf, dass solche Maßnahmen in tatsächlicher Hinsicht unanfechtbar sind. Vor diesem Hintergrund muss im Rahmen einer Gesamtbewertung unter besonderer Berücksichtigung der im koreanischen Recht vorgesehenen Aufsichts- und Rechtsbehelfsmechanismen (siehe Abschnitte 4.7 und 4.8) bewertet werden, ob sich das Fehlen einer Mitteilungspflicht für die Kommunikation zwischen ausländischen Staatsangehörigen auf das Datenschutzniveau auswirkt, das im Beschlussentwurf beurteilt wird.

148. Darüber hinaus stellt der EDSA in diesem Zusammenhang fest, dass das Gesetz die eher weit gefassten Begriffe wie anti-koreanische oder anti-nationale Aktivitäten[71] verwendet und nur schwer vorherzusehen ist, wie diese Begriffe nach koreanischem Recht auszulegen sind. Der EDSA fordert die Europäische Kommission auf, zu überwachen, wie diese Begriffe im koreanischen Recht konkretisiert werden und ob ihre Anwendung in der Praxis den Anforderungen der Verhältnismäßigkeit entspricht, die sich aus dem EU-Recht ergeben.

4.3.2. Keine vorherige unabhängige Genehmigung für die Erhebung von Daten über die Kommunikation zwischen Ausländern

149. In Fällen, in denen personenbezogene Daten aus dem EWR, die aus der Kommunikation zwischen nicht-koreanischen Staatsangehörigen stammen (und die unter einen der oben genannten Anwendungsfälle fallen) in Korea für Zwecke der nationalen Sicherheit verarbeitet werden sollen, unterliegt die Erhebung dieser Daten nicht der vorherigen Genehmigung durch eine unabhängige Stelle (wie dies der Fall ist, wenn mindestens eine der betroffenen Personen koreanischer Staatsangehöriger ist).[72]

150. Insbesondere angesichts der kürzlich ergangenen Urteile des Europäischen Gerichtshofs für Menschenrechte („**EGMR**“) *Big Brother Watch und andere gegen Vereinigtes Königreich* und *Centrum för Rättvisa gegen Schweden* hält es der EDSA für erforderlich, zu prüfen, ob dies eine kritische Schwachstelle des koreanischen Datenschutzrahmens darstellt. In diesem Zusammenhang weist der EDSA darauf hin, dass, wie der EDSA in seinen aktualisierten Empfehlungen zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen[73] hervorgehoben hat, in Artikel 6 Absatz 3 des Vertrags über die Europäische Union niedergelegt ist, dass die Grundrechte, wie sie in der EMRK gewährleistet sind, allgemeine Grundsätze des EU-Rechts 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[74]. Das nach Artikel 46 Absatz 1 DSGVO erforderliche Grundrechtsschutzniveau muss daher auf Grundlage der Bestimmungen dieser Verordnung ermittelt werden, die im Lichte der in der Charta verankerten

[70] EGMR, *Big Brother Watch und andere gegen Vereinigtes Königreich*, 25. Mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, Rn. 337, und EGMR, *Roman Zakharov gegen Russland*, 4. Dezember 2015, ECLI:CE:ECHR:2015:1204JUD004714306, Rn. 234.

[71] Die Europäische Kommission hat erklärt, dass es sich dabei nach Erläuterungen der koreanischen Regierung um „Aktivitäten [handelt], die die Existenz und Sicherheit der Nation, die demokratische Ordnung oder das Überleben und die Freiheit des Volkes bedrohen“, siehe auch Fußnote 319 des Entwurfs des Angemessenheitsbeschlusses.

[72] Siehe Erwägungsgrund 190 des Beschlussentwurfs.

[73] Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, Rn. 10, 11.

[74] Siehe EuGH, C-311/18, *Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximilian Schrems*, 16. Juli 2020, ECLI:EU:C:2020:559 (im Folgenden„*Schrems II*“), Rn. 98.

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. Bei der Auslegung der Charta sind somit die entsprechenden Rechte der EMRK als Mindestschutzstandard zu berücksichtigen, d. h. insoweit, als die Charta in ihrer Auslegung durch den EuGH kein höheres Schutzniveau vorsieht.[75]

151. Der EDSA stellt fest, dass die vorherige (unabhängige) Genehmigung von Überwachungsmaßnahmen zwar als wichtiger Schutz vor Willkür angesehen wird, eine solche Genehmigung jedoch nicht aus der Rechtsprechung des EuGH als absolutes Erfordernis für die Verhältnismäßigkeit von Überwachungsmaßnahmen abgeleitet werden kann. Der EGMR hat nun jedoch ausdrücklich das Erfordernis einer unabhängigen Vorabgenehmigung für die massenweise Erhebung von Kommunikationsdaten eingeführt.[76] Zwar wird dies im Beschlussentwurf nicht ausdrücklich erwähnt, doch geht der EDSA davon aus, dass der Rechtsrahmen der Republik Korea keine Massenüberwachung, sondern nur eine gezielte Überwachung des Telekommunikationsverkehrs vorsieht.[77] Die Europäische Kommission hat diese Sichtweise bestätigt.

152. Allerdings zeigen die oben genannten Entscheidungen des EGMR im Einklang mit der Rechtsprechung des EuGH[78] und der früheren Rechtsprechung des EGMR[79] erneut die Bedeutung einer umfassenden Aufsicht durch unabhängige Aufsichtsbehörden. Der EDSA betont, dass eine unabhängige Aufsicht in allen Phasen des Prozesses des Zugriffs staatlicher Stellen für Zwecke der Strafverfolgung und der nationalen Sicherheit ein wichtiger Schutz vor willkürlichen Überwachungsmaßnahmen und somit für die Beurteilung eines angemessenen Datenschutzniveaus wichtig ist. Die Garantie der Unabhängigkeit der Aufsichtsbehörden im Sinne von Artikel 8 Absatz 3 der Charta soll eine wirksame und zuverlässige Überwachung der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten. Dies gilt insbesondere dann, wenn die Person aufgrund des Wesens der geheimen Überwachung daran gehindert ist, vor oder während der Durchführung der Überwachungsmaßnahme eine Überprüfung zu beantragen oder sich unmittelbar an einem Überprüfungsverfahren zu beteiligen.

153. Das Fehlen einer vorherigen unabhängigen Genehmigung kann für sich genommen bei der Beurteilung eines der Sache nach gleichwertigen Datenschutzniveaus nicht als wesentliche Schwachstelle im koreanischen Recht angesehen werden. Die Beurteilung der Angemessenheit hängt wiederum von allen Umständen des Falles ab, insbesondere von der Wirksamkeit der nachträglichen Aufsicht und der Rechtsschutzmöglichkeiten nach dem koreanischen Recht (siehe weiter unten die Abschnitte 4.7 und 4.8).

---

[75] Siehe EuGH, verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u. a.*, 6. Oktober 2020, Rn. 124.

[76] Siehe EGMR, *Big Brother Watch u. a. gegen Vereinigtes Königreich*, 25. Mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, Rn. 351: „Eine Sammelüberwachung sollte von vornherein einer unabhängigen Genehmigung unterliegen", „eine Sammelüberwachung sollte von einer unabhängigen Stelle genehmigt werden, also einer Stelle, die von der Exekutive unabhängig ist."

[77] Lediglich Anhang II Abschnitt 3.2 enthält eine ausdrückliche Erklärung zu Zwecken der nationalen Sicherheit, in der festgelegt ist, dass die Beschränkungen und Garantien *„gewährleisten, dass die Erhebung und Verarbeitung von Daten auf das zur Erreichung eines legitimen Ziels unbedingt erforderliche Maß beschränkt ist. Dies schließt jede massenhafte und wahllose Erfassung personenbezogener Informationen für Zwecke der nationalen Sicherheit aus*."

[78] Siehe z. B. EuGH, verbundene Rechtssachen C-203/15 und C-698/15 *Tele2 Sverige AB u. a.*, ECLI:EU:C:2016:970.

[79] Siehe z. B. EGMR, *Roman Zakharov gegen Russland*, 4. Dezember 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

4.4. Freiwillige Offenlegung

154. Nach Artikel 83 Absatz 3 TBA können Telekommunikationsdiensteanbieter auf Anfrage freiwillig so genannte „Teilnehmerdaten“[80] an nationale Sicherheits- und Strafverfolgungsbehörden weitergeben. Der EDSA stellt fest, dass Fälle, die personenbezogene Daten betreffen, die aus dem EWR nach Korea übermittelt wurden, zwar selten sein dürften, dass sie jedoch, wie bereits erwähnt, dennoch untersucht werden müssen, um das Datenschutzniveau zu beurteilen.

155. Der EDSA geht davon aus, dass in diesen Fällen die Datenschutzgarantien des PIPA gelten und Behörden sowie Telekommunikationsanbieter diese Anforderungen erfüllen müssen[81] und dass beide für jede Verletzung der Rechte und Freiheiten der betroffenen Personen haftbar gemacht werden können[82]. Darüber hinaus geht der EDSA davon aus, dass Telekommunikationsanbieter solchen Ersuchen nicht nachkommen müssen.

156. Was jedoch das Konzept des Zugriffs nationaler Behörden auf Teilnehmerdaten für Strafverfolgungszwecke und insbesondere für Zwecke der nationalen Sicherheit durch die „freiwillige Offenlegung“ durch Telekommunikationsunternehmen betrifft, so gibt es Bedenken hinsichtlich eines erhöhten Risikos für die Rechte und Freiheiten der betroffenen Personen, insbesondere in Bezug auf ihr Recht auf Information.

157. Gemäß Artikel 58 Absatz 1 Ziffer 2 PIPA gelten die Bestimmungen der Kapitel III bis VII nicht für personenbezogene Informationen, die im Zusammenhang mit der nationalen Sicherheit bereitgestellt werden sollen. In dieser Hinsicht sind beispielsweise die Bestimmungen von Artikel 18 (Beschränkung der zweckfremden Verwendung und Bereitstellung personenbezogener Informationen) und Artikel 20 (Mitteilung über Quellen usw. von bei Dritten erhobenen personenbezogenen Informationen) des PIPA auf solche Ersuchen nicht anwendbar. In Fällen, in denen ein Ersuchen von einer nationalen Sicherheitsbehörde gestellt wird, stellt sich zum einen die Frage, ob Artikel 58 Absatz 1 Ziffer 2 auch der Anwendung des PIPA auf Telekommunikationsanbieter entgegensteht. Zum anderen stellt sich die Frage, ob der Ausschluss der Anwendung von Artikel 20 PIPA in solchen Fällen auch für die entsprechende Bestimmung in Anhang I Abschnitt 3 (Benachrichtigung über personenbezogene Daten, die nicht bei der betroffenen Person erhoben wurden (Artikel 20 des Gesetzes)) gilt. Wenn dies der Fall ist und wenn Artikel 58 Absatz 1 Ziffer 2 auch für Telekommunikationsanbieter gilt, bestünde nach den vorliegenden Informationen die Gefahr, dass keine rechtliche Verpflichtung bestünde, die betroffenen Personen über die freiwillige Offenlegung zu informieren.

158. Der EDSA ist daher besorgt darüber, dass die Informationspflichten wirkungslos gemacht werden könnten, was es den betroffenen Personen erheblich erschweren würde, ihre Datenschutzrechte geltend zu machen, insbesondere im Hinblick auf Rechtsbehelfe. In diesem Zusammenhang sollte die Europäische Kommission den Anwendungsbereich der einschlägigen Bestimmungen klarstellen.

4.5. Weiterverwendung von Daten

159. Der Grundsatz der Zweckbindung ist ein grundlegendes rechtliches Erfordernis des Datenschutzes. Er schreibt vor, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Darüber hinaus ist es Behörden nach EU-Recht gestattet, personenbezogene Daten

[80] Betroffen wären folgende Datensätze: Name, Personenkennzahl, Anschrift und Telefonnummer der Nutzer, Datum, an dem die Nutzer ihren Vertrag unterzeichnen oder beenden, sowie Benutzerkennungscodes (die zur Identifizierung des rechtmäßigen Nutzers von Computersystemen oder Kommunikationsnetzen verwendet werden).

[81] Siehe Erwägungsgründe 164 und 194 des Beschlussentwurfs.

[82] Siehe Erwägungsgrund 166 des Beschlussentwurfs.

zur Verhütung, Untersuchung oder Verfolgung von Straftaten zu verarbeiten, selbst wenn diese Daten ursprünglich zu einem anderen Zweck erhoben wurden, sofern diese Behörden über eine Rechtsgrundlage für die Verarbeitung solcher Daten nach dem einschlägigen Recht verfügen und die Weiterverarbeitung nicht unverhältnismäßig ist.[83]

160. Dementsprechend stellt der EDSA fest, dass der koreanische Datenschutzrahmen ähnliche Garantien und Beschränkungen vorsieht, wie sie im EU-Recht in Bezug auf die Weiterverwendung der für Zwecke der Strafverfolgung und der nationalen Sicherheit erhobenen Informationen vorgesehen sind, z. B. Artikel 3 Absätze 1 und 2 PIPA, Grundsatz der Zweckbindung.

4.6. Weiterübermittlungen und Austausch nachrichtendienstlicher Erkenntnisse

161. Artikel 44 DSGVO sieht vor, dass die Übermittlung und Weiterübermittlung personenbezogener Daten nur erfolgen darf, wenn das durch die DSGVO garantierte Schutzniveau nicht untergraben wird. Daher darf das Schutzniveau für personenbezogene Daten, die aus dem EWR an Korea übermittelt werden, nicht durch die Weiterübermittlung an Empfänger in einem Drittland untergraben werden, d. h. Weiterübermittlungen sollten nur dann zulässig sein, wenn ein fortgesetztes Schutzniveau gewährleistet ist, das in der Sache dem im EU-Recht vorgesehenen gleichwertig ist. Folglich muss bei der Beurteilung, ob ein Drittland ein angemessenes Datenschutzniveau gewährleistet, der Rechtsrahmen des Landes für Weiterübermittlungen berücksichtigt werden. Dies ist unbestritten und entspricht sowohl der Auffassung der Europäischen Kommission[84] als auch der des EDSA.

162. In diesem Zusammenhang nimmt der EDSA zur Kenntnis, dass der EGMR in seinen jüngsten Entscheidungen *Big Brother Watch u. a. gegen Vereinigtes Königreich* und *Centrum för Rättvisa gegen Schweden* Hinweise[85] zu den Datenschutzvorkehrungen gegeben hat, die in den Vertragsstaaten zu beachten sind, wenn personenbezogene Daten an andere Parteien zu Strafverfolgungszwecken und für Zwecke der nationalen Sicherheit in Fällen der massenweisen Datenerhebungen übermittelt werden: „*Zunächst müssen die Umstände, unter denen eine solche Übermittlung erfolgen kann, im innerstaatlichen Recht klar festgelegt sein. Zweitens muss der übermittelnde Staat sicherstellen, dass der empfangende Staat bei der Verarbeitung der Daten über Garantien verfügt, die Missbrauch und unverhältnismäßige Eingriffe verhindern können. Insbesondere muss der empfangende Staat die sichere Speicherung des Materials gewährleisten und seine Weitergabe beschränken. [...] Drittens werden verstärkte Garantien erforderlich sein, wenn klar ist, dass Material, das einer besonderen Geheimhaltung bedarf – wie z. B. vertrauliches journalistisches Material – weitergegeben wird*."[86]

163. Bei der Anwendung dieser Standards stellte der EGMR in *Centrum för Rättvisa gegen Schweden* fest, dass das Fehlen einer ausdrücklichen rechtlichen Verpflichtung, die Erforderlichkeit und Verhältnismäßigkeit des Austauschs nachrichtendienstlicher Erkenntnisse im Hinblick auf seine möglichen Auswirkungen auf das Recht auf Privatsphäre zu bewerten, einen Verstoß gegen Artikel 8 EMRK darstellt. Der EGMR kritisierte, dass aufgrund der Allgemeingültigkeit des Gesetzes Material in der Regel ins Ausland geschickt werden könne, wenn dies als im nationalen Interesse liegend

[83] Siehe Artikel 4 Absatz 2 der Richtlinie zum Datenschutz bei der Strafverfolgung.
[84] Siehe Erwägungsgrund 84 ff. des Beschlussentwurfs.
[85] In den Fällen *Big Brother Watch* und *Centrum för Rättvisa*, bei denen es um Sammelüberwachungsmaßnahmen ging, wurde Folgendes festgestellt: Das Erfordernis von Vorsichtsmaßnahmen, die bei der Übermittlung von Material an andere Parteien zu treffen seien, sei bereits Teil der Kriterien gewesen, die der EGMR im Rahmen der gezielten Überwachung entwickelt habe, und vom EGMR nicht näher konkretisiert worden (siehe *Big Brother Watch u. a. gegen Vereinigtes Königreich*, Rn. 335, 362).
[86] EGMR, *Big Brother Watch u. a. gegen Vereinigtes Königreich*, 25. Mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, Rn. 362.

angesehen werde, und zwar unabhängig davon, ob der ausländische Empfänger ein akzeptables Mindestmaß an Garantien biete.[87]

164. In dem Bewusstsein, dass der Rechtsrahmen Südkoreas keine solche Massenüberwachung vorsieht, ist der EDSA vor dem Hintergrund der oben dargelegten Auswirkungen der Rechtsprechung des EGMR dennoch der Auffassung, dass neben den Anforderungen, die sich aus dem EU-Recht in der Auslegung des EuGH ergeben, die Argumentation des EGMR bei der Beurteilung, ob der Rechtsrahmen für Weiterübermittlungen an ein Drittland angemessene Datenschutzstandards vorsieht, berücksichtigt werden sollte.

1.6.1. Geltender Rechtsrahmen für Weiterübermittlungen durch Strafverfolgungsbehörden

165. In Bezug auf Weiterübermittlungen durch die zuständigen Behörden zu Strafverfolgungszwecken entnimmt der EDSA den Erläuterungen der Europäischen Kommission, dass Anhang I Abschnitt 2 des Beschlussentwurfs über die Beschränkung der Weiterübermittlung auch dann anwendbar ist, wenn die Übermittlung auf der Grundlage eines anderen Gesetzes als des PIPA erfolgt. Diese Bestimmung lautet: „*Werden personenbezogene Informationen einer dritten Partei im Ausland zur Verfügung gestellt, kann es aufgrund der Unterschiede in den Systemen zum Schutz personenbezogener Informationen in verschiedenen Ländern vorkommen, dass sie nicht in den Genuss desselben Schutzniveaus kommen, wie es vom koreanischen Datenschutzgesetz gewährt wird. Dementsprechend werden solche Fälle als „Fälle, in denen der betroffenen Person Nachteile entstehen können" im Sinne von Artikel 17 Absatz 4 des Gesetzes oder als „Fälle, in denen die Interessen einer betroffenen Person oder eines Dritten in unlauterer Weise verletzt werden" im Sinne von Artikel 18 Absatz 2 des Gesetzes und Artikel 14 Absatz 2 der Durchführungsverordnung zu demselben Gesetz betrachtet. Um die Anforderungen dieser Bestimmungen zu erfüllen, müssen der für die Verarbeitung der personenbezogenen Informationen Verantwortliche und der Dritte daher ausdrücklich ein dem Gesetz gleichwertiges Schutzniveau gewährleisten, einschließlich der in rechtlich bindenden Dokumenten wie Verträgen enthaltenen Garantie, dass die betroffene Person ihre Rechte auch nach der Übermittlung personenbezogener Informationen ins Ausland wahrnehmen kann."*[88]

166. Der EDSA begrüßt diese Bestimmung, die unter der Annahme, dass das Datenschutzniveau in Korea für diesen Zweck angemessen ist, die Kontinuität eines im Wesentlichen nach EU-Recht gewährleisteten Schutzniveaus für Weiterübermittlungen gewährleistet. Die Kommission hat bestätigt, dass das Verständnis des EDSA, dass dieser Abschnitt von Anhang I für alle Weiterübermittlungen durch die zuständigen Behörden zu Strafverfolgungszwecken gilt, korrekt ist. Der EDSA weist jedoch darauf hin, dass sichergestellt werden muss, dass diese Regelung in der Praxis ein anhaltendes Schutzniveau sicherstellt, da Unsicherheit darüber bestehen kann, welche vertraglichen Garantien und Verpflichtungen oder anderen ähnlichen Mechanismen genutzt werden können, um ein solches Schutzniveau im Falle einer Verarbeitung zu Strafverfolgungszwecken zu erreichen. In diesem Zusammenhang sollte beispielsweise zusätzlich darauf hingewiesen werden, dass personenbezogene Daten nur an die tatsächlich zuständigen Behörden des Drittlandes weitergegeben werden dürfen.

167. Vorbehaltlich der oben erbetenen Klarstellung, ob die KOFIU unter den Beschlussentwurf fällt, stellt der EDSA fest, dass die offizielle Darstellung des Zugriffs durch staatliche Stellen[89] besagt, dass der Leiter der KOFIU gemäß Artikel 8 Absatz 1 ARUSFTI ausländischen Meldestellen bestimmte Informationen über Finanztransaktionen übermitteln kann, wenn dies zur Erreichung des Zwecks des

[87] Siehe EGMR, *Centrum för Rättvisa gegen Schweden*, 25. Mai 2021, ECLI:CE:ECHR:2021:0525JUD003525208, Rn. 326.
[88] Beschlussentwurf, Anhang I, S. 7.
[89] Siehe Beschlussentwurf, Anhang II.

ARUSFTI für erforderlich erachtet wird[90]. Artikel 8 ARUSFTI selbst sieht keine Verpflichtung vor, festzustellen, ob das andere Land angemessene Datenschutzgarantien bietet und gewährleistet. Anhang II enthält diesbezüglich keine Bezugnahme auf den neuen Abschnitt von Anhang I. Daher fordert der EDSA die Europäische Kommission auf, die Wechselbeziehung zwischen dem einschlägigen Abschnitt in Anhang I über die Beschränkung der Weiterübermittlung und der Rechtsgrundlage für Weiterübermittlungen gemäß dem ARUSFTI zu klären.

4.6.2. Geltender Rechtsrahmen für Weiterübermittlungen für Zwecke der nationalen Sicherheit

168. Der Beschlussentwurf enthält keine Informationen über den Rechtsrahmen für Weiterübermittlungen im Bereich der nationalen Sicherheit. Daher geht der EDSA davon aus, dass Anhang I Abschnitt 2 im Gegensatz zu Strafverfolgungszwecken nicht auf Weiterübermittlungen für Zwecke der nationalen Sicherheit anwendbar ist. Die Artikel 17 und 18 PIPA, die Gegenstand des betreffenden Abschnitts in Anhang I sind, sind Teil von Kapitel III des PIPA, das wiederum nicht für die Verarbeitung personenbezogener Daten für Zwecke der nationalen Sicherheit gilt (Artikel 58 Absatz 1 PIPA).

169. Der EDSA nimmt jedoch an, dass Korea aus Gründen der nationalen Sicherheit personenbezogene Daten an ausländische Nachrichtendienste übermitteln muss und dies auch tut, z. B. um bei der Bekämpfung grenzüberschreitender Bedrohungen der nationalen Sicherheit zusammenzuarbeiten oder ausländische Regierungen vor solchen Bedrohungen zu warnen oder um Unterstützung bei der Identifizierung solcher Bedrohungen zu erhalten.

170. Der EDSA geht davon aus, dass nach Ansicht der Europäischen Kommission Weiterübermittlungen im koreanischen Recht ausreichend durch die Garantien geregelt sind, die sich aus dem übergeordneten verfassungsrechtlichen Rahmen ergeben, insbesondere durch die Grundsätze der Notwendigkeit und Verhältnismäßigkeit, sowie durch die im PIPA geregelten zentralen Datenschutzgrundsätze wie Rechtmäßigkeit und Fairness der Verarbeitung, Zweckbindung, Datenminimierung, Sicherheit und die allgemeinen Verpflichtungen zur Verhinderung des Missbrauchs und der falschen Verwendung personenbezogener Informationen.

171. Der EDSA erkennt die allgemeine Anwendbarkeit dieser zentralen (Datenschutz-)Grundsätze an, äußert jedoch Bedenken, dass diese Garantien sehr allgemeiner Art sind und sich nicht in einer Rechtsgrundlage speziell auf die besonderen Umstände und Bedingungen für die Weiterübermittlung von aus dem EWR übermittelten Daten für Zwecke der nationalen Sicherheit beziehen. Auch wenn diese generellen und übergeordneten Grundsätze allgemein anwendbar sind, fragt sich der EDSA, ob davon ausgegangen werden kann, dass dies die Kriterien der Normenklarheit erfüllt und wirksame und durchsetzbare Garantien hinreichend verankert. Insbesondere in Fällen, in denen der Zugriff auf personenbezogene Daten und ihre Verarbeitung durch staatliche Stellen im Geheimen erfolgt und die Schlüsse, die aus den Daten gezogen werden könnten, besonders schwerwiegend sind, müssen klare und eindeutige Vorschriften erlassen werden. Das Gesetz sollte den Umfang des den zuständigen Behörden eingeräumten Ermessens und die Art und Weise seiner Wahrnehmung hinreichend klar festlegen, um dem Einzelnen angemessenen Schutz zu gewähren. Im Urteil *Schrems II* erinnert der EuGH daran, dass eine Rechtsgrundlage, die Eingriffe in Grundrechte zulässt, selbst den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, festlegen sowie klare und präzise

[90] Siehe Beschlussentwurf, Anhang II, Abschnitt 2.2.3.2. Während ein solcher Austausch nur unter der Bedingung stattfinden darf, dass der ausländische Dienst die Daten nicht für andere Zwecke als den ursprünglichen Zweck der Offenlegung verwenden darf, insbesondere nicht für strafrechtliche Ermittlungen oder Gerichtsverfahren (Artikel 8 Absatz 2 ARUSFTI), kann der Leiter der KOFIU auf Antrag eines anderen Landes der Verwendung dieser Daten für strafrechtliche Ermittlungen oder Gerichtsverfahren wegen Straftaten mit vorheriger Zustimmung des Justizministers zustimmen (Artikel 8 Absatz 3 ARUSFTI).

Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen muss, um den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit zu genügen.[91] Der EDSA befürchtet daher, dass es nicht ausreicht, dass solche Garantien im Allgemeinen in höherrangigem Recht verankert sind, ohne den Begriff der Verhältnismäßigkeit in der jeweiligen rechtlichen Grundlage selbst konkret umzusetzen.

172. Diese Bedenken werden durch die oben genannte Entscheidung des EGMR gestützt, in der das Gericht feststellte, dass eine allgemeine Regel ohne ausdrückliche Verpflichtung, die Notwendigkeit und Verhältnismäßigkeit zu prüfen oder Bedenken hinsichtlich der Privatsphäre zu berücksichtigen, nicht mit dem Recht auf Privatsphäre gemäß Artikel 8 EMRK vereinbar ist. In diesem Zusammenhang stellt der EDSA fest, dass es im Recht des Landes des betreffenden Falls (sowie im Recht Koreas) übergreifende (verfassungsrechtlich garantierte) Grundsätze der Notwendigkeit und Verhältnismäßigkeit gibt, z. B. gemäß der Charta und durch den Beitritt zur EMRK.

173. Der EDSA fordert die Europäische Kommission auf, klarzustellen, auf welcher Rechtsgrundlage, wie und in welchem Umfang und unter welchen spezifischen Bedingungen Nachrichtendienste verpflichtet sind, Belange des Schutzes der Privatsphäre und Datenschutzgarantien zu berücksichtigen, bevor sie personenbezogene Daten für Zwecke der nationalen Sicherheit an ausländische Partner weitergeben. Falls sich eine solche Verpflichtung unmittelbar aus Grundsätzen der Verfassung ergibt, sollte die Europäische Kommission die Anforderungen an die Bestimmtheit und Klarheit des Gesetzes weiter prüfen und bestätigen, dass die allgemeinen Verfassungs- und Datenschutzgrundsätze angemessen angewandt und umgesetzt werden.

4.6.3. Internationale Abkommen

174. Der EDSA stellt fest, dass die Europäische Kommission im Rahmen ihrer Prüfung der Angemessenheit nicht berücksichtigt hat, ob zwischen Korea und Drittländern oder internationalen Organisationen internationale Abkommen geschlossen wurden, die möglicherweise spezifische Bestimmungen für die internationale Übermittlung personenbezogener Daten durch Strafverfolgungsbehörden und/oder Nachrichtendienste an Drittländer enthalten. Nach Ansicht des EDSA dürfte sich der Abschluss bilateraler oder multilateraler Abkommen mit Drittländern für Zwecke der Strafverfolgung oder der Zusammenarbeit von Nachrichtendiensten auf den Datenschutzrechtsrahmen Koreas in der beurteilten Fassung auswirken.

175. Der EDSA fordert die Europäische Kommission daher auf, zu klären, ob solche Abkommen bestehen, unter welchen Bedingungen sie geschlossen werden können, und zu prüfen, ob die Bestimmungen internationaler Abkommen das Schutzniveau für personenbezogene Daten, die aus dem EWR nach Korea übermittelt werden, durch den Rechtsrahmen und die Praxis in Bezug auf die Offenlegung ausländischer Daten für Zwecke der Strafverfolgung und der nationalen Sicherheit beeinträchtigen könnten.

4.7. Aufsicht

176. Der EDSA stellt fest, dass die Aufsicht über Strafverfolgungsbehörden und nationale Sicherheitsbehörden durch eine Kombination verschiedener interner und externer Stellen gewährleistet wird.

177. In diesem Zusammenhang ist darauf hinzuweisen, dass der EuGH wiederholt betont hat, dass eine unabhängige Aufsicht ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ist. Das Konzept der Unabhängigkeit umfasst die Bereiche institutionelle Autonomie, Weisungsfreiheit und materielle Unabhängigkeit. Um eine einheitliche Überwachung und Durchsetzung des Datenschutzrechts zu gewährleisten, müssen die

[91] Siehe *Schrems II*, Rn. 175 und 180.

Aufsichtsbehörden über wirksame Befugnisse, einschließlich Korrektur- und Abhilfebefugnissen, verfügen.

178. Der EDSA stimmt der Schlussfolgerung der Europäischen Kommission zu, dass bei einer Gesamtbewertung davon ausgegangen werden kann, dass Korea über ein unabhängiges und wirksames Aufsichtssystem verfügt, auch wenn mehrere Organe des Aufsichtssystems die oben genannten Anforderungen an sich nicht erfüllen. Beispielsweise verfügen die meisten von ihnen über keine durchsetzbaren Abhilfebefugnisse, sondern müssen sich auf bloße Empfehlungen beschränken, so z. B. die nationale Menschenrechtskommission oder die Behörde für Audits und Inspektionen. Darüber hinaus handelt es sich bei den meisten öffentlichen Stellen nicht um Einrichtungen, die sich ausschließlich mit Datenschutz befassen, sondern in der Regel noch mit anderen Aufgaben im Bereich des Grundrechtsschutzes betraut sind.

179. Gestützt auf die Erläuterungen der Europäischen Kommission stellt der EDSA jedoch fest, dass die Überwachung der Strafverfolgungsbehörden umfassend und ausnahmslos durch die PIPC gewährleistet wird. Daher verfügt die PIPC über Ermittlungs-, Abhilfe- und Durchsetzungsbefugnisse im Rahmen des PIPA und anderer Datenschutzgesetze (z. B. des CPPA), die für den gesamten Bereich des Zugriffs von Strafverfolgungsbehörden und nationalen Sicherheitsbehörden auf personenbezogene Daten gelten.

180. In diesem Zusammenhang möchte der EDSA erneut unterstreichen, dass Aufsichtsbehörden zur Wahrnehmung ihrer Aufgaben und Befugnisse über ausreichende personelle, technische und finanzielle Ressourcen verfügen müssen. Diesbezüglich mangelt es leider an Informationen über die benannten Aufsichtsorgane, insbesondere über die PIPC. Daher fordert der EDSA die Europäische Kommission erneut auf, weitere Informationen zu diesem Thema vorzulegen.

181. Insgesamt weist der EDSA darauf hin, dass der Beschlussentwurf kaum Aussagen, Beispiele oder Zahlen zu den Aufsichtstätigkeiten und der rechtlichen Durchsetzung des Datenschutzrechts durch die Aufsichtsbehörden im Bereich der Strafverfolgung und der nationalen Sicherheit enthält. Sie wären jedoch für eine Bewertung der Wirksamkeit der Aufsichtsorgane hilfreich.

1.8. Gerichtlicher Rechtsbehelf und Rechtsmittel

182. Der EDSA weist darauf hin, dass es für ein angemessenes Datenschutzniveau von wesentlicher Bedeutung ist, dass den betroffenen Personen umfassende Rechtsbehelfe und Rechtsmittel gegen unbefugten Zugriff auf Daten oder deren unberechtigte Verarbeitung zur Verfügung stehen. Diese Rechtsbehelfe müssen so gestaltet sein, dass die betroffene Person Auskunft über die sie betreffenden Daten erhalten und deren Berichtigung oder Löschung verlangen kann.

183. Angesichts der Urteile *Schrems I* und *Schrems II* des EuGH ist klar, dass neben dem Recht, sich an die zuständigen Behörden zu wenden, ein wirksamer Rechtsbehelf im Sinne von Artikel 47 Absatz 1 der Charta für die Annahme der Angemessenheit des Rechts eines Drittstaats von grundlegender Bedeutung ist.

184. Der EDSA erkennt an, dass Korea verschiedene Wege für die Ausübung der Rechte des Einzelnen auf Auskunft, Speicherung, Löschung und Aussetzung im Rahmen des PIPA geschaffen hat. Diese Rechte können gegenüber dem Verantwortlichen selbst oder im Wege einer Beschwerde bei der PIPC oder anderen Aufsichtsbehörden, z. B. der nationalen Menschenrechtskommission, geltend gemacht werden. Darüber hinaus erkennt der EDSA an, dass die Entscheidung des Verantwortlichen oder von Behörden über Ersuchen betroffener Personen auf der Grundlage des Gesetzes über die Verwaltungsgerichtsbarkeit angefochten werden können.

185. Ferner entnimmt der EDSA den Erläuterungen der Europäischen Kommission, dass Personen die Handlungen von Strafverfolgungsbehörden und nationalen Sicherheitsbehörden gemäß dem Gesetz über die Verwaltungsgerichtsbarkeit und dem Verfassungsgerichtsgesetz vor den zuständigen

Gerichten anfechten können und die Möglichkeit haben, Schadensersatz nach dem Staatshaftungsgesetz zu erhalten.[92]

186. In diesem Zusammenhang hat der EDSA jedoch Bedenken bezüglich wirksamer Rechtsbehelfe für Personen in der EU in Fällen, die die nationale Sicherheit betreffen und in denen kein koreanischer Bürger beteiligt ist. Wie in den Ziffern 33ff. ausgeführt, sind die nationalen Sicherheitsbehörden nicht verpflichtet, betroffene Personen über die Erhebung und Verarbeitung ihrer personenbezogenen Daten zu unterrichten. Da es in diesen Fällen erheblich schwieriger ist, einen wirksamen Rechtsschutz zu erlangen, möchte der EDSA darauf hinweisen, dass hier bestimmte rechtliche Garantien erforderlich sind, wenn es sich um aus dem EWR übermittelte Daten handelt. Diese Garantien müssen es betroffenen Personen ermöglichen, auf rechtssichere Weise wirksam gegen eine unrechtmäßige Datenverarbeitung vorzugehen, ohne durch zu enge Verfahrensanforderungen behindert zu werden, z. B. durch Auferlegung einer Beweislast, die sie ohne Kenntnis der Verarbeitung nicht erfüllen können. Darüber hinaus müssen sich betroffene Personen an eine zuständige Stelle wenden können, die die Anforderungen von Artikel 47 der Charta erfüllt, d. h. die befugt ist, festzustellen, ob eine Datenverarbeitung stattfindet, die Rechtmäßigkeit der Verarbeitung zu überprüfen, und die durchsetzbaren Abhilfebefugnisse für den Fall hat, dass die Datenverarbeitung rechtswidrig ist. Vor diesem Hintergrund wäre beispielsweise ein bloßes Beschwerderecht bei der nationalen Menschenrechtskommission nicht ausreichend. Der EDSA fordert die Kommission daher auf, genauer zu erläutern, wie diese Anforderungen in verfahrensrechtlicher und materieller Hinsicht umgesetzt werden, ob sich z. B. betroffene Personen an die PIPC sowie an ein Gericht wenden können, ohne die betreffende Datenverarbeitung nachweisen zu müssen.

187. Darüber hinaus stellt der EDSA fest, dass der Beschlussentwurf einen Mechanismus zur Verweisung von Beschwerden vorsieht, dem zufolge Personen in der EU über ihre nationale Datenschutzbehörde oder den EDSA eine Beschwerde bei der PIPC einreichen können. Nach Abschluss der Untersuchung benachrichtigt dann die PIPC die betroffene Person auf dem gleichen Weg.[93] Der EDSA begrüßt die Bemühungen, den Zugang zu Rechtsbehelfen gegen koreanische nationale Sicherheitsbehörden zu erleichtern. Gleichzeitig plädiert der EDSA dafür, dass ein solcher Verweisungsmechanismus über die europäischen nationalen Datenschutzbehörden und nicht über den EDSA erfolgt, da diese zuständig und näher an der Bearbeitung der individuellen Beschwerden beteiligt sind.

188. Ferner stellt der EDSA einen möglichen Widerspruch in Bezug auf freiwillige Offenlegungen fest. Einerseits heißt es in dem Beschlussentwurf, dass Personen auch gegen die ersuchende Strafverfolgungsbehörde einen Rechtsbehelf einlegen können, wenn ihre Daten nach einem Ersuchen auf freiwillige Offenlegung unrechtmäßig offengelegt werden.[94] Andererseits verweist der Beschlussentwurf auf das Erfordernis der unmittelbaren Auswirkung in Bezug auf das Recht des Einzelnen, die Handlungen von Behörden anzufechten, und führt (nur) verbindliche Offenlegungsanträge als Beispiel für einen Fall an, in dem Verwaltungshandeln als unmittelbare Auswirkung auf das Recht auf Privatsphäre angesehen wird.[95] Der EDSA entnimmt den Erläuterungen der Europäischen Kommission, dass es tatsächlich keine Beschränkung der Rechtsbehelfsmöglichkeiten gegen Ersuchen um freiwillige Offenlegung gibt, und fordert die Europäische Kommission daher auf, dies in dem Beschluss klarzustellen, und zwar sowohl für Strafverfolgung als auch für nationale Sicherheit (anders als der Abschnitt über Strafverfolgung enthält der Abschnitt über freiwillige Offenlegungen für Zwecke der nationalen Sicherheit in diesem Zusammenhang keine ausdrückliche Aussage über Rechtsbehelfe).

[92] Siehe Anhang II Abschnitt 3.2.4 in Verbindung mit Abschnitt 2.4.3.
[93] Siehe Erwägungsgrund 205 und Anhang I, S. 19 des Beschlussentwurfs.
[94] Siehe Erwägungsgrund 166 des Beschlussentwurfs.
[95] Siehe Erwägungsgrund 181 (Strafverfolgung) und Erwägungsgründe 208 und 181 (nationale Sicherheit) des Beschlussentwurfs.