Amtsblatt der Europäischen Union

L 44

Ausgabe in deutscher Sprache

Rechtsvorschriften

65. Jahrgang

24. Februar 2022

Inhalt

([1]) Text von Bedeutung für den EWR.

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

II

(Rechtsakte ohne Gesetzescharakter)

BESCHLÜSSE

DURCHFÜHRUNGSBESCHLUSS (EU) 2022/254 DER KOMMISSION

vom 17. Dezember 2021

gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten durch die Republik Korea im Rahmen des koreanischen Gesetzes über den Schutz personenbezogener Daten

(Bekannt gegeben unter Aktenzeichen C(2021) 9316)

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ([1]), insbesondere auf Artikel 45 Absatz 3,

In Erwägung nachstehender Gründe:

1. EINLEITUNG

(1) Die Verordnung (EU) 2016/679 enthält die Vorschriften für die Übermittlung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter in der Union an Drittländer und internationale Organisationen, soweit die betreffenden Übermittlungen in ihren Anwendungsbereich fallen. Die Vorschriften über internationale Datenübermittlung sind in Kapitel V (Artikel 44 bis 50) der Verordnung festgelegt. Der Fluss personenbezogener Daten in Drittländer und aus Drittländern ist zwar für die Ausweitung des grenzüberschreitenden Handels und der internationalen Zusammenarbeit wesentlich, dennoch darf das unionsweit gewährleistete Schutzniveau für personenbezogene Daten bei Übermittlungen in Drittländer nicht untergraben werden ([2]).

(2) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau bieten. Unter dieser Voraussetzung können personenbezogene Daten nach Artikel 45 Absatz 1 und Erwägungsgrund 103 der Verordnung (EU) 2016/679 ohne weitere Genehmigung an ein Drittland übermittelt werden.

(3) Wie in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 festgelegt, muss die Annahme eines Angemessenheitsbeschlusses auf einer umfassenden Analyse der Rechtsordnung des Drittlands beruhen und zwar sowohl in Bezug auf die für die Datenimporteure geltenden Vorschriften als auch auf die Einschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten. Im Rahmen ihrer Prüfung muss die Kommission feststellen, ob das betreffende Drittland ein Schutzniveau garantiert, das dem innerhalb der Europäischen Union gewährleisteten Schutzniveau „der Sache nach gleichwertig" ist (Erwägungsgrund 104 der Verordnung (EU) 2016/679). Dies ist anhand des EU-Rechts, insbesondere der Verordnung (EU) 2016/679, sowie der Rechtsprechung des Gerichtshofs der Europäischen Union zu prüfen ([3]).

([1]) ABl. L 119 vom 4.5.2016, S. 1.
([2]) Siehe Erwägungsgrund 101 der Verordnung (EU) 2016/679.
([3]) Siehe zuletzt Rechtssache C-311/18, Facebook Ireland/Schrems (im Folgenden „Schrems II"), EU:C:2020:559.

(4) Der Gerichtshof der Europäischen Union hat klargestellt, dass es dazu keines identischen Schutzniveaus bedarf ([4]). Insbesondere können sich die Mittel, auf die das betreffende Drittland für den Schutz personenbezogener Daten zurückgreift, von denen unterscheiden, die in der Union herangezogen werden, sofern sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten ([5]). Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Vorschriften der Union. Die Frage ist vielmehr, ob das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz bietet ([6]). Eine weitere Orientierungshilfe bietet die Referenzgrundlage für Angemessenheit des Europäischen Datenschutzausschusses, mit der dieser Standard weiter präzisiert werden soll ([7]).

(5) Die Kommission hat Recht und Praxis in Korea sorgfältig analysiert. Auf der Grundlage der in den Erwägungsgründen (8)-(208) dargelegten Feststellungen kommt die Kommission zu dem Schluss, dass die Republik Korea ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die von einem Verantwortlichen oder Auftragsverarbeiter in der Union ([8]) an Rechtsträger (z. B. natürliche oder juristische Personen, Organisationen, öffentliche Einrichtungen) in Korea übermittelt werden, die in den Anwendungsbereich des Gesetzes zum Schutz personenbezogener Daten (Gesetz Nr. 10465 vom 29. März 2011, zuletzt geändert durch Gesetz Nr. 16930 vom 4. Februar 2020) fallen. Dies gilt sowohl für die Verantwortlichen als auch für die Auftragsverarbeiter (im koreanischen Gesetz und im Folgenden „Beauftragte“ ([9])) im Sinne der Verordnung (EU) 2016/679. Die Angemessenheitsfeststellung erstreckt sich nicht auf die Verarbeitung personenbezogener Daten für Missionierungstätigkeiten religiöser Organisationen und für die Nominierung von Kandidaten durch politische Parteien sowie auf die Verarbeitung personenbezogener Kreditdaten gemäß dem Kreditdatengesetz durch die Datenverantwortlichen, die der Aufsicht durch die Finanzdienstleistungskommission unterliegen.

(6) Dabei werden die in der Bekanntmachung Nr. 2021-5 (Anhang I) dargelegten zusätzlichen Garantien sowie die offiziellen Erklärungen, Zusicherungen und Pflichten der koreanischen Regierung gegenüber der Kommission (Anhang II) berücksichtigt.

(7) Der Beschluss hat zur Folge, dass die Datenübermittlungen an die Datenverantwortlichen und Auftragsverarbeiter in der Republik Korea ohne weitere Genehmigung vorgenommen werden können. Er wirkt sich nicht auf die unmittelbare Anwendung der Verordnung (EU) 2016/679 auf derartige Rechtsträger aus, wenn die in Artikel 3 der Verordnung festgelegten Bedingungen für den räumlichen Anwendungsbereich der Verordnung erfüllt sind.

2. VORSCHRIFTEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

2.1 Der Datenschutzrahmen in der Republik Korea

(8) Das Rechtssystem für den Schutz der Privatsphäre und den Datenschutz in Korea wurzelt in der am 17. Juli 1948 verkündeten koreanischen Verfassung. Das Recht auf den Schutz personenbezogener Daten ist zwar nicht ausdrücklich in der Verfassung verankert, wird aber dennoch als Grundrecht anerkannt, das sich aus den Verfassungsrechten auf die Würde des Menschen und das Streben nach Glück (Artikel 10), das Privatleben (Artikel 17) und das Kommunikationsgeheimnis (Artikel 18) ableitet. Dies wurde sowohl vom Obersten Gerichtshof ([10]) als auch vom Verfassungsgericht ([11]) bestätigt. Einschränkungen der Grundrechte und -freiheiten (einschließlich des Rechts auf Privatsphäre) dürfen nur dann gesetzlich vorgeschrieben werden, wenn sie für die nationale Sicherheit oder die Aufrechterhaltung der öffentlichen Ordnung für das Gemeinwohl erforderlich sind, und dürfen den Wesensgehalt des betreffenden Rechts oder der betreffenden Freiheit nicht beeinträchtigen (Artikel 37 Absatz 2).

([4]) Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner (im Folgenden „Schrems“), EU:C:2015:650, Rn. 73.
([5]) Schrems, Rn. 74.
([6]) Siehe Mitteilung der Kommission an das Europäische Parlament und den Rat „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt“ (COM(2017)7 vom 10.1.2017, Abschnitt 3.1., S. 6).
([7]) Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254 rev. 01., abrufbar unter folgendem Link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) Dieser Beschluss ist von Bedeutung für den EWR. Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Der Beschluss des Gemeinsamen Ausschusses zur Aufnahme der Verordnung (EU) 2016/679 in Anhang XI des EWR-Abkommens wurde am 6. Juli 2018 vom Gemeinsamen EWR-Ausschuss angenommen und ist am 20. Juli 2018 in Kraft getreten. Die Verordnung fällt somit unter das genannte Abkommen. Für die Zwecke des Beschlusses sollten daher Verweise auf die EU und die EU-Mitgliedstaaten so verstanden werden, dass sie auch die EWR-Staaten umfassen.
([9]) Siehe Abschnitt 2.2.3 dieses Beschlusses.
([10]) Siehe z. B. die Entscheidung des Obersten Gerichtshofs vom 15. Oktober 2015, 2014Da77970 (englische Zusammenfassung von „Lawmaker's disclosure of teachers' trade union members case“ (Rechtssache über die Offenlegung von Mitgliedern der Lehrergewerkschaft durch den Gesetzgeber), abrufbar unter https://www.privacy.go.kr/eng/enforcement_01.do) und die darin zitierte Rechtsprechung, einschließlich der Entscheidung vom 24. Juli 2014 2012Da49933.
([11]) Siehe insbesondere die Entscheidung des Verfassungsgerichts vom 26. Mai 2005, 99Hun-ma51399Hun-ma513 (englische Zusammenfassung abrufbar unter http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) und die Entscheidung vom 23. Dezember 2015, 2014JHun-ma449 2013 Hun-Ba68 (konsolidiert) (englische Zusammenfassung von „Change of resident registration number case“ (Rechtssache über die Änderung der Melderegisternummer) abrufbar unter https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Auch wenn die Verfassung an verschiedenen Stellen auf die Rechte koreanischer Staatsangehörigen verweist, hat das Verfassungsgericht entschieden, dass auch ausländische Staatsangehörige Gegenstand der Grundrechte sind ([12]). Insbesondere stellte das Verfassungsgericht fest, dass der Schutz der Würde und des Wertes des Menschen sowie das Recht, nach Glück zu streben, Rechte eines jeden Menschen sind, nicht nur der Staatsangehörigen ([13]). Darüber hinaus wird nach offiziellen Angaben der koreanischen Regierung ([14]) allgemein anerkannt, dass in den Artikeln 12 bis 22 der Verfassung (zu denen auch die Rechte auf Privatsphäre gehören) grundlegende Menschenrechte verankert sind ([15]). Obwohl es bisher keine Rechtsprechung speziell zum Recht auf Privatsphäre von ausländischen Staatsangehörigen gibt, stützt sich diese Schlussfolgerung auf den Schutz der Menschenwürde und das Streben nach Glück ([16]).

(10) Darüber hinaus hat Korea eine Reihe von Gesetzen im Bereich des Datenschutzes erlassen, die allen Personen, unabhängig von ihrer Staatsangehörigkeit, Schutz bieten ([17]). Für die Zwecke dieses Beschlusses sind folgende Gesetze relevant:

— das Gesetz zum Schutz personenbezogener Daten (Personal Information Protection Act – PIPA),

— das Gesetz über die Nutzung und den Schutz von Kreditdaten, ([18])

— das Gesetz zum Schutz der Privatsphäre bei der Kommunikation.

(11) Das PIPA bildet den allgemeinen Rechtsrahmen für den Datenschutz in der Republik Korea. Es wird durch einen Durchführungserlass (Präsidialerlass Nr. 23169 vom 29. September 2011, zuletzt geändert durch Präsidialerlass Nr. 30892 vom 4. August 2020) (im Folgenden „PIPA-Durchführungserlass“) ergänzt, der wie das PIPA rechtsverbindlich und vollstreckbar ist.

(12) Darüber hinaus enthalten die von der Kommission für den Schutz personenbezogener Daten (Personal Information Protection Commission – PIPC) angenommenen behördlichen „Bekanntmachungen“ weitere Regeln für die Auslegung und Anwendung des PIPA. Auf der Grundlage von Artikel 5 (Pflichten des Staates) und Artikel 14 PIPA (internationale Zusammenarbeit) verabschiedete die PIPC die Bekanntmachung Nr. 2021-1 vom 1. September 2020 (geändert durch die Bekanntmachungen Nr. 2021-1 vom 21. Januar 2021 und Nr. 2021-5 vom 16. November 2021, im Folgenden „Bekanntmachung Nr. 2021-5“) über die Auslegung, Anwendung und Durchsetzung bestimmter Bestimmungen des PIPA. Diese Bekanntmachung enthält Klarstellungen, die für jede Verarbeitung personenbezogener Daten nach dem PIPA gelten, sowie zusätzliche Garantien für personenbezogene Daten, die auf der Grundlage dieses Beschlusses nach Korea übermittelt werden. Die Bekanntmachung ist für die Datenverantwortlichen rechtsverbindlich und kann sowohl von der PIPC als auch von den Gerichten durchgesetzt werden ([19]). Ein Verstoß gegen die in der Bekanntmachung dargelegten Regeln bedeutet einen Verstoß gegen die einschlägigen Bestimmungen des PIPA, die sie ergänzen. Der Inhalt der zusätzlichen Garantien wird daher im Rahmen der Prüfung der einschlägigen PIPA-Artikel analysiert. Weitere Hinweise zum PIPA und dem Durchführungserlass, in dem die Anwendung und Durchsetzung der Datenschutzvorschriften durch die PIPC geregelt ist, finden sich im PIPA-Handbuch und den von der PIPC verabschiedeten Leitlinien ([20]).

([12]) Entscheidung des Verfassungsgerichts vom 29. Dezember 1994, 93 Hun-MA120.
([13]) Entscheidung des Verfassungsgerichts vom 29. November 2001, 99HeonMa494.
([14]) Siehe Anhang II Abschnitt 1.1.
([15]) Siehe auch Artikel 1 des Gesetzes zum Schutz personenbezogener Daten, in dem ausdrücklich der Bezug auf die „Freiheiten und Rechte des Einzelnen“ genommen wird. Konkret heißt es, dass der Zweck dieses Gesetzes darin besteht, „die Verarbeitung und den Schutz personenbezogener Daten zu gewährleisten, um die Freiheit und die Rechte des Einzelnen zu schützen und die Würde und den Wert des Einzelnen weiter zu stärken“. Ebenso wird in Artikel 5 Absatz 1 des Gesetzes zum Schutz personenbezogener Daten die Verantwortung des Staates festgelegt, „Maßnahmen zu ergreifen, um schädliche Folgen der zweckfremden Erhebung, des Missbrauchs und der missbräuchlichen Verwendung personenbezogener Daten, der indiskreten Überwachung und Verfolgung usw. zu verhindern und die Würde des Menschen und die Privatsphäre des Einzelnen zu stärken“.
([16]) Darüber hinaus ist gemäß Artikel 6 Absatz 2 der Verfassung der Status ausländischer Staatsangehöriger nach Maßgabe des Völkerrechts und der Verträge gewährleistet. Korea ist Vertragspartei mehrerer internationaler Abkommen, in denen das Recht auf Privatsphäre garantiert wird, wie des Internationalen Pakts über bürgerliche und politische Rechte (Artikel 17), des Übereinkommens über die Rechte von Menschen mit Behinderungen (Artikel 22) und des Übereinkommens über die Rechte des Kindes (Artikel 16).
([17]) Dazu gehören Vorschriften, die für den Schutz personenbezogener Daten relevant sind, aber nicht in einer Situation gelten, in der personenbezogene Daten in der Union erhoben und gemäß der Verordnung (EU) 2016/679 nach Korea übermittelt werden, z. B. im Gesetz über den Schutz, die Nutzung usw. von Standortdaten.
([18]) Zweck dieses Gesetzes ist die Förderung eines tragfähigen Kreditdatengeschäfts, die Förderung der effizienten Nutzung und des systematischen Managements von Kreditdaten und der Schutz der Privatsphäre vor dem Missbrauch von Kreditdaten (Artikel 1 des Kreditdatengesetzes).
([19]) So haben koreanische Gerichte in einer Reihe von Fällen über die Einhaltung von behördlichen Bekanntmachungen entschieden und koreanische Datenverantwortliche für Verstöße gegen eine Bekanntmachung haftbar gemacht (siehe z. B. die Entscheidung des Obersten Gerichtshofs vom 25. Oktober 2018, in der das Gericht einen Datenverantwortlichen zur Zahlung von Schadenersatz an Einzelpersonen wegen eines Verstoßes gegen die „Bekanntmachung über den Standard für Maßnahmen zur Gewährleistung der Sicherheit personenbezogener Daten“ verurteilte; siehe auch die Entscheidung des Obersten Gerichtshofs vom 25. Oktober 2018, 2018Da219352, die Entscheidung des Obersten Gerichtshofs vom 16. Mai 2016, 2011Da24555 sowie die Entscheidung des Zentralen Bezirksgerichts Seoul vom 13. Oktober 2016, 2014Gahap511956, die Entscheidung des Zentralen Bezirksgerichts Seoul vom 26. Januar 2010, 2009Gahap43176).
([20]) Artikel 12 Absatz 1 PIPA.

(13) Darüber hinaus enthält das Gesetz über die Verwendung und den Schutz von Kreditdaten (im Folgenden „Kreditdatengesetz“) spezifische Vorschriften, die sowohl für „gewöhnliche“ Wirtschaftsbeteiligte als auch für spezialisierte Einrichtungen des Finanzsektors gelten, wenn sie personenbezogene Kreditdaten verarbeiten, d. h. Daten, die zur Feststellung der Kreditwürdigkeit von Parteien bei Finanz- oder Handelsgeschäften erforderlich sind. Dazu gehören insbesondere der Name, die Kontaktdaten, Finanztransaktionen, das Kreditrating, der Versicherungsstatus oder der Kreditsaldo, wenn diese Daten zur Bestimmung der Kreditwürdigkeit einer Person verwendet werden ([21]). Werden solche Daten hingegen für andere Zwecke verwendet (z. B. für die Personalverwaltung), gilt das PIPA in vollem Umfang. Die Einhaltung der spezifischen Datenschutzbestimmungen des Kreditdatengesetzes wird zum Teil von der PIPC (für Handelsorganisationen, siehe Artikel 45-3 des Kreditdatengesetzes) und zum Teil von der Finanzdienstleistungskommission ([22]) (für den Finanzsektor, einschließlich Rating-Agenturen, Banken, Versicherungsgesellschaften, Kreditkassen auf Gegenseitigkeit, spezialisierte Kreditfinanzierungsunternehmen, Finanzdienstleistungsunternehmen, Wertpapierfinanzierungsunternehmen, Kreditgenossenschaften usw., siehe Artikel 45 Absatz 1 des Kreditdatengesetzes in Verbindung mit Artikel 36-2 des Durchführungserlasses zum Kreditdatengesetz und Artikel 38 des Gesetzes über die Finanzdienstleistungskommission) überprüft. In dieser Hinsicht ist der Anwendungsbereich dieses Beschlusses auf Wirtschaftsbeteiligte beschränkt, die der Aufsicht durch die PIPC unterstellt sind ([23]). Die spezifischen Bestimmungen des Kreditdatengesetzes, die in diesem Zusammenhang gelten (in den Fällen, in denen keine spezifischen Bestimmungen bestehen, gelten die allgemeinen PIPA-Bestimmungen), werden in Abschnitt 2.3.11 beschrieben.

2.2 **Sachlicher und persönlicher Anwendungsbereich des PIPA**

(14) Sofern in anderen Gesetzen nicht ausdrücklich anders vorgesehen, wird der Schutz personenbezogener Daten durch das PIPA geregelt (Artikel 6). Der sachliche und persönliche Anwendungsbereich wird durch die definierten Begriffe „personenbezogene Daten“, „Verarbeitung“ und „Verantwortlicher für die Verarbeitung personenbezogener Daten“ bestimmt.

2.2.1 *Definition des Begriffs „personenbezogene Daten“*

(15) Nach Artikel 2 Absatz 1 PIPA handelt es sich bei personenbezogenen Daten um Daten, die sich auf eine lebende Person beziehen und diese direkt – z. B. durch ihren Namen, ihre Melderegisternummer oder ihr Bild – oder indirekt identifizieren lassen, d. h. wenn Daten, durch die für sich genommen keine bestimmte Person identifiziert werden kann, leicht mit anderen Daten verknüpft werden können. Die Frage, ob Daten „leicht“ verknüpft werden können, hängt davon ab, ob eine solche Verknüpfung nach allgemeinem Ermessen wahrscheinlich ist, wobei die Möglichkeit, andere Daten zu erhalten, sowie die Zeit, die Kosten und die Technologie, die zur Identifizierung einer Person erforderlich sind, berücksichtigt werden.

(16) Darüber hinaus gelten pseudonymisierte Daten – d. h. Daten, die nicht zur Identifizierung einer bestimmten Person verwendet oder mit zusätzlichen Informationen verknüpft werden können, um ihren ursprünglichen Zustand wiederherzustellen – als personenbezogene Daten im Sinne des PIPA (Artikel 2 Absatz 1 Buchstabe c PIPA). Umgekehrt sind Daten, die vollständig „anonymisiert“ sind, vom Anwendungsbereich des PIPA ausgeschlossen (Artikel 58-2 PIPA). Dies gilt für Daten, mit denen eine bestimmte Person nicht identifiziert werden kann, selbst wenn sie mit anderen Daten verknüpft werden, wobei der für die Identifizierung erforderliche Zeit-, Kosten- und Technologieaufwand zu berücksichtigen ist.

(17) Dies entspricht dem sachlichen Anwendungsbereich der Verordnung (EU) 2016/679 und den darin genannten Definitionen der Begriffe „personenbezogene Daten“, „Pseudonymisierung“ ([24]) und „anonymisierte Daten“ ([25]).

([21]) Artikel 2 Absatz 1 des Kreditdatengesetzes.

([22]) Die Finanzdienstleistungskommission ist die koreanische Aufsichtsbehörde für den Finanzsektor und setzt in dieser Eigenschaft auch das Kreditdatengesetz durch.

([23]) Sollte sich dies in Zukunft ändern, z. B. durch die Ausweitung der Zuständigkeit der PIPC auf die gesamte Verarbeitung personenbezogener Kreditdaten im Rahmen des Kreditdatengesetzes, könnte erwogen werden, den Angemessenheitsbeschluss dahin gehend zu ändern, dass er auch die Einrichtungen erfasst, die derzeit der Aufsicht der Finanzdienstleistungskommission unterstehen.

([24]) Im PIPA wird unter „pseudonymisierter Verarbeitung“ die Verarbeitung durch Methoden wie die teilweise Löschung personenbezogener Daten oder die teilweise oder vollständige Ersetzung personenbezogener Daten in einer Weise verstanden, dass keine bestimmte Person ohne zusätzliche Informationen erkannt werden kann (Artikel 2 Absätze 1 und 2 PIPA). Dies entspricht der Definition des Begriffs „Pseudonymisierung“ in Artikel 4 Nummer 5 der Verordnung (EU) 2016/679 als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.“

([25]) Insbesondere wird in Erwägungsgrund 26 der Verordnung (EU) 2016/679 klargestellt, dass die Verordnung nicht für anonymisierte Informationen gilt, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies hängt wiederum von allen Mitteln ab, die von dem Datenverantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Feststellung, ob derartige Mittel nach allgemeinem Ermessen wahrscheinlich genutzt werden, müssen alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

2.2.2 *Definition des Begriffs „Verarbeitung“*

(18) Der Begriff „Verarbeitung“ ist im PIPA weit gefasst und bezieht sich auf die Erhebung, Erzeugung, Verbindung, Verknüpfung, Aufzeichnung, Speicherung, Aufbewahrung, Verarbeitung mit Zusatznutzen, Bearbeitung, das Abrufen, die Veröffentlichung, Berichtigung, Wiederherstellung, Verwendung, Bereitstellung und Offenlegung sowie Vernichtung personenbezogener Daten und andere ähnliche Tätigkeiten ([26]). Obwohl sich einige Bestimmungen des PIPA nur auf bestimmte Arten der Verarbeitung beziehen, wie z. B. „Verwendung“, „Bereitstellung“ oder „Erhebung“, ([27]) wird der Begriff „Verwendung“ so ausgelegt, dass er jede andere Art der Verarbeitung als „Erhebung“ oder „Bereitstellung“ (durch Dritte) einschließt. Durch diese weite Auslegung des Begriffs „Verwendung“ wird sichergestellt, dass es keine Schutzlücken in Bezug auf bestimmte Verarbeitungstätigkeiten gibt. Der Begriff der Verarbeitung entspricht daher demselben Begriff in der Verordnung (EU) 2016/679.

2.2.3 *Verantwortlicher für die Verarbeitung personenbezogener Daten und „Beauftragter“*

(19) Das PIPA gilt für Verantwortliche für die Verarbeitung personenbezogener Daten (im Folgenden „Datenverantwortliche“). Ähnlich wie in der Verordnung (EU) 2016/679 umfasst dies jede öffentliche Einrichtung, juristische Person, Organisation oder Einzelperson, die direkt oder indirekt personenbezogene Daten verarbeitet, um im Rahmen ihrer Tätigkeit Akten mit personenbezogenen Daten zu verwalten ([28]). In diesem Zusammenhang bedeutet „Akte mit personenbezogenen Daten“ jeden „Satz oder Sätze personenbezogener Daten, die in systematischer Weise auf der Grundlage einer bestimmten Regel für einen leichten Zugang zu den personenbezogenen Daten geordnet oder zusammengestellt sind“ (Artikel 2 Absatz 4 PIPA) ([29]). Im Innenverhältnis ist der Datenverantwortliche verpflichtet, die Personen, die unter seiner Weisung an der Verarbeitung beteiligt sind, wie Unternehmensleiter oder Mitarbeiter, zu schulen und eine angemessene Kontrolle und Aufsicht auszuüben (Artikel 28 Absatz 1 PIPA).

(20) Besondere Pflichten gelten, wenn ein Datenverantwortlicher (Auslagernder) die Verarbeitung personenbezogener Daten an einen Dritten (Beauftragten) auslagert. Insbesondere muss die Auslagerung durch eine rechtsverbindliche Vereinbarung (in der Regel einen Vertrag) geregelt werden, ([30]) in der der Umfang der ausgelagerten Arbeiten, der Zweck der Verarbeitung, die anzuwendenden technischen und organisatorischen Garantien, die Überwachung durch den Datenverantwortlichen, die Haftung (z. B. Schadenersatz bei Verletzung vertraglicher Pflichten) sowie die Einschränkungen für eine etwaige Unterverarbeitung ([31]) festgelegt sind (Artikel 26 Absätze 1 und 2 PIPA in Verbindung mit Artikel 28 Absatz 1 des Durchführungserlasses) ([32]).

(21) Darüber hinaus muss der Datenverantwortliche Einzelheiten über die ausgelagerte Arbeit und die Identität des Beauftragten veröffentlichen und laufend aktualisieren oder, soweit die ausgelagerte Verarbeitung Direktwerbungstätigkeiten betrifft, den Betroffenen die entsprechenden Informationen direkt mitteilen (Artikel 26 Absätze 2 und 3 PIPA in Verbindung mit Artikel 28 Absätze 2 bis 5 des Durchführungserlasses) ([33]).

(22) Darüber hinaus ist der Datenverantwortliche gemäß Artikel 26 Absatz 4 PIPA in Verbindung mit Artikel 28 Absatz 6 des Durchführungserlasses verpflichtet, den Beauftragten über die erforderlichen Sicherheitsvorkehrungen „zu schulen“ und zu überwachen, auch durch Kontrollen, ob er alle Pflichten des Datenverantwortlichen im Rahmen des PIPA ([34]) und des Auslagerungsvertrags einhält. Verursacht der Beauftragte einen Schaden aufgrund eines Verstoßes gegen das PIPA, so haftet der Datenverantwortliche für seine Handlungen oder Unterlassungen, wie dies bei einem Arbeitnehmer der Fall ist (Artikel 26 Absatz 6 PIPA).

([26]) Artikel 2 Absatz 2 PIPA.

([27]) So beziehen sich beispielsweise die Artikel 15 bis 19 PIPA nur auf die Erhebung, Verwendung und Bereitstellung personenbezogener Daten.

([28]) Artikel 2 Absatz 5 PIPA. Zu den öffentlichen Einrichtungen im Sinne des PIPA gehören alle zentralen Verwaltungsabteilungen oder -stellen und die ihnen angeschlossenen Einrichtungen, die lokalen Gebietskörperschaften, die Schulen und die öffentlichen Unternehmen, an denen die lokalen Gebietskörperschaften beteiligt sind, die Verwaltungsorgane der Nationalversammlung und die Justiz (einschließlich des Verfassungsgerichts) (Artikel 2 Absatz 6 des PIPA in Verbindung mit Artikel 2 des PIPA-Durchführungserlasses).

([29]) Dies entspricht dem sachlichen Anwendungsbereich der Verordnung (EU) 2016/679. Gemäß Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 gilt diese Verordnung für „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ Gemäß Artikel 4 Nummer 6 der Verordnung (EU) 2016/679 wird „Dateisystem“ als „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind“ definiert. Dementsprechend wird in Erwägungsgrund 15 erklärt, dass der Schutz natürlicher Personen „für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten [sollte] wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen.“

([30]) Siehe PIPA-Handbuch, Kapitel III Abschnitt 2 zu Artikel 26 (S. 203-212), in dem erläutert wird, dass sich Artikel 26 Absatz 1 PIPA auf verbindliche Vereinbarungen, wie Verträge oder ähnliche Vereinbarungen, bezieht.

([31]) Gemäß Artikel 26 Absatz 5 PIPA darf der Auftragsverarbeiter personenbezogene Daten nicht über den Rahmen der ausgelagerten Arbeit hinaus verwenden oder sie an Dritte weitergeben. Die Nichteinhaltung dieser Anforderung kann eine strafrechtliche Sanktion gemäß Artikel 71 Nummer 2 PIPA zur Folge haben.

([32]) Die Nichteinhaltung dieser Anforderung kann eine Geldstrafe nach sich ziehen, vgl. Artikel 75 Absatz 4 Nummer 4 PIPA.

([33]) Die Nichteinhaltung dieser Anforderung kann eine Geldstrafe nach sich ziehen, vgl. Artikel 75 Absatz 2 Nummer 1 und Absatz 4 Nummer 5 PIPA.

([34]) Siehe auch Artikel 26 Absatz 7 PIPA, wonach die Artikel 15 bis 25, 27 bis 31, 33 bis 38 und 50 entsprechend für den Auftragsverarbeiter gelten.

(23) Obwohl das PIPA daher keine unterschiedlichen Konzepte für „Datenverantwortliche" und „Auftragsverarbeiter" verwendet, gelten für die Auslagerung im Wesentlichen die gleichen Pflichten und Schutzmaßnahmen wie für die Beziehung zwischen Datenverantwortlichen und Auftragsverarbeitern gemäß der Verordnung (EU) 2016/679.

2.2.4 *Sonderbestimmungen für Informations- und Kommunikationsdiensteanbieter*

(24) Zwar gilt das PIPA für die Verarbeitung personenbezogener Daten durch jeden Datenverantwortlichen, doch enthalten einige Bestimmungen besondere Vorschriften (lex specialis) für die Verarbeitung personenbezogener Daten von „Nutzern" durch „Informations- und Kommunikationsdiensteanbieter" ([35]). Unter dem Begriff „Nutzer" sind Personen zu verstehen, die Informations- und Kommunikationsdienste nutzen (Artikel 2 Absatz 1 Nummer 4 des Gesetzes zur Förderung der Nutzung von Informations- und Kommunikationsnetzen und des Datenschutzes, im Folgenden „Netzgesetz"). Dies setzt voraus, dass die betroffene Person entweder direkt Telekommunikationsdienste eines koreanischen Telekommunikationsanbieters in Anspruch nimmt oder Informationsdienste nutzt, ([36]) die gewerblich (d. h. zu Erwerbszwecken) von einer Einrichtung angeboten werden, die ihrerseits auf die Dienste eines in Korea lizenzierten oder eingetragenen Telekommunikationsanbieters angewiesen ist ([37]). In beiden Fällen ist die Einrichtung, die an die spezifischen PIPA-Bestimmungen gebunden ist, eine Einrichtung, die einen Online-Dienst direkt für eine Person (d. h. einen Nutzer) anbietet.

(25) Eine Angemessenheitsfeststellung betrifft dagegen ausschließlich das Schutzniveau für personenbezogene Daten, die von einem Verantwortlichen oder Auftragsverarbeiter in der Union an eine Stelle in einem Drittland (in diesem Fall in der Republik Korea) übermittelt werden. Im letztgenannten Fall haben Personen in der Union in der Regel nur eine direkte Beziehung zu dem „Datenexporteur" in der Union und nicht zu einem koreanischen Informations- und Kommunikationsdiensteanbieter ([38]). Daher werden die Sonderbestimmungen des PIPA in Bezug auf personenbezogene Daten von Nutzern von Informations- und Kommunikationsdiensten allenfalls in begrenzten Situationen auf personenbezogene Daten anwendbar sein, die im Rahmen dieses Beschlusses übermittelt werden.

2.2.5 *Ausnahme von einigen Bestimmungen des PIPA*

(26) Gemäß Artikel 58 Absatz 1 PIPA ist die Anwendung eines Teils des PIPA (d. h. der Artikel 15 bis 57) in Bezug auf vier Kategorien der Datenverarbeitung ausgeschlossen ([39]). Insbesondere die Teile des PIPA, die sich mit den besonderen Gründen für die Verarbeitung, bestimmten Datenschutzpflichten, den ausführlichen Vorschriften für die Ausübung individueller Rechte sowie den Regeln für die Beilegung von Streitigkeiten durch den Schlichtungsausschuss für Streitigkeiten in Zusammenhang mit personenbezogenen Daten befassen, finden keine Anwendung. Andere Grundbestimmungen des PIPA bleiben anwendbar, insbesondere die allgemeinen Bestimmungen über die Grundsätze des Datenschutzes (Artikel 3 PIPA) – einschließlich der Grundsätze der Rechtmäßigkeit, der Zweckbestimmung und der Zweckbindung, der Datenminimierung, der Datenrichtigkeit und der Sicherheit – sowie die Rechte des Einzelnen (auf Auskunft, Berichtigung, Löschung und Aussetzung der Verarbeitung, siehe Artikel 4 PIPA). Darüber hinaus werden in Artikel 58 Absatz 4 PIPA spezielle Pflichten für diese Verarbeitungstätigkeiten auferlegt, insbesondere in Bezug auf Datenminimierung, begrenzte Datenspeicherung, Sicherheitsmaßnahmen und die Bearbeitung von Beschwerden ([40]). Folglich können Einzelpersonen immer noch eine Beschwerde bei der PIPC einreichen, wenn diese Grundsätze und Pflichten nicht eingehalten werden, und die PIPC ist befugt, im Falle der Nichteinhaltung Durchsetzungsmaßnahmen zu ergreifen.

([35]) Siehe insbesondere Artikel 18 Absatz 2 und Kapitel VI PIPA.

([36]) Informationsdienste umfassen sowohl die Bereitstellung von Informationen als auch Vermittlungsdienste für die Bereitstellung von Informationen.

([37]) Siehe Artikel 2 Absatz 1 Nummer 3 (in Verbindung mit Artikel 2 Absatz 1 Nummern 2, 4) des Netzgesetzes und Artikel 2 Absätze 6 und 8 des Gesetzes über Telekommunikationsunternehmen.

([38]) Soweit koreanische Informations- und Kommunikationsdiensteanbieter eine direkte Beziehung zu Einzelpersonen in der EU haben (indem sie Online-Dienste anbieten), könnte dies gemäß Artikel 3 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 zu einer direkten Anwendung dieser Verordnung führen.

([39]) Gemäß Artikel 58 Absatz 2 PIPA gelten die Artikel 15, 22, 27 Absätze 1 bis 2 sowie Artikel 34 und 37 nicht für personenbezogene Daten, die mithilfe von visuellen Datenverarbeitungsgeräten verarbeitet werden, die an offenen Orten eingerichtet und betrieben werden. Da diese Bestimmung den Einsatz von Videoüberwachung innerhalb Koreas betrifft, d. h. die direkte Erhebung personenbezogener Daten von Personen in Korea, ist sie für den Zweck dieses Beschlusses, der die Übermittlung personenbezogener Daten von Verantwortlichen oder Auftragsverarbeitern in der EU an Einrichtungen in Korea betrifft, nicht relevant. Darüber hinaus gelten gemäß Artikel 58 Absatz 3 PIPA Artikel 15 (Erhebung und Verwendung personenbezogener Daten), Artikel 30 (Pflicht zur Erstellung einer öffentlichen Datenschutzerklärung) und Artikel 31 (Pflicht zur Ernennung eines Datenschutzbeauftragten) nicht für personenbezogene Daten, die zum Betrieb von Gruppen oder Freundschaftsvereinen (z. B. Hobbyclubs) verarbeitet werden. Da solche Gruppen ihrer Natur nach persönlich sind und keine Verbindung zu einer beruflichen oder kommerziellen Tätigkeit haben, ist keine besondere Rechtsgrundlage (wie die Einwilligung der betroffenen Personen) erforderlich, um ihre Daten in diesem Zusammenhang zu erheben und zu verwenden. Alle anderen Bestimmungen des PIPA (z. B. Datenminimierung, Zweckbindung, Rechtmäßigkeit der Verarbeitung, Sicherheit und Rechte des Einzelnen) gelten jedoch weiterhin. Außerdem würde jede Verarbeitung personenbezogener Daten, die über den Zweck der Bildung einer sozialen Gruppe hinausgeht, nicht unter die Ausnahmeregelung fallen.

([40]) Insbesondere ist nach Artikel 58 Absatz 4 PIPA die Pflicht vorgesehen, personenbezogene Daten nur in dem Umfang zu verarbeiten, der zur Erreichung des beabsichtigten Zwecks erforderlich ist, sie für einen Mindestzeitraum zu verarbeiten und die erforderlichen Vorkehrungen für die sichere Verwaltung und angemessene Verarbeitung dieser personenbezogenen Daten zu treffen. Letzteres umfasst technische, organisatorische und physische Sicherheitsvorkehrungen sowie Maßnahmen zur Gewährleistung der ordnungsgemäßen Bearbeitung von Einzelbeschwerden.

(27) Erstens gilt die teilweise Ausnahme für personenbezogene Daten, die gemäß dem Statistikgesetz für die Verarbeitung durch öffentliche Einrichtungen erhoben werden. Nach Angaben der koreanischen Regierung betreffen die in diesem Zusammenhang verarbeiteten personenbezogenen Daten in der Regel koreanische Staatsangehörige und können nur ausnahmsweise Informationen über ausländische Staatsangehörige enthalten, nämlich im Falle von Statistiken über die Ein- und Ausreise in das bzw. aus dem Staatsgebiet oder über ausländische Investitionen. Aber auch in diesen Fällen werden solche Daten normalerweise nicht von Verantwortlichen oder Auftragsverarbeitern in der Union übermittelt, sondern direkt von öffentlichen Behörden in Korea erhoben ([41]). Darüber hinaus unterliegt die Verarbeitung von Daten nach dem Statistikgesetz, ähnlich wie in Erwägungsgrund 162 der Verordnung (EU) 2016/679 vorgesehen, mehreren Bedingungen und Garantien. So enthält das Statistikgesetz besondere Pflichten, wie die Gewährleistung von Genauigkeit, Kohärenz und Unparteilichkeit, die Sicherstellung der Vertraulichkeit von Einzelpersonen, den Schutz der Daten der Befragten von statistischen Abfragen, auch um zu verhindern, dass diese Daten für andere Zwecke als die Erstellung von Statistiken verwendet werden, und die Anforderung an die Mitarbeiter zur Vertraulichkeit ([42]). Bei der Verarbeitung von Statistiken durch öffentliche Stellen müssen unter anderem auch die Grundsätze der Datenminimierung, der Zweckbindung und der Sicherheit beachtet werden (Artikel 3 und Artikel 58 Absatz 4 PIPA), und der Einzelne muss seine Rechte (auf Auskunft, Berichtigung, Löschung und Sperrung, siehe Artikel 4 PIPA) wahrnehmen können. Schließlich müssen die Daten in anonymisierter oder pseudonymisierter Form verarbeitet werden, soweit dadurch der Zweck der Verarbeitung erfüllt werden kann (Artikel 3 Absatz 7 PIPA).

(28) Zweitens bezieht sich Artikel 58 Absatz 1 PIPA auf personenbezogene Daten, die für die Analyse von Informationen über die nationale Sicherheit erhoben oder angefordert werden. Der Anwendungsbereich und die Folgen dieser teilweisen Ausnahme werden in Erwägungsgrund (149) näher beschrieben.

(29) Drittens gilt die teilweise Ausnahme für die vorübergehende Verarbeitung personenbezogener Daten, wenn dies aus Gründen der öffentlichen Sicherheit oder Ordnung, einschließlich der öffentlichen Gesundheit, dringend erforderlich ist. Diese Kategorie wird von der PIPC eng ausgelegt und wurde nach den vorliegenden Informationen noch nie verwendet. Sie kommt nur in Notfällen zur Anwendung, die dringende Maßnahmen erfordern, z. B. um Infektionserreger aufzuspüren oder Opfer von Naturkatastrophen zu retten und ihnen zu helfen ([43]). Selbst in diesen Fällen gilt die teilweise Ausnahme nur für die Verarbeitung personenbezogener Daten während eines begrenzten Zeitraums zur Durchführung einer solchen Maßnahme. Die Fälle, in denen dies auf die von diesem Beschluss erfassten Übermittlungen von Daten zutreffen könnte, sind sogar noch begrenzter, da die Wahrscheinlichkeit gering ist, dass die von der Union an koreanische Betreiber übermittelten personenbezogenen Daten derart sind, dass ihre anschließende Verarbeitung für solche Notfälle „dringend erforderlich" wäre.

(30) Schließlich gilt die teilweise Ausnahme für personenbezogene Daten, die von der Presse, für Missionierungstätigkeiten religiöser Organisationen oder für die Nominierung von Kandidaten durch politische Parteien erhoben oder verwendet werden. Die Ausnahme findet nur Anwendung, wenn personenbezogene Daten von der Presse, religiösen Organisationen oder politischen Parteien für diese spezifischen Zwecke (d. h. journalistische Tätigkeiten, Missionierung und die Nominierung politischer Kandidaten) verarbeitet werden. Verarbeiten diese Einrichtungen personenbezogene Daten für andere Zwecke, z. B. für die Personalverwaltung oder die interne Verwaltung, gilt das PIPA in vollem Umfang.

(31) In Bezug auf die Verarbeitung personenbezogener Daten durch die Presse für journalistische Tätigkeiten ist die Abwägung zwischen der Meinungsfreiheit und anderen Rechten (einschließlich des Rechts auf Privatsphäre) im Gesetz über die Schiedsverfahren und Rechtsbehelfe usw. für durch Presseberichte verursachte Schäden (im Folgenden „Pressegesetz") geregelt ([44]). Insbesondere ist in Artikel 5 des Pressegesetzes festgelegt, dass die

([41]) In diesem Zusammenhang sind öffentliche Einrichtungen gemäß Artikel 33 des Statistikgesetzes verpflichtet, die Daten der Befragten zu schützen, auch um zu verhindern, dass diese Daten für andere Zwecke als die Erstellung von Statistiken verwendet werden.

([42]) Artikel 2 Absätze 2 bis 3, Artikel 30 Absatz 2, Artikel 33 und 34 des Statistikgesetzes.

([43]) PIPA-Handbuch, Abschnitt über Artikel 58.

([44]) So müssen Presseberichte gemäß Artikel 4 des Pressegesetzes unparteiisch und objektiv sein, im öffentlichen Interesse liegen, die Würde und den Wert des Menschen achten und dürfen weder andere Personen verleumden noch deren Rechte, die öffentliche Moral oder die soziale Ethik verletzen.

Presse (d. h. Rundfunkanstalten, Zeitungen, Zeitschriften oder Online-Zeitungen), Internet-Nachrichtendienste oder Internet-Multimedia-Sender die Privatsphäre von Personen nicht verletzen dürfen. Kommt es dennoch zu einem Verstoß gegen die Privatsphäre, muss dieser unverzüglich gemäß den im Gesetz festgelegten Verfahren behoben werden. In diesem Zusammenhang räumt das Gesetz Personen, die durch eine Presseberichterstattung geschädigt wurden, eine Reihe von Rechten ein, darunter das Recht auf die Veröffentlichung einer Berichtigung einer falschen Behauptung, auf eine Richtigstellung durch eine gegensätzliche Behauptung oder auf einen weiteren Bericht (wenn eine Presseberichterstattung Vorwürfe bezüglich vermeintlicher Straftaten betrifft, von denen die Person später freigesprochen wird) ([45]). Beschwerden von Einzelpersonen können von den Presseunternehmen direkt (über eine Ombudsperson) ([46]), durch Schlichtung oder Schiedsverfahren (vor einer speziellen Schiedskommission für die Presse) ([47]) oder vor Gericht beigelegt werden. Einzelpersonen können auch eine Entschädigung erhalten, wenn sie aufgrund einer rechtswidrigen Handlung der Presse (vorsätzlich oder fahrlässig) einen finanziellen Schaden, eine Verletzung des Persönlichkeitsrechts oder eine andere emotionale Belastung erlitten haben ([48]). Die Presse ist nach dem Gesetz von der Haftung befreit, sofern ein Pressebericht, der in die Rechte einer Person eingreift, nicht gegen gesellschaftliche Werte verstößt und entweder mit Einwilligung der betroffenen Person oder im öffentlichen Interesse veröffentlicht wird (und es hinreichende Gründe gibt, anzunehmen, dass der Bericht der Wahrheit entspricht) ([49]).

(32) Die Verarbeitung personenbezogener Daten durch die Presse für journalistische Tätigkeiten unterliegt daher besonderen Garantien, die sich aus dem Pressegesetz ergeben. Es gibt jedoch keine derartigen zusätzlichen Garantien, die die Anwendung der Ausnahmen für die Verarbeitungstätigkeiten durch religiöse Organisationen und politische Parteien in einer mit den Artikeln 85, 89 und 91 der Verordnung (EU) 2016/679 vergleichbaren Weise einrahmen. Die Kommission hält es daher für angemessen, religiöse Organisationen, soweit sie personenbezogene Daten für ihre Missionierungstätigkeiten verarbeiten, und politische Parteien, soweit sie personenbezogene Daten im Zusammenhang mit der Nominierung von Kandidaten verarbeiten, vom Anwendungsbereich dieses Beschlusses auszunehmen.

2.3 **Garantien, Rechte und Pflichten**

2.3.1 *Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben*

(33) Die Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen.

(34) Dieser Grundsatz ist in Artikel 3 Absätze 1 und 2 PIPA verankert und wird durch Artikel 59 PIPA bekräftigt, wonach die Verarbeitung personenbezogener Daten „durch Betrug, mit unzulässigen oder ungerechten Mitteln", „ohne rechtliche Befugnis" oder „unter Befugnisüberschreitung" verboten ist ([50]). Diese allgemeinen Grundsätze der rechtmäßigen Verarbeitung werden in den Artikeln 15 bis 19 PIPA erläutert, in denen die verschiedenen Rechtsgrundlagen für die Verarbeitung (d.h. Erhebung, Nutzung und Weitergabe an Dritte) einschließlich der Umstände, unter denen diese eine Änderung des Zwecks beinhalten kann (Artikel 18 PIPA), dargelegt sind.

([45]) Artikel 15 bis 17 des Pressegesetzes.

([46]) Jedes Presse- oder Medienunternehmen muss über eine eigene Ombudsperson verfügen, um möglichen Schäden durch die Presse vorzubeugen und sie zu beheben (z. B. durch Empfehlungen zur Korrektur von Presseberichten, die falsch sind oder den Ruf anderer schädigen), Artikel 6 des Pressegesetzes.

([47]) Die Kommission besteht aus 40 bis 90 Schiedskommissaren, die vom Minister für Kultur, Sport und Tourismus aus dem Kreis der Richter, Rechtsanwälte, Personen, die seit mindestens 10 Jahren in der Presse tätig sind, oder anderen Personen mit Fachkenntnissen im Bereich der Presse ernannt werden. Schiedskommissare dürfen nicht gleichzeitig öffentliche Bedienstete, Mitglieder politischer Parteien oder Journalisten sein. Gemäß Artikel 8 des Pressegesetzes müssen die Schiedskommissare ihre Aufgaben unabhängig ausüben und dürfen bei der Ausübung dieser Aufgaben weder Weisungen noch Anordnungen unterworfen sein. Darüber hinaus gelten besondere Vorschriften zur Vermeidung von Interessenkonflikten, z. B. durch den Ausschluss bestimmter Kommissare von der Bearbeitung einzelner Fälle, wenn ihr Ehepartner oder Verwandte an dem Fall beteiligt sind (Artikel 10 des Pressegesetzes). Die Kommission kann Streitigkeiten durch Schlichtung oder Schiedsverfahren beilegen, sie kann aber auch Empfehlungen zur Behebung von Verstößen aussprechen (Abschnitt 5 des Pressegesetzes)

([48]) Artikel 30 des Pressegesetzes.

([49]) Artikel 5 des Pressegesetzes.

([50]) Gemäß Artikel 59 PIPA ist es jeder Person, „die personenbezogene Daten verarbeitet oder jemals verarbeitet hat", untersagt, „sich personenbezogene Daten zu beschaffen oder die Einwilligung zur Verarbeitung personenbezogener Daten durch Betrug, unzulässige oder ungerechte Mittel einzuholen", „personenbezogene Daten, die im Rahmen der Geschäftstätigkeit eingeholt wurden, unbefugt weiterzugeben oder Dritten zur Verfügung zu stellen" oder „personenbezogene Daten anderer Personen ohne rechtliche Befugnis oder unter Überschreitung ihrer Befugnisse zu beschädigen, zerstören, verändern, fälschen oder offenzulegen". Ein Verstoß gegen dieses Verbot kann strafrechtliche Sanktionen nach sich ziehen, siehe Artikel 71 Absätze 5 und 6 und Artikel 72 Absatz 2 PIPA. Nach Artikel 70 Absatz 2 PIPA kann außerdem strafrechtlich geahndet werden, wer sich personenbezogene Daten, die von Dritten verarbeitet werden, durch Betrug oder andere unlautere Mittel oder Methoden verschafft oder sie einem Dritten zu gewinnbringenden oder unlauteren Zwecken zur Verfügung stellt, sowie wer ein solches Verhalten unterstützt oder veranlasst.

(35) Gemäß Artikel 15 Absatz 1 PIPA darf ein Datenverantwortlicher personenbezogene Daten (im Rahmen des Erhebungszwecks) nur aus einer begrenzten Anzahl von Rechtsgründen erheben. Dazu gehören: 1) die Einwilligung der betroffenen Person ([51]) (Nummer 1), 2) die Erforderlichkeit, einen Vertrag mit der betroffenen Person zu erfüllen (Nummer 4), 3) eine besondere gesetzliche Genehmigung oder die Erforderlichkeit zur Erfüllung einer rechtlichen Pflicht (Nummer 2), die Erforderlichkeit ([52]) für eine öffentliche Einrichtung, die gesetzlich vorgeschriebenen Aufgaben in ihrem Zuständigkeitsbereich zu erfüllen, 4) die offensichtliche Erforderlichkeit zum Schutz von Leib und Leben oder der Eigentumsinteressen der betroffenen Person oder eines Dritten vor einer unmittelbaren Gefahr (nur wenn die betroffene Person nicht in der Lage ist, ihren Willen zu äußern, oder wenn keine vorherige Einwilligung eingeholt werden kann) (Nummer 5), 5) die Erforderlichkeit zur Verwirklichung des „berechtigten Interesses" des Datenverantwortlichen, wenn dieses das Interesse der betroffenen Person „offensichtlich überwiegt" (und nur dann, wenn die Verarbeitung in einem „wesentlichen Zusammenhang" mit dem berechtigten Interesse steht und nicht über das hinausgeht, was angemessen ist) (Nummer 6) ([53]). Diese Gründe für die Verarbeitung entsprechen im Wesentlichen den in Artikel 6 der Verordnung (EU) 2016/679 festgelegten Gründen, einschließlich dem Grund des „berechtigten Interesse", der dem Grund des „berechtigten Interesse" in Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 entspricht.

(36) Einmal erhobene personenbezogene Daten dürfen im Rahmen des Erhebungszwecks (Artikel 15 Absatz 1 PIPA) oder „in einem angemessenen Zusammenhang" mit dem Erhebungszweck verwendet werden, wobei mögliche Nachteile für die betroffene Person zu berücksichtigen sind und die erforderlichen Sicherheitsvorkehrungen (z. B. Verschlüsselung) ergriffen werden müssen (Artikel 15 Absatz 3 PIPA). Um festzustellen, ob der Verwendungszweck in einem „angemessenen Zusammenhang" mit dem ursprünglichen Erhebungszweck steht, werden in dem Durchführungserlass spezifische Kriterien festgelegt, die denen des Artikels 6 Absatz 4 der Verordnung (EU) 2016/679 ähneln. Insbesondere muss ein erheblicher Bezug zum ursprünglichen Zweck bestehen, die zusätzliche Verwendung muss vorhersehbar sein (z. B. im Hinblick auf die Umstände, unter denen die Daten erhoben wurden) und, soweit möglich, müssen die Daten pseudonymisiert werden ([54]). Die spezifischen Kriterien, die ein Datenverantwortlicher bei dieser Prüfung anwendet, müssen vorab in der Datenschutzerklärung offengelegt werden ([55]). Darüber hinaus ist der Datenschutzbeauftragte (siehe Erwägungsgrund (94)) ausdrücklich verpflichtet zu prüfen, ob die weitere Verwendung innerhalb dieser Vorgaben erfolgt.

([51]) Die Einwilligung muss freiwillig, in Kenntnis der Sachlage und auf einem der gesetzlich vorgeschriebenen Wegen erteilt werden. In jedem Fall darf die Einwilligung nicht durch Betrug, unzulässige oder anderweitig ungerechte Mittel eingeholt werden (Artikel 59 Absatz 1 PIPA). Erstens haben die betroffenen Personen gemäß Artikel 4 Nummer 2 PIPA das Recht, „eine Einwilligung zu erteilen oder nicht" und „den Umfang der Einwilligung zu wählen", und sollten darüber unterrichtet werden (Artikel 15 Absatz 2, Artikel 16 Absätze 2 und 3, Artikel 17 Absatz 2 und Artikel 18 Absatz 3 PIPA). Artikel 22 Absatz 5 PIPA enthält eine weitere Garantie, wonach der Datenverantwortliche die Bereitstellung von Waren oder Dienstleistungen nicht verweigern darf, wenn dies die freie Entscheidung des Einzelnen bei der Erteilung seiner Einwilligung beeinträchtigen könnte. Dies schließt Situationen ein, in denen nur bestimmte Arten der Verarbeitung der Einwilligung bedürfen (während andere auf einem Vertrag beruhen), und umfasst auch die Weiterverarbeitung personenbezogener Daten, die im Zusammenhang mit der Bereitstellung von Waren oder Dienstleistungen erhoben wurden. Zweitens muss der Datenverantwortliche gemäß Artikel 15 Absatz 2, Artikel 17 Absätze 2 und 3 und Artikel 18 Absatz 3 PIPA bei einem Ersuchen um Einwilligung die betroffene Person über die „Einzelheiten" der einschlägigen personenbezogenen Daten (z. B. dass es sich um sensible Daten handelt, siehe Artikel 17 Absatz 2 Nummer 2 Buchstabe a des PIPA-Durchführungserlasses), den Zweck der Verarbeitung, die Speicherfrist und alle Empfänger der Daten unterrichten. Ein solches Ersuchen muss „in einer ausdrücklich erkennbaren Weise" gestellt werden, wodurch einwilligungspflichtige Angelegenheiten von anderen Angelegenheiten unterschieden werden (Artikel 22 Absätze 1 bis 4 PIPA). Drittens sind in Artikel 17 Absatz 1 Nummern 1 bis 6 des PIPA-Durchführungserlasses die spezifischen Methoden zur Einholung der Einwilligung durch den Datenverantwortlichen festgelegt, wie die schriftliche Einwilligung mit Unterschrift der betroffenen Person oder die Einwilligung per (Rück-)E-Mail. Im Rahmen des PIPA wird den Personen zwar kein allgemeines Recht auf Widerruf der Einwilligung eingeräumt, sie haben jedoch das Recht, die Aussetzung der Verarbeitung der sie betreffenden Daten zu erwirken, was im Falle der Ausübung dieses Rechts zur Beendigung der Verarbeitung und zur Löschung der Daten führt (siehe Erwägungsgrund 78 über das Recht auf Aussetzung).

([52]) Nach Angaben der PIPC können sich öffentliche Einrichtungen nur dann auf diesen Grund berufen, wenn die Verarbeitung personenbezogener Daten unvermeidbar ist, d. h. es muss für die Einrichtung unmöglich oder unverhältnismäßig schwierig sein, ihre Aufgaben ohne Verarbeitung der Daten zu erfüllen.

([53]) Gemäß Artikel 39-3 PIPA werden den Informations- und Kommunikationsdiensteanbietern besondere (strengere) Pflichten in Bezug auf die Erhebung und Verwendung personenbezogener Daten ihrer Nutzer auferlegt. Insbesondere wird verlangt, dass der Anbieter die Einwilligung des Nutzers einholt, nachdem er ihn über den Zweck der Erhebung oder Verwendung, die Kategorien der zu erfassenden personenbezogenen Daten und den Zeitraum, in dem die Daten verarbeitet werden, informiert hat (Artikel 39-3 Absatz 1 PIPA). Dies gilt auch, wenn sich einer dieser Aspekte ändert. Die Nichteinholung der Einwilligung zur Datenerhebung ist strafbar (Artikel 71 Absätze 4 und 5 PIPA). In Ausnahmefällen können personenbezogene Daten von Nutzern von Informations- und Kommunikationsdiensteanbietern ohne vorherige Einholung einer Einwilligung erhoben oder verwendet werden. Dies trifft zu, 1) wenn es aus wirtschaftlichen und technischen Gründen offensichtlich schwierig ist, eine gewöhnliche Einwilligung hinsichtlich der personenbezogenen Daten einzuholen, die für die Erfüllung des Vertrags über die Bereitstellung von Informations- und Kommunikationsdiensten erforderlich sind (z. B. wenn personenbezogene Daten wie Rechnungsdaten, Zugangsprotokolle und Zahlungsaufzeichnungen zwangsläufig im Rahmen der Vertragserfüllung erstellt werden), 2) wenn es für die Abrechnung von Gebühren nach der Bereitstellung von Informations- und Kommunikationsdiensten erforderlich ist oder 3) wenn dies durch andere Gesetze erlaubt ist (z. B. gemäß Artikel 21 Absatz 1 Nummer 6 des Gesetzes über den Verbraucherschutz im elektronischen Geschäftsverkehr dürfen Unternehmer personenbezogene Daten des gesetzlichen Vormunds eines Minderjährigen erheben, um sicherzustellen, dass eine gültige Einwilligung im Namen des Minderjährigen vorliegt) (Artikel 39-3 Absatz 2 PIPA). In jedem Fall dürfen Informations- und Kommunikationsdiensteanbieter die Bereitstellung von Diensten nicht allein aus dem Grund verweigern, dass der Nutzer nicht mehr personenbezogene Daten angibt als das erforderliche Minimum (d. h. die Daten, die für die Ausführung der wesentlichen Elemente des betreffenden Dienstes erforderlich sind), siehe Artikel 39-3 Absatz 3 PIPA.

([54]) Siehe Artikel 14-2 des PIPA-Durchführungserlasses.

([55]) Artikel 14-2 Absatz 2 des PIPA-Durchführungserlasses.

(37) Ähnliche (aber etwas strengere) Regeln gelten für die Weitergabe von Daten an Dritte. Gemäß Artikel 17 Absatz 1 PIPA ist die Weitergabe personenbezogener Daten an Dritte auf der Grundlage einer Einwilligung ([56]) oder im Rahmen des Erhebungszwecks zulässig, wenn die Daten aus einem der in Artikel 15 Absatz 1 Nummern 2, 3 und 5 PIPA vorgesehenen rechtlichen Gründen erhoben worden sind. Dies schließt insbesondere eine Weitergabe aufgrund eines „berechtigten Interesses" des Datenverantwortlichen aus Darüber hinaus ist nach Artikel 17 Absatz 4 PIPA die Weitergabe an Dritte zulässig, wenn sie „in einem angemessenen Zusammenhang" mit dem Zweck der Erhebung steht, wobei auch hier mögliche Nachteile für die betroffene Person zu berücksichtigen sind und die erforderlichen Sicherheitsvorkehrungen (z. B. Verschlüsselung) ergriffen werden müssen. Bei der Beurteilung, ob die Bestimmung in einem angemessenen Zusammenhang mit dem Zweck der Erhebung steht, sind dieselben Faktoren wie in Erwägungsgrund (36) beschrieben zu berücksichtigen, und es gelten dieselben Garantien (z. B. in Bezug auf die Transparenz durch die Datenschutzerklärung und die Einbeziehung des Datenschutzbeauftragten).

(38) Der Erhalt personenbezogener Daten durch einen koreanischen Datenverantwortlichen aus der Union gilt als „Erhebung" im Sinne von Artikel 15 PIPA. In der Bekanntmachung Nr. 2021-5 (Anhang I Abschnitt I zu diesem Beschluss) wird klargestellt, dass der Zweck, zu dem die Daten von der betreffenden EU-Einrichtung übermittelt wurden, für den koreanischen Datenverantwortlichen den Zweck der Erhebung darstellt. Folglich sind koreanische Datenverantwortliche, die personenbezogene Daten aus der Union erhalten, grundsätzlich verpflichtet, diese Daten im Rahmen des Zwecks der Übermittlung gemäß Artikel 17 PIPA zu verarbeiten.

(39) Besondere Einschränkungen gelten für den Fall, dass der Datenverantwortliche die personenbezogenen Daten zu einem anderen Zweck als dem der Erhebung verwenden oder an einen Dritten weitergeben will ([57]). Nach Artikel 18 Absatz 2 PIPA darf ein privater Datenverantwortlicher personenbezogene Daten ausnahmsweise ([58]) für einen anderen Zweck verwenden oder an einen Dritten weitergeben: 1) auf der Grundlage einer zusätzlichen (d. h. gesonderten) Einwilligung der betroffenen Person, 2) wenn dies in besonderen gesetzlichen Bestimmungen vorgesehen ist oder 3) wenn es zum Schutz von Leib und Leben oder von Eigentumsinteressen der betroffenen Person oder eines Dritten vor einer unmittelbaren Gefahr offensichtlich erforderlich ist (nur wenn die betroffene Person nicht in der Lage ist, ihren Willen zu äußern, oder wenn keine vorherige Einwilligung eingeholt werden kann) ([59]).

(40) Öffentliche Einrichtungen können in bestimmten Situationen personenbezogene Daten auch für einen anderen Zweck verwenden oder an Dritte weitergeben. Dies gilt auch für Fälle, in denen es öffentlichen Einrichtungen sonst nicht möglich wäre, ihre gesetzlich vorgeschriebenen Aufgaben zu erfüllen, vorbehaltlich der Genehmigung durch die PIPC. Darüber hinaus können öffentliche Einrichtungen personenbezogene Daten an eine andere Behörde oder ein Gericht weitergeben, wenn dies für die Ermittlung und Verfolgung von Straftaten oder eine Anklageerhebung, für ein Gericht zur Erfüllung seiner Aufgaben im Zusammenhang mit einem laufenden Gerichtsverfahren oder für die Vollstreckung einer strafrechtlichen Sanktion oder einer Betreuungs- oder Sorgerechtsverfügung erforderlich ist ([60]). Sie können personenbezogene Daten auch an eine ausländische Regierung oder eine internationale Organisation weitergeben, um einer rechtlichen Pflicht aus einem Vertrag oder einem internationalen Übereinkommen nachzukommen; in diesem Fall müssen sie auch die Anforderungen für grenzüberschreitende Datenübermittlungen erfüllen (siehe Erwägungsgrund (90)).

(41) Die Grundsätze der Rechtmäßigkeit und der Verarbeitung nach Treu und Glauben werden daher im koreanischen Rechtsrahmen in einer Weise umgesetzt, die im Wesentlichen der Verordnung (EU) 2016/679 entspricht, indem die Verarbeitung nur aus rechtmäßigen und klar definierten Gründen erlaubt wird. Darüber hinaus ist die Verarbeitung in allen genannten Fällen nur dann zulässig, wenn sie nicht „zur unfairen Beeinträchtigung" der Interessen der betroffenen Person oder eines Dritten führt, was eine Interessenabwägung erfordert. Darüber hinaus sind in Artikel 18 Absatz 5 PIPA zusätzliche Garantien für den Fall vorgesehen, dass der Datenverantwortliche die personenbezogenen Daten an einen Dritten weitergibt; dazu kann die Aufforderung gehören, den Zweck und die Art der Nutzung einzuschränken oder besondere Sicherheitsvorkehrungen zu ergreifen. Der Dritte ist seinerseits verpflichtet, die geforderten Vorkehrungen zu ergreifen.

([56]) Verstöße gegen Artikel 17 Absatz 1 Nummer 1 PIPA können strafrechtlich geahndet werden (Artikel 71 Absatz 1 PIPA).

([57]) Der „beabsichtigte Zweck" ist der Zweck, für den die Daten erhoben wurden. Werden die Daten beispielsweise auf der Grundlage der Einwilligung der betroffenen Person erhoben, ist der beabsichtigte Zweck der Zweck, über die die Person gemäß Artikel 15 Absatz 2 PIPA informiert wird.

([58]) Vgl. Artikel 18 Absatz 1 PIPA. Verstöße gegen Artikel 18 Absätze 1 und 2 PIPA können strafrechtlich geahndet werden (Artikel 71 Absatz 2 PIPA).

([59]) Die Verwendung personenbezogener Daten oder ihre Weitergabe an Dritte durch Informations- und Kommunikationsdiensteanbieter zu einem anderen Zweck als dem ursprünglichen darf nur aus den in Artikel 18 Absatz 2 Nummern 1 und 2 PIPA genannten Gründen erfolgen (d. h. wenn eine zusätzliche Einwilligung eingeholt wird oder wenn besondere gesetzliche Bestimmungen bestehen). Siehe Artikel 18 Absatz 2 PIPA.

([60]) Sofern die Verarbeitung nicht für die Ermittlung von Straftaten, die Anklageerhebung und die Strafverfolgung erforderlich ist, sind öffentliche Einrichtungen, die personenbezogene Daten zu einem anderen Zweck als dem der Erhebung verwenden oder an Dritte weitergeben (z. B. wenn dies gesetzlich ausdrücklich erlaubt oder zur Erfüllung eines Vertrags erforderlich ist), verpflichtet, die Rechtsgrundlage für die Verarbeitung, ihren Zweck und ihren Umfang auf ihrer Website oder im Amtsblatt zu veröffentlichen und Aufzeichnungen zu führen (Artikel 18 Absatz 4 PIPA in Verbindung mit Artikel 15 des PIPA-Durchführungserlasses).

(42) Gemäß Artikel 28-2 PIPA ist schließlich die (Weiter-)Verarbeitung pseudonymisierter Daten ohne die Einwilligung der betroffenen Person für die Zwecke der Statistik, der wissenschaftlichen Forschung ([61]) und der Archivierung im öffentlichen Interesse vorbehaltlich besonderer Garantien zulässig. Ähnlich wie in der Verordnung (EU) 2016/679 ([62]) wird daher mit dem PIPA die (Weiter-)Verarbeitung personenbezogener Daten für solche Zwecke innerhalb eines Rahmens erleichtert, in dem angemessene Garantien zum Schutz der Rechte des Einzelnen vorgesehen sind. Im PIPA wird die Pseudonymisierung nicht als mögliche Schutzmaßnahme, sondern als Voraussetzung für die Durchführung bestimmter Verarbeitungen für die Zwecke der Statistik, der wissenschaftlichen Forschung und der Archivierung im öffentlichen Interesse vorgeschrieben (z. B. um die Daten ohne Einwilligung verarbeiten zu können oder um verschiedene Datensätze miteinander zu verknüpfen).

(43) Darüber hinaus sind im PIPA eine Reihe spezieller Garantien vorgesehen, insbesondere in Bezug auf die erforderlichen technischen und organisatorischen Maßnahmen, die Führung von Aufzeichnungen, die Einschränkung der gemeinsamen Nutzung von Daten und den Umgang mit möglichen Risiken der erneuten Identifizierung. Durch die Kombination der verschiedenen in den Erwägungsgründen (44)-(48) beschriebenen Garantien wird sichergestellt, dass die Verarbeitung personenbezogener Daten in diesem Zusammenhang Schutzmaßnahmen unterliegt, die denjenigen, die gemäß der Verordnung (EU) 2016/679 erforderlich wären, der Sache nach gleichwertig wären.

(44) Zuallererst und vor allem ist nach Artikel 28-5 Absatz 1 PIPA die Verarbeitung pseudonymisierter Daten zum Zwecke der Identifizierung einer bestimmten Person verboten. Sollten bei der Verarbeitung pseudonymisierter Daten dennoch Daten erzeugt werden, die die Identifizierung einer Person ermöglichen, muss der Datenverantwortliche die Verarbeitung unverzüglich aussetzen und diese Daten vernichten (Artikel 28-5 Absatz 2 PIPA). Die Nichteinhaltung dieser Bestimmungen wird mit Geldbußen geahndet und stellt eine Straftat dar ([63]). Somit ist eine solche erneute Identifizierung selbst in Situationen, in denen es *praktisch* möglich wäre, die Person erneut zu identifizieren, *gesetzlich* verboten.

(45) Zweitens muss der Datenverantwortliche bei der (Weiter-)Verarbeitung pseudonymisierter Daten zu solchen Zwecken besondere technische, organisatorische und physische Maßnahmen ergreifen, um die Sicherheit der Daten zu gewährleisten (einschließlich der gesonderten Speicherung und Verwaltung der Daten, die zur Wiederherstellung des ursprünglichen Zustands der pseudonymisierten Daten erforderlich sind) ([64]). Darüber hinaus müssen Aufzeichnungen über die verarbeiteten pseudonymisierten Daten, den Zweck der Verarbeitung, die Verwendungshistorie und etwaige Drittempfänger geführt werden (Artikel 29-5 Absatz 2 des PIPA-Durchführungserlasses).

(46) Drittens und letztens enthält das PIPA spezielle Garantien, um die Identifizierung von Personen durch Dritte zu verhindern, wenn die Daten weitergegeben werden. Insbesondere dürfen die Datenverantwortlichen bei der Weitergabe pseudonymisierter Daten an Dritte zum Zwecke der Statistik, der wissenschaftlichen Forschung oder der Archivierung im öffentlichen Interesse keine Informationen einbeziehen, die zur Identifizierung einer bestimmten Person verwendet werden könnten (Artikel 28-2 Absatz 2 PIPA) ([65]).

(47) Genauer gesagt ist nach dem PIPA zwar die Verknüpfung pseudonymisierter Daten (die von verschiedenen Datenverantwortlichen verarbeitet werden) zum Zwecke der Statistik, der wissenschaftlichen Forschung oder der Archivierung im öffentlichen Interesse zulässig, doch ist diese Befugnis spezialisierten Einrichtungen vorbehalten, die über besondere Sicherheitsvorkehrungen verfügen (Artikel 28-3 Absatz 1 PIPA) ([66]). Bei der Beantragung einer Verknüpfung von pseudonymisierten Daten muss ein Datenverantwortlicher unter anderem

([61]) Wissenschaftliche Forschung wird in Artikel 2 Absatz 8 PIPA definiert als „Forschung, die wissenschaftliche Methoden anwendet, wie Technologieentwicklung und -demonstration, Grundlagenforschung, angewandte Forschung und privat finanzierte Forschung". Diese Kategorien entsprechen den in Erwägungsgrund 159 der Verordnung (EU) 2016/679 genannten Kategorien.

([62]) Siehe Artikel 5 Absatz 1 Buchstabe b und Artikel 89 Absätze 1 bis 2 sowie die Erwägungsgründe 50 und 157 der Verordnung (EU) 2016/679.

([63]) Siehe Artikel 28-6 Absatz 1, Artikel 71 Absatz 4-3 und Artikel 75 Absatz 2 Nummer 4-4 PIPA.

([64]) Artikel 28-4 PIPA und Artikel 29-5 des PIPA-Durchführungserlasses. Die Nichteinhaltung dieser Pflicht wird mit verwaltungs- und strafrechtlichen Sanktionen geahndet, vgl. Artikel 73 Absatz 1 und Artikel 75 Absatz 2 Nummer 6 PIPA.

([65]) Verstöße gegen diese Anforderungen können strafrechtliche Sanktionen nach sich ziehen (Artikel 71 Absatz 2 PIPA). Die PIPC begann sofort mit der Durchsetzung dieser neuen Vorschriften, z. B. in ihrer Entscheidung vom 28. April 2021, in der sie eine Geldbuße und Abhilfemaßnahmen gegen ein Unternehmen verhängte, das neben anderen Verstößen gegen das PIPA auch die Anforderungen von Artikel 28-2 Absatz 2 PIPA nicht erfüllt hatte, siehe https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Um als eine solche spezialisierte Einrichtung (eine „Fachstelle für Datenverknüpfung") benannt zu werden, muss ein Antrag an die PIPC zusammen mit Belegen eingereicht werden, die unter anderem die Anlagen und die Ausstattung für die sichere Verknüpfung pseudonymisierter Daten darlegen und bestätigen, dass der Antragsteller mindestens drei Vollzeitmitarbeiter mit Fachkenntnissen oder Erfahrung im Bereich des Schutzes personenbezogener Daten beschäftigt (Artikel 29-2 Absätze 1 bis 2 des PIPA-Durchführungserlasses). Detaillierte Anforderungen, z. B. in Bezug auf die Qualifikation des Personals, verfügbare Anlagen, Sicherheitsvorkehrungen, interne Strategien und Verfahren sowie finanzielle Anforderungen, sind in der Bekanntmachung 2020-9 der PIPC über die Verknüpfung und Freigabe von pseudonymisierten Daten (Anhang I) festgelegt. Eine Benennung als Fachstelle für Datenverknüpfung kann von der PIPC (nach einer Anhörung) aus bestimmten Gründen widerrufen werden, z. B. wenn die Stelle die für die Benennung erforderlichen Sicherheitsanforderungen nicht mehr erfüllt oder wenn es im Zusammenhang mit der Datenverknüpfung zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist (Artikel 29-2 Absätze 5 und 6 des PIPA-Durchführungserlasses). Die PIPC muss jede Benennung (bzw. jeden Widerruf der Benennung) einer Fachstelle für Datenverknüpfung veröffentlichen (Artikel 29-2 Absatz 7 des PIPA-Durchführungserlasses).

Unterlagen über die zu verknüpfenden Daten, den Zweck der Verknüpfung sowie die vorgeschlagenen Sicherheitsvorkehrungen für die Verarbeitung der verknüpften Daten vorlegen ([67]). Um die Verknüpfung zu ermöglichen, muss der Datenverantwortliche die zu verknüpfenden Daten an die spezialisierte Einrichtung senden und einen „Kombinationsschlüssel" (d. h. die Informationen, die zur Pseudonymisierung verwendet wurden) an die Koreanische Internet- und Sicherheitsbehörde übermitteln ([68]). Letztere generiert „Kombinationsschlüssel-Verknüpfungsdaten" (die es ermöglichen, die Kombinationsschlüssel verschiedener Antragsteller zu verknüpfen, um eine Verbindung der Datensätze zu erreichen) und stellt sie der spezialisierten Einrichtung zur Verfügung ([69]).

(48) Der Datenverantwortliche, der die Verknüpfung beantragt, kann die verknüpften Daten in den Räumlichkeiten der spezialisierten Einrichtung analysieren, in einem Raum, in dem besondere technische, physische und administrative Sicherheitsvorkehrungen ergriffen werden (Artikel 29-3 des PIPA-Durchführungserlasses). Datenverantwortliche, die einen Datensatz für eine solche Verknüpfung zur Verfügung stellen, dürfen die verknüpften Daten nur nach einer weiteren Pseudonymisierung oder Anonymisierung und mit Genehmigung dieser speziellen Einrichtung außerhalb der Einrichtung verwenden (Artikel 28-3 Absatz 2 PIPA) ([70]). Bei der Prüfung, ob eine solche Genehmigung zu erteilen ist, prüft die Einrichtung den Zusammenhang zwischen den verknüpften Daten und dem Zweck der Verarbeitung sowie die Frage, ob ein spezieller Sicherheitsplan für die Verwendung dieser Daten erstellt wurde ([71]). Der Export der verknüpften Informationen außerhalb der Einrichtung ist nicht zulässig, wenn die Informationen Daten enthalten, die die Identifizierung einer Person ermöglichen würden ([72]). Schließlich überwacht die PIPC die durch die spezialisierte Einrichtung erfolgende Verknüpfung und Freigabe pseudonymisierter Daten (Artikel 29-4 Absatz 3 des PIPA-Durchführungserlasses).

2.3.2 *Verarbeitung besonderer Kategorien von personenbezogenen Daten*

(49) Wenn besondere Kategorien von Daten verarbeitet werden, sollten besondere Garantien vorhanden sein.

(50) Das PIPA enthält spezielle Regeln für die Verarbeitung sensibler Daten; ([73]) diese sind definiert als personenbezogene Daten, die Informationen über die Weltanschauung, den Glauben, den Beitritt zu oder den Austritt aus einer Gewerkschaft oder politischen Partei, die politischen Meinungen, die Gesundheit und das Sexualleben einer Person offenbaren, sowie andere personenbezogene Daten, die die Privatsphäre der betroffenen Person „deutlich" gefährden können und per Präsidialerlass als sensible Daten eingestuft wurden ([74]). Nach den Erläuterungen der PIPC wird der Begriff „Sexualleben" so ausgelegt, dass er auch die sexuelle Ausrichtung oder die sexuellen Vorlieben des Einzelnen umfasst ([75]). Darüber hinaus werden in Artikel 18 des Durchführungserlasses weitere Kategorien sensibler Daten hinzugefügt, insbesondere DNA-Informationen aus Gentests und Daten aus dem Strafregister. Durch die neueste Änderung des PIPA-Durchführungserlasses wurde der Begriff der sensiblen Daten weiter erweitert, indem auch personenbezogene Daten, die Aufschluss über die Rasse oder die ethnische Herkunft geben, sowie biometrische Informationen einbezogen wurden ([76]). Nach dieser Änderung entspricht der Begriff der sensiblen Daten im PIPA im Wesentlichen dem Begriff in Artikel 9 der Verordnung (EU) 2016/679.

(51) Gemäß Artikel 23 Absatz 1 PIPA und ähnlich wie in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung sensibler Daten generell untersagt, sofern nicht eine der aufgezählten Ausnahmen vorliegt ([77]). Diese beschränken die Verarbeitung auf Fälle, in denen der Datenverantwortliche die betroffene Person

([67]) Artikel 8 Absätze 1 und 2 der Bekanntmachung 2020-9 über die Verknüpfung und Freigabe von pseudonymisierten Daten.
([68]) Artikel 2 Absätze 3 und 6 und Artikel 9 Absatz 1 der Bekanntmachung 2020-9 über die Verknüpfung und Freigabe von pseudonymisierten Daten.
([69]) Artikel 2 Absatz 4 und Artikel 9 Absätze 2 und 3 der Bekanntmachung 2020-9 über die Verknüpfung und Freigabe von pseudonymisierten Daten. Die spezialisierte Einrichtung muss die Verknüpfungsdaten des Kombinationsschlüssels nach der Verknüpfung unverzüglich vernichten (Artikel 9 Absatz 4 der Bekanntmachung).
([70]) Verstöße gegen die Anforderungen an die Verknüpfung von Datensätzen können strafrechtliche Sanktionen nach sich ziehen (Artikel 71 Absatz 4-2 PIPA). Siehe auch Artikel 29-2 Absatz 4 des PIPA-Durchführungserlasses.
([71]) Das Verfahren zur Genehmigung einer Freigabe verknüpfter Daten ist in Artikel 11 der Bekanntmachung 2020-9 über die Verknüpfung und Freigabe von pseudonymisierten Daten dargelegt. Insbesondere muss die spezialisierte Einrichtung einen „Überprüfungsausschuss für die Freigabe" einrichten, der sich aus Mitgliedern zusammensetzt, die über umfangreiche Kenntnisse und einschlägige Erfahrung im Bereich des Datenschutzes verfügen.
([72]) Artikel 29-2 Absatz 4 des PIPA-Durchführungserlasses und Bekanntmachung Nr. 2020-9, Artikel 11.
([73]) Die Notwendigkeit, besondere Schutzvorkehrungen für die Verarbeitung sensibler Daten wie Daten über Gesundheit oder Sexualverhalten vorzusehen, wurde auch vom koreanischen Verfassungsgericht anerkannt, siehe Entscheidung des Verfassungsgerichts vom 31. Mai 2007, HunMa 1139.
([74]) Artikel 23 Absatz 1 PIPA.
([75]) Siehe auch PIPA-Handbuch, Kapitel III Abschnitt 2 über Artikel 23 (S. 157-164).
([76]) Es handelt sich um personenbezogene Daten, die sich aus einer spezifischen technischen Verarbeitung von Daten über physische, physiologische oder verhaltensbezogene Merkmale einer Person zum Zwecke ihrer eindeutigen Identifizierung ergeben.
([77]) Die Nichteinhaltung dieser Anforderungen kann Sanktionen gemäß Artikel 71 Nummer 3 PIPA nach sich ziehen.

gemäß Artikel 15 und 17 PIPA unterrichtet und eine gesonderte Einwilligung einholt (d. h. getrennt von der Einwilligung für die Verarbeitung anderer personenbezogener Daten) oder in denen die Verarbeitung gesetzlich vorgeschrieben oder zulässig ist. Die Behörden können auch biometrische Daten, DNA-Informationen aus Gentests, personenbezogene Daten, die Aufschluss über die Rasse oder die ethnische Herkunft geben, und Daten aus dem Strafregister aus Gründen verarbeiten, die ausschließlich ihnen zur Verfügung stehen (z. B. wenn sie für die Untersuchung von Straftaten oder für Gerichtsverfahren erforderlich sind) ([78]). Daher sind die Rechtsgrundlagen für die Verarbeitung sensibler Daten begrenzter als für andere Arten personenbezogener Daten und nach dem koreanischen Recht sogar noch restriktiver als nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679.

(52) Darüber hinaus wird in Artikel 23 Absatz 2 des PIPA – dessen Nichteinhaltung Sanktionen nach sich ziehen kann ([79]) – die besondere Bedeutung der Gewährleistung einer angemessenen Sicherheit beim Umgang mit sensiblen Daten hervorgehoben, damit diese „nicht verloren gehen oder gestohlen, weitergegeben, gefälscht, verändert oder beschädigt werden können". Zwar handelt es sich hierbei um eine allgemeine Anforderung gemäß Artikel 29 PIPA, doch wird in Artikel 3 Absatz 4 klargestellt, dass das Sicherheitsniveau an die Art der verarbeiteten personenbezogenen Daten anzupassen ist, was bedeutet, dass die besonderen Risiken bei der Verarbeitung sensibler Daten berücksichtigt werden müssen. Darüber hinaus muss die Datenverarbeitung stets so erfolgen, dass die Privatsphäre der betroffenen Person „so wenig wie möglich beeinträchtigt wird", und soweit möglich „durch Anonymisierung" (Artikel 3 Absätze 6 und 7 PIPA). Diese Anforderungen sind besonders wichtig, wenn die Verarbeitung sensible Daten betrifft.

2.3.3 *Zweckbindung*

(53) Personenbezogene Daten sollten für einen bestimmten Zweck und in einer Weise erhoben werden, die mit dem Zweck der Verarbeitung nicht unvereinbar ist.

(54) Dieser Grundsatz wird durch Artikel 3 Absätze 1 und 2 PIPA gewährleistet, wonach der Datenverantwortliche den Zweck der Verarbeitung „genau und ausdrücklich" anzugeben hat, personenbezogene Daten in einer für diesen Zweck geeigneter Weise verarbeiten muss und sie nicht über diesen Zweck hinaus verwenden darf. Der allgemeine Grundsatz der Zweckbindung wird auch in den Artikel 15 Absatz 1, Artikel 18 Absatz 1, Artikel 19 und – für Auftragsverarbeiter (sogenannte „Beauftragte") – in Artikel 26 Absatz 1 Nummern 1, 5 und 7 PIPA bekräftigt. Insbesondere dürfen personenbezogene Daten grundsätzlich nur im Rahmen des Zwecks, für den sie erhoben wurden, verwendet und an Dritte weitergegeben werden (Artikel 15 Absatz 1 und Artikel 17 Absatz 1 Nummer 2). Die Verarbeitung für einen kompatiblen Zweck, d. h. „in einem angemessenen Zusammenhang mit dem ursprünglichen Zweck der Erhebung", ist nur zulässig, wenn sie sich nicht nachteilig auf die betroffenen Personen auswirkt und wenn die erforderlichen Sicherheitsvorkehrungen (z. B. Verschlüsselung) ergriffen werden (Artikel 15 Absatz 3 und Artikel 17 Absatz 4 PIPA). Um festzustellen, ob die Weiterverarbeitung einem kompatiblen Zweck dient, werden im PIPA-Durchführungserlass spezifische Kriterien aufgeführt, die denen in Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 ähneln (siehe Erwägungsgrund (36)).

(55) Wie in Erwägungsgrund (38) erläutert, ist der Zweck der Datenerhebung im Falle koreanischer Datenverantwortlicher, die personenbezogene Daten aus der Union erhalten, der Zweck, zu dem die Daten übermittelt werden. Eine Änderung des Zwecks durch den Datenverantwortlichen ist nur ausnahmsweise, in bestimmten (aufgezählten) Fällen, zulässig (Artikel 18 Absatz 2 Nummer 1-3 PIPA, siehe auch Erwägungsgrund (39)). Soweit eine Zweckänderung gesetzlich zulässig ist, müssen in den entsprechenden Rechtsvorschriften wiederum das Grundrecht auf Schutz der Privatsphäre und auf Datenschutz sowie die in der koreanischen Verfassung verankerten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit gewahrt werden. Darüber hinaus sind in Artikel 18 Absätze 2 und 5 PIPA zusätzliche Garantien vorgesehen, insbesondere das Erfordernis, dass eine solche Zweckänderung nicht „zur unfairen Beeinträchtigung der Interessen einer betroffenen Person führen" darf, sodass stets eine Interessenabwägung erforderlich ist. Damit wird ein Schutzniveau gewährleistet, das im Wesentlichen demjenigen nach Artikel 5 Absatz 1 Buchstabe b und Artikel 6 in Verbindung mit Erwägungsgrund 50 der Verordnung (EU) 2016/679 entspricht.

2.3.4 *Richtigkeit der Daten und Datenminimierung*

(56) Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Ferner müssen sie dem Zweck angemessen und dafür erheblich sein und dürfen das für die Zwecke der Verarbeitung notwendige Maß nicht überschreiten.

([78]) Gemäß Artikel 18 des PIPA-Durchführungserlasses sind die dort aufgeführten Datenkategorien von den Bestimmungen des Artikels 23 Absatz 1 des Gesetzes ausgenommen, wenn sie von einer öffentlichen Einrichtung gemäß Artikel 18 Absatz 2 Nummern 5 bis 9 PIPA verarbeitet werden.

([79]) Siehe Artikel 73 Nummer 1 und Artikel 75 Absatz 2 Nummer 6 PIPA.

(57) Der Grundsatz der Richtigkeit wird in ähnlicher Weise in Artikel 3 Absatz 3 PIPA anerkannt, wonach personenbezogene Daten „richtig, vollständig und auf dem neuesten Stand sein müssen, soweit dies für die Zwecke, für die sie verarbeitet werden, erforderlich ist". Die Datenminimierung ist in Artikel 3 Absätze 1 und 6 und Artikel 16 Absatz 1 PIPA festgelegt; dort heißt es, dass der Datenverantwortliche personenbezogene Daten (nur) in dem für den beabsichtigten Zweck „erforderlichen Mindestmaß" erheben darf und dass die Beweislast diesbezüglich bei ihm liegt. Sofern sich der Erhebungszweck durch die Verarbeitung von Daten in anonymisierter Form erfüllen lässt, sollten die Datenverantwortlichen dies anstreben (Artikel 3 Absatz 7 PIPA).

2.3.5 *Speicherbegrenzung*

(58) Personenbezogene Daten dürfen grundsätzlich nur so lange gespeichert werden, wie dies für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist.

(59) Der Grundsatz der Speicherbegrenzung ist ebenfalls in Artikel 21 Absatz 1 PIPA verankert; ([80]) danach ist der Datenverantwortliche verpflichtet, personenbezogene Daten unverzüglich nach Erreichen des Verarbeitungszwecks oder nach Ablauf der Speicherfrist (je nachdem, was früher eintritt) zu „vernichten", ([81]) sofern nicht eine weitere Speicherung gesetzlich vorgeschrieben ist ([82]). Im letzteren Fall sind die betreffenden personenbezogenen Daten „getrennt von anderen personenbezogenen Daten zu speichern und zu verwalten" (Artikel 21 Absatz 3 PIPA).

(60) Artikel 21 Absatz 1 PIPA findet keine Anwendung, wenn pseudonymisierte Daten für statistische Zwecke, wissenschaftliche Forschung oder die Archivierung im öffentlichen Interesse verarbeitet werden ([83]). Um auch in diesem Fall den Grundsatz der begrenzten Datenspeicherung zu gewährleisten, sind die Datenverantwortlichen gemäß der Bekanntmachung 2021-5 verpflichtet, die Daten gemäß Artikel 58-2 PIPA zu anonymisieren, wenn die Daten nicht nach Erfüllung des spezifischen Verarbeitungszwecks vernichtet wurden ([84]).

2.3.6 *Datensicherheit*

(61) Personenbezogene Daten müssen in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet und den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung einschließt. Zu diesem Zweck müssen Unternehmer geeignete technische oder organisatorische Maßnahmen treffen, um personenbezogene Daten vor möglichen Bedrohungen zu schützen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik, der mit ihnen verbundenen Kosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte des Einzelnen bewertet werden.

(62) Ein ähnlicher Sicherheitsgrundsatz ist in Artikel 3 Absatz 4 PIPA verankert, wonach die Datenverantwortlichen verpflichtet sind, „die personenbezogenen Daten in einer sicheren Weise entsprechend den Verarbeitungsmethoden, der Art usw. der personenbezogenen Daten zu verwalten, wobei sie der Möglichkeit einer Verletzung der Rechte der betroffenen Person und der Schwere der einschlägigen Risiken Rechnung tragen". Darüber hinaus hat der Datenverantwortliche „personenbezogene Daten so zu verarbeiten, dass die Möglichkeit eines Eingriffs in die Privatsphäre der betroffenen Person so gering wie möglich gehalten wird", und sich in diesem Zusammenhang zu bemühen, personenbezogene Daten möglichst in anonymer Weise oder pseudonymisierter Form zu verarbeiten (Artikel 3 Absätze 6 und 7 PIPA).

(63) Diese allgemeinen Anforderungen werden in Artikel 29 PIPA weiter ausgeführt, wonach jeder Datenverantwortliche „die technischen, organisatorischen und physischen Maßnahmen ergreift, wie die Erstellung eines internen Verwaltungsplans und die Aufbewahrung von Anmeldeprotokollen usw., die erforderlich sind, um die durch den Präsidialerlass vorgeschriebene Sicherheit zu gewährleisten, sodass die personenbezogenen Daten nicht verloren

([80]) Artikel 8 (in Verbindung mit Artikel 8-2 des Durchführungserlasses), Artikel 11 (in Verbindung mit Artikel 12 Absatz 2 des Durchführungserlasses).

([81]) Zu den Methoden der Vernichtung personenbezogener Daten siehe Artikel 16 des PIPA-Durchführungserlasses. Gemäß Artikel 21 Absatz 2 PIPA umfasst dies „die erforderlichen Maßnahmen zur Verhinderung der Wiederherstellung und Wiederaufnahme".

([82]) Die Nichteinhaltung dieser Anforderungen kann strafrechtliche Sanktionen nach sich ziehen (Artikel 73 Absatz 1-2 PIPA). Gemäß Artikel 39-6 PIPA sind Informations- und Kommunikationsdiensteanbieter zusätzlich verpflichtet, personenbezogene Daten von Nutzern zu löschen, die die angebotenen Informations- und Kommunikationsdienste mindestens ein Jahr lang nicht in Anspruch genommen haben (es sei denn, eine weitere Aufbewahrung ist gesetzlich vorgeschrieben oder wird von der betreffenden Person beantragt). Die Betroffenen müssen 30 Tage vor Ablauf der Jahresfrist über die beabsichtigte Löschung ihrer Daten informiert werden (Artikel 39-6 Absatz 2 PIPA und Artikel 48-5 Absatz 3 des PIPA-Durchführungserlasses). Ist eine weitergehende Aufbewahrung gesetzlich vorgeschrieben, müssen die auf Vorrat gespeicherten Daten getrennt von anderen Informationen über die Nutzer aufbewahrt werden und dürfen nur in Übereinstimmung mit diesem Gesetz verwendet oder offengelegt werden (Artikel 48-5 Absätze 1 und 2 des PIPA-Durchführungserlasses).

([83]) Artikel 28-7 PIPA.

([84]) Bekanntmachung Nr. 2021-5 (Anhang I), Abschnitt 4.

gehen oder gestohlen, weitergegeben, gefälscht, verändert oder beschädigt werden können." In Artikel 30 Absatz 1 des PIPA-Durchführungserlasses werden diese Maßnahmen spezifiziert, indem auf 1) die Formulierung und Umsetzung eines internen Verwaltungsplans für die sichere Verarbeitung personenbezogener Daten, 2) Zugangskontrollen und -beschränkungen, 3) den Einsatz von Verschlüsselungstechnologien zur sicheren Speicherung und Übermittlung personenbezogener Daten, 4) Anmeldeprotokolle, 5) Sicherheitsprogramme und 6) physische Maßnahmen wie ein sicheres Speicher- oder Sperrsystem hingewiesen wird ([85]).

(64) Darüber hinaus gelten besondere Pflichten, wenn es zu einer Verletzung des Schutzes personenbezogener Daten kommt (Artikel 34 PIPA in Verbindung mit Artikel 39 und 40 des PIPA-Durchführungserlasses) ([86]). Insbesondere ist der Datenverantwortliche verpflichtet, die betroffenen Personen unverzüglich über die Einzelheiten der Verletzung zu unterrichten, ([87]) einschließlich Informationen über (obligatorische) Gegenmaßnahmen, die der Datenverantwortliche ergriffen hat, und darüber, was die betroffenen Personen tun können, um das Risiko eines Schadens zu minimieren (Artikel 34 Absätze 1 und 2 PIPA) ([88]). Betrifft die Verletzung des Schutzes personenbezogener Daten mindestens 1 000 Personen, so meldet der Datenverantwortliche die Datenschutzverletzung und die ergriffenen Gegenmaßnahmen unverzüglich auch der PIPC und der koreanischen Internet- und Sicherheitsbehörde, die technische Unterstützung leisten kann (Artikel 34 Absatz 3 PIPA in Verbindung mit Artikel 39 des PIPA-Durchführungserlasses). Die Datenverantwortlichen haften für Schäden, die sich aus Verletzungen des Schutzes personenbezogener Daten ergeben, gemäß den Bestimmungen des Zivilgesetzes über die Haftung aus unerlaubter Handlung (siehe auch Abschnitt 2.5 über Rechtsbehelfe) ([89]).

(65) Bei der Erfüllung seiner Sicherheitspflichten muss der Datenverantwortliche von einem Datenschutzbeauftragten unterstützt werden, zu dessen Aufgaben unter anderem der Aufbau eines internen Kontrollsystems gehört, „um die Verbreitung, den Missbrauch und die missbräuchliche Verwendung personenbezogener Daten zu verhindern" (Artikel 31 Absatz 2 Nummer 4 PIPA). Darüber hinaus ist der Datenverantwortliche verpflichtet, seine Mitarbeiter, die personenbezogene Daten verarbeiten, einer „angemessenen Kontrolle und Aufsicht" zu unterziehen, auch im Hinblick auf die sichere Verwaltung der Daten; dazu gehört auch die erforderliche Schulung der Mitarbeiter (Artikel 28 Absätze 1 und 2 PIPA). Schließlich muss der Datenverantwortliche im Falle einer Unterverarbeitung dem „Beauftragten" Anforderungen u. a. an die sichere Verwaltung personenbezogener Daten („technische und organisatorische Garantien") auferlegen und deren Umsetzung durch Kontrollen überwachen (Artikel 26 Absätze 1 und 4 PIPA in Verbindung mit Artikel 28 Absatz 1 Nummern 3 und 4 und Absatz 6 des PIPA-Durchführungserlasses).

2.3.7 *Transparenz*

(66) Betroffene Personen müssen über die Hauptmerkmale der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden.

([85]) In Bezug auf die Verarbeitung personenbezogener Daten durch Informations- und Kommunikationsdiensteanbieter ist in Artikel 39-5 PIPA ausdrücklich festgelegt, dass die Zahl der Personen, die personenbezogene Daten von Nutzern verarbeiten, auf ein Minimum beschränkt werden muss. Darüber hinaus müssen die Informations- und Kommunikationsdiensteanbieter sicherstellen, dass personenbezogene Daten der Nutzer nicht über das Informations- und Kommunikationsnetz an die Öffentlichkeit gelangen (Artikel 39-10 Absatz 1 PIPA). Offengelegte Informationen müssen auf Antrag der PIPC gelöscht oder gesperrt werden (Artikel 39-10 Absatz 2 PIPA). Generell unterliegen Informations- und Kommunikationsdiensteanbieter (und Dritte, die personenbezogene Daten von Nutzern erhalten) zusätzlichen Sicherheitspflichten, die in Artikel 48-2 des PIPA-Durchführungserlasses aufgeführt sind, z. B. die Entwicklung und Umsetzung eines internen Verwaltungsplans in Bezug auf Sicherheitsvorkehrungen, Maßnahmen zur Gewährleistung der Zugangskontrolle, Verschlüsselung, Verwendung von Software zur Erkennung von Schadprogrammen usw.

([86]) Darüber hinaus besteht ein allgemeines Verbot, personenbezogene Daten ohne rechtliche Befugnis zu beschädigen, zerstören, verändern, fälschen oder weiterzugeben, siehe Artikel 59 Nummer 3 PIPA.

([87]) Die Anforderung, die betroffene Person über die Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, gilt nicht für pseudonymisierte Daten, die für die Zwecke der Statistik, der wissenschaftlichen Forschung oder der Archivierung im öffentlichen Interesse verarbeitet werden (Artikel 28-7 PIPA, in dem eine Ausnahme von Artikel 34 Absatz 1 und Artikel 39-4 PIPA vorgesehen ist). Die Sicherstellung einer individuellen Benachrichtigung würde bedeuten, dass der Datenverantwortliche Personen aus dem pseudonymisierten Datensatz identifizieren müsste, was nach Artikel 28-5 PIPA ausdrücklich verboten ist. Die allgemeine Anforderung zur Meldung von Verletzungen des Schutzes personenbezogener Daten (an die PIPC) gilt jedoch weiterhin.

([88]) Die Anforderungen bezüglich der Benachrichtigung, einschließlich des Zeitplans und der Möglichkeit einer „stufenweisen" Benachrichtigung, werden in Artikel 40 des PIPA-Durchführungserlasses näher erläutert. Für Informations- und Kommunikationsdiensteanbieter gelten strengere Vorschriften, da sie verpflichtet sind, die betroffene Person und die PIPC innerhalb von 24 Stunden nach Bekanntwerden des Verlusts, des Diebstahls oder der Weitergabe personenbezogener Daten zu benachrichtigen (Artikel 39-4 Absatz 1 PIPA). Diese Benachrichtigung muss Einzelheiten über die personenbezogenen Daten, die weitergegeben wurden, den Zeitpunkt, zu dem dies geschah, die Maßnahmen, die der Nutzer ergreifen kann, die Reaktionsmaßnahmen des Anbieters und die Kontaktdaten der Stelle, an die der Nutzer Fragen richten kann, enthalten (Artikel 39-4 Absatz 1 Nummern 1 bis 5 PIPA). Wenn es einen berechtigten Grund gibt, z. B. weil die Kontaktdaten des Nutzers nicht vorliegen, können andere Mittel der Benachrichtigung verwendet werden, z. B. durch Veröffentlichung der Informationen auf einer Website (Artikel 39-4 Absatz 1 PIPA in Verbindung mit Artikel 48-4 Absatz 4 ff. des PIPA-Durchführungserlasses). In diesem Fall muss die PIPC über die Gründe informiert werden (Artikel 34-4 Absatz 3 PIPA).

([89]) Siehe z. B. die Entscheidungen des Obersten Gerichtshofs vom 26. Dezember 2012, 2011Da59834, 2011Da59858 und 2011Da59841. Eine englische Zusammenfassung ist abrufbar unter: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Dies wird im koreanischen System auf unterschiedliche Weise gewährleistet. Neben dem Auskunftsrecht nach Artikel 4 Nummer 1 (allgemein) und Artikel 20 Absatz 1 PIPA (für die von Dritten erhobenen personenbezogenen Daten) sowie dem Auskunftsrecht gemäß Artikel 35 PIPA besteht eine allgemeine Transparenzanforderung in Bezug auf den Zweck der Verarbeitung (Artikel 3 Absatz 1 PIPA) und spezifische Transparenzanforderungen für den Fall, dass die Verarbeitung auf einer Einwilligung beruht (Artikel 15 Absatz 2, Artikel 17 Absatz 2 und Artikel 18 Absatz 3 PIPA) ([90]). Darüber hinaus sind bestimmte Datenverantwortliche, bei denen die Verarbeitung bestimmte Schwellenwerte überschreitet, ([91]) gemäß Artikel 20 Absatz 2 PIPA verpflichtet, die betroffene Person, deren personenbezogene Daten sie von einem Dritten erhalten haben, über die Informationsquelle, den Zweck der Verarbeitung und das Recht der betroffenen Person, die Aussetzung der Verarbeitung zu verlangen, zu benachrichtigen, es sei denn, eine solche Benachrichtigung erweist sich als unmöglich, weil keine Kontaktdaten vorhanden sind. Ausnahmen gelten für bestimmte Akten mit personenbezogenen Daten im Besitz von Behörden, insbesondere für Akten mit Daten, die für die nationale Sicherheit, andere besonders wichtige („schwerwiegende") nationale Interessen oder für die Zwecke der Strafverfolgung verarbeitet werden, oder wenn die Übermittlung zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde, jedoch nur, wenn die auf dem Spiel stehenden öffentlichen oder privaten Interessen gegenüber den Rechten der betroffenen Personen „ausdrücklich überwiegen" (Artikel 20 Absatz 4 PIPA). Dies erfordert eine Abwägung betroffenen Interessen.

(68) Darüber hinaus ist in Artikel 3 Absatz 5 PIPA festgelegt, dass die Datenverantwortlichen ihre Datenschutzerklärungen (und andere Informationen in Zusammenhang mit der Verarbeitung personenbezogener Daten) veröffentlichen müssen. Diese Anforderung wird in Artikel 30 PIPA in Verbindung mit Artikel 31 des PIPA-Durchführungserlasses näher erläutert. Nach diesen Bestimmungen muss die öffentliche Datenschutzerklärung unter anderem Folgendes enthalten: 1) die Arten der verarbeiteten personenbezogenen Daten, 2) den Zweck der Verarbeitung, 3) die Speicherfrist, 4) die Angabe, ob personenbezogene Daten an Dritte weitergegeben werden, ([92]) 5) etwaige Unterverarbeitungen, 6) Informationen über die Rechte der betroffenen Person und wie sie diese ausüben kann und 7) Kontaktdaten (einschließlich des Namens des Datenschutzbeauftragten oder der internen Abteilung, die für die Einhaltung der Datenschutzvorschriften und die Bearbeitung von Beschwerden zuständig ist). Die Datenschutzerklärung ist in einer für die betroffenen Personen leicht erkennbaren Weise öffentlich zugänglich zu machen (Artikel 30 Absatz 2 PIPA) ([93]) und ständig zu aktualisieren (Artikel 31 Absatz 2 des PIPA-Durchführungserlasses).

(69) Öffentliche Einrichtungen unterliegen einer zusätzlichen Pflicht, insbesondere die folgenden Informationen bei der PIPC zu melden: 1) den Namen der öffentlichen Einrichtung, 2) die Gründe und Zwecke der Verarbeitung der personenbezogenen Daten, 3) die Einzelheiten der gespeicherten personenbezogenen Daten, 4) die Art der Verarbeitung, 5) die Speicherfrist, 6) die Zahl der betroffenen Personen, deren personenbezogene Daten gespeichert werden, 7) die Abteilung, die die Anträge der betroffenen Personen bearbeitet und 8) die Empfänger der personenbezogenen Daten, wenn die Daten routinemäßig oder wiederholt bereitgestellt werden (Artikel 32 Absatz 1 PIPA) ([94]). Die registrierten Akten mit personenbezogenen Daten werden von der PIPC veröffentlicht und müssen auch von öffentlichen Einrichtungen in ihrer Datenschutzerklärungen erwähnt werden (Artikel 30 Absatz 1 und Artikel 32 Absatz 4 PIPA).

(70) Um die Transparenz für betroffene Personen in der Union, deren personenbezogene Daten auf der Grundlage dieses Beschlusses nach Korea übermittelt werden, zu erhöhen, werden in Abschnitt 3 Ziffern i und ii der Bekanntmachung 2021-5 (Anhang I) zusätzliche Transparenzanforderungen festgelegt. Erstens müssen koreanische Datenverantwortliche, die auf der Grundlage dieses Beschlusses personenbezogene Daten aus der Union erhalten, die betroffenen Personen unverzüglich (und in jedem Fall spätestens einen Monat nach der Übermittlung) über den Namen und die Kontaktdaten der übermittelnden und der empfangenden Stelle,

([90]) Insbesondere wenn personenbezogene Daten mit der Einwilligung einer Person verarbeitet werden, muss der Datenverantwortliche die Person über den Zweck der Verarbeitung, Einzelheiten über die zu verarbeitenden Daten, den Empfänger der Daten, den Zeitraum, für den personenbezogene Daten gespeichert und verwendet werden, sowie über die Tatsache informieren, dass die Person berechtigt ist, ihre Einwilligung zu verweigern (und über alle Nachteile, die sich daraus ergeben können).

([91]) Gemäß Artikel 15-2 Absatz 1 des PIPA-Durchführungserlasses betrifft dies Datenverantwortliche, die sensible Daten von mindestens 50 000 betroffenen Personen oder „normale" personenbezogene Daten von mindestens einer Million betroffenen Personen verarbeiten. In Artikel 15-2 Absatz 2 des PIPA-Durchführungserlasses sind die Methoden und der Zeitpunkt der Benachrichtigung festgelegt und in Artikel 15-2 Absatz 3 die Pflicht, bestimmte Aufzeichnungen darüber zu führen. Darüber hinaus gelten besondere Vorschriften für bestimmte Kategorien von Informations- und Kommunikationsdiensteanbieter (solche, die im Vorjahr einen Umsatz von mindestens 10 Milliarden Won erzielt haben, oder solche, die in den drei Monaten vor Ende des Vorjahres im Durchschnitt täglich personenbezogene Daten von mindestens einer Million Nutzern gespeichert oder verwaltet haben), die verpflichtet sind, die Nutzer regelmäßig über die Verwendung ihrer personenbezogenen Daten zu informieren, es sei denn, dies erweist sich aufgrund fehlender Kontaktdaten als unmöglich (Artikel 39-8 PIPA und Artikel 48-6 des PIPA-Durchführungserlasses).

([92]) Gemäß den von der koreanischen Regierung erhaltenen Informationen beinhaltet dies die Pflicht, den/die Empfänger in den öffentlichen Datenschutzerklärungen einzeln aufzuführen.

([93]) Weitere Modalitäten sind in Artikel 31 Absatz 3 des PIPA-Durchführungserlasses festgelegt.

([94]) Die Registrierungspflicht gilt nicht für bestimmte Arten von Akten mit personenbezogenen Daten, z. B. solche, in denen Angelegenheiten im Zusammenhang mit der nationalen Sicherheit, diplomatischen Geheimnissen, strafrechtlichen Ermittlungen, Strafverfolgung, Bestrafung, Ermittlungen von Straftaten im Zusammenhang mit der Besteuerung oder Akten, die sich ausschließlich auf die interne Arbeitsleistung beziehen, gespeichert sind (Artikel 32 Absatz 2 PIPA).

die übermittelten personenbezogenen Daten (oder Kategorien personenbezogener Daten), den Zweck der Erhebung durch den koreanischen Datenverantwortlichen, die Speicherfrist und die nach dem PIPA geltenden Rechte unterrichten. Zweitens müssen die betroffenen Personen bei der Weitergabe von personenbezogenen Daten, die sie auf der Grundlage dieses Beschlusses von der Union erhalten haben, an Dritte unter anderem über den Empfänger, die zu übermittelnden personenbezogenen Daten oder Kategorien personenbezogener Daten, das Land, an das die Daten weitergegeben werden (sofern zutreffend), sowie über die nach dem PIPA geltenden Rechte unterrichtet werden ([95]). Dadurch wird nach der Bekanntmachung sichergestellt, dass EU-Bürger weiterhin über die für die Verarbeitung ihrer Daten Verantwortlichen Bescheid wissen und ihre Rechte gegenüber den betreffenden Stellen ausüben können.

(71) Gemäß Abschnitt 3 Ziffer iii der Bekanntmachung (Anhang I) sind bestimmte begrenzte und qualifizierte Ausnahmen von diesen zusätzlichen Transparenzpflichten zulässig, die im Wesentlichen denjenigen der Verordnung (EU) 2016/679 entsprechen. Insbesondere ist die Unterrichtung der betroffenen Personen in der Union nicht erforderlich, 1) wenn und solange es notwendig ist, die Unterrichtung aus bestimmten Gründen des öffentlichen Interesses zu beschränken (z. B. wenn die Informationen für die Zwecke der nationalen Sicherheit oder für laufende strafrechtliche Ermittlungen verarbeitet werden), sofern diese Ziele des öffentlichen Interesses offensichtlich Vorrang vor den Rechten der betroffenen Person haben, 2) wenn die betroffene Person bereits über die Informationen verfügt, 3) wenn und solange wahrscheinlich ist, dass die Unterrichtung zur Schädigung einer betroffenen Person oder eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde, sofern diese Rechte oder Interessen eindeutig Vorrang vor den Rechten der betroffenen Person haben oder 4) wenn es keine Kontaktdaten der betroffenen Personen gibt oder ein unverhältnismäßiger Aufwand erforderlich wäre, um sie zu unterrichten. Bei der Entscheidung darüber, ob die betroffene Person kontaktiert werden kann oder ob dies einen unverhältnismäßigen Aufwand erfordern würde, ist die Möglichkeit einer Zusammenarbeit mit dem Datenexporteur aus der EU zu berücksichtigen.

(72) Die Vorschriften in den Erwägungsgründen (67)-(71) gewährleisten daher in Bezug auf die Transparenz ein im Wesentlichen gleichwertiges Schutzniveau wie die Bestimmungen der Verordnung (EU) 2016/679.

2.3.8 *Rechte des Einzelnen*

(73) Betroffene Personen sollten bestimmte Rechte besitzen, die gegenüber dem Datenverantwortlichen oder dem Auftragsverarbeiter durchgesetzt werden können, insbesondere ein Auskunftsrecht, das Recht auf Berichtigung, das Recht, der Verarbeitung zu widersprechen, und das Recht auf Löschung von Daten. Gleichzeitig können diese Rechte Beschränkungen unterliegen, sofern diese Beschränkungen notwendig und verhältnismäßig sind, um wichtige Ziele von allgemeinem öffentlichem Interesse zu schützen.

(74) Gemäß Artikel 3 Absatz 5 PIPA muss der Datenverantwortliche die in Artikel 4 PIPA aufgeführten und in den Artikeln 35 bis 37, Artikel 39 und 39-2 PIPA näher beschriebenen Rechte der betroffenen Person gewährleisten.

(75) Erstens hat der Einzelne ein Recht auf Information und Auskunft. Wenn der Datenverantwortliche personenbezogene Daten von einem Dritten erhoben hat – was immer der Fall sein wird, wenn die Daten aus der Union übermittelt werden –, haben die betroffenen Personen im Allgemeinen das Recht, Informationen über 1) die „Quelle" der erhobenen personenbezogenen Daten (d. h. den Übermittler), 2) den Zweck der Verarbeitung und 3) die Tatsache zu erhalten, dass die betroffene Person berechtigt ist, die Aussetzung der Verarbeitung zu verlangen (Artikel 20 Absatz 1 PIPA). Es gelten begrenzte Ausnahmen, nämlich dann, wenn es wahrscheinlich ist, dass eine solche Unterrichtung zur Schädigung eines Dritten an Leib und Leben oder „zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen" eines Dritten führen würde, jedoch nur dann, wenn diese Interessen eines Dritten gegenüber den Rechten der betroffenen Person „ausdrücklich überwiegen" (Artikel 20 Absatz 4 Nummer 2 PIPA).

(76) Darüber hinaus haben die betroffenen Personen gemäß Artikel 35 Absätze 1 und 3 PIPA in Verbindung mit Artikel 41 Absatz 4 des PIPA-Durchführungserlasses das Recht auf Auskunft über ihre personenbezogenen Daten ([96]). Das Auskunftsrecht umfasst die Bestätigung der Verarbeitung, Informationen über die Art der verarbeiteten Daten, den Zweck der Verarbeitung, die Speicherfrist sowie die Weitergabe an Dritte und die Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten (Artikel 4 Nummer 3 PIPA in Verbindung

([95]) Bekanntmachung Nr. 2021-5, Abschnitt 3 Ziffer ii (Anhang I).

([96]) Gemäß Artikel 35 Absatz 3 PIPA in Verbindung mit Artikel 42 Absatz 2 des PIPA-Durchführungserlasses kann der Datenverantwortliche die Auskunft aus „triftigen Gründen" (d. h. aus gerechtfertigten Gründen, z. B. wenn mehr Zeit benötigt wird, um zu prüfen, ob der Zugang gewährt werden kann) verzögern, muss die betroffene Person jedoch innerhalb von 10 Tagen über eine solche Rechtfertigung unterrichten und sie darüber informieren, wie sie gegen diese Entscheidung vorgehen kann; sobald der Grund für die Verzögerung nicht mehr besteht, muss die Auskunft erteilt werden.

mit Artikel 41 Absatz 1 des PIPA-Durchführungserlasses) ([97]). Die Auskunft kann nur dann (in Form einer teilweisen Auskunft) beschränkt ([98]) oder verweigert werden, wenn dies gesetzlich vorgesehen ist, ([99]) wenn dies zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde (Artikel 35 Absatz 4 PIPA) ([100]). Letzteres bedeutet, dass zwischen den verfassungsrechtlich geschützten Rechten und Freiheiten des Einzelnen einerseits und den Rechten und Freiheiten anderer Personen andererseits abgewogen werden muss. Wird die Auskunft eingeschränkt oder verweigert, muss der Datenverantwortliche die betroffene Person über die Gründe hierfür und die Rechtsbehelfsmöglichkeiten gegen die Entscheidung unterrichten (Artikel 41 Absatz 5, Artikel 42 Absatz 2 des PIPA-Durchführungserlasses).

(77) Zweitens haben die betroffenen Personen das Recht auf Berichtigung oder Löschung ([101]) ihrer personenbezogenen Daten, „sofern in anderen Rechtsvorschriften nicht ausdrücklich etwas anderes bestimmt ist“ (Artikel 36 Absätze 1 und 2 PIPA) ([102]). Sobald ein Antrag eingeht, muss der Datenverantwortliche die Angelegenheit unverzüglich prüfen, die erforderlichen Maßnahmen ergreifen ([103]) und die betroffene Person innerhalb von 10 Tagen davon in Kenntnis setzen. Kann dem Antrag nicht stattgegeben werden, so muss diese Unterrichtung die Gründe für die Ablehnung und die Rechtsbehelfsmöglichkeiten enthalten (siehe Artikel 36 Absatz 4 PIPA in Verbindung mit Artikel 43 Absatz 3 des PIPA-Durchführungserlasses) ([104]).

(78) Schließlich haben die betroffenen Personen das Recht auf unverzügliche ([105]) Aussetzung der Verarbeitung ihrer personenbezogenen Daten, sofern nicht eine der aufgezählten Ausnahmen zutrifft (Artikel 37 Absätze 1 und 2 PIPA) ([106]). Der Datenverantwortliche kann den Antrag ablehnen, 1) wenn dies gesetzlich ausdrücklich erlaubt oder zur Erfüllung rechtlicher Pflichten erforderlich („unvermeidlich“) ist, 2) wenn die Aussetzung zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde, 3) wenn eine öffentliche Einrichtung ihre gesetzlich vorgeschriebenen Aufgaben ohne die Verarbeitung der Daten nicht erfüllen kann oder 4) wenn die betroffene Person den zugrunde liegenden Vertrag mit dem Datenverantwortlichen nicht ausdrücklich kündigt, obwohl die Erfüllung des Vertrags ohne eine solche Datenverarbeitung undurchführbar wäre. In diesem Fall muss der Datenverantwortliche die betroffene Person unverzüglich über die Gründe für die Verweigerung und die Rechtsbehelfsmöglichkeiten unterrichten (Artikel 37 Absatz 2 PIPA in Verbindung mit Artikel 44 Absatz 2 des PIPA-Durchführungserlasses). Gemäß Artikel 37 Absatz 4 PIPA hat der Datenverantwortliche bei der Erfüllung des Aussetzungsantrags unverzüglich „die erforderlichen Maßnahmen einschließlich der Vernichtung der betreffenden personenbezogenen Daten“ zu treffen ([107]).

(79) Das Recht auf Aussetzung der Verarbeitung gilt auch, wenn personenbezogene Daten für die Zwecke der Direktwerbung verwendet werden, d. h. um für Waren oder Dienstleistungen zu werben oder zum Kauf

([97]) Die Auskunft über personenbezogene Daten, die von einer öffentlichen Einrichtung verarbeitet werden, kann direkt bei der Einrichtung oder indirekt durch einen Antrag bei der PIPC beantragt werden, die den Antrag unverzüglich weiterleitet (Artikel 35 Absatz 2 PIPA und Artikel 41 Absatz 3 des PIPA-Durchführungserlasses).

([98]) Gemäß Artikel 42 Absatz 1 des PIPA-Durchführungserlasses ist der Datenverantwortliche verpflichtet, eine teilweise Auskunft zu erteilen, wenn zumindest ein Teil der Informationen nicht unter die Verweigerungsgründe fällt.

([99]) In den entsprechenden Rechtsvorschriften müssen wiederum das Grundrecht auf Schutz der Privatsphäre und auf Datenschutz sowie die in der koreanischen Verfassung verankerten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit gewahrt werden.

([100]) Darüber hinaus können öffentliche Einrichtungen die Auskunft verweigern, wenn dies die Erfüllung bestimmter Aufgaben, einschließlich laufender Prüfungen oder der Auferlegung, Erhebung oder Rückzahlung von Steuern, erheblich erschweren würde (Artikel 35 Absatz 4 PIPA).

([101]) In diesem Fall muss der Datenverantwortliche Maßnahmen ergreifen, um die Wiederherstellung der personenbezogenen Daten zu verhindern, siehe Artikel 36 Absatz 3 PIPA.

([102]) Solche Rechtsvorschriften müssen den Anforderungen der Verfassung genügen, wonach ein Grundrecht nur dann beschränkt werden darf, wenn dies für die nationale Sicherheit oder die Aufrechterhaltung der öffentlichen Ordnung zum Wohl der Allgemeinheit erforderlich ist, und nicht den Wesensgehalt der Freiheit oder des Rechts berühren darf (Artikel 37 Absatz 2 der Verfassung).

([103]) In Artikel 43 Absatz 2 des PIPA-Durchführungserlasses ist ein besonderes Verfahren für den Fall vorgesehen, dass der Datenverantwortliche Akten mit personenbezogenen Daten verarbeitet, die von einem anderen Datenverantwortlichen bereitgestellt wurden.

([104]) Das Versäumnis, die erforderlichen Maßnahmen zur Berichtigung oder Löschung personenbezogener Daten zu ergreifen, sowie die fortlaufende Nutzung oder Weitergabe dieser Daten an Dritte kann strafrechtliche Sanktionen nach sich ziehen (Artikel 73 Absatz 2 PIPA).

([105]) Gemäß Artikel 44 Absatz 2 des PIPA-Durchführungserlasses unterrichtet der Datenverantwortliche die betroffene Person innerhalb von 10 Tagen nach Eingang des Antrags darüber, dass er die Verarbeitung ordnungsgemäß ausgesetzt hat.

([106]) In Bezug auf öffentliche Einrichtungen kann das Recht auf Aussetzung der Verarbeitung in Bezug auf Informationen, die in registrierten Akten mit personenbezogenen Daten enthalten sind, ausgeübt werden (Artikel 37 in Verbindung mit Artikel 32 PIPA). Eine solche Registrierung ist in einer begrenzten Anzahl von Situationen nicht erforderlich, z. B. wenn die Akten mit personenbezogenen Daten die nationale Sicherheit, strafrechtliche Ermittlungen, diplomatische Beziehungen usw. betreffen (Artikel 32 Absatz 2 PIPA).

([107]) Die Nichteinhaltung dieser Anforderungen kann strafrechtliche Sanktionen nach sich ziehen (Artikel 73 Absatz 3 PIPA).

dieser anzuregen. Darüber hinaus erfordert eine solche Weiterverarbeitung im Allgemeinen die gesonderte (zusätzliche) Einwilligung der betroffenen Person (siehe Artikel 15 Absatz 1 Nummer 1, Artikel 17 Absatz 2 Nummer 1 PIPA) ([108]). Bei der Einholung dieser Einwilligung muss der Datenverantwortliche die betroffene Person insbesondere über die beabsichtigte Verwendung der Daten für die Zwecke der Direktwerbung – d. h. die Tatsache, dass sie möglicherweise im Rahmen der Werbung oder des Kaufangebots für Waren oder Dienstleistungen kontaktiert wird – in einer „ausdrücklich erkennbaren Weise" unterrichten (Artikel 22 Absätze 2 und 4 PIPA in Verbindung mit Artikel 17 Absatz 2 Nummer 1 des PIPA-Durchführungserlasses).

(80) Um die Ausübung der Rechte des Einzelnen zu erleichtern, muss der Datenverantwortliche spezielle Verfahren einrichten und diese öffentlich zugänglich machen (Artikel 38 Absatz 4 PIPA) ([109]). Dazu gehören auch Verfahren zur Erhebung von Einwänden gegen die Ablehnung eines Antrags (Artikel 38 Absatz 5 PIPA). Der Datenverantwortliche hat sicherzustellen, dass das Verfahren zur Ausübung der Rechte „datenschutzfreundlich" und nicht schwieriger ist als das Verfahren zur Erhebung der personenbezogenen Daten; dies umfasst auch die Pflicht, Informationen über das Verfahren auf seiner Website bereitzustellen (Artikel 41 Absatz 2, Artikel 43 Absatz 1 und Artikel 44 Absatz 1 des PIPA-Durchführungserlasses) ([110]). Einzelpersonen können einen Vertreter bevollmächtigen, einen solchen Antrag zu stellen (Artikel 38 Absatz 1 PIPA in Verbindung mit Artikel 45 des PIPA-Durchführungserlasses). Der Datenverantwortliche ist zwar berechtigt, eine Gebühr zu erheben (und im Falle eines Antrags auf Zusendung von Kopien personenbezogener Daten auch Postgebühren), doch muss der Betrag „im Rahmen der für die Bearbeitung [des Antrags] tatsächlich erforderlichen Kosten" festgelegt werden; falls der Datenverantwortliche den Antrag ausgelöst hat, darf keine Gebühr (auch keine Postgebühr) erhoben werden (Artikel 38 Absatz 3 PIPA in Verbindung mit Artikel 47 des PIPA-Durchführungserlasses).

(81) Das PIPA und der Durchführungserlass enthalten keine allgemeinen Bestimmungen, die sich mit der Problematik von Entscheidungen befassen, die sich auf die betroffene Person auswirken und ausschließlich auf der automatisierten Verarbeitung personenbezogener Daten beruhen. Bei personenbezogenen Daten, die in der Union erhoben wurden, wird jedoch jede Entscheidung, die auf einer automatisierten Verarbeitung beruht, typischerweise vom Verantwortlichen in der Union getroffen (der eine direkte Beziehung zu der betroffenen Person unterhält) und unterliegt somit der Verordnung (EU) 2016/679 ([111]). Dazu gehören auch Übermittlungsszenarien, bei denen die Verarbeitung von einem ausländischen (z. B. koreanischen) Unternehmer vorgenommen wird, der als Beauftragter (Auftragsverarbeiter) im Namen des Verantwortlichen in der EU (oder als Unterauftragsverarbeiter im Namen des Auftragsverarbeiters in der EU, der die Daten von einem Verantwortlichen in der EU erhalten hat, der sie erhoben hat) handelt, der dann auf dieser Grundlage die Entscheidung trifft. Daher ist es unwahrscheinlich, dass das Fehlen besonderer Vorschriften für die automatisierte Entscheidungsfindung im PIPA das Schutzniveau der nach diesem Beschluss übermittelten personenbezogenen Daten beeinträchtigt.

(82) Ausnahmsweise gelten die Bestimmungen über die Transparenz auf Anfrage (Artikel 20) und die Rechte des Einzelnen (Artikel 35 bis 37) sowie die individuelle Unterrichtungspflicht für Informations- und Kommunikationsdiensteanbieter (Artikel 39-8 PIPA) nicht für pseudonymisierte Informationen, wenn diese für die Zwecke der Statistik, der wissenschaftlichen Forschung oder der Archivierung im öffentlichen Interesse verarbeitet werden (Artikel 28-7 PIPA) ([112]). Im Einklang mit dem Ansatz in Artikel 11 Absatz 2 (in Verbindung mit Erwägungsgrund 57) der Verordnung (EU) 2016/679 ist dies dadurch gerechtfertigt, dass der Datenverantwortliche zur Gewährleistung der Transparenz oder zur Gewährung von Rechten des Einzelnen feststellen müsste, ob (und wenn ja, welche) Daten mit der antragstellenden Person in Verbindung stehen, was nach dem PIPA ausdrücklich verboten ist (Artikel 28-5 Absatz 1 PIPA). Besteht eine solche erneute Identifizierung darin, die Pseudonymisierung für den gesamten (pseudonymisierten) Datensatz rückgängig zu machen, so würden die personenbezogenen Daten aller anderen betroffenen Personen einem erhöhten Risiko ausgesetzt werden. Während sich die Verordnung (EU) 2016/679 auf Situationen bezieht, in denen eine erneute Identifizierung praktisch unmöglich ist, wird im PIPA ein strengerer Ansatz verfolgt, indem die erneute Identifizierung in allen Situationen, in denen pseudonymisierte Daten verarbeitet werden, ausdrücklich verboten wird.

(83) Wie in den Erwägungsgründen (74)-(82) beschrieben, sind daher im koreanischen System Vorschriften über die Rechte der betroffenen Person enthalten, die ein Schutzniveau bieten, das im Wesentlichen dem der Verordnung (EU) 2016/679 entspricht.

([108]) Der Schlichtungsausschuss für Streitigkeiten (siehe Erwägungsgrund 133) hat sich mit mehreren Fällen befasst, in denen sich Einzelpersonen über die Verwendung ihrer Daten für die Zwecke der Direktwerbung ohne Einwilligung beschwert haben; in diesen Fällen wurden beispielsweise Entschädigungen gezahlt und personenbezogene Daten durch den Datenverantwortlichen gelöscht (siehe z. B. Schlichtungsausschuss 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)).

([109]) Siehe auch Artikel 30 Absatz 1 Nummer 5 PIPA über die Datenschutzerklärung, die unter anderem Informationen über die dem Einzelnen zur Verfügung stehenden Rechte und deren Ausübung enthalten muss.

([110]) Siehe auch Artikel 39-7 Absatz 2 PIPA in Bezug auf die Informations- und Kommunikationsdiensteanbieter.

([111]) Hingegen wird dies in dem Ausnahmefall, dass der koreanische Unternehmer eine direkte Beziehung zu der betroffenen Person in der EU unterhält, typischerweise darauf zurückzuführen sein, dass er die Person in der Europäischen Union gezielt angesprochen hat, indem er ihr Waren oder Dienstleistungen angeboten oder ihr Verhalten beobachtet hat. In diesem Szenario gilt für den koreanischen Unternehmer selbst die Verordnung (EU) 2016/679 (Artikel 3 Absatz 2), sodass er das EU-Datenschutzrecht unmittelbar einhalten muss.

([112]) Siehe auch die Bekanntmachung 2021-5, in der bestätigt wird, dass Abschnitt III PIPA (einschließlich Artikel 28-7) nur dann gilt, wenn pseudonymisierte Daten für die wissenschaftliche Forschung, für Statistiken oder für die Archivierung im öffentlichen Interesse verarbeitet werden, siehe Anhang I Abschnitt 4 dieses Beschlusses.

2.3.9 *Weiterübermittlungen*

(84) Das Schutzniveau für personenbezogene Daten, die aus der Union an Datenverantwortliche in der Republik Korea übermittelt werden, darf nicht durch die Weiterübermittlung dieser Daten an Empfänger in einem Drittland beeinträchtigt werden.

(85) Solche „Weiterübermittlungen" stellen aus Sicht des koreanischen Datenverantwortlichen internationale Übermittlungen aus der Republik Korea dar. In dieser Hinsicht unterscheidet das PIPA zwischen der Auslagerung der Verarbeitung an einen Beauftragten (d. h. einen Auftragsverarbeiter) und der Übermittlung personenbezogener Daten an Dritte ([113]).

(86) Erstens muss der koreanische Datenverantwortliche bei der Auslagerung der Verarbeitung personenbezogener Daten an eine in einem Drittland ansässige Stelle die Einhaltung der Bestimmungen des PIPA über die Auslagerung sicherstellen (Artikel 26 PIPA). Dies umfasst die Einführung eines rechtsverbindlichen Instruments, mit dem unter anderem die Verarbeitung durch den Beauftragten auf den Zweck der ausgelagerten Arbeit beschränkt, technische und organisatorische Garantien vorgeschrieben und die Unterverarbeitung eingeschränkt werden (siehe Artikel 26 Absatz 1 PIPA), sowie die Veröffentlichung von Informationen über die ausgelagerte Arbeit. Darüber hinaus ist der Datenverantwortliche verpflichtet, den Beauftragten über die erforderlichen Sicherheitsvorkehrungen „aufzuklären" und zu überwachen, auch durch Kontrollen, ob er alle Pflichten des Datenverantwortlichen im Rahmen des PIPA ([114]) und des Auslagerungsvertrags einhält.

(87) Verursacht der Beauftragte durch eine gegen das PIPA verstoßende Verarbeitung personenbezogener Daten einen Schaden, so haftet dafür der Datenverantwortliche, wie dies auch bei den Mitarbeitern des Datenverantwortlichen der Fall wäre (Artikel 26 Absatz 6 PIPA). Der koreanische Datenverantwortliche bleibt daher für die ausgelagerten personenbezogenen Daten verantwortlich und muss sicherstellen, dass der ausländische Beauftragte die Daten in Übereinstimmung mit dem PIPA verarbeitet. Verstößt der Beauftragte bei der Verarbeitung der Daten gegen das PIPA, kann der koreanische Datenverantwortliche dafür haftbar gemacht werden, dass er seiner Pflicht, die Einhaltung des PIPA zu gewährleisten, nicht nachgekommen ist, z. B. durch seine Aufsicht über den Beauftragten. Die in den Auslagerungsvertrag aufgenommenen Garantien und die Verantwortung des koreanischen Datenverantwortlichen für die Handlungen des Beauftragten gewährleisten die Kontinuität des Schutzes, wenn die Verarbeitung personenbezogener Daten an eine Stelle außerhalb Koreas ausgelagert wird.

(88) Zweitens können koreanische Datenverantwortliche personenbezogene Daten an Dritte mit Sitz außerhalb Koreas weitergeben. Das PIPA enthält zwar eine Reihe von Rechtsgrundlagen, die eine Übermittlung an Dritte im Allgemeinen zulassen, doch wenn der Dritte außerhalb Koreas ansässig ist, muss der Datenverantwortliche grundsätzlich ([115]) die Einwilligung der betroffenen Person einholen, ([116]) nachdem er sie über 1) die Art der personenbezogenen Daten, 2) den Empfänger der personenbezogenen Daten, 3) den Zweck der Übermittlung im Sinne des vom Empfänger verfolgten Zwecks der Verarbeitung, 4) die Speicherfrist für die Verarbeitung durch den Empfänger sowie 5) die Tatsache, dass die betroffene Person ihre Einwilligung verweigern kann, unterrichtet hat (Artikel 17 Absätze 2 und 3 PIPA). Gemäß dem Abschnitt über die Transparenz in der Bekanntmachung 2021-5 (siehe Erwägungsgrund (70)) müssen die betroffenen Personen über das Drittland, an das ihre Daten übermittelt werden sollen, unterrichtet werden. Damit wird sichergestellt, dass die betroffenen Personen in der Union in voller Kenntnis der Sachlage entscheiden können, ob sie einer Übermittlung ins Ausland zustimmen oder nicht. Außerdem darf der Datenverantwortliche keinen Vertrag mit dem Drittempfänger abschließen, der gegen das PIPA verstößt, d. h. der Vertrag darf keine Pflichten enthalten, die den Anforderungen des PIPA an den Datenverantwortlichen widersprechen würden ([117]).

([113]) Für Informations- und Kommunikationsdiensteanbieter gelten besondere Vorschriften. Gemäß Artikel 39-12 PIPA müssen die Informations- und Kommunikationsdiensteanbieter die Einwilligung des Nutzers grundsätzlich für jede Übermittlung von personenbezogenen Daten ins Ausland einholen. Werden personenbezogene Daten im Rahmen der Auslagerung von Verarbeitungsvorgängen, einschließlich der Speicherung, übermittelt, ist eine Einwilligung nicht erforderlich, wenn die betroffenen Personen zuvor direkt oder durch öffentliche Bekanntmachung in einer Weise, die einen leichten Auskunft ermöglicht, über 1) die Einzelheiten der zu übermittelnden Daten, 2) das Land, in das die Daten übermittelt werden (sowie Datum und Methode der Übermittlung), 3) den Namen des Empfängers und 4) den Zweck der Verwendung und Aufbewahrung durch den Empfänger informiert wurden (Artikel 39-12 Absatz 3 PIPA). Darüber hinaus gelten in diesem Fall die allgemeinen Anforderungen für die Auslagerung. Für jede Übermittlung müssen besondere Sicherheitsvorkehrungen, die Bearbeitung von Beschwerden und Streitigkeiten sowie andere Maßnahmen zum Schutz der Nutzerdaten getroffen werden (Artikel 48-10 des PIPA-Durchführungserlasses).

([114]) Siehe auch Artikel 26 Absatz 7 PIPA, wonach die Artikel 15 bis 25, 27 bis 31, 33 bis 38 und 50 entsprechend für den Auftragsverarbeiter gelten.

([115]) Werden personenbezogene Daten von Nutzern durch Informations- und Kommunikationsdiensteanbieter an Dritte übermittelt, so bedarf dies stets der Einwilligung des Nutzers (Artikel 39-12 Absatz 2 PIPA).

([116]) Wie in Fußnote 51 näher erläutert wird, ist eine solche Einwilligung nur dann gültig, wenn sie freiwillig, in Kenntnis der Sachlage und für den bestimmten Fall erteilt wird.

([117]) Siehe auch Artikel 39-12 Absatz 1 PIPA in Bezug auf die Informations- und Kommunikationsdiensteanbieter.

(89) Personenbezogene Daten können ohne Einwilligung der betroffenen Person an Dritte (im Ausland) weitergegeben werden, wenn der Zweck der Weitergabe „in einem angemessenen Zusammenhang" mit dem ursprünglichen Zweck der Erhebung steht (Artikel 17 Absatz 4 PIPA, siehe Erwägungsgrund (36)). Bei der Entscheidung, ob personenbezogene Daten für einen „verbundenen" Zweck weitergegeben werden sollen, muss der Datenverantwortliche jedoch berücksichtigen, ob die Weitergabe Nachteile für den Einzelnen mit sich bringt und ob die erforderlichen Sicherheitsvorkehrungen (z. B. Verschlüsselung) ergriffen worden sind. In Anbetracht der Tatsache, dass das Drittland, in das personenbezogene Daten übermittelt werden, möglicherweise keinen ähnlichen Schutz bietet wie das PIPA, wird in Abschnitt 2 der Bekanntmachung 2021-5 anerkannt, dass derartige Nachteile entstehen und nur vermieden werden können, wenn der koreanische Datenverantwortliche und der im Ausland ansässige Empfänger durch ein rechtsverbindliches Instrument (z. B. einen Vertrag) ein Schutzniveau sicherstellen, das dem durch das PIPA gewährleisteten Schutzniveau – auch in Bezug auf die Rechte der betroffenen Personen – gleichwertig ist.

(90) Besondere Regeln gelten für die „zweckentfremdete" Weitergabe, d. h. die Weitergabe von Daten an einen Dritten für einen neuen (nicht zusammenhängenden) Zweck, die nur aus einem der in Artikel 18 Absatz 2 PIPA genannten Gründe erfolgen darf (vgl. Erwägungsgrund (39)). Aber auch unter diesen Bedingungen ist die Weitergabe an Dritte ausgeschlossen, wenn sie zur „unfairer Beeinträchtigung" der Interessen der betroffenen Person oder eines Dritten führen könnte; dies erfordert einer Interessenabwägung. Darüber hinaus muss der Datenverantwortliche gemäß Artikel 18 Absatz 5 PIPA zusätzliche Garantien anwenden, wie die Aufforderung an den Dritten, den Zweck und die Methode der Verarbeitung einzuschränken oder besondere Sicherheitsvorkehrungen zu ergreifen. In Anbetracht der Tatsache, dass das Drittland, in das personenbezogene Daten übermittelt werden, möglicherweise keinen ähnlichen Schutz bietet wie das PIPA, wird in Abschnitt 2 der Bekanntmachung 2021-5 anerkannt, dass eine solche „unfaire Beeinträchtigung" der Interessen des betroffenen Person oder eines Dritten nur dann vermieden werden kann, wenn der koreanische Datenverantwortliche und der Empfänger im Ausland durch ein rechtsverbindliches Instrument (z. B. einen Vertrag) ein dem PIPA gleichwertiges Schutzniveau gewährleisten, auch in Bezug auf die Rechte der betroffenen Person.

(91) Durch die Vorschriften in den Erwägungsgründen (86)-(90) wird daher die Kontinuität des Schutzes bei der Weiterübermittlung personenbezogener Daten (an einen „Beauftragten" oder einen Dritten) aus der Republik Korea in einer Weise gewährleistet, die im Wesentlichen den Bestimmungen der Verordnung (EU) 2016/679 entspricht.

2.3.10 *Rechenschaftspflicht*

(92) Nach dem Grundsatz der Rechenschaftspflicht müssen Daten verarbeitende Unternehmen geeignete technische und organisatorische Maßnahmen treffen, um ihren Datenschutzpflichten wirksam nachzukommen und dies, insbesondere gegenüber der zuständigen Aufsichtsbehörde, nachweisen zu können.

(93) Gemäß Artikel 3 Absätze 6 und 8 PIPA hat der Datenverantwortliche personenbezogene Daten so zu verarbeiten, dass die Möglichkeit einer Verletzung der Privatsphäre der betroffenen Person „so gering wie möglich gehalten wird", und er hat das Vertrauen der betroffenen Person zu gewinnen, indem er die im PIPA und anderen damit zusammenhängenden Gesetzen vorgesehenen Pflichten und Verantwortlichkeiten beachtet und erfüllt. Dazu gehört die Erstellung eines internen Verwaltungsplans (Artikel 29 PIPA) sowie eine angemessene Schulung und Aufsicht des Personals (Artikel 28 PIPA).

(94) Um die Rechenschaftspflicht zu gewährleisten, werden die Datenverantwortlichen durch Artikel 31 PIPA in Verbindung mit Artikel 32 des PIPA-Durchführungserlasses verpflichtet, einen Datenschutzbeauftragten zu benennen, der „umfassend für die Verarbeitung personenbezogener Daten verantwortlich ist". Der Datenschutzbeauftragte hat insbesondere folgende Aufgaben zu erfüllen: 1) Erstellung und Durchführung eines Plans zum Schutz personenbezogener Daten und Ausarbeitung der Datenschutzerklärung, 2) regelmäßige Erhebungen über den Stand und die Praxis der Verarbeitung personenbezogener Daten, um etwaige Mängel zu beheben, 3) Bearbeitung von Beschwerden und Abhilfemaßnahmen, 4) Einrichtung eines internen Kontrollsystems, um die Offenlegung, den Missbrauch oder die missbräuchliche Verwendung personenbezogener Daten zu verhindern, 5) Ausarbeitung und Durchführung eines Schulungsprogramms, 6) Schutz, Kontrolle und Verwaltung von Akten mit personenbezogenen Daten und 7) Vernichtung personenbezogener Daten, sobald der Zweck der Verarbeitung erreicht ist oder die Speicherfrist abgelaufen ist. Bei der Erfüllung dieser Aufgaben kann der Datenschutzbeauftragte den Stand der Verarbeitung personenbezogener Daten und die damit verbundenen Systeme überprüfen und Informationen darüber anfordern (Artikel 31 Absatz 3 PIPA). Erhält der Datenschutzbeauftragte Kenntnis von einem Verstoß gegen das PIPA oder andere einschlägige Datenschutzvorschriften, so ergreift er unverzüglich Abhilfemaßnahmen und meldet diese der Geschäftsleitung (im Folgenden „Leiter") des Datenverantwortlichen, falls erforderlich (Artikel 31 Absatz 4 PIPA). Nach Artikel 31 Absatz 5 PIPA dürfen dem Datenschutzbeauftragten bei der Ausübung dieser Aufgaben keine ungerechtfertigten Nachteile entstehen.

(95) Darüber hinaus müssen sich die Datenverantwortlichen proaktiv um die Durchführung einer Abschätzung der Folgen für die Privatsphäre bemühen, wenn die Verwaltung von Akten mit personenbezogenen Daten ein Risiko für die Privatsphäre mit sich bringt (Artikel 33 Absatz 8 PIPA). Auf der Grundlage von Artikel 33 Absätze 1 und 2 PIPA in Verbindung mit den Artikeln 35, 36 und 38 des PIPA-Durchführungserlasses sind Faktoren wie die Art und der Charakter der verarbeiteten Daten (insbesondere, ob es sich um sensible Informationen handelt), ihr Umfang, die Speicherfrist und die Wahrscheinlichkeit von Verletzungen des Schutzes personenbezogener Daten für die Bewertung des Risikos für die Rechte der betroffenen Personen von Bedeutung. Mit der Abschätzung der Folgen für die Privatsphäre soll sichergestellt werden, dass die Risikofaktoren für den Schutz der Privatsphäre sowie etwaige Sicherheits- oder sonstige Gegenmaßnahmen analysiert und verbesserungsbedürftige Aspekte aufgezeigt werden (siehe Artikel 33 Absatz 1 PIPA in Verbindung mit Artikel 38 des PIPA-Durchführungserlasses).

(96) Öffentliche Einrichtungen sind verpflichtet, eine Abschätzung der Folgen der Verarbeitung von bestimmten personenbezogenen Daten durchzuführen, die ein höheres Risiko für mögliche Verletzungen der Privatsphäre mit sich bringt (Artikel 33 Absatz 1 PIPA). Gemäß Artikel 35 des PIPA-Durchführungserlasses gilt dies unter anderem für Akten, die sensible Daten über mindestens 50 000 betroffene Personen enthalten, für Akten, die mit anderen Akten abgeglichen werden und infolgedessen Daten über mindestens 500 000 betroffene Personen enthalten, oder für Akten, die Daten über mindestens eine Million betroffene Personen enthalten. Das Ergebnis einer von einer öffentlichen Einrichtung durchgeführten Folgenabschätzung muss der PIPC mitgeteilt werden (Artikel 33 Absatz 1 PIPA), die eine Stellungnahme abgeben kann (Artikel 33 Absatz 3 PIPA).

(97) Schließlich heißt es in Artikel 13 PIPA, dass die PIPC die erforderlichen Maßnahmen zur Förderung und Unterstützung von „selbstregulierenden Datenschutzmaßnahmen" der Datenverantwortlichen ergreift, u. a. durch Schulungen zum Datenschutz, die Förderung und Unterstützung von Organisationen, die sich mit dem Datenschutz befassen, und durch Unterstützung der Datenverantwortlichen bei der Erarbeitung und Durchführung von Selbstregulierungsvorschriften. Darüber hinaus soll sie das ePRIVACY-Mark-System einführen und erleichtern. In diesem Zusammenhang ist in Artikel 32-2 PIPA in Verbindung mit den Artikeln 34-2 bis 34-8 des PIPA-Durchführungserlasses die Möglichkeit vorgesehen, zu bescheinigen, dass das/die System(e) eines Datenverantwortlichen für die Verarbeitung personenbezogener Daten und für den Schutz dieser Daten den Anforderungen des PIPA entsprechen. Nach diesen Vorschriften kann eine Zertifizierung ([118]) (für einen Zeitraum von drei Jahren) erteilt werden, wenn der Datenverantwortliche die von der PIPC festgelegten Kriterien für die Zertifizierung erfüllt, darunter die Einrichtung von organisatorischen, technischen und physischen Sicherheitsvorkehrungen zum Schutz personenbezogener Daten ([119]). Die PIPC muss die für die Zertifizierung relevanten Systeme des Datenverantwortlichen mindestens einmal pro Jahr überprüfen, um die Wirksamkeit der Zertifizierung aufrechtzuerhalten, wobei dies zum Widerruf der Zertifizierung führen kann (Artikel 32 Absatz 4 PIPA in Verbindung mit Artikel 34-5 des PIPA-Durchführungserlasses, „Follow-up-Management").

(98) Im koreanischen Rechtsrahmen wird daher der Grundsatz der Rechenschaftspflicht in einer Weise umgesetzt, die ein Schutzniveau gewährleistet, das im Wesentlichen dem der Verordnung (EU) 2016/679 entspricht, indem unter anderem verschiedene Mechanismen vorgesehen sind, um die Einhaltung des PIPA zu gewährleisten und nachzuweisen.

2.3.11 *Besondere Vorschriften für die Verarbeitung personenbezogener Kreditdaten*

(99) Wie in Erwägungsgrund (13) beschrieben, werden im Kreditdatengesetz besondere Vorschriften für die Verarbeitung personenbezogener Kreditdaten durch Wirtschaftsbeteiligte festgelegt. Bei der Verarbeitung personenbezogener Kreditdaten müssen die Wirtschaftsbeteiligten daher die allgemeinen Anforderungen des PIPA einhalten, es sei denn, das Kreditdatengesetz enthält spezifischere Vorschriften. Dies trifft z. B. zu, wenn sie im Rahmen eines Geschäftsvorgangs mit einer Person Daten zu einer Kreditkarte oder einem Bankkonto verarbeiten. Als sektorale Rechtsvorschrift für die Verarbeitung von (personenbezogenen und nicht personenbezogenen) Kreditdaten beinhaltet das Kreditdatengesetz nicht nur spezifische Datenschutzgarantien (z. B. in Bezug auf Transparenz und Sicherheit), sondern regelt auch ganz allgemein die besonderen Umstände, unter denen personenbezogene Kreditdaten verarbeitet werden dürfen. Dies spiegelt sich insbesondere in den detaillierten Anforderungen für die Verwendung, die Übermittlung von Daten an Dritte und die Speicherung dieser Daten wider.

(100) Wie das PIPA beruht auch das Kreditdatengesetz auf dem Grundsatz der Rechtmäßigkeit und Verhältnismäßigkeit. Erstens ist nach Artikel 15 Absatz 1 des Kreditdatengesetzes die Erhebung personenbezogener Kreditdaten im Einklang mit Artikel 3 Absätze 1 und 2 PIPA nur mit angemessenen und fairen Mitteln und in dem geringstmöglichen Umfang zulässig, der für einen bestimmten Zweck erforderlich ist. Zweitens wird im Kreditdatengesetz speziell die Rechtmäßigkeit der Verarbeitung personenbezogener Kreditdaten geregelt, indem ihre Erhebung, Verwendung und Übermittlung an Dritte eingeschränkt wird und diese Verarbeitungstätigkeiten generell von der Einwilligung der betroffenen Person abhängig gemacht werden.

([118]) Beabsichtigt der Datenverantwortliche, im Rahmen seiner Geschäftstätigkeit auf die Zertifizierung hinzuweisen oder für sie zu werben, kann er außerdem das von der PIPC geschaffene Zeichen für den Schutz personenbezogener Daten verwenden. Siehe Artikel 34-7 des PIPA-Durchführungserlasses.

([119]) Seit November 2018 wurde das „Personal Information & Information Security Management System" (ISMS-P) entwickelt, mit dem zertifiziert wird, dass die Datenverantwortlichen ein umfassendes Management-System betreiben.

(101) Persönliche Kreditdaten können auf der Grundlage eines der im PIPA vorgesehenen Gründe oder auf der Grundlage spezifischer, im Kreditdatengesetz festgelegter Gründe erhoben werden. Da in Artikel 45 der Verordnung (EU) 2016/679 eine Übermittlung personenbezogener Daten durch einen Verantwortlichen oder einen Auftragsverarbeiter in der Union vorausgesetzt wird, die direkte Erhebung (z. B. bei der Person oder auf einer Website) durch einen Datenverantwortlichen in Korea jedoch nicht erfasst wird, sind für diesen Beschluss nur die Einwilligung und die nach dem PIPA verfügbaren Gründe relevant. Zu diesen Gründen gehören insbesondere Fälle, in denen die Übermittlung zur Erfüllung eines Vertrags mit der betreffenden Person oder zur Wahrung der berechtigten Interessen des koreanischen Datenverantwortlichen erforderlich ist (Artikel 15 Absatz 1 Nummern 4 und 6 PIPA) ([120]).

(102) Einmal erhobene persönliche Kreditdaten können folgendermaßen verwendet werden: 1) für den ursprünglichen Zweck, für den sie durch die Person (direkt) bereitgestellt wurden, ([121]) 2) für einen Zweck, der mit dem ursprünglichen Zweck der Erhebung vereinbar ist, ([122]) 3) um zu entscheiden, ob eine von der Person gewünschte Geschäftsbeziehung aufgenommen oder aufrechterhalten werden soll, ([123]) 4) für die Zwecke der Statistik, der Forschung und der Archivierung im öffentlichen Interesse, ([124]) wenn die Informationen pseudonymisiert sind ([125]), 5) wenn eine weitere Einwilligung eingeholt wird oder 6) in Übereinstimmung mit dem Gesetz.

(103) Beabsichtigt ein Wirtschaftsbeteiligter, personenbezogene Kreditdaten an einen Dritten weiterzugeben, muss er die Einwilligung der betroffenen Person einholen, ([126]) nachdem er sie über den Empfänger der Daten, den Zweck der Verarbeitung durch den Empfänger, die Einzelheiten der zu übermittelnden Daten, die Speicherfrist durch den Empfänger und das Recht, die Einwilligung zu verweigern, unterrichtet hat (Artikel 32 Absatz 1 des Kreditdatengesetzes und Artikel 28 Absatz 2 des Durchführungserlasses zum Kreditdatengesetz) ([127]). Diese Anforderung an die Einwilligung gilt nicht in bestimmten Situationen, nämlich wenn personenbezogene Kreditdaten weitergegeben werden: ([128]) 1) an einen Beauftragten zum Zwecke der Auslagerung, ([129]) 2) an einen Dritten im Falle einer Unternehmensübertragung, -spaltung oder -fusion, 3) für die Zwecke der Statistik, der Forschung und der Archivierung im öffentlichen Interesse, wenn die Daten pseudonymisiert sind, 4) für einen Zweck, der mit dem ursprünglichen Zweck der Erhebung vereinbar ist, 5) an einen Dritten, der die Daten verwendet, um eine Forderung gegen die betroffene Person einzutreiben, ([130]) 6) zur Befolgung eines gerichtlichen Beschlusses, 7) an

([120]) Das Kreditdatengesetz enthält auch andere Rechtsgrundlagen für die Erhebung, z. B. wenn dies gesetzlich vorgeschrieben ist, wenn die Daten von einer öffentlichen Einrichtung gemäß den Rechtsvorschriften über die Informationsfreiheit veröffentlicht werden oder wenn die Daten in einem sozialen Netzwerk verfügbar sind. Damit sich der Wirtschaftsbeteiligte auf den letzten Grund berufen kann, muss er nachweisen können, dass sich die Erhebung im Rahmen der Einwilligung der betroffenen Person hält, und zwar auf der Grundlage einer angemessenen („objektiven“) Auslegung und unter Berücksichtigung der Art der Daten, der Absicht und des Zwecks der Veröffentlichung in dem sozialen Netzwerk, der Frage, ob der Zweck der Erhebung für diesen Zweck „äußerst relevant“ ist, usw. (Artikel 13 des Durchführungserlasses zum Kreditdatengesetz). Wie in Erwägungsgrund (101) erläutert, sind diese Gründe jedoch im Falle einer Übermittlung im Prinzip nicht relevant.

([121]) Beispielsweise, wenn Kreditdaten im Rahmen eines Geschäftsvorgangs mit der betreffenden Person erstellt/zur Verfügung gestellt werden. Dieser Grund kann jedoch nicht geltend gemacht werden, um personenbezogene Kreditdaten für Direktwerbung zu verwenden (siehe Artikel 33 Absatz 1 Nummer 3 des Kreditdatengesetzes).

([122]) Zur Feststellung, ob der Verwendungszweck mit dem ursprünglichen Erhebungszweck vereinbar ist, müssen die folgenden Faktoren berücksichtigt werden: 1) die Beziehung („Relevanz“) zwischen den beiden Zwecken, 2) die Art und Weise, in der die Daten erhoben wurden, 3) die Auswirkungen der Verwendung auf die Person und 4) die Anwendung geeigneter Sicherheitsvorkehrungen wie Pseudonymisierung (vgl. Artikel 32 Absatz 6 Nummer 9-4 des Kreditdatengesetzes).

([123]) So müsste ein Datenverantwortlicher beispielsweise persönliche Kreditdaten, die er von einer Person erhalten hat, bei der Entscheidung, ob er die Laufzeit eines Kredits an diese Person verlängert, berücksichtigen.

([124]) Artikel 33 des Kreditdatengesetzes in Verbindung mit Artikel 32 Absatz 6 Nummern 9-2, 9-4 und 10 des Kreditdatengesetzes.

([125]) Pseudonymisierung wird in Artikel 2 Absatz 15 des Kreditdatengesetzes als Verarbeitung personenbezogener Kreditdaten definiert, welche auf eine Weise erfolgt, durch die sichergestellt wird, dass Einzelpersonen anhand der Daten – außer in Verbindung mit zusätzlichen Informationen – nicht mehr identifiziert werden können. Obwohl das Kreditdatengesetz besondere Garantien für die Verarbeitung pseudonymisierter Daten zu Zwecken der Statistik, Forschung und Archivierung im öffentlichen Interesse enthält (Artikel 40-2 des Kreditdatengesetzes), gelten diese Vorschriften nicht für Handelsorganisationen. Letztere unterliegen stattdessen weiterhin den besonderen Anforderungen von Abschnitt III PIPA, wie in den Erwägungsgründen (42)-(48) erläutert. Gemäß Artikel 40-3 des Kreditdatengesetzes ist die Verarbeitung pseudonymisierter Kreditdaten – sofern sie für die Zwecke der Statistik, der wissenschaftlichen Forschung oder der Archivierung im öffentlichen Interesse erfolgt – von den Anforderungen an die Transparenz und die Rechte des Einzelnen ausgenommen, ähnlich wie bei der Ausnahme in Artikel 28-7 PIPA und vorbehaltlich der Garantien in Abschnitt III PIPA, die in den Erwägungsgründen (42)-(48) ausführlicher beschrieben wurden.

([126]) Dies gilt nicht, wenn die Daten an einen Dritten weitergegeben werden, um personenbezogene Kreditdaten richtig und auf dem neuesten Stand zu halten, solange die Weitergabe im Rahmen des ursprünglichen Zwecks der Verarbeitung bleibt (Artikel 32 Absatz 1 des Kreditdatengesetzes). Dies kann beispielsweise der Fall sein, wenn einer Rating-Agentur aktuelle Daten zur Verfügung gestellt werden, um die Richtigkeit ihrer Aufzeichnungen zu gewährleisten.

([127]) Wenn es nicht möglich ist, die genannten Informationen zur Verfügung zu stellen, genügt es unter Umständen, die betroffene Person an den Drittempfänger zu verweisen, damit diese die erforderlichen Auskünfte erhält.

([128]) Da die Weitergabe personenbezogener Kreditdaten ins Ausland im Rahmen des Kreditdatengesetzes nicht ausdrücklich geregelt ist, müssen solche Weitergaben den in Abschnitt 2 der Bekanntmachung Nr. 2021-5 vorgeschriebenen Garantien für die Weitergabe entsprechen.

([129]) Die Auslagerung der Verarbeitung personenbezogener Kreditdaten darf nur auf der Grundlage eines schriftlichen Vertrags und im Einklang mit den Anforderungen von Artikel 26 Absätze 1 bis 3 und 5 PIPA erfolgen, wie in Erwägungsgrund (20)beschrieben (Artikel 17 des Kreditdatengesetzes und Artikel 14 des Durchführungserlasses zum Kreditdatengesetz). Der Beauftragte darf die Daten nicht über den Rahmen der ausgelagerten Aufgaben hinaus verwenden, und das auslagernde Unternehmen muss besondere Sicherheitsanforderungen (z. B. Verschlüsselung) einführen und den Beauftragten darüber aufklären, wie er verhindern kann, dass die Kreditdaten verloren gehen bzw. gestohlen, weitergegeben, verändert oder gefährdet werden.

([130]) Siehe auch Artikel 28 Absatz 10 Nummern 1, 2 und 6 des Durchführungserlasses zum Kreditdatengesetz.

einen Staatsanwalt oder einen Polizeibeamten in einer Notsituation, in der eine Gefahr für Leib und/oder Leben der Person besteht und keine Zeit für den Erlass einer richterlichen Anordnung vorhanden ist, ([131]) 8) an die zuständigen Steuerbehörden zwecks Einhaltung der Steuervorschriften oder 9) in Übereinstimmung mit anderen Gesetzen. Im Falle einer Weitergabe aus einem dieser Gründe muss die betroffene Person im Voraus darüber unterrichtet werden (Artikel 32 Absatz 7 des Kreditdatengesetzes).

(104) Ferner wird im Kreditdatengesetz die Dauer der Verarbeitung personenbezogener Kreditdaten auf der Grundlage eines der genannten Gründe zur Verwendung oder Weitergabe an Dritte nach Beendigung der Geschäftsbeziehung mit der betreffenden Person ausdrücklich geregelt ([132]). Es dürfen lediglich Daten gespeichert werden, die für den Aufbau oder die Aufrechterhaltung der Geschäftsbeziehung erforderlich sind, wobei zusätzliche Sicherheitsvorkehrungen ergriffen werden müssen (sie sind getrennt von Kreditdaten von Personen, die in einer laufenden Geschäftsbeziehung stehen, zu speichern, durch besondere Sicherheitsvorkehrungen zu schützen und nur für befugte Personen zugänglich zu machen) ([133]). Alle anderen Daten sind zu löschen (Artikel 17-2 Absatz 1 Nummer 2 des Durchführungserlasses zum Kreditdatengesetz). Um festzustellen, welche Daten für die Geschäftsbeziehung erforderlich waren, müssen verschiedene Faktoren berücksichtigt werden, darunter die Frage, ob es möglich gewesen wäre, die Beziehung ohne die Daten herzustellen, und ob sie sich unmittelbar auf die Waren oder Dienstleistungen beziehen, die der Person zur Verfügung gestellt wurden (Artikel 17-2 Absatz 2 des Durchführungserlasses zum Kreditdatengesetz).

(105) Selbst in Fällen, in denen personenbezogene Kreditdaten grundsätzlich über das Ende der Geschäftsbeziehung hinaus gespeichert werden dürfen, müssen sie innerhalb von drei Monaten, nachdem der weitere Zweck der Verarbeitung erreicht wurde, ([134]) oder auf jeden Fall nach fünf Jahren gelöscht werden (Artikel 20-2 des Kreditdatengesetzes). Unter bestimmten Umständen können personenbezogene Kreditdaten länger als fünf Jahre gespeichert werden, insbesondere wenn dies erforderlich ist, um einer gesetzlichen Pflicht nachzukommen, wenn dies für die grundlegenden Interessen in Bezug auf das Leben, den Körper oder das Eigentum einer Person erforderlich ist, für die Archivierung von pseudonymisierten Daten (die für die Zwecke der wissenschaftlichen Forschung, der Statistik oder der Archivierung im öffentlichen Interesse verwendet wurden) oder für Versicherungszwecke (insbesondere für Versicherungsleistungen oder zur Verhinderung eines Versicherungsbetruges) ([135]). In diesen Ausnahmefällen gelten besondere Sicherheitsvorkehrungen (z. B. Unterrichtung der betroffenen Person über die Weiterverwendung, Trennung der aufbewahrten Daten von den Daten, die sich auf Personen beziehen, zu denen noch eine Geschäftsbeziehung besteht, Einschränkung der Auskunftsrechte, siehe Artikel 17-2 Absätze 1 und 2 des Durchführungserlasses zum Kreditdatengesetz).

(106) Im Kreditdatengesetz werden auch die Grundsätze der Richtigkeit und der Datenqualität weiter präzisiert, indem vorgeschrieben wird, dass personenbezogene Kreditdaten „registriert, geändert und verwaltet“ werden, um sie richtig und auf dem neuesten Stand zu halten (Artikel 18 Absatz 1 des Kreditdatengesetzes und Artikel 15 Absatz 3 des Durchführungserlasses zum Kreditdatengesetz) ([136]). Bei der Übermittlung von Kreditdaten an bestimmte andere Stellen (z. B. Rating-Agenturen) sind die Wirtschaftsbeteiligten außerdem ausdrücklich verpflichtet, die Richtigkeit der Daten zu überprüfen, um sicherzustellen, dass nur korrekte Daten vom Empfänger registriert und verwaltet werden (Artikel 15 Absatz 1 des Durchführungserlasses zum Kreditdatengesetz in Verbindung mit Artikel 18 Absatz 1 des Kreditdatengesetzes). Im Allgemeinen sind nach dem Kreditdatengesetz Aufzeichnungen über die Erhebung, Verwendung, Weitergabe an Dritte und Vernichtung personenbezogener Kreditdaten zu führen (Artikel 20 Absatz 2 des Kreditdatengesetzes) ([137]).

(107) Darüber hinaus unterliegt die Verarbeitung personenbezogener Kreditdaten besonderen Anforderungen in Bezug auf die Datensicherheit. So müssen nach dem Kreditdatengesetz technische, physische und organisatorische Maßnahmen ergriffen werden, um den unrechtmäßigen Zugang zu Computersystemen sowie die Veränderung, Zerstörung oder sonstige Gefährdung der verarbeiteten Daten zu verhindern (z. B. durch Zugangskontrollen, siehe Artikel 19 des Kreditdatengesetzes und Artikel 16 des Durchführungserlasses zum Kreditdatengesetz). Darüber hinaus muss beim Austausch personenbezogener Kreditdaten mit einem Dritten eine Vereinbarung geschlossen werden, in der spezifische Sicherheitsvorkehrungen festgelegt sind (Artikel 19 Absatz 2 des Kreditdatengesetzes). Kommt es zu einer Verletzung des Schutzes personenbezogener Kreditdaten, sind Maßnahmen zur Schadensbegrenzung zu ergreifen und die betroffenen Personen unverzüglich zu unterrichten (Artikel 39-4 Absätze 1 bis 2 des Kreditdatengesetzes). Darüber hinaus muss der Datenschutzbeauftragte über die Unterrichtung der Personen und die durchgeführten Maßnahmen informiert werden (Artikel 39-4 Absatz 4 des Kreditdatengesetzes).

([131]) In diesem Fall muss unverzüglich eine richterliche Anordnung beantragt werden. Wird die Anordnung nicht innerhalb von 36 Stunden ausgestellt, müssen die erhaltenen Daten unverzüglich gelöscht werden (Artikel 32 Absatz 6 Nummer 6 des Kreditdatengesetzes).

([132]) Zum Beispiel, weil die vertraglichen Pflichten erfüllt wurden, eine der Parteien ihr Kündigungsrecht ausgeübt hat usw., siehe Artikel 17-2 Absatz 5 des Durchführungserlasses zum Kreditdatengesetz.

([133]) Artikel 20–2 Absatz 1 des Kreditdatengesetzes und Artikel 17-2 Absatz 1 Nummer 1 des Durchführungserlasses zum Kreditdatengesetz.

([134]) Dabei wird berücksichtigt, dass die Löschung oft nicht sofort möglich ist, sondern in der Regel bestimmte Schritte erfordert (z. B. die Trennung der zu löschenden Daten von anderen Daten und die Durchführung der Löschung, ohne dass die Stabilität der Datensysteme beeinträchtigt wird), deren Umsetzung einige Zeit in Anspruch nimmt.

([135]) Artikel 20-2 Absatz 2 des Kreditdatengesetzes.

([136]) Artikel 18 Absatz 2 des Kreditdatengesetzes und Artikel 15 Absatz 4 des Durchführungserlasses zum Kreditdatengesetz enthalten spezifischere Vorschriften in Bezug auf die Pflicht zur Führung von Aufzeichnungen, z. B. für Aufzeichnungen über Daten, die einer Person zum Nachteil gereichen können, wie Daten über Straffälligkeit und Konkurs.

([137]) In Bezug auf andere Mechanismen der Rechenschaftspflicht sind bestimmte Organisationen (z. B. Genossenschaften und öffentlichrechtliche Körperschaften, siehe Artikel 21 Absatz 2 des Durchführungserlasses zum Kreditdatengesetz) nach dem Kreditdatengesetz verpflichtet, einen „Kreditdatenverwalter bzw. -beauftragten“ zu ernennen, der für die Überwachung der Einhaltung des Kreditdatengesetzes zuständig ist und die Aufgaben des „Datenschutzbeauftragten“ nach dem PIPA wahrnimmt (Artikel 20 Absätze 3 und 4 des Kreditdatengesetzes).

(108) Im Kreditdatengesetz sind auch besondere Transparenzpflichten festgelegt, wenn die Einwilligung zur Verwendung oder Weitergabe personenbezogener Kreditdaten eingeholt werden soll (Artikel 32 Absatz 4 und Artikel 34-2 des Kreditdatengesetzes und Artikel 30-3 des Durchführungserlasses zum Kreditdatengesetz) und ganz allgemein, bevor Daten an einen Dritten weitergegeben werden (Artikel 32 Absatz 7 des Kreditdatengesetzes) ([138]). Darüber hinaus haben Einzelpersonen das Recht, auf Anfrage Informationen über die Verwendung und Weitergabe ihrer Kreditdaten an Dritte in den letzten drei Jahren vor der Anfrage zu erhalten (einschließlich des Zwecks und der Zeitpunkte einer solchen Verwendung oder Weitergabe) ([139]).

(109) Nach dem Kreditdatengesetz haben Einzelpersonen auch ein Recht auf Auskunft über ihre persönlichen Kreditdaten (Artikel 38 Absatz 1 des Kreditdatengesetzes) und auf Berichtigung unrichtiger Daten (Artikel 38 Absätze 2 bis 3 des Kreditdatengesetzes) ([140]). Neben dem allgemeinen Recht auf Löschung nach dem PIPA (siehe Erwägungsgrund (77)) ist im Kreditdatengesetz ein spezielles Recht auf Löschung personenbezogener Kreditdaten vorgesehen, die über die in Erwägungsgrund (104) genannten Speicherfristen hinaus aufbewahrt wurden, d. h. fünf Jahre (für personenbezogene Kreditdaten, die zur Begründung oder Aufrechterhaltung einer Geschäftsbeziehung erforderlich waren) oder drei Monate (für andere Arten personenbezogener Kreditdaten) ([141]). Ein Antrag auf Löschung kann ausnahmsweise abgelehnt werden, wenn eine weitere Speicherung unter den in Erwägungsgrund (105). beschriebenen Umständen erforderlich ist. Beantragt eine Person die Löschung von Daten, auf die eine der Ausnahmen zutrifft, so müssen für die betroffenen Kreditdaten besondere Sicherheitsvorkehrungen ergriffen werden (Artikel 38-3 Absatz 3 des Kreditdatengesetzes und Artikel 33-3 des Durchführungserlasses zum Kreditdatengesetz). Beispielsweise müssen die Daten getrennt von anderen Informationen gespeichert werden, dürfen nur von einer befugten Person eingesehen werden und müssen besonderen Sicherheitsvorkehrungen unterworfen sein.

(110) Abgesehen von den in Erwägungsgrund (109) genannten Rechten hat jede betroffene Person nach dem Kreditdatengesetz das Recht, einen Datenverantwortlichen aufzufordern, sie nicht mehr zu Direktwerbungszwecken zu kontaktieren (Artikel 37 Absatz 2 des Gesetzes), sowie ein Recht auf Datenübertragbarkeit. Was Letzteres betrifft, so können Einzelpersonen gemäß dem Kreditdatengesetz die Übermittlung ihrer persönlichen Kreditdaten an sich selbst oder an bestimmte Dritte (z. B. Finanzinstitute und Kreditrating-Unternehmen) beantragen. Die personenbezogenen Kreditdaten müssen in einem Format verarbeitet und an den Dritten übermittelt werden, das von einem informationsverarbeitenden Gerät (z. B. einem Computer) verarbeitet werden kann.

(111) Soweit im Kreditdatengesetz spezifischere Vorschriften als im PIPA enthalten sind, ist die Kommission daher der Ansicht, dass auch diese Vorschriften ein Schutzniveau gewährleisten, das dem durch die Verordnung (EU) 2016/679 gewährleisteten Schutzniveau der Sache nach gleichwertig ist.

2.4 **Aufsicht und Durchsetzung**

(112) Um sicherzustellen, dass in der Praxis ein angemessenes Datenschutzniveau gewährleistet ist, sollte eine unabhängige Aufsichtsbehörde mit der Befugnis zur Überwachung und Durchsetzung der Einhaltung der Datenschutzvorschriften eingerichtet werden. Diese Behörde sollte bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse vollkommen unabhängig und unparteiisch handeln.

2.4.1 *Unabhängige Aufsicht*

(113) In der Republik Korea ist die unabhängige Behörde, die für die Überwachung und Durchsetzung des PIPA zuständig ist, die PIPC. Die PIPC setzt sich aus einem Vorsitzenden, einem stellvertretenden Vorsitzenden und sieben Kommissionsmitgliedern zusammen. Der Vorsitzende und der stellvertretende Vorsitzende werden vom Präsidenten auf Vorschlag des Premierministers ernannt. Von den Kommissionsmitgliedern werden zwei vom Präsidenten auf Vorschlag des Vorsitzenden und fünf auf Vorschlag der Nationalversammlung ernannt (davon zwei auf Vorschlag von Vertretern der politischen Partei, der der Präsident angehört und drei auf Vorschlag von Vertretern anderer politischer Parteien (Artikel 7-2 Absatz 2 PIPA), wodurch das Ernennungsverfahren nicht

([138]) Dazu gehören eine allgemeine Informationspflicht (Artikel 32 Absatz 7 des Kreditdatengesetzes) und eine spezielle Transparenzpflicht für den Fall, dass Daten, anhand derer die Kreditwürdigkeit einer Person bestimmt werden kann, an bestimmte Einrichtungen wie Rating-Agenturen und Kreditdatenauskunfteien weitergegeben werden (Artikel 35-3 des Kreditdatengesetzes und Artikel 30-3 der Durchführungsverordnung zum Kreditdatengesetz), oder für den Fall, dass eine Geschäftsbeziehung auf der Grundlage der von einem Dritten erhaltenen persönlichen Kreditdaten abgelehnt oder abgebrochen wird (Artikel 36 des Kreditdatengesetzes und Artikel 31 der Durchführungsverordnung zum Kreditdatengesetz).

([139]) Artikel 35 des Kreditdatengesetzes. Bestimmte Handelsorganisationen, z. B. Genossenschaften und öffentlich-rechtliche Körperschaften (Artikel 21 Absatz 2 des Durchführungserlasses zum Kreditdatengesetz), unterliegen zusätzlichen Transparenzanforderungen; so müssen sie z. B. bestimmte Informationen öffentlich zugänglich machen (Artikel 31 des Kreditdatengesetzes) und Einzelpersonen über mögliche Nachteile für ihre Kreditwürdigkeit informieren, wenn sie Finanztransaktionen tätigen, die ein Kreditrisiko darstellen (Artikel 35-2 des Kreditdatengesetzes).

([140]) Hinsichtlich der Bedingungen und Ausnahmen vom Recht auf Auskunft und Berichtigung gelten die Vorschriften des PIPA (erläutert in den Erwägungsgründen (76)-(77)). Darüber hinaus sind weitere Modalitäten in Artikel 38 Absätze 4 bis 8 des Kreditdatengesetzes und Artikel 33 des Durchführungserlasses zum Kreditdatengesetz festgelegt. Insbesondere muss ein Wirtschaftsbeteiligter, der unzutreffende Kreditdaten berichtigt oder gelöscht hat, die betroffene Person darüber informieren. Darüber hinaus ist jeder Dritte, an den diese Daten in den vorangegangenen sechs Monaten weitergegeben wurden, zu benachrichtigen, und die betroffene Person ist darüber zu unterrichten. Ist die betroffene Person mit der Bearbeitung ihres Antrags auf Berichtigung nicht zufrieden, kann sie sich an den Datenschutzbeauftragten wenden, der die Handlungen des Datenverantwortlichen überprüft und Abhilfemaßnahmen anordnen kann.

([141]) Artikel 38-3 des Kreditdatengesetzes.

parteiisch wird) ([142]). Dieses Verfahren steht im Einklang mit den Anforderungen, die für die Ernennung von Mitgliedern von Datenschutzbehörden in der Union gelten (Artikel 53 Absatz 1 der Verordnung (EU) 2016/679). Darüber hinaus dürfen die Kommissionsmitglieder keine gewinnorientierten Geschäfte betreiben, keine politischen Aktivitäten ausüben und keine Ämter in der öffentlichen Verwaltung oder in der Nationalversammlung bekleiden (Artikel 7-6 und Artikel 7-7 Absatz 1 Nummer 3 PIPA) ([143]). Für alle Kommissionsmitglieder gelten besondere Vorschriften, nach denen sie im Falle eines möglichen Interessenkonflikts nicht an den Beratungen teilnehmen dürfen (Artikel 7-11 PIPA). Die PIPC wird von einem Sekretariat unterstützt (Artikel 7-13) und kann Unterkommissionen (bestehend aus drei Kommissionsmitgliedern) einsetzen, um geringfügige Verstöße und wiederkehrende Angelegenheiten zu behandeln (Artikel 7-12 PIPA).

(114) Jedes Mitglied der PIPC wird für drei Jahre ernannt und kann einmal wieder ernannt werden (Artikel 7-4 Absatz 1 PIPA). Kommissionsmitglieder können nur unter bestimmten Umständen entlassen werden, nämlich wenn sie aufgrund einer langfristigen geistigen oder körperlichen Behinderung nicht mehr in der Lage sind, ihr Amt auszuüben, wenn sie gegen das Gesetz verstoßen oder wenn einer der Gründe für die Amtsenthebung vorliegt (Artikel 7-5 PIPA) ([144]). Dadurch erhalten sie einen institutionellen Schutz bei der Ausübung ihrer Aufgaben.

(115) Im Allgemeinen wird die Unabhängigkeit der PIPC in Artikel 7 Absatz 1 PIPA ausdrücklich garantiert, und nach Artikel 7-5 Absatz 2 PIPA sind die Kommissionsmitglieder verpflichtet, ihre Aufgaben unabhängig, nach dem Gesetz und nach ihrem Gewissen zu erfüllen ([145]). Die beschriebenen institutionellen und verfahrenstechnischen Garantien, auch in Bezug auf die Ernennung und Entlassung seiner Mitglieder, gewährleisten, dass die PIPC völlig unabhängig und frei von externen Einflüssen oder Anweisungen handelt. Als zentrale Verwaltungsbehörde stellt die PIPC jährlich einen eigenen Haushaltsplan auf (der vom Finanzministerium als Teil des Gesamthaushaltsplans vor der Verabschiedung durch die Nationalversammlung geprüft wird) und ist für ihre eigene Personalverwaltung zuständig. Die PIPC verfügt über ein Budget von derzeit rund 35 Millionen EUR und beschäftigt 154 Mitarbeiter (darunter 40 auf Informations- und Kommunikationstechnologie spezialisierte Mitarbeiter, 32 Mitarbeiter mit Schwerpunkt Ermittlungen und 40 Rechtssachverständige).

(116) Die Aufgaben und Befugnisse der PIPC sind hauptsächlich in den Artikeln 7-8 und 7-9 sowie in den Artikeln 61 bis 66 PIPA geregelt ([146]). Zu den Aufgaben von PIPC gehören insbesondere die Beratung zu Gesetzen und Vorschriften im Zusammenhang mit dem Datenschutz, die Entwicklung von Datenschutzstrategien und -leitlinien, die Untersuchung von Verstößen gegen die Rechte des Einzelnen, die Bearbeitung von Beschwerden und die Schlichtung von Streitigkeiten, die Durchsetzung der Einhaltung des PIPA, die Gewährleistung von Bildung und Förderung im Bereich des Datenschutzes sowie der Austausch und die Zusammenarbeit mit Datenschutzbehörden in Drittländern ([147]).

(117) Auf der Grundlage von Artikel 68 PIPA in Verbindung mit Artikel 62 des PIPA-Durchführungserlasses wurden bestimmte Aufgaben der PIPC an die koreanische Internet- und Sicherheitsbehörde delegiert, und zwar 1) Bildung und Öffentlichkeitsarbeit, 2) Schulung von Fachleuten und Entwicklung von Kriterien für Datenschutz-Folgenabschätzungen, 3) Bearbeitung von Anträgen auf Benennung einer sogenannten Einrichtung für Datenschutz-Folgenabschätzungen, 4) Bearbeitung von Anträgen auf indirekten Auskunft über die personenbezogenen Daten im Besitz von Behörden (Artikel 35 Absatz 2 PIPA) und 5) Anforderung von Materialien und Durchführung von

([142]) Zu Kommissionsmitgliedern der PIPC können nur Personen ernannt werden, die die folgenden Kriterien erfüllen: leitende Beamte, die für Angelegenheiten im Bereich der personenbezogenen Daten zuständig sind, ehemalige Richter, Staatsanwälte oder Rechtsanwälte, die mindestens 10 Jahre lang beruflich tätig waren, ehemalige Führungskräfte mit Erfahrung im Datenschutz, die mehr als drei Jahre in einer öffentlichen Einrichtung oder Organisation tätig waren oder die von einer solchen Einrichtung oder Organisation empfohlen wurden und ehemalige außerordentliche Professoren mit Fachkenntnissen im Datenschutzbereich, die mindestens fünf Jahre lang in einer akademischen Einrichtung tätig waren (Artikel 7-2 PIPA).

([143]) Siehe auch Artikel 4-2 des PIPA-Durchführungserlasses.

([144]) Siehe Artikel 7-7 PIPA, wonach nichtkoreanische Staatsangehörige und Mitglieder politischer Parteien keine Mitglieder der PIPC werden können. Das Gleiche gilt für Personen, gegen die bestimmte strafrechtliche Sanktionen verhängt wurden, die innerhalb der letzten fünf Jahre durch ein Disziplinarverfahren aus dem Amt entfernt wurden usw. (Artikel 7-7 PIPA in Verbindung mit Artikel 33 des Gesetzes über öffentliche Bedienstete).

([145]) In Artikel 7 Absatz 2 PIPA wird zwar auf die allgemeine, in Artikel 18 des Gesetzes über die Regierungsorganisation niedergelegte Befugnis des Premierministers verwiesen, mit Zustimmung des Präsidenten jede rechtswidrige oder ungerechtfertigte Verfügung einer zentralen Verwaltungsbehörde auszusetzen oder zu widerrufen, aber der PIPC wird eine solche Befugnis im Rahmen ihrer Ermittlungs- und Durchsetzungsbefugnisse nicht gewährt (siehe Artikel 7 Absatz 2 Nummern 1 und 2 PIPA). Nach den Erklärungen der koreanischen Regierung soll Artikel 18 des Gesetzes über die Regierungsorganisation dem Premierminister die Möglichkeit einräumen, unter außergewöhnlichen Umständen zu handeln, z. B. um eine Meinungsverschiedenheit zwischen verschiedenen Regierungsstellen zu schlichten. Seit der Verabschiedung dieser Bestimmung im Jahr 1963 hat der Premierminister jedoch noch nie von dieser Befugnis Gebrauch gemacht.

([146]) Sofern dies für die Erfüllung der Aufgaben nach Artikel 7-9 Absatz 1 PIPA erforderlich ist, kann der Datenschutzbeauftragte die Stellungnahmen von einschlägigen öffentlichen Bediensteten, Datenschutzexperten, zivilgesellschaftlichen Organisationen und einschlägigen Wirtschaftsbeteiligten einholen. Darüber hinaus kann die PIPC einschlägige Unterlagen anfordern, Empfehlungen für Verbesserungen aussprechen und deren Umsetzung überprüfen (Artikel 7-9 Absätze 2 bis 5 PIPA).

([147]) Siehe auch Artikel 9 PIPA (dreijährlicher Gesamtplan für den Schutz personenbezogener Daten), Artikel 12 PIPA (Standardleitlinien für den Schutz personenbezogener Daten), Artikel 13 PIPA (Maßnahmen zur Förderung und Unterstützung der Selbstregulierung).

Kontrollen im Zusammenhang mit Beschwerden, die über das sogenannte Datenschutz-Callcenter eingehen. Im Rahmen der Bearbeitung von Beschwerden über das Datenschutz-Callcenter leitet die koreanische Internet- und Sicherheitsbehörde den Fall an die PIPC oder an die Staatsanwaltschaft weiter, wenn sie einen Verstoß gegen das Gesetz feststellt. Die Möglichkeit, eine Beschwerde beim Datenschutz-Callcenter einzureichen, hindert Einzelpersonen nicht daran, direkt eine Beschwerde bei der PIPC einzureichen oder sich an die PIPC zu wenden, sollte ihre Beschwerde ihrer Ansicht nach von der koreanischen Internet- und Sicherheitsbehörde nicht zufriedenstellend bearbeitet worden sein.

2.4.2 *Durchsetzung, einschließlich Sanktionen*

(118) Um die Einhaltung des PIPA zu gewährleisten, hat der Gesetzgeber an die PIPC sowohl Ermittlungs- als auch Durchsetzungsbefugnisse übertragen, die von Empfehlungen bis hin zu Geldbußen reichen. Diese Befugnisse werden durch eine Regelung strafrechtlicher Sanktionen ergänzt.

(119) In Bezug auf die Ermittlungsbefugnisse kann die PIPC, sofern ein Verstoß gegen das PIPA vermutet wird oder gemeldet wurde oder wenn dies zum Schutz der Rechte der betroffenen Personen vor Verstößen erforderlich ist, Kontrollen vor Ort durchführen und alle relevanten Materialien (wie Artikel und Dokumente) von den Datenverantwortlichen anfordern (Artikel 63 PIPA in Verbindung mit Artikel 60 des PIPA-Durchführungserlasses) ([148]).

(120) In Bezug auf die Durchsetzung kann die PIPC gemäß Artikel 61 Absatz 2 PIPA den Datenverantwortlichen Empfehlungen zur Verbesserung des Schutzes personenbezogener Daten bei bestimmten Verarbeitungstätigkeiten geben. Die Datenverantwortlichen müssen sich nach Treu und Glauben bemühen, diese Empfehlungen umzusetzen, und sind verpflichtet, die PIPC über das Ergebnis zu informieren. Darüber hinaus kann die PIPC Abhilfemaßnahmen anordnen, wenn berechtigte Gründe für die Annahme bestehen, dass ein Verstoß gegen das PIPA vorliegt und die Unterlassung von Maßnahmen wahrscheinlich zu einem schwer zu behebenden Schaden führen wird (Artikel 64 Absatz 1 PIPA) ([149]). In Abschnitt 5 der Bekanntmachung 2021-5 (Anhang I) wird mit verbindlicher Wirkung klargestellt, dass diese Bedingungen bei der Verletzung einer PIPA-Bestimmung, mit der die Datenschutzrechte natürlicher Personen in Bezug auf personenbezogene Daten gewährleistet werden, erfüllt sind ([150]). Zu den Maßnahmen, zu denen die PIPC befugt ist, gehören die Anordnung der Einstellung des Verhaltens, das den Verstoß verursacht hat, die vorübergehende Aussetzung der Datenverarbeitung oder andere notwendige Maßnahmen. Die Nichterfüllung einer Abhilfemaßnahme kann mit einer Geldbuße in Höhe von maximal 50 Millionen Won geahndet werden (Artikel 75 Absatz 2 Nummer 13 PIPA).

(121) In Bezug auf bestimmte Behörden (wie die Nationalversammlung, zentrale Verwaltungsbehörden, lokale Gebietskörperschaften und Gerichte) ist in Artikel 64 Absatz 4 PIPA vorgesehen, dass die PIPC eine der in Erwägungsgrund (120) genannten Abhilfemaßnahmen „empfehlen" kann und dass diese Behörden verpflichtet sind, einer solchen Empfehlung nachzukommen, sofern keine außergewöhnlichen Umstände vorliegen. Gemäß Abschnitt 5 der Bekanntmachung 2021-5 handelt es sich dabei um außergewöhnliche tatsächliche oder rechtliche Umstände, die der PIPC zum Zeitpunkt der Abgabe seiner Empfehlung nicht bekannt waren. Die betroffene Behörde kann sich nur dann auf solche außergewöhnlichen Umstände berufen, wenn sie eindeutig nachweist, dass kein Verstoß vorliegt, und die PIPC feststellt, dass dies tatsächlich nicht der Fall ist. Andernfalls ist die Behörde verpflichtet, der Empfehlung der PIPC zu folgen und eine „Abhilfemaßnahme zu ergreifen, unter anderem die sofortige Einstellung der betreffenden Handlung, und Schadenersatz zu leisten."

(122) Die PIPC kann auch andere Verwaltungsbehörden mit spezifischen Zuständigkeiten nach sektoralen Rechtsvorschriften (z. B. Gesundheit, Bildung) ersuchen, allein oder gemeinsam mit der PIPC eine Untersuchung von (mutmaßlichen) Verstößen gegen den Datenschutz durch Datenverantwortliche, die in diesen Sektoren in ihrem Zuständigkeitsbereich tätig sind, durchzuführen und Abhilfemaßnahmen anzuordnen (Artikel 63 Absätze 4 bis 5 PIPA). In diesem Fall legt die PIPC die Gründe, den Gegenstand und den Umfang der Untersuchung fest ([151]). Die zuständige Verwaltungsbehörde muss ihrerseits der PIPC einen Kontrollplan vorlegen und die PIPC über das Ergebnis der Kontrolle informieren. Die PIPC kann eine spezifische Abhilfemaßnahme empfehlen, die von der betreffenden Behörde nach Möglichkeit umgesetzt werden muss. In jedem Fall schränkt ein solches Ersuchen die Befugnis der PIPC, eigene Untersuchungen durchzuführen oder Sanktionen zu verhängen, nicht ein.

([148]) Die Mitglieder der PIPC können außerdem die Räumlichkeiten des Datenverantwortlichen betreten, um den Stand des Geschäftsbetriebs, die Aufzeichnungen, Unterlagen usw. zu prüfen (Artikel 63 Absatz 2 PIPA). Siehe auch Artikel 45-3 des Kreditdatengesetzes und Artikel 36-4 des Durchführungserlasses zum Kreditdatengesetz in Bezug auf die Befugnisse der PIPC nach diesem Gesetz.

([149]) Siehe auch Artikel 45-4 des Kreditdatengesetzes in Bezug auf die Befugnisse der PIPC nach dem Kreditdatengesetz.

([150]) In Abschnitt 5 der Bekanntmachung heißt es: „Wesentliche Gründe für die Annahme, dass eine Verletzung des Schutzes personenbezogener Daten vorliegt und bei Untätigkeit ein schwer zu behebender Schaden im Sinne von Artikel 64 Absätze 1 und 2 PIPA wahrscheinlich ist, beziehen sich auf eine Verletzung der Grundsätze, Rechte und Pflichten, die im Gesetz zum Schutz der Rechte natürlicher Personen an personenbezogenen Daten enthalten sind." Gleiches gilt für die Befugnisse der PIPC gemäß Artikel 45-4 des Kreditdatengesetzes.

([151]) Artikel 60 des PIPA-Durchführungserlasses.

(123) Zusätzlich zu ihren Abhilfebefugnissen kann die PIPC bei Verstößen gegen verschiedene Vorschriften des PIPA Geldbußen zwischen 10 und 50 Millionen Won verhängen (Artikel 75 PIPA) ([152]). Dazu gehören unter anderem die Nichteinhaltung der Anforderungen an die Rechtmäßigkeit der Verarbeitung, das Versäumnis, die erforderlichen Sicherheitsvorkehrungen zu ergreifen, das Versäumnis, die betroffenen Personen im Falle einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, die Nichteinhaltung der Anforderungen an die Weiterverarbeitung, das Versäumnis, eine Datenschutzerklärung auszuarbeiten und zu veröffentlichen, das Versäumnis, einen Datenschutzbeauftragten zu benennen, oder das Versäumnis, auf Ersuchen der betroffenen Person in Ausübung ihrer individuellen Rechte tätig zu werden, sowie bestimmte Verfahrensverstöße (Verweigerung der Zusammenarbeit bei einer Untersuchung). Bei Verstößen gegen mehrere Bestimmungen des PIPA durch denselben Datenverantwortlichen kann für jeden einzelnen Verstoß eine Geldbuße verhängt werden, wobei die Zahl der betroffenen Personen bei der Festsetzung der Höhe der Geldbuße berücksichtigt wird.

(124) Darüber hinaus kann die PIPC bei begründetem Verdacht auf einen Verstoß gegen das PIPA oder andere „Datenschutzgesetze" bei der zuständigen Ermittlungsbehörde (z. B. der Staatsanwaltschaft, siehe Artikel 65 Absatz 1 PIPA) Strafanzeige erstatten. Darüber hinaus kann die PIPC dem Datenverantwortlichen empfehlen, Disziplinarmaßnahmen gegen die verantwortliche Person zu ergreifen (einschließlich der verantwortlichen Führungskraft, siehe Artikel 65 Absatz 2 PIPA). Nach Erhalt einer solchen Empfehlung muss der Datenverantwortliche dieser nachkommen ([153]) und das Ergebnis der PIPC schriftlich mitteilen (Artikel 65 des PIPA in Verbindung mit Artikel 58 des PIPA-Durchführungserlasses).

(125) Bei Empfehlungen gemäß Artikel 61, Abhilfemaßnahmen gemäß Artikel 64, Anklagen oder Empfehlungen für Disziplinarmaßnahmen gemäß Artikel 65 und der Verhängung von Geldbußen gemäß Artikel 75 PIPA kann die PIPC den Sachverhalt – d. h. den Verstoß, die Einrichtung, die gegen das Gesetz verstoßen hat, und die auferlegte (n) Maßnahme(n) – durch Veröffentlichung auf ihrer Website oder in einer allgemeinen, landesweit erscheinenden Tageszeitung bekannt machen (Artikel 66 PIPA in Verbindung mit Artikel 61 Absatz 1 des PIPA-Durchführungserlasses) ([154]).

(126) Schließlich wird die Einhaltung der Datenschutzanforderungen des PIPA (sowie anderer „Datenschutzgesetze") durch ein System strafrechtlicher Sanktionen unterstützt. In diesem Zusammenhang enthalten die Artikel 70 bis 73 PIPA Strafbestimmungen, die entweder zu einer Geldbuße (zwischen 20 und 100 Millionen Won) oder zu einer Freiheitsstrafe (mit einer Höchststrafe zwischen 2 und 10 Jahren) führen können. Zu den einschlägigen Verstößen gehören unter anderem die Verwendung personenbezogener Daten oder die Weitergabe solcher Daten an Dritte ohne die erforderliche Einwilligung, die Verarbeitung sensibler Daten entgegen dem Verbot in Artikel 23 Absatz 1 PIPA, die Nichteinhaltung geltender Sicherheitsvorschriften mit der Folge, dass personenbezogene Daten verloren gehen bzw. gestohlen, weitergegeben, gefälscht, verändert oder beschädigt werden, das Versäumnis, die erforderlichen Maßnahmen zur Berichtigung, Löschung oder Sperrung personenbezogener Daten zu ergreifen, oder die unrechtmäßige Übermittlung personenbezogener Daten in ein Drittland ([155]). Gemäß Artikel 74 PIPA haftet in jedem dieser Fälle der Angestellte, Beauftragte oder Vertreter des Datenverantwortlichen sowie der Datenverantwortliche selbst ([156]).

(127) Neben den im PIPA vorgesehenen strafrechtlichen Sanktionen kann die missbräuchliche Verwendung personenbezogener Daten auch eine Straftat nach dem Strafgesetzbuch darstellen. Dies gilt insbesondere für die Verletzung des Brief- und Schriftgeheimnisses und des Geheimnisses elektronischer Aufzeichnungen (Artikel 316), die Weitergabe von dem Berufsgeheimnis unterliegenden Daten (Artikel 317), den Betrug unter Verwendung von Computern (Artikel 347-2) sowie die Veruntreuung und den Vertrauensbruch (Artikel 355).

(128) Das koreanische System kombiniert daher verschiedene Arten von Sanktionen, von Abhilfemaßnahmen über Verwaltungsstrafen bis hin zu strafrechtlichen Sanktionen, die eine besonders starke abschreckende Wirkung auf die Datenverantwortlichen und die mit den Daten umgehenden Personen haben dürften. Unmittelbar nach seiner Einrichtung im Jahr 2020 begann die PIPC, von ihren Befugnissen Gebrauch zu machen. Aus dem PIPC-Jahresbericht 2021 geht hervor, dass die PIPC bereits eine Reihe von Empfehlungen ausgesprochen, Geldbußen verhängt

([152]) Wenn die von einem Datenverantwortlichen betriebenen Systeme zur Verarbeitung und zum Schutz personenbezogener Daten als mit dem PIPA konform zertifiziert wurden, die Zertifizierungskriterien gemäß Artikel 34-2 Absatz 1 des PIPA-Durchführungserlasses aber tatsächlich nicht erfüllt wurden, oder im Falle eines schwerwiegenden Verstoßes gegen ein „[personenbezogenes] Datenschutzgesetz", kann die PIPC die Zertifizierung widerrufen (Artikel 32-2 Absätze 3 und 5 PIPA). Die PIPC benachrichtigt den Datenverantwortlichen von diesem Widerruf und gibt dies entweder öffentlich bekannt oder veröffentlicht es auf ihrer Website oder im Amtsblatt (Artikel 34-4 des PIPA-Durchführungserlasses). Für Verstöße gegen das Kreditdatengesetz sind außerdem Geldbußen (Artikel 52 des Kreditdatengesetzes) und strafrechtliche Sanktionen (Artikel 50 des Kreditdatengesetzes) vorgesehen.

([153]) Gemäß Artikel 58 Absatz 2 des PIPA-Durchführungserlasses muss der Datenverantwortliche der PIPC eine begründete Erklärung vorlegen, wenn die Befolgung der Empfehlung aufgrund besonderer Umstände „nicht praktikabel" ist.

([154]) Bei der Entscheidung darüber, ob eine solche Veröffentlichung erfolgen soll, berücksichtigt die PIPC den Inhalt und die Schwere des Verstoßes, seine Dauer und Häufigkeit sowie seine Folgen (Ausmaß des Schadens). Die betroffene Einrichtung wird vorher informiert und erhält die Möglichkeit, sich zu verteidigen. Siehe Artikel 61 Absätze 2 und 3 des PIPA-Durchführungserlasses.

([155]) Siehe Artikel 71 Nummer 2 in Verbindung mit Artikel 18 Absatz 1 PIPA (Nichteinhaltung der Bedingungen in Artikel 17 Absatz 3 PIPA, auf den in Artikel 18 Absatz 1 verwiesen wird). Siehe auch Artikel 75 Absatz 2 Nummer 1 in Verbindung mit Artikel 17 Absatz 2 PIPA (Versäumnis, der betroffenen Person die erforderlichen Informationen zur Verfügung zu stellen gemäß Artikel 17 Absatz 2 PIPA, auf den in Artikel 17 Absatz 3 verwiesen wird).

([156]) Darüber hinaus können nach Artikel 74-2 PIPA alle Gelder, Waren oder sonstigen Gewinne, die infolge des Verstoßes erzielt wurden, eingezogen werden, oder, wenn eine Einziehung nicht möglich ist, der rechtswidrig erlangte Vorteil „eingetrieben" werden.

und Abhilfemaßnahmen angeordnet hat, und zwar sowohl gegen den öffentlichen Sektor (rund 34 Behörden) als auch gegen private Unternehmen (rund 140 Unternehmen) ([157]). Zu den bemerkenswerten Fällen gehören beispielsweise die Verhängung einer Geldbuße in Höhe von 6,7 Mrd. Won im Dezember 2020 gegen ein Unternehmen, das gegen verschiedene Bestimmungen des PIPA verstoßen hatte (u. a. Sicherheitsanforderungen, Anforderungen an die Einwilligung für die Übermittlung der Daten an Dritte und Transparenzanforderungen) ([158]), und einer Geldbuße in Höhe von 103,3 Mio. Won im April 2021 gegen ein KI-Technologieunternehmen, das u. a. gegen die Vorschriften über die Rechtmäßigkeit der Verarbeitung, insbesondere die Einwilligung, und die Verarbeitung pseudonymisierter Daten verstoßen hatte ([159]). Im August 2021 schloss die PIPC eine weitere Untersuchung der Tätigkeit von drei Unternehmen ab, die zu Abhilfemaßnahmen und der Verhängung von Geldbußen von bis zu 6,47 Mrd. Won führte (u. a. wegen unterlassener Unterrichtung von Personen über die Weitergabe personenbezogener Daten an Dritte, einschließlich der Übermittlung an Drittländer) ([160]). Außerdem hat Südkorea bereits vor der jüngsten Reform erhebliche Erfolge bei der Durchsetzung der Vorschriften erzielt, wobei die zuständigen Behörden das gesamte Spektrum der Durchsetzungsmaßnahmen eingesetzt haben, einschließlich Verwaltungsstrafen, Abhilfemaßnahmen und „Namensnennung und Offenlegung" in Bezug auf eine Vielzahl von Datenverantwortlichen, einschließlich Kommunikationsdiensteanbieter (Korea Communications Commission), sowie Wirtschaftsbeteiligte, Finanzinstitute, Behörden, Universitäten und Krankenhäuser (Ministerium für Inneres und Sicherheit) ([161]). Auf dieser Grundlage kommt die Kommission zu dem Schluss, dass das koreanische System die wirksame Durchsetzung der Datenschutzvorschriften in der Praxis gewährleistet und damit ein Schutzniveau garantiert, das im Wesentlichen dem der Verordnung (EU) 2016/679 entspricht.

2.5 **Rechtsbehelfe**

(129) Um einen angemessenen Schutz und insbesondere die Durchsetzung der Rechte des Einzelnen zu gewährleisten, sollten der betroffenen Person wirksame behördliche und gerichtliche Rechtsbehelfe, einschließlich Schadenersatz, zur Verfügung stehen.

(130) Das koreanische System stellt dem Einzelnen verschiedene Mechanismen zur Verfügung, um seine Rechte wirksam durchzusetzen und einen (gerichtlichen) Rechtsbehelf geltend zu machen.

(131) Personen, die der Ansicht sind, dass ihre Datenschutzrechte oder -interessen verletzt wurden, können sich in einem ersten Schritt an den jeweiligen Datenverantwortlichen wenden. Gemäß Artikel 30 Absatz 1 Nummer 5 PIPA muss die Datenschutzerklärung des Datenverantwortlichen unter anderem Informationen über die Rechte der betroffenen Personen und deren Ausübung enthalten. Darüber hinaus muss sie Kontaktdaten – wie den Namen und die Telefonnummer des Datenschutzbeauftragten oder der für den Datenschutz zuständigen Abteilung – enthalten, damit Beschwerden eingereicht werden können. Im Unternehmen des Datenverantwortlichen ist der Datenschutzbeauftragte mit der Bearbeitung von Beschwerden, der Verabschiedung von Abhilfemaßnahmen im Falle eines Verstoßes gegen den Datenschutz und der Entschädigung betraut (Artikel 31 Absatz 2 Nummer 3 und Absatz 4 PIPA). Letzteres ist beispielsweise im Falle einer Verletzung des Schutzes personenbezogener Daten von Bedeutung, da der Datenverantwortliche die betroffene Person u. a. über die Kontaktstelle(n) für die Meldung von Schäden unterrichten muss (Artikel 34 Absatz 1 Nummer 5 PIPA).

(132) Darüber hinaus werden Einzelpersonen im PIPA mehrere Möglichkeiten geboten, gegen Datenverantwortliche vorzugehen. Erstens kann jede Person, die der Ansicht ist, dass ihre Datenschutzrechte oder -interessen durch den Datenverantwortlichen verletzt wurden, einen solchen Verstoß direkt bei der PIPC und/oder einer der von der PIPC für die Entgegennahme und Bearbeitung von Beschwerden benannten spezialisierten Einrichtungen melden; dazu gehört auch die koreanische Internet- und Sicherheitsbehörde, die zu diesem Zweck ein Callcenter für personenbezogene Daten (das sogenannte „Datenschutz-Callcenter") betreibt (Artikel 62 Absätze 1 und 2 PIPA in Verbindung mit Artikel 59 des PIPA-Durchführungserlasses). Das Datenschutz-Callcenter untersucht und stellt

([157]) Siehe den PIPC-Jahresbericht 2021, S. 50-55 unter https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK (nur auf Koreanisch verfügbar).

([158]) Siehe unter https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK (nur auf Koreanisch verfügbar).

([159]) Siehe unter https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8 (nur auf Koreanisch verfügbar).

([160]) Siehe unter https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK (nur auf Koreanisch verfügbar).

([161]) Siehe z. B. den Jahresbericht 2020 unter https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 (nur auf Koreanisch verfügbar) und die Beispiele auf Englisch abrufbar unter https://www.privacy.go.kr/eng/enforcement_02.do.

Verstöße fest, berät in Bezug auf die Verarbeitung personenbezogener Daten (Artikel 62 Absatz 3 PIPA) und kann Verstöße an die PIPC melden (kann aber selbst keine Durchsetzungsmaßnahmen ergreifen). Das Datenschutz-Callcenter erhält eine große Anzahl von Beschwerden oder Anfragen (z. B. 177 457 im Jahr 2020, 159 255 im Jahr 2019 und 164 497 im Jahr 2018) ([162]). Nach Angaben der PIPC gingen bei der PIPC selbst zwischen August 2020 und August 2021 rund 1 000 Beschwerden ein. Die PIPC kann als Reaktion auf eine Beschwerde einen Verbesserungsvorschlag unterbreiten, Abhilfemaßnahmen ergreifen, eine „Anklage" bei der zuständigen Ermittlungsbehörde (einschließlich eines Staatsanwalts) erheben oder eine Empfehlung für Disziplinarmaßnahmen aussprechen (siehe Artikel 61, 64 und 65 PIPA). Entscheidungen der PIPC (z. B. die Verweigerung der Bearbeitung einer Beschwerde oder die Zurückweisung einer Beschwerde in der Sache) können nach dem Gesetz über die Verwaltungsgerichtsbarkeit angefochten werden ([163]).

(133) Zweitens können betroffene Personen gemäß den Artikeln 40 bis 50 PIPA in Verbindung mit den Artikeln 48-14 bis 57 des PIPA-Durchführungserlasses Ansprüche bei einem sogenannten „Streitschlichtungsausschuss" geltend machen; dieser setzt sich aus Vertretern zusammen, die vom Vorsitzenden der PIPC aus Mitgliedern des höheren Verwaltungsdienstes der PICP und aus Personen ernannt werden, die aufgrund ihrer Erfahrung im Bereich des Datenschutzes aus bestimmten infrage kommenden Gruppen ausgewählt werden (siehe Artikel 40 Absätze 2, 3 und 7 PIPA, Artikel 48-14 des PIPA-Durchführungserlasses) ([164]). Die Möglichkeit, eine Schlichtung vor dem Schlichtungsausschuss in Anspruch zu nehmen, bietet einen alternativen Weg, um Abhilfe zu schaffen, schränkt jedoch nicht das Recht des Einzelnen ein, sich stattdessen an die PIPC oder Gerichte zu wenden. Zur Prüfung des Falles kann der Ausschuss die Streitparteien auffordern, die erforderlichen Unterlagen vorzulegen und/oder einschlägige Zeugen vorzuladen (Artikel 45 PIPA). Nach Klärung der Angelegenheit erstellt der Ausschuss einen Entwurf für einen Schlichtungsspruch ([165]), dem die Mehrheit seiner Mitglieder zustimmen muss. Der Schlichtungsentwurf kann die Aussetzung des Verstoßes, die erforderlichen Abhilfemaßnahmen (einschließlich Rückgabe oder Entschädigung) sowie alle Maßnahmen umfassen, die erforderlich sind, um eine Wiederholung des gleichen Verstoßes oder ähnlicher Verstöße zu verhindern (Artikel 47 Absatz 1 PIPA). Stimmen beide Parteien dem Schlichtungsspruch zu, hat er die gleiche Wirkung wie ein gerichtlicher Vergleich (Artikel 47 Absatz 5 PIPA). Es ist keiner der Parteien verwehrt, während der Schlichtung ein Gerichtsverfahren einzuleiten; in diesem Fall wird die Schlichtung ausgesetzt (siehe Artikel 48 Absatz 2 PIPA) ([166]). Aus den jährlichen Zahlen der PIPC geht hervor, dass Einzelpersonen regelmäßig das Verfahren vor dem Schlichtungsausschuss in Anspruch nehmen, das häufig zu einem erfolgreichen Abschluss führt. So bearbeitete der Ausschuss im Jahr 2020 126 Fälle, von denen 89 vor dem Ausschuss gelöst wurden (davon 77 Fälle, in denen die Parteien bereits vor Abschluss des Schlichtungsverfahrens eine Einigung erzielten, und 12 Fälle, in denen die Parteien den Schlichtungsvorschlag akzeptierten), was einer Schlichtungsquote von 70,6 % entspricht ([167]). Im Jahr 2019 bearbeitete der Ausschuss 139 Fälle, von denen 92 geklärt werden konnten, was einer Schlichtungsquote von 62,2 % entspricht.

(134) Wenn mindestens 50 Personen einen Schaden erlitten haben oder ihre Datenschutzrechte in gleicher oder ähnlicher Weise infolge desselben Vorfalls verletzt wurden, ([168]) kann eine betroffene Person oder eine Datenschutzorganisation zudem eine kollektive Streitschlichtung im Namen einer solchen Gesamtheit beantragen; andere betroffene Personen können beantragen, einer solchen Schlichtung beizutreten, die vom Streitschlichtungsausschuss öffentlich bekannt gegeben wird (Artikel 49 Absätze 1 bis 3 PIPA in Verbindung mit den Artikeln 52 bis 54 des PIPA-Durchführungserlasses) ([169]). Der Schlichtungsausschuss kann mindestens eine Person, die das

([162]) Siehe den PIPC-Jahresbericht 2021, S. 174. Im Jahr 2020 betrafen diese Beschwerden beispielsweise die Erhebung von Daten ohne Einwilligung, die Nichteinhaltung von Transparenzpflichten, Verstöße gegen das PIPA durch Auftragsverarbeiter, unzureichende Sicherheitsvorkehrungen, die Nichtbeantwortung von Anfragen betroffener Personen sowie allgemeine Anfragen.

([163]) Insbesondere kann die betroffene Person Rechtsmittel gegen die Ausübung oder Verweigerung der Ausübung öffentlicher Gewalt durch eine Verwaltungsbehörde einlegen (Artikel 2 Absatz 1 Nummer 1 und Artikel 3 Nummer 1 des Gesetzes über die Verwaltungsgerichtsbarkeit). Ausführlichere Informationen zu den verfahrensrechtlichen Aspekten, einschließlich der Zulässigkeitsvoraussetzungen, finden sich in Erwägungsgrund (181).

([164]) Alle Mitglieder sind für eine bestimmte Zeit im Amt und können nur aus wichtigem Grund entlassen werden (siehe Artikel 40 Absatz 5 und Artikel 41 PIPA). Darüber hinaus enthält Artikel 42 PIPA Garantien zum Schutz vor Interessenkonflikten.

([165]) Siehe Artikel 44 PIPA. Außerdem kann er einen Entwurf eines Vergleichs vorschlagen und einen Vergleich ohne Schlichtung empfehlen (siehe Artikel 46 PIPA).

([166]) Darüber hinaus kann der Ausschuss die Schlichtung ablehnen, wenn er diese angesichts der Art der Streitigkeit für unangemessen hält oder weil der Antrag auf Schlichtung zu einem unlauteren Zweck gestellt wurde (Artikel 48 PIPA).

([167]) Siehe den PIPC-Jahresbericht 2021, S. 179-180. Diese Fälle betrafen unter anderem Verstöße gegen das Erfordernis der Einwilligung zur Datenerhebung, den Grundsatz der Zweckbindung und die Rechte der betroffenen Personen.

([168]) Siehe Artikel 49 Absatz 1 PIPA, wonach betroffene Personen einen Schaden oder eine Verletzung ihrer Rechte „in gleicher oder ähnlicher Weise" erleiden müssen, und Artikel 52 Nummer 2 des PIPA-Durchführungserlasses, in dem gefordert wird, dass „die wesentlichen Aspekte des Vorfalls entweder sachlich oder rechtlich gleich sind".

([169]) Darüber hinaus können auch nicht an der Schlichtung beteiligte Personen Vorteile aus einem von dem Datenverantwortlichen anerkannten kollektiven Schlichtungsspruch ziehen, da der Schlichtungsausschuss dem Datenverantwortlichen empfehlen kann, einen Entschädigungsplan auszuarbeiten und vorzulegen, der (auch) diese Personen einbezieht (Artikel 49 Absatz 5 PIPA).

gemeinsame Interesse am geeignetsten vertritt, als Parteivertreter auswählen (Artikel 49 Absatz 4 PIPA). Lehnt der Datenverantwortliche die kollektive Streitschlichtung ab oder akzeptiert er den Schlichtungsspruch nicht, können bestimmte Organisationen ([170]) eine Sammelklage einreichen, um gegen den Verstoß vorzugehen (Artikel 51 bis 57 PIPA).

(135) Drittens hat die betroffene Person im Falle einer Verletzung des Schutzes der Privatsphäre, durch die sie einen „Schaden" erleidet, ein Recht auf angemessene Rechtsbehelfe in einem „zügigen und fairen Verfahren" (Artikel 4 Nummer 5 in Verbindung mit Artikel 39 PIPA) ([171]). Der Datenverantwortliche kann sich durch den Nachweis des fehlenden Verschuldens („Vorsatz" oder Fahrlässigkeit) exkulpieren. Wenn die betroffene Person durch Verlust, Diebstahl, Verbreitung, Fälschung, Veränderung oder Beschädigung ihrer personenbezogenen Daten einen Schaden erleidet, kann das Gericht unter Berücksichtigung einer Reihe von Faktoren eine Entschädigung bis zum Dreifachen des tatsächlichen Schadens festsetzen (Artikel 39 Absätze 3 und 4 PIPA). Alternativ kann die betroffene Person einen „angemessenen Betrag" als Entschädigung verlangen, der 3 Millionen Won nicht übersteigt (Artikel 39-2 Absätze 1 und 2 PIPA). Darüber hinaus kann nach dem Zivilgesetz von jeder Person Schadenersatz verlangt werden, „die einer anderen Person durch eine rechtswidrige Handlung vorsätzlich oder fahrlässig einen Schaden zufügt", ([172]) oder von einer Person, „die eine andere Person, ihre Freiheit oder ihren Ruhm verletzt oder einer anderen Person ein seelisches Leid zugefügt hat" ([173]). Eine solche deliktische Haftung aufgrund der Verletzung von Datenschutzvorschriften wurde vom Obersten Gerichtshof bestätigt ([174]). Wurde der Schaden durch rechtswidriges Handeln einer Behörde verursacht, kann darüber hinaus ein Anspruch auf Entschädigung nach dem Gesetz über staatlichen Schadenersatz geltend gemacht werden ([175]). Ein Anspruch nach dem Gesetz über staatlichen Schadenersatz kann bei einem speziellen „Schadenersatzrat" (Compensation Council) oder direkt vor den koreanischen Gerichten erhoben werden ([176]). Die Haftung des Staates deckt auch immaterielle Schaden (z. B. seelisches Leid) ab ([177]). Handelt es sich bei dem Opfer um einen Ausländer, findet das Gesetz über staatlichen Schadenersatz Anwendung, sofern das Herkunftsland koreanischen Staatsangehörigen ebenfalls staatlichen Schadenersatz gewährleistet ([178]).

(136) Viertens hat der Oberste Gerichtshof anerkannt, dass Einzelpersonen das Recht haben, Unterlassungsansprüche geltend zu machen, wenn ihre verfassungsmäßigen Rechte, einschließlich des Rechts auf den Schutz personenbezogener Daten, verletzt werden ([179]). In diesem Zusammenhang kann ein Gericht beispielsweise anordnen, dass die Datenverantwortlichen eine rechtswidrige Tätigkeit aussetzen oder einstellen. Darüber hinaus können Datenschutzrechte, einschließlich der durch das PIPA geschützten Rechte, durch zivilrechtliche Klagen durchgesetzt werden. Diese horizontale Anwendung des verfassungsrechtlichen Schutzes der Privatsphäre auf die Beziehungen zwischen privaten Parteien wurde vom Obersten Gerichtshof anerkannt ([180]).

([170]) Es handelt sich dabei um Verbraucherverbände oder gemeinnützige Nichtregierungsorganisationen mit einer bestimmten Mitgliederzahl, deren erklärtes Ziel der Datenschutz ist (im letzteren Fall allerdings mit der zusätzlichen Bedingung, dass mindestens 100 betroffene Personen, die von der gleichen (Art von) Rechtsverletzung betroffen sind, einen Antrag auf Einreichung einer Sammelklage eingereicht haben). Siehe Artikel 51 PIPA.

([171]) In den Artikeln 43 bis 43-3 des Kreditdatengesetzes ist auch die Pflicht zum Ersatz von Schäden festgelegt, die sich aus Verstößen gegen dieses Gesetz ergeben.

([172]) Artikel 750 des Zivilgesetzes.

([173]) Artikel 751 Absatz 1 des Zivilgesetzes.

([174]) Siehe z. B. die Entscheidung des Obersten Gerichtshofs vom 30. Mai 2018, 2015Da251539, 251546, 251553, 251560, 251577. Darüber hinaus bestätigte der Oberste Gerichtshof, dass Verletzungen des Schutzes personenbezogener Daten zu einem Schadenersatzanspruch nach dem Zivilgesetz führen können, siehe Entscheidung des Obersten Gerichtshofs vom 26. Dezember 2012, 2011Da59834, 59858, 59841 (englische Zusammenfassung abrufbar unter http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). In diesem Fall stellte der Oberste Gerichtshof klar, dass bei der Beurteilung der Frage, ob eine Person eine seelische Belastung erlitten hat, die als ersatzfähiger Schaden anzusehen ist, mehrere Faktoren zu berücksichtigen sind, wie die Art und die Merkmale der durchgesickerten Daten, die Identifizierbarkeit der Person aufgrund der Verletzung, die Möglichkeit des Zugriffs auf die Daten durch Dritte, das Ausmaß der Verbreitung der personenbezogenen Daten, die Frage, ob dies zu zusätzlichen Verletzungen der Rechte des Einzelnen geführt hat, die Art und Weise, wie die personenbezogenen Daten verwaltet und geschützt wurden, usw.

([175]) Auf der Grundlage des Gesetzes über staatlichen Schadenersatz können sie Anspruch auf Schadenersatz für Schäden erheben, die ihnen öffentliche Bedienstete unter Verstoß gegen das Gesetz bei der Ausübung ihres Amtes zugefügt haben (Artikel 2 Absatz 1 des Gesetzes).

([176]) Artikel 9 und 12 des Gesetzes über staatlichen Schadenersatz. Mit dem Gesetz wurden entsprechende Bezirksräte eingerichtet (unter dem Vorsitz des stellvertretenden Staatsanwalts der entsprechenden Staatsanwaltschaft) sowie ein Zentralrat (unter dem Vorsitz des stellvertretenden Justizministers) und ein Sonderrat (unter dem Vorsitz des stellvertretenden Verteidigungsministers), in dessen Zuständigkeit Schadenersatzansprüche für Schäden fallen, die durch militärisches Personal oder Zivilbeschäftigte des Militärs verursacht wurden. Grundsätzlich werden Schadenersatzansprüche von den Bezirksräten bearbeitet, die einen Fall unter bestimmten Umständen an den Zentral- bzw. Sonderrat verweisen müssen, z. B. wenn der Schadenersatz einen bestimmten Betrag übersteigt oder wenn die betroffene Person eine erneute Beratung beantragt. Die Mitglieder aller Räte werden vom Justizminister ernannt (es handelt sich z. B. um öffentliche Bedienstete des Justizministeriums, Justizbeamten, Rechtsanwälte und Experten für staatlichen Schadenersatz) und sie unterliegen besonderen Vorschriften über Interessenkonflikte (siehe Artikel 7 des Durchführungserlassen zum Gesetz über staatlichen Schadenersatz).

([177]) Siehe Artikel 8 des Gesetzes über staatlichen Schadenersatz (der auf das Zivilgesetz verweist) sowie Artikel 751 des Zivilgesetzes.

([178]) Artikel 7 des Gesetzes über staatlichen Schadenersatz.

([179]) Entscheidung des Obersten Gerichtshofs vom 12. April 1996, 93Da40614 und Entscheidung vom 2. September 2011, 2008Da42430 (englische Zusammenfassung abrufbar unter https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Siehe z. B. die Entscheidung des Obersten Gerichtshofs vom 2. September 2011, 2008Da42430, (englische Zusammenfassung abrufbar unter https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Schließlich können Einzelpersonen gemäß der Strafprozessordnung (Artikel 223) bei einem Staatsanwalt oder einem Beamten der Kriminalpolizei einen Strafantrag stellen ([181]).

(138) Das koreanische System bietet daher verschiedene Möglichkeiten, einen Rechtsbehelf einzulegen, angefangen bei leicht zugänglichen, kostengünstigen Möglichkeiten (z. B. durch Kontaktaufnahme mit dem Datenschutz-Callcenter oder durch (kollektive) Schlichtung) bis hin zu verwaltungsrechtlichen Schritten (vor der PIPC) und gerichtlichen Schritten, wobei auch die Möglichkeit besteht, Schadenersatz zu fordern.

3. ZUGANG ZU UND VERWENDUNG VON AUS DER EUROPÄISCHEN UNION ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IN DER REPUBLIK KOREA

(139) Die Kommission hat auch die Einschränkungen und Garantien geprüft, einschließlich der Kontrollmechanismen und der Rechtsbehelfe für den Einzelnen, die nach koreanischem Recht in Bezug auf die Erhebung und nachfolgende Verwendung personenbezogener Daten durch koreanische Behörden, die im öffentlichen Interesse an Datenverantwortliche in Korea übermittelt wurden, insbesondere zur Strafverfolgung und zur nationalen Sicherheit (im Folgenden „staatlicher Zugriff"), verfügbar sind. In diesem Zusammenhang hat die koreanische Regierung der Kommission offizielle Erklärungen, Zusicherungen und Pflichten zukommen lassen, die auf höchster Minister- und Behördenebene unterzeichnet wurden und in Anhang II dieses Beschlusses enthalten sind.

(140) Bei der Beurteilung der Frage, ob die Bedingungen für den staatlichen Zugriff auf Daten, die gemäß diesem Beschluss an die Republik Korea übermittelt werden, das Kriterium der „wesentlichen Gleichwertigkeit" nach Artikel 45 Absatz 1 der Verordnung (EU) 2016/679 in der Auslegung des Gerichtshofs der Europäischen Union im Lichte der Charta der Grundrechte erfüllen, hat die Kommission insbesondere die folgenden Kriterien berücksichtigt.

(141) Erstens muss jede Einschränkung des Rechts auf den Schutz personenbezogener Daten gesetzlich vorgesehen sein, und die gesetzliche Grundlage für den Eingriff in dieses Recht muss selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts festlegen ([182]).

(142) Zweitens: Um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten nur insoweit gelten dürfen, als dies in einer demokratischen Gesellschaft zur Verwirklichung spezifischer Ziele von allgemeinem Interesse, die den von der Union anerkannten Zielen gleichwertig sind, unbedingt erforderlich ist, muss die Rechtsvorschrift des betreffenden Drittlands, nach der der Eingriff zulässig ist, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, sodass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen ([183]). In der Rechtsvorschrift muss insbesondere angegeben sein, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf; ([184]) ferner muss die Erfüllung dieser Anforderungen einer unabhängigen Aufsicht unterliegen ([185]).

(143) Drittens müssen diese Rechtsvorschriften und ihre Anforderungen nach dem nationalen Recht rechtsverbindlich sein. Dies betrifft in erster Linie die Behörden des betreffenden Drittlandes, aber diese rechtlichen Anforderungen müssen auch vor Gericht gegen diese Behörden durchsetzbar sein ([186]). Insbesondere müssen betroffene Personen die Möglichkeit haben, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken ([187]).

3.1 **Allgemeiner Rechtsrahmen**

(144) Die Einschränkungen und Garantien für die Erhebung und anschließende Verwendung personenbezogener Daten durch koreanische Behörden ergeben sich aus dem übergeordneten verfassungsrechtlichen Rahmen, den speziellen Gesetzen, in denen ihre Tätigkeiten in den Bereichen Strafverfolgung und nationale Sicherheit geregelt sind, sowie aus den Vorschriften, die speziell für die Verarbeitung personenbezogener Daten gelten.

([181]) Wie in Erwägungsgrund (127) erläutert, kann die missbräuchliche Verwendung von Daten eine Straftat nach dem Strafgesetzbuch darstellen.

([182]) Siehe Schrems II, Rn. 174 und 175 und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch Rechtssache C-623/17, Privacy International, EU:C:2020:790, Rn. 65 sowie die verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., EU:C:2020:791, Rn. 175.

([183]) Siehe Schrems II, Rn. 176 und 181 und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssachen Privacy International, Rn. 68 und La Quadrature du Net u. a., Rn. 132.

([184]) Siehe Schrems II, Rn. 176. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssachen Privacy International, Rn. 68 und La Quadrature du Net u. a., Rn. 132.

([185]) Siehe Schrems II, Rn. 179.

([186]) Siehe Schrems II, Rn. 181 und 182.

([187]) Siehe Schrems I, Rn. 95 und Schrems II, Rn. 194. In diesem Zusammenhang hat der EuGH insbesondere betont, dass die Einhaltung von Artikel 47 der Charta der Grundrechte, der das Recht auf einen wirksamen Rechtsbehelf vor einem unabhängigen und unparteiischen Gericht garantiert, „für das in der Union erforderliche Schutzniveau maßgebend ist und [von der] Kommission [festgestellt werden] muss, bevor sie einen Angemessenheitsbeschluss im Sinne von Art. 45 Abs. 1 der [Verordnung (EU) 2016/679] erlässt" (Schrems II, Rn. 186).

(145) Erstens unterliegt der Zugriff auf personenbezogene Daten durch koreanische Behörden den allgemeinen Grundsätzen der Rechtmäßigkeit, Erforderlichkeit und Verhältnismäßigkeit, die sich aus der koreanischen Verfassung ergeben ([188]). Insbesondere ist die Einschränkung der Grundrechte und -freiheiten (einschließlich des Rechts auf Schutz der Privatsphäre und des Briefgeheimnisses) ([189]) nur per Gesetz und nur dann zulässig, wenn dies für die nationale Sicherheit oder zur Aufrechterhaltung der öffentlichen Ordnung für das Gemeinwohl erforderlich ist. Solche Einschränkungen dürfen den Wesensgehalt des betreffenden Rechts oder der betreffenden Freiheit nicht beeinträchtigen. Speziell für Durchsuchungen und Beschlagnahmen ist in der Verfassung vorgesehen, dass sie nur nach Maßgabe der Gesetze, auf der Grundlage einer richterlichen Anordnung und unter Einhaltung eines ordnungsgemäßen Verfahrens durchgeführt werden dürfen ([190]). Schließlich kann sich der Einzelne vor dem Verfassungsgericht auf seine Rechte und Freiheiten berufen, wenn er glaubt, dass sie von Behörden bei der Ausübung ihrer Befugnisse verletzt worden sind ([191]). Ebenso haben Personen, die durch eine rechtswidrige Handlung, die ein öffentlicher Bediensteter in Ausübung seiner Dienstpflichten begangen hat, geschädigt wurden, Anspruch auf einen angemessenen Schadenersatz ([192]).

(146) Zweitens spiegeln sich, wie in den Abschnitten 3.2.1 und 3.3.1 ausführlicher beschrieben, die in Erwägungsgrund (145) genannten allgemeinen Grundsätze auch in den speziellen Gesetzen wider, in denen die Befugnisse der Strafverfolgungs- und nationalen Sicherheitsbehörden geregelt sind. In Bezug auf strafrechtliche Ermittlungen ist beispielsweise in der Strafprozessordnung (Criminal Procedure Act –CPA) festgelegt, dass Zwangsmaßnahmen nur dann ergriffen werden dürfen, wenn dies in der CPA ausdrücklich vorgesehen ist und nur soweit, wie es zur Erreichung des Ermittlungszwecks erforderlich ist ([193]). Ebenso ist nach Artikel 3 des Gesetzes zum Schutz der Privatsphäre in der Kommunikation (Communications Privacy Protection Act – CPPA) der Zugang zu privater Kommunikation nur auf gesetzlicher Grundlage und vorbehaltlich der darin festgelegten Einschränkungen und Garantien zulässig. Im Bereich der nationalen Sicherheit heißt es im Gesetz über den nationalen Nachrichtendienst (im Folgenden „NIS-Gesetz"), dass jeder Zugang zu Kommunikations- oder Standortdaten gesetzeskonform sein muss und dass Machtmissbrauch und Gesetzesverstöße strafrechtliche Sanktionen nach sich ziehen ([194]).

(147) Drittens unterliegt die Verarbeitung personenbezogener Daten durch Behörden, auch für die Zwecke der Strafverfolgung und der nationalen Sicherheit, den Datenschutzbestimmungen des PIPA ([195]). Nach Artikel 5 Absatz 1 des PIPA sind die Behörden grundsätzlich verpflichtet, Strategien auszuarbeiten, um den „Missbrauch personenbezogener Daten, indiskrete Überwachung und Verfolgung usw. zu verhindern und die Achtung der Menschenwürde und der Privatsphäre des Einzelnen zu verbessern." Darüber hinaus muss jeder Datenverantwortliche personenbezogene Daten so verarbeiten, dass die Wahrscheinlichkeit eines Eingriffs in die Privatsphäre der betroffenen Person möglichst gering ist (Artikel 3 Absatz 6 PIPA).

(148) Für die Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken gelten alle Anforderungen des PIPA, die in Abschnitt 2 ausführlich beschrieben wurden. Dazu gehören die Grundprinzipien (wie Rechtmäßigkeit und Verarbeitung nach Treu und Glauben, Zweckbindung, Richtigkeit, Datenminimierung, Speicherbegrenzung, Sicherheit und Transparenz), Pflichten (z. B. in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten und sensible Daten) und Rechte (auf Auskunft, Berichtigung, Löschung und Aussetzung der Verarbeitung).

(149) Die Verarbeitung personenbezogener Daten zu Zwecken der nationalen Sicherheit unterliegt im Rahmen des PIPA zwar einer begrenzten Anzahl von Bestimmungen, doch gelten die Grundprinzipien sowie die Vorschriften über Aufsicht, Durchsetzung und Rechtsbehelfe ([196]). In den Artikeln 3 und 4 PIPA sind die allgemeinen Datenschutzgrundsätze (Rechtmäßigkeit und Verarbeitung nach Treu und Glauben, Zweckbindung, Richtigkeit, Datenminimierung, Sicherheit und Transparenz) sowie die Rechte des Einzelnen (Recht auf Information, Auskunftsrecht, Recht auf Berichtigung, Löschung und Aussetzung der Verarbeitung) festgelegt ([197]). Nach Artikel 4 Absatz 5 PIPA haben betroffene Personen außerdem das Recht, für Schäden, die sich aus der Verarbeitung der personenbezogenen Daten ergeben, in einem zügigen und fairen Verfahren eine angemessene Wiedergutmachung

([188]) Siehe Anhang II Abschnitt 1.1.

([189]) Artikel 37 Absatz 2 der Verfassung.

([190]) Artikel 16 und Artikel 12 Absatz 3 der Verfassung. In Artikel 12 Absatz 3 der Verfassung sind darüber hinaus die außergewöhnlichen Umstände festgelegt, unter denen Durchsuchungen oder Beschlagnahmen ohne richterliche Anordnung durchgeführt werden können (wobei eine nachträgliche Anordnung nach wie vor erforderlich ist), d. h. bei flagranten Delikten oder bei Straftaten, die mit einer Freiheitsstrafe von mindestens drei Jahren bedroht sind, wenn die Gefahr besteht, dass Beweise vernichtet werden oder der Verdächtige verschwindet.

([191]) Artikel 68 Absatz 1 des Gesetzes über das Verfassungsgericht.

([192]) Artikel 29 Absatz 1 der Verfassung.

([193]) Artikel 199 Absatz 1 CPA. Im Allgemeinen müssen die Behörden bei der Ausübung ihrer Befugnisse nach dem CPA die Grundrechte von Verdächtigen und anderen betroffenen Personen achten (Artikel 198 Absatz 2 CPA).

([194]) Artikel 14 des NIS-Gesetzes.

([195]) Siehe Anhang II Abschnitt 1.2.

([196]) Artikel 58 Absatz 1 Nummer 2 PIPA. Siehe auch Abschnitt 6 der Bekanntmachung Nr. 2021-5 (Anhang I). Diese Ausnahme von gewissen Bestimmungen des PIPA gilt nur, wenn personenbezogene Daten „für die Zwecke der nationalen Sicherheit" verarbeitet werden. Sobald die nationale Sicherheitslage, die die Datenverarbeitung rechtfertigt, beendet ist, kann die Ausnahme nicht mehr angewandt werden und es gelten alle Anforderungen des PIPA.

([197]) Diese Rechte dürfen nur dann eingeschränkt werden, wenn dies gesetzlich vorgesehen ist, und zwar in dem Umfang und für die Dauer, die erforderlich und verhältnismäßig sind, um ein wichtiges Ziel des öffentlichen Interesses zu schützen, oder wenn die Gewährung des Rechts zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde. Siehe Abschnitt 6 der Bekanntmachung Nr. 2021-5.

zu erhalten. Ergänzt wird dies durch spezifischere Pflichten, personenbezogene Daten nur in dem zur Erreichung des beabsichtigten Zwecks erforderlichen Mindestmaß und für die Mindestdauer zu verarbeiten, die erforderlichen Maßnahmen zur Gewährleistung einer sicheren Datenverwaltung und einer angemessenen Verarbeitung zu ergreifen (z. B. technische, organisatorische und physische Sicherheitsvorkehrungen) sowie Maßnahmen zur angemessenen Behandlung individueller Beschwerden zu ergreifen ([198]). Schließlich gelten die allgemeinen Grundsätze der Rechtmäßigkeit, Erforderlichkeit und Verhältnismäßigkeit nach der koreanischen Verfassung (siehe Erwägungsgrund (145)) auch für die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit.

(150) Diese allgemeinen Einschränkungen und Garantien können von Einzelpersonen vor unabhängigen Aufsichtsgremien (z. B. der PIPC und/oder der Nationalen Menschenrechtskommission, siehe die Erwägungsgründe (177)-(178)) und vor Gerichten (siehe die Erwägungsgründe (179)-(183)) geltend gemacht werden, um einen Rechtsbehelfe einzulegen.

3.2 **Zugriff und Verwendung durch koreanische Behörden für Strafverfolgungszwecke**

(151) In den Rechtsvorschriften der Republik Korea sind neben einer Reihe von Einschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten für die Zwecke der Strafverfolgung Aufsichtsmechanismen und Rechtsbehelfe vorgesehen;, die den in den Erwägungsgründen (141) bis (143) dieses Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Bewertung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten.

3.2.1 *Rechtsgrundlagen, Einschränkungen und Garantien*

(152) Von koreanischen Datenverantwortlichen verarbeitete personenbezogene Daten, die nach diesem Beschluss ([199]) aus der Union übermittelt würden, können von koreanischen Behörden zu Strafverfolgungszwecken im Rahmen einer Durchsuchung oder Beschlagnahme (auf der Grundlage des CPA), durch den Zugriff auf Kommunikationsdaten (auf der Grundlage des CPPA) oder durch die Einholung von Teilnehmerdaten durch Ersuchen um freiwillige Offenlegung (auf der Grundlage des Gesetzes über Telekommunikationsunternehmen, Telecommunications Business Act – TBA) erhoben werden ([200]).

3.2.1.1 Durchsuchung und Beschlagnahme

(153) Gemäß dem CPA darf eine Durchsuchung oder Beschlagnahme nur erfolgen, wenn eine Person einer Straftat verdächtigt wird, die Durchsuchung oder Beschlagnahme für die Ermittlungen erforderlich ist und ein Zusammenhang zwischen den Ermittlungen und der zu durchsuchenden Person oder dem zu untersuchenden oder zu beschlagnahmenden Gegenstand hergestellt wird ([201]). Darüber hinaus darf eine Durchsuchung oder Beschlagnahme (wie jede Zwangsmaßnahme) nur in dem geringstmöglichen Umfang genehmigt/durchgeführt werden ([202]). Bei Durchsuchungen von Computerfestplatten oder anderen Datenträgern werden grundsätzlich nur die erforderlichen (kopierten oder ausgedruckten) Daten selbst und nicht der gesamte Datenträger beschlagnahmt ([203]). Der Datenträger darf nur dann beschlagnahmt werden, wenn es als im Wesentlichen unmöglich erachtet wird, die erforderlichen Daten getrennt auszudrucken oder zu kopieren, oder wenn es als im Wesentlichen nicht praktikabel erachtet wird, den Zweck der Durchsuchung auf andere Weise zu erfüllen ([204]). Im CPA werden daher klare und präzise Regeln für den Umfang und die Anwendung dieser Maßnahmen festgelegt, um sicherzustellen, dass der Eingriff in die Rechte des Einzelnen im Falle einer Durchsuchung oder Beschlagnahme das Maß des Erforderlichen für eine bestimmte strafrechtliche Ermittlung nicht überschreitet und in einem angemessenen Verhältnis zum verfolgten Zweck steht.

([198]) Artikel 58 Absatz 4 PIPA.

([199]) Siehe Anhang II Abschnitt 2.1. In der offiziellen Erklärung der koreanischen Regierung (Anhang II Abschnitt 2.1) wird auch auf die Möglichkeit verwiesen, Daten über Finanztransaktionen zum Zwecke der Verhinderung von Geldwäsche und Terrorismusfinanzierung auf der Grundlage des Gesetzes über die Meldung und Nutzung genau bestimmter Finanztransaktionsdaten (Act on Reporting and Using Specified Financial Transaction Information – ARUSFTI) zu erheben. Gemäß dem ARUSFTI sind jedoch nur die Datenverantwortlichen zur Offenlegung verpflichtet, die personenbezogene Kreditdaten gemäß des Kreditdatengesetzes verarbeiten und der Aufsicht der Finanzdienstleistungskommission unterliegen (siehe Erwägungsgrund (13)). Da die Verarbeitung personenbezogener Kreditdaten durch diese Datenverantwortlichen vom Anwendungsbereich dieses Beschlusses ausgenommen ist, ist das ARUSFTI für die vorliegende Prüfung nicht relevant.

([200]) In Artikel 3 CPPA wird auch das Militärgerichtsgesetz als mögliche Rechtsgrundlage für die Erhebung von Kommunikationsdaten genannt. Im Militärgerichtsgesetz ist jedoch die Erhebung von Daten über militärisches Personal geregelt und es ist nur in einigen wenigen Fällen auf Zivilisten anwendbar (beispielsweise kann ein Militärgericht angerufen werden, wenn militärisches Personal und Zivilisten gemeinsam eine Straftat begehen oder wenn eine Straftat gegen das Militär begangen wird, siehe Artikel 2 des Militärgerichtsgesetzes). In jedem Fall enthält es allgemeine Bestimmungen für Durchsuchungen und Beschlagnahmen, die denen des CPA ähneln (siehe z. B. Artikel 146 bis 149 und 153 bis156 des Militärgerichtsgesetzes) und in denen beispielsweise vorgesehen ist, dass Post nur dann beschlagnahmt werden darf, wenn dies für eine Untersuchung erforderlich ist und auf der Grundlage einer Anordnung des Militärgerichts. Für die Erhebung der Daten elektronischer Kommunikation gelten nach diesem Gesetz die Einschränkungen und Garantien des CPPA. Siehe Anhang II Abschnitt 2.2.2 und Fußnote 50.

([201]) Artikel 215 Absätze 1 und 2 CPA. Siehe auch Artikel 106 Absatz 1, Artikel 107 und 109 CPA, wonach die Gerichte Durchsuchungen und Beschlagnahmen durchführen können, solange die betroffenen Gegenstände oder Personen als mit einem bestimmten Fall verbunden angesehen werden. Siehe Anhang II Abschnitt 2.2.1.2.

([202]) Artikel 199 Absatz 1 CPA.

([203]) Artikel 106 Absatz 3 CPA.

([204]) Artikel 106 Absatz 3 CPA.

(154) Im Hinblick auf die Verfahrensgarantien ist nach dem CPA für die Durchführung einer Durchsuchung oder Beschlagnahme eine richterliche Anordnung erforderlich ([205]). Eine Durchsuchung oder Beschlagnahme ohne richterliche Anordnung ist nur ausnahmsweise zulässig, nämlich in dringenden Fällen, ([206]) an Ort und Stelle bei der Festnahme oder Verhaftung eines Tatverdächtigen ([207]) oder wenn ein Gegenstand von einem Tatverdächtigen oder einer dritten Person (bei personenbezogenen Daten von der betroffenen Person selbst) entsorgt oder freiwillig übergeben wird ([208]). Unzulässige Durchsuchungen und Beschlagnahmen werden strafrechtlich geahndet, ([209]) und alle Beweise, die unter Verstoß gegen das CPA erhoben wurden, gelten als unzulässig ([210]). Schließlich müssen die betroffenen Personen stets unverzüglich über eine Durchsuchung oder Beschlagnahme (einschließlich der Beschlagnahme ihrer Daten) unterrichtet werden, ([211]) was wiederum die Ausübung ihrer materiellen Rechte und ihres Rechts auf Rechtsbehelf ermöglicht (siehe insbesondere die Möglichkeit, die Vollstreckung eines Beschlagnahmebeschlusses anzufechten, vgl. Erwägungsgrund (180)).

3.2.1.2 Zugriff auf Kommunikationsdaten

(155) Auf der Grundlage des CPPA können die koreanischen Strafverfolgungsbehörden zwei Arten von Maßnahmen ergreifen: ([212]) zum einen die Erhebung von „Kommunikationsbestätigungsdaten" ([213]), die das Datum des Telekommunikationsvorgangs, seine Anfangs- und Endzeit, die Zahl der ausgehenden und eingehenden Anrufe sowie die Rufnummer der anderen Person, die Häufigkeit der Nutzung, und Protokolldateien über die Nutzung von Telekommunikationsdiensten und Standortdaten (z. B. von den Sendemasten, die die Signale empfangen) umfassen und zum anderen „kommunikationsbeschränkende Maßnahmen", zu denen sowohl die Erhebung von Inhaltsdaten herkömmlicher Postsendungen als auch die direkte Überwachung des Inhalts eines Telekommunikationsvorgangs gehören ([214]).

(156) Auf Kommunikationsbestätigungsdaten darf nur zugegriffen werden, wenn dies zur Durchführung strafrechtlicher Ermittlungen oder zur Vollstreckung einer Strafe ([215]) auf der Grundlage einer gerichtlichen Anordnung erforderlich ist ([216]). In diesem Zusammenhang ist es nach dem CPPA erforderlich, dass sowohl im Antrag auf die Anordnung (z. B. über die Gründe für den Antrag, die Beziehung zur Zielperson bzw. zum Teilnehmer und die erforderlichen Daten) als auch in der Anordnung selbst (z. B. über das Ziel, den Zweck und den Umfang der Maßnahme) detaillierte Angaben gemacht werden ([217]). Eine Erhebung ohne richterliche Anordnung ist nur dann zulässig, wenn aus Gründen der Dringlichkeit keine richterliche Genehmigung eingeholt werden kann; in

([205]) Artikel 215 Absätze 1 und 2 CPA, Artikel 113 CPA. Bei der Beantragung einer solchen Anordnung muss die betreffende Behörde Unterlagen vorlegen, aus denen hervorgeht, warum eine Person einer Straftat verdächtigt wird, dass die Durchsuchung, Inspektion oder Beschlagnahme erforderlich ist und dass die zu beschlagnahmenden Gegenstände existieren (Artikel 108 Absatz 1 der Strafprozessordnung). In der Anordnung sind unter anderem der Name des Tatverdächtigen und die Bezeichnung der Straftat, der Ort, die Person oder die Gegenstände, die durchsucht werden sollen, oder die Gegenstände, die beschlagnahmt werden sollen, das Ausstellungsdatum und die Geltungsdauer zu nennen (Artikel 114 Absatz 1 in Verbindung mit Artikel 219 CPA). Siehe Anhang II Abschnitt 2.2.1.2.

([206]) Dazu gehören Situationen, in denen es aufgrund der Dringlichkeit am Tatort unmöglich ist, eine Anordnung einzuholen (Artikel 216 Absatz 3 CPA); diese muss anschließend jedoch unverzüglich nachgeholt werden (Artikel 216 Absatz 3 CPA).

([207]) Artikel 216 Absätze 1 und 2 CPA.

([208]) Artikel 218 CPA. Wie in Anhang II Abschnitt 2.2.1.2 erläutert, werden freiwillig übergebene Gegenstände nur dann als Beweismaterial in einem Gerichtsverfahren zugelassen, wenn kein begründeter Zweifel an der Freiwilligkeit der Übergabe besteht, was der Staatsanwalt nachweisen muss.

([209]) Artikel 321 des Strafgesetzes.

([210]) Artikel 308-2 CPA. Die betroffene Person (und ihr Rechtsbeistand) dürfen ferner bei der Vollstreckung einer angeordneten Durchsuchung oder Beschlagnahme anwesend sein, sodass sie zum Zeitpunkt der Vollstreckung auch Widerspruch erheben können (Artikel 121 und 219 CPA).

([211]) Artikel 121 und 122 CPA (in Bezug auf die Durchsuchung) und Artikel 219 in Verbindung mit Artikel 106 Absatz 4 CPA (in Bezug auf die Beschlagnahme).

([212]) Siehe auch Anhang II Abschnitt 2.2.2.1. Solche Maßnahmen können mit der obligatorischen Unterstützung von Telekommunikationsdiensteanbieter ergriffen werden, wenn diese eine schriftliche Genehmigung von einem Gericht erhalten haben (Artikel 9 Absatz 2 CPPA), die von den Diensteanbietern aufbewahrt werden muss (Artikel 15-2 CPPA und Artikel 12 des CPPA-Durchführungserlasses). Telekommunikationsdiensteanbieter können die Zusammenarbeit verweigern, wenn die in der schriftlichen Genehmigung des Gerichts angegebenen Daten der betroffenen Person (z. B. die Telefonnummer) unrichtig sind, und sie dürfen unter keinen Umständen die für die Telekommunikation verwendeten Passwörter offenlegen (Artikel 9 Absatz 4 CPPA).

([213]) Artikel 2 Absatz 11 CPPA.

([214]) Siehe Artikel 2 Absatz 6 CPPA, der sich auf „Zensur" bezieht (Öffnen von Post ohne Einwilligung des Betroffenen oder die Aneignung von Wissen über ihren Inhalt, die Aufzeichnung oder die Vorenthaltung ihres Inhalts auf anderem Wege) und Artikel 2 Absatz 7 CPPA, der sich auf „Abhören" bezieht (Erfassung oder Aufzeichnung des Inhalts von Telekommunikation durch Abhören oder Mitlesen der Geräusche, Wörter, Symbole oder Bilder eines Kommunikationsvorgangs mittels elektronischer und mechanischer Geräte ohne Einwilligung des Betroffenen oder die Störung der Übertragung und des Empfangs).

([215]) Artikel 13 Absatz 1 CPPA. Siehe auch Anhang II Abschnitt 2.2.2.3. Darüber hinaus dürfen Echtzeit-Standortverfolgungsdaten und Kommunikationsbestätigungsdaten, die eine bestimmte Basisstation betreffen, nur für die Untersuchung schwerer Straftaten oder in Fällen erhoben werden, in denen es sonst schwierig wäre, die Ausführung einer Straftat zu verhindern oder Beweise zu sammeln (Artikel 13 Absatz 2 CPPA). Dies spiegelt die Notwendigkeit wider, im Einklang mit dem Grundsatz der Verhältnismäßigkeit zusätzliche Garantien für Maßnahmen vorzusehen, die besonders stark in die Privatsphäre eingreifen.

([216]) Artikel 13 und 6 CPPA.

([217]) Siehe Artikel 13 Absätze 3 und 9 in Verbindung mit Artikel 6 Absätze 4 und 6 CPPA.

diesem Fall muss die Anordnung eingeholt und der Telekommunikationsdiensteanbieter unmittelbar nach der Anforderung der Daten informiert werden ([218]). Wenn das Gericht die nachträgliche Genehmigung verweigert, müssen die erhobenen Daten vernichtet werden ([219]).

(157) Als zusätzliche Garantien in Bezug auf die Erhebung von Kommunikationsbestätigungsdaten werden im CPPA besondere Anforderungen an die Aufzeichnung und Transparenz gestellt ([220]). So müssen sowohl die Strafverfolgungsbehörden ([221]) als auch die Telekommunikationsanbieter ([222]) Aufzeichnungen über die gestellten Anträge und die Weitergabe von Daten führen. Darüber hinaus müssen die Strafverfolgungsbehörden die betroffenen Personen grundsätzlich über die Erhebung ihrer Kommunikationsbestätigungsdaten unterrichten ([223]). Eine solche Unterrichtung kann nur in Ausnahmefällen auf der Grundlage einer Genehmigung des Leiters der zuständigen Bezirksstaatsanwaltschaft aufgeschoben werden ([224]). Die Genehmigung darf nur erteilt werden, wenn die Unterrichtung 1) die Gefährdung der nationalen Sicherheit und der öffentlichen Sicherheit und Ordnung, 2) Tod oder Körperverletzung, 3) die Behinderung eines fairen Gerichtsverfahrens (z. B. durch die Vernichtung von Beweismaterial oder die Bedrohung von Zeugen) oder 4) die Verleumdung des Verdächtigen, der Opfer oder anderer mit dem Fall in Verbindung stehender Personen oder die Verletzung ihrer Privatsphäre nach sich ziehen kann. In diesen Fällen muss die Unterrichtung innerhalb von 30 Tagen erfolgen, sobald die Gründe für den Aufschub nicht mehr bestehen ([225]). Die betroffenen Personen haben das Recht, bei der Unterrichtung Auskunft über die Gründe für die Erhebung ihrer Daten zu erhalten ([226]).

(158) Strengere Regeln gelten für kommunikationsbeschränkende Maßnahmen, die nur dann angewandt werden dürfen, wenn wesentliche Gründe für den Verdacht vorliegen, dass bestimmte im CPPA ausdrücklich aufgeführte schwere Straftaten geplant sind, begangen werden oder begangen wurden ([227]). Außerdem dürfen kommunikationsbeschränkende Maßnahmen nur als letztes Mittel ergriffen werden, wenn es schwierig ist, auf andere Weise die Begehung einer Straftat zu verhindern, einen Straftäter festzunehmen oder Beweise zu sammeln ([228]). Damit die Verletzung der Privatsphäre bei der Kommunikation so gering wie möglich ist, müssen diese Maßnahmen unverzüglich eingestellt werden, sobald die Fortsetzung des Zugriffs nicht mehr erforderlich ist ([229]). Daten, die auf unrechtmäßige Weise durch kommunikationsbeschränkende Maßnahmen erhoben wurden, werden nicht als Beweismaterial in Gerichts- oder Disziplinarverfahren zugelassen ([230]).

(159) Im Hinblick auf die Verfahrensgarantien ist für die Durchführung kommunikationsbeschränkender Maßnahmen nach dem CPPA eine richterliche Anordnung erforderlich ([231]). Auch in diesem Fall sind nach dem CPPA der Antrag auf Erlass einer richterlichen Anordnung und die Anordnung selbst mit detaillierten Informationen zu versehen, ([232]) einschließlich der Begründung des Antrags und der zu erhebenden Kommunikationsdaten (die sich auf den Verdächtigen beziehen müssen, gegen den ermittelt wird.) ([233]) Solche Maßnahmen dürfen nur dann ohne

([218]) Artikel 13 Absatz 2 CPPA.
([219]) Artikel 13 Absatz 3 CPPA.
([220]) Siehe Anhang II Abschnitt 2.2.2.3.
([221]) Artikel 13 Absätze 5 und 6 CPPA.
([222]) Artikel 13 Absatz 7 CPPA. Darüber hinaus müssen die Telekommunikationsanbieter dem Ministerium für Wissenschaft und IKT zweimal jährlich einen Bericht über die Offenlegung von Kommunikationsbestätigungsdaten erstatten.
([223]) Siehe Artikel 13-3 Absatz 7 CPPA in Verbindung mit Artikel 9-2 CPPA. Insbesondere müssen Einzelpersonen innerhalb von 30 Tagen nach einer Entscheidung über die (Nicht-)Strafverfolgung oder innerhalb von 30 Tagen nach einem Jahr nach einer Entscheidung über die Aussetzung der Anklageerhebung unterrichtet werden (obwohl die Unterrichtung in jedem Fall innerhalb von 30 Tagen nach einem Jahr nach Erhebung der Daten erfolgen muss), siehe Artikel 13-3 Absatz 1 CPPA.
([224]) Artikel 13-3 Absätze 2 bis 3 CPPA.
([225]) Artikel 13-3 Absatz 4 CPPA.
([226]) Artikel 13-3 Absatz 5 CPPA. Auf Antrag der betroffenen Person hat der Staatsanwalt oder der Beamte der Kriminalpolizei innerhalb von 30 Tagen nach Eingang des Antrags die Gründe schriftlich mitzuteilen, es sei denn, es liegt eine der Ausnahmen für einen Aufschub der Unterrichtung vor (Artikel 13-3 Absatz 6 CPPA).
([227]) Zu diesen Straftaten gehören etwa Aufstände, Drogenkriminalität oder Sprengstoffkriminalität sowie Straftaten im Zusammenhang mit der nationalen Sicherheit, den diplomatischen Beziehungen oder Militärstützpunkten und -anlagen, siehe Artikel 5 Absatz 1 CPPA. Siehe auch Anhang II Abschnitt 2.2.2.2.
([228]) Artikel 3 Absatz 2 und Artikel 5 Absatz 1 CPPA.
([229]) Artikel 2 des CPPA-Durchführungserlasses.
([230]) Artikel 4 CPPA.
([231]) Artikel 6 Absätze 1, 2 und 5 bis 6 CPPA.
([232]) In einem Antrag auf Erlass einer Anordnung sind folgende Punkte darzulegen: 1) die wesentlichen Gründe für den (Prima-facie-) Verdacht, dass eine der aufgeführten Straftaten geplant ist, begangen wird oder begangen wurde, sowie etwaige Belege, 2) die kommunikationsbeschränkenden Maßnahmen sowie ihr Ziel, Umfang und Zweck sowie der Durchführungszeitraum und 3) der Ort, an dem die Maßnahmen durchgeführt werden sollen, und die Art und Weise ihrer Durchführung (Artikel 6 Absatz 4 CPPA und Artikel 4 Absatz 1 des CPPA-Durchführungserlasses). In der entsprechenden Anordnung sind die Arten der Maßnahmen sowie ihr Ziel, Umfang und Durchführungszeitraum sowie der Ort und die Art und Weise ihrer Durchführung festzulegen (Artikel 6 Absatz 6 CPPA).
([233]) Ziel einer kommunikationsbeschränkenden Maßnahme müssen bestimmte Postsendungen oder Telekommunikationsnachrichten sein, die der Verdächtige sendet oder empfängt, oder die Postsendungen oder Telekommunikationsnachrichten, die der Verdächtige während eines bestimmten Zeitraums sendet oder empfängt (Artikel 5 Absatz 2 CPPA).

Anordnung ergriffen werden, wenn eine unmittelbare Bedrohung durch die organisierte Kriminalität oder eine andere schwere Straftat, die unmittelbar zum Tod oder zur schweren Körperverletzung führen kann, droht und ein Notfall vorliegt, der die Durchführung des regulären Verfahrens unmöglich macht ([234]). In diesem Fall muss jedoch unmittelbar nach der Maßnahme ein Antrag auf Anordnung gestellt werden ([235]). Kommunikationsbeschränkende Maßnahmen dürfen nur über einen Zeitraum von zwei Monaten durchgeführt werden ([236]) und können nur mit gerichtlicher Genehmigung verlängert werden, wenn die Voraussetzungen für die Durchführung der Maßnahmen weiterhin gegeben sind ([237]). Der verlängerte Zeitraum darf insgesamt ein Jahr bzw. drei Jahre bei bestimmten besonders schweren Straftaten (z. B. Verbrechen in Zusammenhang mit Aufständen, Angriffen aus dem Ausland, der nationalen Sicherheit) nicht überschreiten ([238]).

(160) Wie bei der Erhebung von Kommunikationsbestätigungsdaten sind Telekommunikationsanbieter ([239]) und Strafverfolgungsbehörden ([240]) nach dem CPPA verpflichtet, Aufzeichnungen über die Durchführung von kommunikationsbeschränkenden Maßnahmen zu führen, und es ist eine Unterrichtung der betroffenen Person vorgesehen, die in Ausnahmefällen aufgeschoben werden kann, wenn dies aus wichtigen Gründen des öffentlichen Interesses erforderlich ist ([241]).

(161) Schließlich wird die Nichteinhaltung mehrerer Einschränkungen und Garantien des CPPA (z. B. die Pflicht zur Einholung einer richterlichen Anordnung, zur Führung von Aufzeichnungen und zur Benachrichtigung der betroffenen Person) sowohl im Hinblick auf die Erhebung von Kommunikationsbestätigungsdaten als auch auf den Einsatz von kommunikationsbeschränkenden Maßnahmen strafrechtlich geahndet ([242]).

(162) Die Befugnisse der Strafverfolgungsbehörden zur Erhebung von Kommunikationsdaten auf der Grundlage des CPPA (sowohl der Kommunikationsinhalts- als auch der Kommunikationsbestätigungsdaten) sind daher durch klare und präzise Regeln eingeschränkt und unterliegen einer Reihe von Garantien. Diese Garantien gewährleisten insbesondere die Aufsicht über die Durchführung solcher Maßnahmen, sowohl vorab (durch vorherige gerichtliche Genehmigung) als auch im Nachhinein (durch Aufzeichnungs- und Berichterstattungspflichten), und erleichtern den Zugang des Einzelnen zu wirksamen Rechtsbehelfen (indem sie sicherstellen, dass er über die Erhebung seiner Daten unterrichtet wird).

3.2.1.3 Ersuchen um freiwillige Offenlegung von Teilnehmerdaten

(163) Zusätzlich zu den in den Erwägungsgründen (153)-(162) beschriebenen Zwangsmaßnahmen können die koreanischen Strafverfolgungsbehörden Telekommunikationsanbieter um freiwillige Übermittlung von „Kommunikationsdaten“ zur Unterstützung eines Strafverfahrens, einer Ermittlung oder der Vollstreckung einer Strafe ersuchen (Artikel 83 Absatz 3 TBA). Diese Möglichkeit besteht nur in Bezug auf begrenzte Datensätze, d. h. den Namen, die Melderegisterzahl, die Anschrift und die Telefonnummer von Nutzern, das jeweilige Datum, an dem die Nutzer ihren Vertrag abgeschlossen oder beendet haben, sowie Nutzeridentifikationscodes (d. h. Codes, die zur Identifizierung des rechtmäßigen Nutzers von Computersystemen oder Kommunikationsnetzen verwendet werden) ([243]). Da nur Personen, die direkt Dienste eines koreanischen Telekommunikationsanbieters in Anspruch nehmen, als „Nutzer“ gelten, ([244]) fallen EU-Bürger, deren Daten in die Republik Korea übermittelt wurden, normalerweise nicht in diese Kategorie ([245]).

(164) Für solche freiwilligen Offenlegungen gelten unterschiedliche Einschränkungen, sowohl für die Ausübung der Befugnisse der Strafverfolgungsbehörde als auch für die Antwort des Telekommunikationsanbieters. Generell müssen die Strafverfolgungsbehörden im Einklang mit den verfassungsrechtlichen Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit (Artikel 12 Absatz 1 und Artikel 37 Absatz 2 der Verfassung) handeln, auch wenn sie die freiwillige Offenlegung der Daten anfordern. Darüber hinaus müssen sie das PIPA einhalten,

([234]) Artikel 8 Absatz 1 CPPA. Die Datenerhebung in dringenden Fällen hat jedoch stets gemäß einer „Erklärung über die Dringlichkeit von Zensur- oder Abhörmaßnahmen“ zu erfolgen und die Behörde, die die Erhebung durchführt, muss ein Eilmaßnahmenregister führen (Artikel 8 Absatz 4 CPPA).

([235]) Liegt der Strafverfolgungsbehörde nicht innerhalb von 36 Stunden eine gerichtliche Genehmigung vor, so ist die Erhebung unverzüglich einzustellen (Artikel 8 Absatz 2 CPPA); in diesem Fall werden die erhobenen Daten, wie in Anhang II Abschnitt 2.2.2.2 erläutert, in der Regel vernichtet. Das Gericht ist auch in Fällen zu benachrichtigen, in denen eine Eilmaßnahme innerhalb kurzer Zeit abgeschlossen wurde, sodass eine gerichtliche Genehmigung nicht mehr erforderlich ist (z. B. wenn der Verdächtige unmittelbar nach Überwachungsbeginn festgenommen wird, siehe Artikel 8 Absatz 5 CPPA). In diesem Fall müssen dem Gericht Informationen über Zweck, Ziel, Umfang, Zeitraum, Ort und Art der Erhebung vorgelegt sowie die Gründe genannt werden, warum kein Antrag auf gerichtliche Genehmigung gestellt wurde (Artikel 8 Absätze 6 bis 7 CPPA).

([236]) Artikel 6 Absatz 7 CPPA. Wird das Ziel der Maßnahmen innerhalb dieses Zeitraums früher erreicht, müssen die Maßnahmen unverzüglich eingestellt werden.

([237]) Artikel 6 Absätze 7 bis 8 CPPA.

([238]) Artikel 6 Absatz 8 CPPA.

([239]) Artikel 9 Absatz 3 CPPA.

([240]) Artikel 18 Absatz 1 des CPPA-Durchführungserlasses.

([241]) Insbesondere muss die Staatsanwaltschaft die Person innerhalb von 30 Tagen nach Erstellung einer Anklageschrift oder einer Entscheidung, keine Anklage zu erheben oder eine Festnahme vorzunehmen, unterrichten (Artikel 9-2 Absatz 1 CPPA). Die Unterrichtung kann mit Zustimmung des Leiters der Bezirksstaatsanwaltschaft aufgeschoben werden, wenn sie wahrscheinlich die nationale Sicherheit ernsthaft gefährden oder die öffentliche Sicherheit und Ordnung stören würde oder wenn sie wahrscheinlich zu einer erheblichen Schädigung eines Dritten an Leib und Leben führen würde (Artikel 9-2 Absätze 4 bis 6 CPPA).

([242]) Artikel 16 und 17 CPPA.

([243]) Artikel 83 Absatz 3 TBA. Siehe auch Anhang II Abschnitt 2.2.3.

([244]) Artikel 2 Absatz 9 TBA.

([245]) Siehe auch Anhang II Abschnitt 2.2.3.

insbesondere indem sie nur ein Mindestmaß an personenbezogenen Daten erheben, soweit dies zur Erreichung eines rechtmäßigen Zwecks erforderlich ist, und zwar in einer Weise, die die Auswirkungen auf die Privatsphäre des Einzelnen möglichst gering hält (z. B. Artikel 3 Absätze 1 und 6 PIPA). So muss ein Ersuchen um Offenlegung von Kommunikationsdaten auf der Grundlage des TBA schriftlich erfolgen und Ausführungen über die Gründe für das Ersuchen, die Verbindung zu dem betreffenden Nutzer und den Umfang der angeforderten Daten enthalten ([246]).

(165) Die Telekommunikationsanbieter sind nicht verpflichtet, solchen Ersuchen nachzukommen, und dürfen dies nur in Übereinstimmung mit dem PIPA tun. So müssen sie insbesondere die verschiedenen Interessen gegeneinander abwägen und dürfen die Daten nicht weitergeben, wenn dies zur unfairen Beeinträchtigung der Interessen der betroffenen Person oder eines Dritten führen könnte ([247]). Dies trifft zum Beispiel zu, wenn die ersuchende Behörde ihre Befugnisse offensichtlich missbraucht hat ([248]). Die Telekommunikationsanbieter müssen Aufzeichnungen über die Offenlegungen im Rahmen des TBA führen und dem Minister für Wissenschaft und IKT zweimal pro Jahr Bericht erstatten ([249]).

(166) Darüber hinaus müssen Telekommunikationsanbieter gemäß Abschnitt 3 der Bekanntmachung Nr. 2021-5 (Anhang I) grundsätzlich die betroffene Person unterrichten, wenn sie einem Ersuchen freiwillig nachkommen ([250]). Auf diese Weise kann die betroffene Person ihre Rechte wahrnehmen und im Falle einer unrechtmäßigen Weitergabe ihrer Daten Rechtsbehelfe einlegen, und zwar entweder gegen den Datenverantwortlichen (z. B. für die Weitergabe der Daten unter Verstoß gegen das Datenschutzgesetz oder für die Beantwortung eines eindeutig unverhältnismäßigen Ersuchens) oder gegen die Strafverfolgungsbehörde (z. B. für Handlungen, die über die Grenzen des Erforderlichen und Angemessenen hinausgehen, oder für die Nichteinhaltung der Verfahrensvorschriften des TBA).

3.2.2 *Weitere Verwendung der erhobenen Daten*

(167) Die Verarbeitung personenbezogener Daten, die von koreanischen Strafverfolgungsbehörden erhoben werden, unterliegt allen Anforderungen des PIPA, einschließlich der Zweckbindung (Artikel 3 Absätze 1 bis 2 PIPA), der Rechtmäßigkeit der Nutzung und der Weitergabe an Dritte (Artikel 15, 17 und 18 PIPA), der internationalen Übermittlung (Artikel 17 und 18 PIPA in Verbindung mit Abschnitt 2 der Bekanntmachung 2021-5) ([251]), der Verhältnismäßigkeit bzw. Datenminimierung (Artikel 3 Absätze 1 und 6 PIPA) und der Speicherbegrenzung (Artikel 21 PIPA) ([252]).

(168) Die Verwendung von Kommunikationsinhaltsdaten, die im Rahmen von kommunikationsbeschränkenden Maßnahmen erworben wurden, wird im CPPA ausdrücklich auf folgende Situationen beschränkt: bei Ermittlung, Verfolgung oder Verhütung schwerer Straftaten, ([253]) bei Disziplinarverfahren wegen dieser Straftaten, bei Schadenersatzansprüchen, die von einer an der Kommunikation beteiligten Partei geltend gemacht werden, oder wenn dies durch andere Gesetze ausdrücklich erlaubt ist ([254]). Darüber hinaus darf der erfasste Inhalt der Telekommunikation über das Internet nur mit Genehmigung des Gerichts, das die kommunikationsbeschränkenden Maßnahmen genehmigt hat, ([255]) gespeichert werden, um die Daten für die Ermittlung, Verfolgung oder Verhütung schwerer Straftaten zu verwenden ([256]). Im Allgemeinen ist es nach dem CPPA verboten, vertrauliche Daten, die durch kommunikationsbeschränkende Maßnahmen eingeholt wurden, weiterzugeben und solche Daten zu verwenden, um den Ruf derjenigen zu schädigen, die von den Maßnahmen betroffen waren ([257]).

3.2.3 *Aufsicht*

(169) Die Tätigkeit der Strafverfolgungsbehörden wird in Korea von verschiedenen Stellen beaufsichtigt ([258]).

([246]) Artikel 83 Absatz 4 TBA. Ist wegen Dringlichkeit ein schriftliches Ersuchen nicht möglich, so muss dieses vorgelegt werden, sobald der Grund für die Dringlichkeit nicht mehr besteht (Artikel 83 Absatz 4 TBA).

([247]) Artikel 18 Absatz 2 PIPA.

([248]) Entscheidung des Obersten Gerichtshofs vom 10. März 2016, 2012Da105482. Siehe auch Anhang II Abschnitt 2.2.3 über diese Entscheidung des Verfassungsgerichts.

([249]) Artikel 83 Absätze 5 bis 6 TBA.

([250]) Diese Anforderung unterliegt begrenzten und qualifizierten Ausnahmen, insbesondere wenn und solange dadurch eine laufende strafrechtliche Ermittlung gefährdet würde oder die Schädigung eines Dritten an Leib und Leben wahrscheinlich ist, sofern diese Rechte oder Interessen eindeutig Vorrang vor den Rechten der betroffenen Person haben. Siehe Abschnitt 3 Ziffer III Nummer 1 der Bekanntmachung.

([251]) Insbesondere sind die koreanischen Behörden verpflichtet, durch ein rechtsverbindliches Instrument ein dem PIPA gleichwertiges Schutzniveau zu gewährleisten, siehe auch Erwägungsgrund (90).

([252]) Siehe auch Anhang II Abschnitt 1.2.

([253]) Siehe Erwägungsgrund (158).

([254]) Artikel 12 CPPA. Siehe Anhang II Abschnitt 2.2.2.2.

([255]) Der Staatsanwalt oder der Polizeibeamte, der die kommunikationsbeschränkenden Maßnahmen durchführt, muss innerhalb von 14 Tagen nach Beendigung der Maßnahmen die zu speichernden Telekommunikationsdaten auswählen und die gerichtliche Genehmigung beantragen (Polizeibeamte haben den Antrag an einen Staatsanwalt zu richten, der wiederum den Antrag bei Gericht einreicht), siehe Artikel 12-2 Absätze 1 und 2 CPPA.

([256]) Ein Antrag auf Genehmigung muss Angaben zu den kommunikationsbeschränkenden Maßnahmen, eine Zusammenfassung der Ergebnisse der Maßnahmen, die Gründe für die Aufbewahrung (mit unterstützenden Unterlagen) und die Informationen über die zu speichernden Telekommunikationsdaten enthalten (Artikel 12-2 Absatz 3 CPPA). Wird kein Antrag gestellt, müssen die erfassten Daten innerhalb von 14 Tagen nach Beendigung der kommunikationsbeschränkenden Maßnahme gelöscht werden (Artikel 12-2 Absatz 5 CPPA), bei Ablehnung des Antrags innerhalb von sieben Tagen (Artikel 12-2 Absatz 5 CPPA). In beiden Fällen muss dem Gericht, das die Erhebung genehmigt hat, innerhalb von sieben Tagen ein Bericht über die Löschung übermittelt werden.

([257]) Artikel 11 Absatz 2 des CPPA-Durchführungserlasses.

([258]) Siehe Anhang II Abschnitt 2.3.

(170) Erstens unterliegt die Polizei der internen Aufsicht durch einen Generalinspektor, ([259]) der die Rechtmäßigkeitskontrolle durchführt, auch im Hinblick auf mögliche Menschenrechtsverletzungen. Diese Behörde wurde zur Umsetzung des Gesetzes über Prüfungen im öffentlichen Sektor eingerichtet, mit dem die Einrichtung von Stellen für die Eigenprüfung gefördert und spezifische Anforderungen an deren Zusammensetzung und Aufgaben festgelegt werden. So wird der Leiter einer Stelle für die Eigenprüfung nach dem Gesetz für einen Zeitraum von zwei bis fünf Jahren von einer Person außerhalb der zuständigen Behörde (z. B. ein ehemaliger Richter oder Professor) ernannt ([260]). Er kann nur aus berechtigten Gründen entlassen werden (z. B. wenn er aus gesundheitlichen Gründen nicht in der Lage ist, seine Aufgaben zu erfüllen, oder wenn gegen ihn ein Disziplinarverfahren eingeleitet wird) ([261]) und seine Unabhängigkeit ist weitestgehend gewährleistet ([262]). Die Behinderung einer Eigenprüfung wird mit Geldbußen geahndet ([263]). Die Prüfungsberichte (die Empfehlungen, Anträge auf Disziplinarmaßnahmen, Anträge auf Schadenersatz oder Korrekturen enthalten können) werden dem Leiter der zuständigen Behörde, dem Rechnungshof (Board of Audit and Inspection – BAI), ([264]) übermittelt und im Allgemeinen veröffentlicht ([265]). Die Ergebnisse der Umsetzung des Berichts müssen auch dem BAI mitgeteilt werden ([266]) (siehe Erwägungsgrund (173) über die Aufsichtsfunktion und -befugnisse des BAI).

(171) Zweitens überwacht die PIPC die Einhaltung des PIPA und anderer Gesetze zum Schutz der Privatsphäre natürlicher Personen bei der Datenverarbeitung durch Strafverfolgungsbehörden, einschließlich der Gesetze, die die Sammlung von (elektronischen) Beweismitteln zu Strafverfolgungszwecken regeln, wie in Abschnitt 3.2.1 beschrieben ([267]). Da die PIPC insbesondere die Rechtmäßigkeit und die Datenerhebung und -verarbeitung nach Treu und Glauben überwacht (Artikel 3 Absatz 1 PIPA), gegen die verstoßen wird, wenn personenbezogene Daten unter Verletzung dieser Gesetze abgerufen und verwendet werden, ([268]) kann die PIPC auch die Einhaltung der in Abschnitt 3.2.1 beschriebenen Einschränkungen und Garantien untersuchen und durchsetzen ([269]). Bei der Ausübung dieser Aufsichtsfunktion kann die PIPC von all ihren Untersuchungs- und Abhilfebefugnissen Gebrauch machen, wie in Abschnitt 2.4.2 ausführlich beschrieben. Bereits vor der jüngsten Reform des PIPA (d. h. in ihrer früheren Aufsichtsfunktion für den öffentlichen Sektor) nahm die PIPC mehrere Aufsichtstätigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden wahr, z. B. im Zusammenhang mit der Vernehmung von Verdächtigen (Fall Nr. 2013-16 vom 26. August 2013) sowie in Bezug auf die Benachrichtigung von Personen über die Verhängung von Geldbußen (Fall Nr. 2015-02-04 vom 26. Januar 2015) und die gemeinsame Nutzung von Daten mit anderen Behörden (Fall Nr. 2018-15-146 vom 9. Juli 2018, Fall Nr. 2018-25-308 vom 10. Dezember 2018, Fall Nr. 2019-02-015 vom 29. Januar 2019), die Erfassung von Fingerabdrücken oder Fotos (Fall Nr. 2019-17-273 vom 9. September 2019) und den Einsatz von Drohnen (Fall Nr. 2020-01-004 vom 13. Januar 2020). In diesen Fällen untersuchte die PIPC die Einhaltung mehrerer Bestimmungen des PIPA (z. B. die Rechtmäßigkeit der Verarbeitung, die Grundsätze der Zweckbindung und der Datenminimierung), aber auch einschlägige Bestimmungen anderer Gesetze, wie des Strafverfahrensgesetzes, und gab erforderlichenfalls Empfehlungen ab, um die Verarbeitung mit den Datenschutzanforderungen in Einklang zu bringen.

(172) Drittens gibt es eine unabhängige Aufsicht durch die Nationale Menschenrechtskommission ([270]) (National Human Rights Commission – NHRC), die im Rahmen ihres allgemeinen Mandats zum Schutz der in den Artikeln 10 bis 22 der Verfassung verankerten Grundrechte Verstöße gegen das Recht auf Privatsphäre und Briefgeheimnis untersuchen kann. Die NHRC setzt sich aus 11 Kommissionsmitgliedern zusammen, die bestimmte Qualifikationen aufweisen müssen ([271]) und vom Präsidenten nach einem gesetzlich festgelegten Verfahren ernannt werden. Im Einzelnen werden vier Kommissionsmitglieder auf Vorschlag der Nationalversammlung, vier auf Vorschlag des Präsidenten und drei auf Vorschlag des Obersten Richters des Obersten Gerichtshofs ernannt ([272]). Der Vorsitzende wird vom Präsidenten aus dem Kreis der Kommissionsmitglieder ernannt und muss von der Nationalversammlung bestätigt werden ([273]). Die Kommissionsmitglieder (einschließlich des Vorsitzenden) werden

([259]) Siehe Anhang II Abschnitt 2.3.1. Siehe auch https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Ebenso werden die Prüfer auf der Grundlage bestimmter, im Gesetz festgelegter Bedingungen ernannt, siehe Artikel 16 ff. des Gesetzes über die Prüfungen im öffentlichen Sektor.
([261]) Artikel 8 bis 11 des Gesetzes über Prüfungen im öffentlichen Sektor.
([262]) Artikel 7 des Gesetzes über Prüfungen im öffentlichen Sektor.
([263]) Artikel 41 des Gesetzes über Prüfungen im öffentlichen Sektor.
([264]) Artikel 23 Absatz 1 des Gesetzes über Prüfungen im öffentlichen Sektor.
([265]) Artikel 26 des Gesetzes über Prüfungen im öffentlichen Sektor.
([266]) Artikel 23 Absatz 3 des Gesetzes über Prüfungen im öffentlichen Sektor.
([267]) Siehe Artikel 7-8 Absätze 3 und 4 und Artikel 7-9 Absatz 5 PIPA.
([268]) Bekanntmachung der PIPC Nr. 2021-5 (Anhang I Abschnitt 6).
([269]) Siehe auch Anhang II Abschnitt 2.3.4.
([270]) Artikel 1 des National Human Rights Commission Act (Gesetz über die nationale Menschenrechtskommission, im Folgenden „NHRC-Gesetz“).
([271]) In die Kommission berufen werden können Personen, die 1) mindestens zehn Jahre lang und mindestens als außerordentlicher Professor an einer Universität oder einem zugelassenen Forschungsinstitut gearbeitet haben, 2) mindestens zehn Jahre als Richter, Staatsanwalt oder Rechtsanwalt tätig gewesen sind, 3) mindestens zehn Jahre im Bereich der Menschenrechte gearbeitet haben (z. B. für eine gemeinnützige Organisation, eine Nichtregierungsorganisation oder eine internationale Organisation) oder 4) von zivilgesellschaftlichen Gruppen empfohlen worden sind (Artikel 5 Absatz 3 des NHRC-Gesetzes). Darüber hinaus ist es den Mitgliedern der NHRC nach ihrer Berufung untersagt, gleichzeitig ein Amt in der Nationalversammlung, in einem Gemeinderat oder in einer anderen Regierung oder Verwaltung auf nationaler oder lokaler Ebene (als öffentlicher Bediensteter) auszuüben (siehe Artikel 10 des NHRC-Gesetzes).
([272]) Artikel 5 Absätze 1 und 2 des NHRC-Gesetzes.
([273]) Artikel 5 Absatz 5 des NHRC-Gesetzes.

für eine verlängerbare Amtszeit von drei Jahren ernannt und dürfen nur abberufen werden, wenn sie zu einer Freiheitsstrafe verurteilt wurden oder wegen anhaltender körperlicher oder geistiger Schwäche nicht mehr in der Lage sind, ihre Aufgaben wahrzunehmen (in diesem Fall müssen zwei Drittel der Kommissionsmitglieder der Abberufung zustimmen) ([274]). Im Rahmen der Untersuchungen kann die NHRC die Vorlage von sachdienlichen Unterlagen verlangen, Inspektionen durchführen und Personen zur Anhörung vorladen ([275]). Im Hinblick auf Abhilfebefugnisse kann die NHRC (öffentliche) Empfehlungen zur Verbesserung oder Korrektur bestimmter Strategien und Vorgehensweisen aussprechen, worauf die Behörden mit einem vorgeschlagenen Umsetzungsplan antworten müssen ([276]). Setzt die betreffende Behörde die Empfehlungen nicht um, so muss sie die Kommission darüber unterrichten, ([277]) die ihrerseits die Nationalversammlung über dieses Versäumnis informieren und/oder es öffentlich machen kann. Nach der offiziellen Erklärung der koreanischen Regierung (Anhang II Abschnitt 2.3.5) halten sich die koreanischen Behörden im Allgemeinen an die Empfehlungen der NHRC und haben einen starken Anreiz dafür, da ihre Umsetzung im Rahmen einer allgemeinen, kontinuierlichen Prüfung unter der Aufsicht des Büros des Premierministers beurteilt wurde. Wie die jährlichen Zahlen über ihre Tätigkeit zeigen, überwacht die NHRC aktiv die Tätigkeit der Strafverfolgungsbehörden entweder auf der Grundlage von Einzelpetitionen oder durch Untersuchungen von Amts wegen ([278]).

(173) Viertens wird die allgemeine Aufsicht über die Rechtmäßigkeit der Tätigkeit der Behörden vom Rechnungshof wahrgenommen, der zunächst die Einnahmen und Ausgaben des Staates prüft, aber auch allgemein die Einhaltung der Pflichten von Behörden, die Funktionsweise der öffentlichen Verwaltung zu verbessern ([279]). Der Rechnungshof ist formell dem Präsidenten der Republik Korea unterstellt, hat in Bezug auf seine Aufgaben jedoch eine unabhängige Stellung inne ([280]). Darüber hinaus genießt er volle Unabhängigkeit bei der Ernennung, Entlassung und Organisation seines Personals sowie bei der Aufstellung seines Haushalts ([281]). Der BAI besteht aus einem Vorsitzenden (der vom Präsidenten mit Zustimmung der Nationalversammlung ernannt wird) ([282]) und sechs Kommissionsmitgliedern (die vom Präsidenten auf Vorschlag des Vorsitzenden ernannt werden), ([283]) die bestimmte, gesetzlich festgelegte Qualifikationen aufweisen müssen ([284]) und nur im Falle eines Amtsenthebungsverfahrens, einer Verurteilung zu einer Freiheitsstrafe oder der Unfähigkeit zur Ausübung ihres Amtes aufgrund langfristiger geistiger oder körperlicher Schwäche entlassen werden können ([285]). Der Rechnungshof führt jährlich eine allgemeine Prüfung durch, kann aber auch Sonderprüfungen zu Fragen von besonderem Interesse vornehmen. Bei der Durchführung einer Prüfung oder Kontrolle kann der BAI die Vorlage von Unterlagen und die Anwesenheit von Personen verlangen ([286]). Der BAI kann Empfehlungen aussprechen, Disziplinarmaßnahmen beantragen oder eine Strafanzeige einreichen ([287]).

(174) Schließlich übt die Nationalversammlung die parlamentarische Aufsicht über die öffentlichen Behörden in Form von Untersuchungen und Kontrollen ([288]) ihrer Tätigkeit aus ([289]). Sie kann die Offenlegung von Dokumenten verlangen, Zeugen vorladen, ([290]) Abhilfemaßnahmen empfehlen (wenn sie rechtswidrige oder unangemessene Handlungen

([274]) Artikel 7 Absatz 1 und Artikel 8 des NHRC-Gesetzes.
([275]) Artikel 36 des NHRC-Gesetzes. Gemäß Artikel 6 Absatz 7 des Gesetzes darf die Vorlage von Unterlagen oder Gegenständen verweigert werden, wenn dies die Vertraulichkeit von Staatsangelegenheiten beeinträchtigen würde und wesentliche negative Auswirkungen auf die Staatssicherheit oder die diplomatischen Beziehungen haben könnte oder wenn es ein schwerwiegendes Hindernis für eine strafrechtliche Ermittlung oder ein anhängiges Gerichtsverfahren darstellen würde. In solchen Fällen kann die Kommission den Leiter der zuständigen Behörde erforderlichenfalls um weitere Informationen bitten, um zu prüfen, ob die Verweigerung der Auskunftserteilung gerechtfertigt ist, und der Behördenleiter muss diesem Ersuchen nach Treu und Glauben nachkommen.
([276]) Artikel 25 Absätze 1 und 3 des NHRC-Gesetzes.
([277]) Artikel 25 Absatz 4 des NHRC-Gesetzes.
([278]) So erhielt die NHRC zwischen 2015 und 2019 jährlich zwischen 1 380 und 1 699 Petitionen gegen Strafverfolgungsbehörden und bearbeitete eine ebenso hohe Zahl (z. B. im Jahr 2018 bearbeitete sie 1 546 und im Jahr 2019 1 249 Beschwerden gegen die Polizei); sie führte auch mehrere Untersuchungen von Amts wegen durch, die im NHRC-Jahresbericht 2018 (abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) und im Jahresbericht 2019 (abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217) ausführlicher beschrieben werden.
([279]) Artikel 20 und 24 des Gesetzes über den Rechnungshof (Act on the Board of Audit and Inspection, im Folgenden „BAI-Gesetz“). Siehe Anhang II 2.3.2.
([280]) Artikel 2 Absatz 1 des BAI-Gesetzes.
([281]) Artikel 2 Absatz 2 des BAI-Gesetzes.
([282]) Artikel 4 Absatz 1 des BAI-Gesetzes.
([283]) Artikel 5 Absatz 1 und Artikel 6 des BAI-Gesetzes.
([284]) Beispielsweise müssen sie mindestens zehn Jahre als Richter, Staatsanwalt oder Rechtsanwalt gearbeitet haben, mindestens acht Jahre als Beamter oder als Professor oder Inhaber einer höheren Stelle an einer Hochschule tätig gewesen sein oder mindestens zehn Jahre lang in einem börsennotierten Unternehmen oder einer staatlich finanzierten Einrichtung gearbeitet haben (davon mindestens fünf Jahre als Geschäftsführer), siehe Artikel 7 des BAI-Gesetzes. Darüber hinaus sind den Mitgliedern des Prüfungsausschusses politische Tätigkeiten und das gleichzeitige Innehaben von Ämtern in der Nationalversammlung, in Verwaltungsbehörden, in den vom Rechnungshof geprüften und kontrollierten Organisationen oder von sonstigen vergüteten Ämtern oder Positionen untersagt (Artikel 9 des BAI-Gesetzes).
([285]) Artikel 8 des BAI-Gesetzes.
([286]) Siehe z. B. Artikel 27 des BAI-Gesetzes.
([287]) Artikel 24 und Artikel 31 bis 35 des BAI-Gesetzes.
([288]) Artikel 128 des Gesetzes über die Nationalversammlung und Artikel 2, 3 und 15 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung. Es werden jährliche allgemeine Kontrollen der Regierungsangelegenheiten sowie Untersuchungen zu spezifischen Fragen durchgeführt.
([289]) Siehe Anhang Abschnitt 2.2.3.
([290]) Artikel 10 Absatz 1 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung. Siehe auch Artikel 128 und 129 des Gesetzes über die Nationalversammlung.

feststellt) ([291]) und die Ergebnisse ihrer Feststellungen veröffentlichen ([292]). Verlangt die Nationalversammlung, dass Abhilfemaßnahmen ergriffen werden – die beispielsweise die Gewährung einer Entschädigung, die Einleitung von Disziplinarmaßnahmen oder die Verbesserung interner Verfahren umfassen können –, muss die betreffende Behörde unverzüglich handeln und der Nationalversammlung über das Ergebnis berichten ([293]).

3.2.4 *Rechtsbehelfe*

(175) Das koreanische System bietet verschiedene (gerichtliche) Möglichkeiten, Rechtsschutz einschließlich Schadenersatz zu erhalten.

(176) Erstens gewährt das PIPA dem Einzelnen ein Recht auf Auskunft, Berichtigung, Löschung und Sperrung in Bezug auf personenbezogene Daten, die zu Strafverfolgungszwecken verarbeitet werden ([294]).

(177) Zweitens können Einzelpersonen die verschiedenen im PIPA vorgesehenen Rechtsbehelfe in Anspruch nehmen, wenn ihre Daten von einer Strafverfolgungsbehörde unter Verstoß gegen das PIPA oder unter Verletzung der Einschränkungen und Garantien für die Erhebung personenbezogener Daten in anderen Gesetzen (d. h. dem CPA oder CPPA, siehe Erwägungsgrund (171)) verarbeitet wurden. So können natürliche Personen bei der PIPC Beschwerden einlegen (unter anderem über das von der koreanischen Internet- und Sicherheitsbehörde betriebene Datenschutz-Callcenter) ([295]) oder bei dem Schlichtungsausschuss für Streitigkeiten über personenbezogene Daten ([296]). Diese Rechtsbehelfsmöglichkeiten unterliegen keinen weiteren Zulässigkeitsvoraussetzungen. Auf der Grundlage des Gesetzes über die Verwaltungsgerichtsbarkeit können Einzelpersonen darüber hinaus die Entscheidungen oder die Untätigkeit der PIPC anfechten (siehe Erwägungsgrund (132)).

(178) Drittens kann jede Person ([297]) eine Beschwerde bei der NHRC über eine Verletzung des Rechts auf Privatsphäre und Datenschutz durch eine koreanische Strafverfolgungsbehörde einreichen. Die NHRC kann die Korrektur oder Verbesserung einschlägiger Gesetze, Einrichtungen, Strategien oder Vorgehensweisen ([298]) oder die Durchführung von Abhilfemaßnahmen wie Schlichtungsverfahren ([299]), Abstellung der Menschenrechtsverletzung, Schadenersatz und Maßnahmen zur Verhütung eines erneuten Vorkommens der gleichen oder ähnlicher Verletzungen empfehlen ([300]). Nach der offiziellen Erklärung der koreanischen Regierung (Anhang II Abschnitt 2.4.2) kann dies auch die Löschung unrechtmäßig erhobener personenbezogener Daten umfassen. Die NHRC ist zwar nicht befugt, verbindliche Entscheidungen zu treffen, bietet aber einen informelleren, kostengünstigeren und leichter zugänglichen Rechtsbehelf, insbesondere weil, wie in Anhang II, Abschnitt 2.4.2 erläutert, der Nachweis einer tatsächlichen Schädigung nicht erforderlich ist, damit eine Beschwerde geprüft werden kann ([301]). Dadurch wird sichergestellt, dass Beschwerden von Einzelpersonen über die Erhebung ihrer Daten geprüft werden können, selbst wenn eine Person nicht in der Lage ist, nachzuweisen, dass ihre Daten tatsächlich erhoben wurden (z. B. weil die Person noch nicht benachrichtigt wurde). Aus den jährlichen Tätigkeitsberichten der NHRC geht hervor, dass auch Einzelpersonen in der Praxis von dieser Möglichkeit Gebrauch machen, um die Tätigkeit der Strafverfolgungsbehörden anzufechten, auch im Hinblick auf den Umgang mit personenbezogenen Daten ([302]). Ist eine Person mit dem Ergebnis eines Verfahrens vor der NHRC nicht zufrieden, kann sie die Entscheidungen der NHRC (z. B. die

([291]) Artikel 16 Absatz 2 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([292]) Artikel 12-2 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([293]) Artikel 16 Absatz 3 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([294]) Dieses Recht kann direkt gegenüber der zuständigen Behörde oder indirekt über die PIPC ausgeübt werden (Artikel 35 Absatz 2 PIPA). Wie in den Erwägungsgründen (76)-(78) näher beschrieben, gelten Ausnahmen von diesen Rechten nur, wenn sie zum Schutz wichtiger (öffentlicher) Interessen erforderlich sind.
([295]) Artikel 62 PIPA.
([296]) Artikel 40 bis 50 PIPA und Artikel 48-2 bis 57 des PIPA-Durchführungserlasses. Siehe auch Anhang II Abschnitt 2.4.1.
([297]) Wie in Anhang II Abschnitt 2.4.2 erläutert, wird in Artikel 4 des NHRC-Gesetzes Bezug auf Bürger und in der Republik Korea ansässige Ausländer genommen; der Begriff der Ansässigkeit ist jedoch eher in Zusammenhang mit der Gerichtsbarkeit und nicht territorial zu verstehen. Wenn daher die Grundrechte eines Ausländers außerhalb Koreas von nationalen Einrichtungen in Korea verletzt werden, kann die betroffene Person eine Beschwerde bei der NHRC einreichen. Dies wäre der Fall, wenn koreanische Behörden auf unrechtmäßige Weise auf nach Korea übermittelte personenbezogene Daten eines Ausländers zugreifen. Siehe insbesondere die Erläuterungen unter https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Artikel 44 des NHRC-Gesetzes.
([299]) Außerdem kann zur Beilegung einer Beschwerde ein Schlichtungsverfahren beantragt werden, siehe Artikel 42 ff. des NHRC-Gesetzes.
([300]) Artikel 42 Absatz 4 des NHRC-Gesetzes. Darüber hinaus kann die NHRC im Falle eines andauernden Verstoßes, der wahrscheinlich einen schwer zu behebenden Schaden verursacht, wenn er nicht beachtet wird, dringende Abhilfemaßnahmen ergreifen, siehe Artikel 48 des NHRC-Gesetzes.
([301]) Eine Beschwerde ist grundsätzlich innerhalb eines Jahres nach der Menschenrechtsverletzung einzureichen; allerdings kann die NHRC beschließen, eine Beschwerde zu untersuchen, die nach Ablauf dieser Frist eingereicht wird, solange die straf- oder zivilrechtliche Verjährungsfrist noch nicht verstrichen ist (Artikel 32 Absatz 1 Nummer 4 des NHRC-Gesetzes).
([302]) So hat der NHRC in der Vergangenheit Beschwerden bearbeitet und Empfehlungen zu rechtswidrigen Beschlagnahmen und Verstößen gegen die Pflicht zur Unterrichtung von Personen über eine Beschlagnahme abgegeben (siehe S. 80 und 91 des NHRC-Jahresberichts 2018, abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), sowie zur rechtswidrigen Verarbeitung personenbezogener Daten durch Polizei, Staatsanwaltschaft und Gerichte (siehe S. 157-158 des NHRC-Jahresberichts 2019, abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, und S. 76 des Jahresberichts 2019, abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

Entscheidung, die Untersuchung einer Beschwerde nicht fortzusetzen ([303])) und die Empfehlungen vor den koreanischen Gerichten gemäß dem Gesetz über die Verwaltungsgerichtsbarkeit anfechten (siehe Erwägungsgrund (181)) ([304]). Darüber hinaus kann ein Verfahren vor der NHRC den Zugang zu Gerichten weiter erleichtern, da eine Person gemäß den in den Erwägungsgründen (181)-(183) beschriebenen Verfahren weitere Rechtsmittel gegen die Behörde einlegen könnte, die ihre Daten nach den Feststellungen der NHRC unrechtmäßig verarbeitet hat.

(179) Schließlich stehen verschiedene Rechtsbehelfe zur Verfügung, die es dem Einzelnen ermöglichen, sich auf die in Abschnitt 3.2.1 beschriebenen Einschränkungen und Garantien zu berufen, um Rechtsschutz zu erhalten ([305]).

(180) In Bezug auf Beschlagnahmen (einschließlich von Daten) besteht nach dem CPA die Möglichkeit, die Vollstreckung eines Beschlagnahmebeschlusses durch eine „Quasi-Beschwerde" anzufechten, indem beim zuständigen Gericht ein Antrag auf Widerruf oder Änderung einer Verfügung eines Staatsanwalts oder Polizeibeamten gestellt wird ([306]).

(181) Generell können Einzelpersonen die Handlungen ([307]) oder Unterlassungen ([308]) von Behörden (einschließlich Strafverfolgungsbehörden) nach dem Gesetz über die Verwaltungsgerichtsbarkeit anfechten ([309]). Eine Verwaltungsmaßnahme gilt als „anfechtbare Verfügung", wenn sie sich unmittelbar auf die Rechte und Pflichten der Bürger auswirkt, ([310]) was, wie die koreanische Regierung bestätigt (Anhang II Abschnitt 2.4.3), bei Maßnahmen zur Erhebung personenbezogener Daten zutrifft. Dies gilt sowohl für die direkte Erhebung von Daten (z. B. durch das Abfangen von Nachrichten) als auch für verpflichtende Offenlegungsersuchen (z. B. an einen Diensteanbieter) und für Ersuchen um freiwillige Zusammenarbeit. Damit eine Klage nach dem Gesetz über die Verwaltungsgerichtsbarkeit zulässig ist, muss der Kläger ein rechtliches Interesse an der Geltendmachung seines Anspruchs haben ([311]). Nach der Rechtsprechung des Obersten Gerichtshofs wird ein „rechtliches Interesse" als „rechtlich geschütztes Interesse" ausgelegt, d. h. als ein unmittelbares und konkretes Interesse, das durch Gesetze und Vorschriften, auf denen verwaltungsrechtliche Verfügungen beruhen, geschützt ist (im Unterschied zu einem allgemeinen, mittelbaren und abstrakten öffentlichen Interesse) ([312]). Natürliche Personen haben ein rechtliches Interesse, wenn Verstöße gegen die Einschränkungen und Garantien für die Erhebung ihrer personenbezogenen Daten zu Strafverfolgungszwecken (nach speziellen Gesetzen oder gemäß dem PIPA) begangen werden. Auf der Grundlage des Gesetzes über die Verwaltungsgerichtsbarkeit kann ein Gericht beschließen, eine rechtswidrige Verfügung zu widerrufen oder zu ändern, die Nichtigkeit festzustellen (d. h. festzustellen, dass eine Verfügung keine Rechtswirkung hat oder in der Rechtsordnung nicht vorhanden ist) oder festzustellen, dass eine Unterlassung rechtswidrig ist ([313]). Ein rechtskräftiges Urteil nach dem Gesetz über die Verwaltungsgerichtsbarkeit ist für die Parteien bindend ([314]).

([303]) Wenn die NHRC ausnahmsweise nicht in der Lage ist, bestimmte Unterlagen einzusehen oder Einrichtungen zu inspizieren, weil diese in Zusammenhang mit Staatsgeheimnissen stehen, die erhebliche Auswirkungen auf die Staatssicherheit oder die diplomatischen Beziehungen haben könnten, oder wenn die Einsichtnahme oder Inspektion ein schwerwiegendes Hindernis für eine strafrechtliche Ermittlung oder ein anhängiges Gerichtsverfahren darstellen würde, sodass die NHRC eine Untersuchung, die erforderlich ist, um die Begründetheit einer Petition zu beurteilen, nicht durchführen kann, muss sie der betroffenen Person gemäß Artikel 39 des NHRC-Gesetzes die Gründe für die Ablehnung der Beschwerde mitteilen. In diesem Fall kann die betroffene Person die Entscheidung der NHRC nach dem Gesetz über die Verwaltungsgerichtsbarkeit anfechten.

([304]) Siehe z. B. die Entscheidung des Seoul High Court vom 18. April 2008, 2007NU27259, bestätigt durch die Entscheidung des Obersten Gerichtshofs vom 9. Oktober 2008, 2008Du7854, sowie die Entscheidung des Seoul High Court vom 2. Februar 2018, 2017NU69382.

([305]) Siehe Anhang II 2.4.3.

([306]) Artikel 417 CPA in Verbindung mit Artikel 414 Absatz 2 CPA. Siehe auch die Entscheidung 97Mo66 des Obersten Gerichtshofs vom 29. September 1997.

([307]) Im Gesetz über die Verwaltungsgerichtsbarkeit ist von einer „Verfügung" die Rede, d. h. von der Ausübung oder Verweigerung der Ausübung öffentlicher Gewalt in einem bestimmten Fall.

([308]) Nach dem Gesetz über die Verwaltungsgerichtsbarkeit handelt es sich dabei um das längere Versäumnis einer Verwaltungsbehörde, eine bestimmte Verfügung zu erlassen, das einer entsprechenden rechtlichen Pflicht zuwiderläuft.

([309]) Eine verwaltungsrechtliche Anfechtung kann zunächst vor dem Verwaltungsbeschwerdeausschuss bestimmter Behörden (z. B. NIS, NHRC) erhoben werden, oder vor dem zentralen Verwaltungsbeschwerdeausschuss, der der Kommission für Korruptionsbekämpfung und bürgerliche Rechte unterstellt ist (Artikel 6 des Verwaltungsbeschwerdegesetzes und Artikel 18 Absatz 1 des Gesetzes über die Verwaltungsgerichtsbarkeit). Allerdings kann nach dem Gesetz über die Verwaltungsgerichtsbarkeit auch direkt vor den koreanischen Gerichten geklagt werden.

([310]) Entscheidung des Obersten Gerichtshofs vom 22. Oktober 1999, 98Du18435, Entscheidung des Obersten Gerichtshofs vom 8. September 2000, 99Du1113, Entscheidung des Obersten Gerichtshofs vom 27. September 2012, 2010Du3541.

([311]) Artikel 12, 35 und 36 des Gesetzes über die Verwaltungsgerichtsbarkeit. Darüber hinaus müssen ein Antrag auf Widerruf oder Änderung einer Verfügung und ein Antrag auf Feststellung der Rechtswidrigkeit einer Unterlassung innerhalb von 90 Tagen ab dem Tag eingereicht werden, an dem die Person von der Verfügung bzw. Unterlassung Kenntnis erlangt, und grundsätzlich nicht später als ein Jahr nach Erlass der Verfügung/nach der Unterlassung, es sei denn, es liegen berechtigte Gründe vor (Artikel 20 und Artikel 38 Absatz 2 des Gesetzes über die Verwaltungsgerichtsbarkeit). Der Begriff „berechtigte Gründe" wurde weit ausgelegt und muss unter Berücksichtigung aller Umstände des Falles geprüft werden, ob die Zulassung einer verspäteten Klage gesellschaftlich akzeptabel ist (Entscheidung des Obersten Gerichtshofs vom 28. Juni 1991, 90Nu6521). Wie von der koreanischen Regierung in Abschnitt 2.4.3 des Anhangs II bestätigt, gehören zu berechtigten Gründen beispielsweise (aber nicht ausschließlich) Verzögerungsgründe, die die betroffene Partei nicht zu verantworten hat, (d. h. Situationen, die sich der Kontrolle des Klägers entziehen, z. B. wenn dieser nicht über die Erhebung seiner personenbezogenen Daten unterrichtet wurde) oder höhere Gewalt (z. B. Naturkatastrophen, Kriege).

([312]) Entscheidung des Obersten Gerichtshofs vom 26. März 2006, 2006Du330.

([313]) Artikel 2 und 4 des Gesetzes über die Verwaltungsgerichtsbarkeit.

([314]) Artikel 30 Absatz 1 des Gesetzes über die Verwaltungsgerichtsbarkeit.

(182) Neben der Anfechtung staatlicher Maßnahmen im Wege der Verwaltungsgerichtsbarkeit können Einzelpersonen auch eine Verfassungsbeschwerde beim Verfassungsgericht wegen einer Verletzung ihrer Grundrechte durch die Ausübung oder Nichtausübung staatlicher Gewalt (mit Ausnahme von Gerichtsurteilen) einreichen ([315]). Etwaige andere verfügbare Rechtsbehelfe müssen zuvor erschöpft worden sein. Ausländer können nach der Rechtsprechung des Verfassungsgerichts Verfassungsbeschwerde einlegen, soweit ihre Grundrechte in der koreanischen Verfassung anerkannt werden (siehe die Erläuterungen in Abschnitt 1.1) ([316]). Das Verfassungsgericht kann die Ausübung der Staatsgewalt, die zu der Verletzung geführt hat, für ungültig erklären oder feststellen, dass eine bestimmte Unterlassung verfassungswidrig ist ([317]). In diesem Fall ist die betreffende Behörde verpflichtet, Maßnahmen zu ergreifen, um der Entscheidung des Gerichts zu entsprechen.

(183) Darüber hinaus können natürliche Personen vor den koreanischen Gerichten auf Schadenersatz klagen. Dazu gehört in erster Linie die Möglichkeit, gemäß Artikel 39 eine Entschädigung für von Strafverfolgungsbehörden begangene Verstöße gegen das PIPA zu fordern (siehe auch Erwägungsgrund (135)). Auf der Grundlage des Gesetzes über staatlichen Schadenersatz können Einzelpersonen ganz allgemein Anspruch auf Schadenersatz für Schäden erheben, die ihnen öffentliche Bedienstete unter Verstoß gegen das Gesetz bei der Ausübung ihres Amtes zugefügt haben (siehe auch Erwägungsgrund (135)) ([318]).

(184) Durch die in den Erwägungsgründen (176)-(183) beschriebenen Mechanismen stehen betroffenen Personen wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung, die es ihnen insbesondere ermöglichen, ihre Rechte durchzusetzen, unter anderem das Auskunftsrecht hinsichtlich ihrer personenbezogenen Daten oder das Recht auf Berichtigung oder Löschung dieser Daten.

3.3 **Zugriff und Verwendung durch koreanische Behörden für die Zwecke der nationalen Sicherheit**

(185) Das Recht der Republik Korea umfasst eine Reihe von Einschränkungen und Garantien in Bezug auf den Zugriff zu und die Verwendung von personenbezogenen Daten für die Zwecke der nationalen Sicherheit; ferner sieht es Aufsichtsmechanismen und Rechtsbehelfe vor, die den in den Erwägungsgründen (141) bis (143) dieses Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Prüfung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten.

3.3.1 *Rechtsgrundlagen, Einschränkungen und Garantien*

(186) In der Republik Korea darf auf personenbezogene Daten zu Zwecken der nationalen Sicherheit auf der Grundlage des CPPA, des TBA und des Gesetzes über die Terrorismusbekämpfung zum Schutz der Bürger und der öffentlichen Sicherheit (im Folgenden „Antiterrorismusgesetz“) zugegriffen werden ([319]). Die wichtigste Behörde ([320]) mit Zuständigkeiten im Bereich der nationalen Sicherheit ist der nationale Nachrichtendienst (National Intelligence Service – NIS) ([321]). Die Erhebung und Verwendung personenbezogener Daten durch den NIS muss den

([315]) Artikel 68 Absatz 1 des Gesetzes über das Verfassungsgericht. Verfassungsbeschwerden müssen innerhalb von 90 Tagen, nachdem die Person Kenntnis von der Verletzung ihrer Rechte erlangt hat, und innerhalb eines Jahres nach der Verletzung selbst eingereicht werden. Wie auch in Anhang II Abschnitt 2.4.3. erläutert, ist eine Klage angesichts der Tatsache, dass auf Rechtsstreitigkeiten nach dem Gesetz über das Verfassungsgericht gemäß Artikel 40 des Gesetzes über das Verfassungsgericht das Verfahren des Gesetzes über die Verwaltungsgerichtsbarkeit angewandt wird, dennoch zulässig, wenn „berechtigte Gründe“ nach der in der Fußnote 312 beschriebenen Auslegung der Rechtsprechung des Obersten Gerichtshofs vorliegen. Wenn zunächst andere Rechtsbehelfe zu erschöpfen sind, muss die Verfassungsbeschwerde innerhalb von 30 Tagen nach der rechtskräftigen Entscheidung über einen solchen Rechtsbehelf eingelegt werden (Artikel 69 des Gesetzes über das Verfassungsgericht).

([316]) Entscheidung des Verfassungsgerichts vom 29. November 2001, 99HeonMa194.

([317]) Artikel 75 Absatz 3 des Gesetzes über das Verfassungsgericht.

([318]) Artikel 2 Absatz 1 des Gesetzes über staatlichen Schadenersatz.

([319]) Siehe Anhang II Abschnitt 3.1.

([320]) In Ausnahmefällen können auch Polizei und Staatsanwaltschaft personenbezogene Daten für die Zwecke der nationalen Sicherheit erheben (siehe Fußnote 327 und Anhang II Abschnitt 3.2.1.2). Darüber hinaus hat der koreanische militärische Nachrichtendienst (Unterstützungskommando für Sicherheit im Verteidigungsbereich, das dem Verteidigungsministerium unterstellt ist) Befugnisse im Bereich der nationalen Sicherheit. Wie in Anhang II Abschnitt 3.1 erläutert, ist es jedoch nur für militärische Nachrichtendienste zuständig und überwacht die Zivilbevölkerung nur, wenn dies zur Erfüllung seiner militärischen Aufgaben erforderlich ist. Ermittlungen können gegen militärisches Personal, Zivilbeschäftigte des Militärs, Personen in militärischer Ausbildung, Reservisten oder Rekrutierer sowie Kriegsgefangene geführt werden (Artikel 1 des Militärgerichtsgesetzes). Bei der Erhebung von Kommunikationsdaten für die Zwecke der nationalen Sicherheit unterliegt das Defense Security Support Command den Einschränkungen und Garantien, die im CPPA und in dem entsprechenden Durchführungserlass festgelegt sind.

([321]) Die Aufgaben des NIS sind die Beschaffung, Zusammenstellung und Weiterleitung von Informationen über das Ausland (d. h allgemeinen Informationen über Trends und Entwicklungen im Ausland oder über die Tätigkeiten staatlicher Akteure), von Nachrichten in Zusammenhang mit der Abwehr von Spionage (einschließlich Militär- und Industriespionage), Terrorismus und den Tätigkeiten internationaler Verbrechersyndikate, von Nachrichten über bestimmte Arten von Straftaten gegen die öffentliche und nationale Sicherheit (z. B. Aufstände im Inland, Angriffe aus dem Ausland) und von Nachrichten in Zusammenhang mit der Gewährleistung der Cybersicherheit und der Prävention oder Abwehr von Cyberangriffen und -bedrohungen (Artikel 4 Absatz 2 des NIS-Gesetzes). Siehe auch Anhang II Abschnitt 3.1.

einschlägigen gesetzlichen Bestimmungen (einschließlich PIPA und CPPA) ([322]) und den vom Präsidenten ausgearbeiteten und von der Nationalversammlung überprüften allgemeinen Leitlinien entsprechen ([323]). Grundsätzlich muss der NIS politische Neutralität wahren und die Freiheit und die Rechte natürlicher Personen schützen ([324]). Darüber hinaus dürfen die Mitarbeiter des NIS ihre Amtsgewalt nicht dazu missbrauchen, Institutionen, Organisationen oder Einzelpersonen zu etwas zu zwingen, wozu sie nicht (gesetzlich) verpflichtet sind, und sie dürfen niemanden bei der Ausübung seiner Rechte behindern ([325]).

3.3.1.1 Zugriff auf Kommunikationsdaten

(187) Auf der Grundlage des CPPA können koreanische Behörden ([326]) Kommunikationsbestätigungsdaten (d. h das Datum des Telekommunikationsvorgangs, seine Anfangs- und Endzeit, die Zahl der ausgehenden und eingehenden Anrufe sowie die Rufnummer der anderen Person, die Häufigkeit der Nutzung, Protokolldateien über die Nutzung von Telekommunikationsdiensten und Standortdaten, siehe Erwägungsgrund (155)) und Kommunikationsinhaltsdaten (durch kommunikationsbeschränkende Maßnahmen, siehe Erwägungsgrund (155)) für die Zwecke der Strafverfolgung und der nationalen Sicherheit (gemäß dem Mandat des NIS, siehe die obige Fußnote 322) erheben. Diese Befugnisse beziehen sich auf zwei Arten von Daten: 1) Kommunikation, bei der eine oder beide Parteien koreanische Staatsangehörige sind ([327]) und 2) Kommunikation a) aus Ländern, die der Republik Korea feindlich gesinnt sind, b) von ausländischen Behörden, Organisationen oder Staatsangehörigen, die antikoreanischer Aktivitäten verdächtigt werden ([328]) oder c) von Mitgliedern von Organisationen auf der koreanischen Halbinsel, die faktisch nicht unter die Staatshoheit der Republik Korea fallen, und der im Ausland sitzender Dachorganisation ([329]). Kommunikationsdaten von EU-Bürgern, die auf der Grundlage dieses Beschlusses von der Union an die Republik Korea übermittelt wird, können daher nur dann nach dem CPPA für die Zwecke der nationalen Sicherheit erhoben werden (vorbehaltlich der in den Erwägungsgründen (188)-(192) genannten Bedingungen), wenn die Kommunikation entweder zwischen einem EU-Bürger und einem koreanischen Staatsangehörigen stattfindet oder – falls sie ausschließlich Kommunikation zwischen nichtkoreanischen Staatsangehörigen betreffen – unter eine der drei genannten Kategorien 2a), b) und c) fallen.

(188) In beiden Szenarien dürfen Kommunikationsbestätigungsdaten nur zur Abwehr von Gefahren für die nationale Sicherheit erhoben werden, ([330]) während kommunikationsbeschränkende Maßnahmen nur ergriffen werden dürfen, wenn eine schwerwiegende Gefahr für die nationale Sicherheit besteht und die Erhebung zur Abwehr dieser Gefahr erforderlich ist ([331]). Darüber hinaus darf der Zugriff auf den Inhalt eines Kommunikationsvorgangs nur das letzte Mittel zur Gewährleistung der nationalen Sicherheit sein und es müssen Anstrengungen unternommen werden, um die Verletzung der Privatsphäre bei der Kommunikation so gering wie möglich zu halten ([332]) und so sicherzustellen, dass sie in einem angemessenen Verhältnis zu dem angestrebten Ziel der nationalen Sicherheit steht. Sowohl Kommunikationsinhaltsdaten als auch Kommunikationsbestätigungsdaten dürfen nur über einen Zeitraum von höchstens vier Monaten erhoben werden und die Erhebung muss unverzüglich eingestellt werden, wenn das verfolgte Ziel früher erreicht wird ([333]). Sind die entsprechenden Voraussetzungen weiterhin erfüllt, kann die Frist mit vorheriger Genehmigung eines Gerichts (für die in Erwägungsgrund (189) beschriebenen Maßnahmen) oder des Präsidenten (für die in Erwägungsgrund (190) beschriebenen Maßnahmen) ([334]) um bis zu vier Monate verlängert werden.

(189) Die gleichen Verfahrensgarantien gelten für die Erhebung von Kommunikationsbestätigungs- und den Kommunikationsinhaltdaten ([335]). Handelt es sich bei mindestens einer der an der Kommunikation beteiligten Personen um einen koreanischen Staatsangehörigen, muss der Nachrichtendienst einen schriftlichen Antrag an die Oberste Staatsanwaltschaft stellen, die ihrerseits eine Anordnung bei einem Obersten Richter des Obersten

([322]) Siehe auch Artikel 14, 22 und 23 des NIS-Gesetzes.
([323]) Artikel 4 Absatz 2 des NIS-Gesetzes.
([324]) Artikel 3 Absatz 1, Artikel 6 Absatz 2, Artikel 11 und Artikel 21 des NIS-Gesetzes. Siehe auch die Vorschriften über Interessenkonflikte, insbesondere die Artikel 10 und 12 des NIS-Gesetzes.
([325]) Artikel 13 des NIS-Gesetzes.
([326]) Dazu gehören die Nachrichtendienste (d. h. der NIS und das Unterstützungskommando für Sicherheit im Verteidigungsbereich) und die Polizei bzw. Staatsanwaltschaft.
([327]) Artikel 7 Absatz 1 Nummer 1 CPPA.
([328]) Wie die koreanische Regierung in der Fußnote 244 des Anhangs II erläutert, bezieht sich dies auf Aktivitäten, die eine Gefahr für den Fortbestand und die Sicherheit der Nation, die demokratische Ordnung oder das Überleben und die Freiheit der Bevölkerung darstellen.
([329]) Artikel 7 Absatz 1 Nummer 2 CPPA.
([330]) Artikel 13-4 CPPA.
([331]) Artikel 7 Absatz 1 CPPA.
([332]) Artikel 3 Absatz 2 CPPA. Darüber hinaus müssen kommunikationsbeschränkende Maßnahmen unverzüglich eingestellt werden, sobald sie nicht mehr erforderlich sind, um sicherzustellen, dass der Eingriff in die Kommunikationsgeheimnisse des Einzelnen auf ein Minimum beschränkt bleibt (Artikel 2 des CPPA-Durchführungserlasses).
([333]) Artikel 7 Absatz 2 CPPA.
([334]) In dem schriftlich zu stellenden Antrag auf Genehmigung der Verlängerung der Überwachungsmaßnahmen sind die Gründe für die Verlängerung zu nennen und es sind Belege beizufügen (Artikel 7 Absatz 2 CPPA und Artikel 5 des CPPA-Durchführungserlasses).
([335]) Siehe Artikel 13-4 Absatz 2 CPPA und Artikel 37 Absatz 4 des CPPA-Durchführungserlasses, nach denen die Verfahren für die Erhebung von Kommunikationsinhaltsdaten auch für die Erhebung von Kommunikationsbestätigungsdaten gelten. Siehe auch Anhang II Abschnitt 3.2.1.1.1.

Gerichtshofs beantragen muss ([336]). Im CPPA sind die Informationen aufgeführt, die im Antrag an die Staatsanwaltschaft, im Antrag auf Erlass der Anordnung und in der Anordnung selbst enthalten sein müssen. Dazu gehören insbesondere die Begründung des Antrags und die Hauptgründe für den Verdacht, Belege sowie Informationen über den Zweck, den Empfänger (d. h. die Zielperson(en)), den Umfang und die Dauer der geplanten Maßnahme ([337]). Eine Erhebung ohne Anordnung darf nur dann erfolgen, wenn eine die nationale Sicherheit gefährdende Verschwörung vorliegt und Dringlichkeit besteht, sodass es unmöglich ist, die genannten Verfahren zu durchlaufen ([338]). Auch in diesem Fall muss jedoch unmittelbar nach der Maßnahme ein Antrag auf Anordnung gestellt werden ([339]). Im CPPA werden daher der Umfang und die Bedingungen dieser Arten der Datenerhebung klar definiert und sie unterliegen besonderen (Verfahrens-)Garantien (einschließlich einer vorherigen gerichtlichen Genehmigung), wodurch sichergestellt wird, dass der Einsatz solcher Maßnahmen auf das erforderliche und verhältnismäßige Maß beschränkt wird. Darüber hinaus schließt die Pflicht, sowohl im Antrag auf Erlass einer Anordnung als auch in der Anordnung selbst detaillierte Daten anzugeben, die Möglichkeit eines anlassunabhängigen Zugangs aus.

(190) Für die Kommunikation zwischen nichtkoreanischen Staatsangehörigen, die unter eine der drei in Erwägungsgrund (187) aufgeführten Kategorien fällt, ist ein Antrag beim Direktor des NIS zu stellen, der nach Prüfung der Angemessenheit der vorgeschlagenen Maßnahmen vorab die schriftliche Genehmigung des Präsidenten der Republik Korea einholen muss ([340]). Der vom Nachrichtendienst erstellte Antrag muss dieselben detaillierten Informationen enthalten wie ein Antrag auf eine gerichtliche Anordnung (siehe Erwägungsgrund (189)), insbesondere über die Begründung des Antrags und die Hauptgründe für den Verdacht, Belege und Informationen über die Zwecke, die Zielperson(en), den Umfang und die Dauer der geplanten Maßnahmen ([341]). In dringenden Fällen ([342]) ist vorab die Genehmigung des Ministers einzuholen, dem der jeweilige Nachrichtendienst untersteht; der Nachrichtendienst muss jedoch unmittelbar nach Ergreifen der Eilmaßnahmen die Genehmigung des Präsidenten beantragen ([343]). Auch in Bezug auf die Erhebung der Kommunikationsdaten zwischen ausschließlich nicht-koreanischen Staatsangehörigen beschränkt das CPPA den Einsatz solcher Maßnahmen auf das erforderliche und verhältnismäßige Maß, indem es die begrenzten Kategorien von Personen, die solchen Maßnahmen unterworfen werden können, klar eingrenzt und detaillierte Kriterien festlegt, die die Nachrichtendienste nachweisen müssen, um einen Antrag auf Erhebung von Daten zu rechtfertigen. Außerdem wird so die Möglichkeit eines anlassunabhängigen Zugangs ausgeschlossen. Zwar werden solche Maßnahmen nicht im Voraus unabhängig genehmigt, doch wird die unabhängige Aufsicht im Nachhinein insbesondere durch die PIPC und die NHRC gewährleistet (siehe z. B. Erwägungsgründe (199)-(200)).

(191) Darüber hinaus werden im CPPA mehrere zusätzliche Sicherheitsvorkehrungen vorgesehen, die zu einer Ex-post-Kontrolle beitragen und dem Einzelnen den Zugang zu wirksamen Rechtsbehelfen erleichtern. Erstens sind im CPPA für alle Arten von Erhebungen zu Zwecken der nationalen Sicherheit unterschiedliche Aufzeichnungs- und Meldeanforderungen vorgesehen. Insbesondere wenn die Nachrichtendienste private Unternehmen um ihre Zusammenarbeit ersuchen, müssen sie ihnen die gerichtliche Anordnung bzw. die Genehmigung des Präsidenten oder eine Kopie des Deckblatts einer Erklärung über die Dringlichkeit von Zensurmaßnahmen vorlegen, die das betreffende Unternehmen in seinen Akten aufbewahren muss ([344]). Werden private Wirtschaftsbeteiligte zur Zusammenarbeit gezwungen, müssen sowohl die ersuchende Behörde als auch der betreffende Wirtschaftsbeteiligte Aufzeichnungen über den Zweck und den Zielgegensand der Maßnahmen sowie über das Datum der

([336]) Artikel 6 Absätze 5 und 8, Artikel 7 Absatz 1 Nummer 1 und Absatz 3 CPPA in Verbindung mit Artikel 7 Absätze 3 und 4 des CPPA-Durchführungserlasses.

([337]) Siehe Artikel 7 Absatz 3 und Artikel 6 Absatz 4 CPPA (für den Antrag des Nachrichtendienstes), Artikel 4 des CPPA-Durchführungserlasses (für den Antrag der Staatsanwaltschaft) und Artikel 7 Absatz 3 und Artikel 6 Absatz 6 CPPA (für die Anordnung).

([338]) Artikel 8 CPPA.

([339]) Artikel 8 Absätze 2 und 8 CPPA. Die Erhebung ist unverzüglich einzustellen, wenn die gerichtliche Genehmigung nicht innerhalb von 36 Stunden ab dem Zeitpunkt der Maßnahme eingeholt wird. In Fällen, in denen die Überwachung innerhalb kurzer Zeit abgeschlossen wird, sodass das Einholen einer gerichtlichen Genehmigung ausgeschlossen ist, muss der Leiter der zuständigen Obersten Staatsanwaltschaft den Vorsitzenden des zuständigen Gerichts darüber unterrichten, der auf dieser Grundlage die Rechtmäßigkeit der Erhebung prüfen kann (Artikel 8 Absätze 5 und 7 CPPA). In der Mitteilung sind Zweck, Ziel, Umfang, Zeitraum, Ort und Art der Erhebung anzugeben sowie die Gründe zu nennen, warum vor der Durchführung der Maßnahme kein entsprechender Antrag gestellt wurde (Artikel 8 Absatz 6 CPPA). Generell dürfen die Nachrichtendienste Eilmaßnahmen nur in Übereinstimmung mit einer „Erklärung über die Dringlichkeit von Zensur- oder Abhörmaßnahmen“ ergreifen und müssen ein Eilmaßnahmenregister führen (Artikel 8 Absatz 4 CPPA).

([340]) Artikel 8 Absätze 1 und 2 des CPPA-Durchführungserlasses.

([341]) Artikel 8 Absatz 3 des CPPA-Durchführungserlasses in Verbindung mit Artikel 6 Absatz 4 CPPA.

([342]) Das heißt in Fällen, in denen die Maßnahme wegen einer die nationale Sicherheit gefährdenden Verschwörung getroffen wird, nicht genügend Zeit bleibt, um die Genehmigung des Präsidenten einzuholen und die Unterlassung von Eilmaßnahmen zu einer Beeinträchtigung der nationalen Sicherheit führen könnte (Artikel 8 Absatz 8 CPPA).

([343]) Artikel 8 Absatz 9 CPPA. Die Erhebung ist unverzüglich einzustellen, wenn die Genehmigung nicht innerhalb von 36 Stunden nach der Antragstellung eingeht.

([344]) Artikel 9 Absatz 2 CPPA und Artikel 12 des CPPA-Durchführungserlasses. Siehe Artikel 13 des CPPA-Durchführungserlasses über die Möglichkeit, Poststellen und Telekommunikationsdiensteanbieter zur Unterstützung zu verpflichten. Private Unternehmen, die Daten offenlegen sollen, dürfen dies verweigern, wenn in der Anordnung bzw. Genehmigung oder Erklärung über die Dringlichkeit von Zensurmaßnahmen eine falsche Kennung genannt wird (z. B. eine Telefonnummer, die einer anderen als der angegebenen natürlichen Person zugeordnet ist). In jedem Fall dürfen sie die für die Kommunikation verwendeten Passwörter nicht offenlegen (Artikel 9 Absatz 4 CPPA).

Durchführung führen ([345]). Darüber hinaus haben die Nachrichtendienste dem Direktor des NIS über die von ihnen gesammelten Daten und die Ergebnisse der Überwachungstätigkeit Bericht zu erstatten ([346]).

(192) Zweitens müssen Personen über die Erhebung ihrer Daten (Kommunikationsbestätigungsdaten oder den Kommunikationsinhalt) zu Zwecken der nationalen Sicherheit unterrichtet werden, wenn es sich um Kommunikation handelt, bei der mindestens eine der Parteien koreanischer Staatsangehöriger ist ([347]). Diese Unterrichtung muss schriftlich innerhalb von 30 Tagen nach Beendigung der Datenerhebung erfolgen (auch wenn die Daten im Rahmen des Eilverfahrens erhoben wurden) und kann nur aufgeschoben werden, wenn und solange die nationale Sicherheit gefährdet oder das Leben und die körperliche Unversehrtheit von Personen beeinträchtigt würde ([348]). Unabhängig von einer solchen Unterrichtung können Einzelpersonen auf verschiedenen Wegen Rechtsbehelfe erlangen, wie in Abschnitt 3.3.4 näher erläutert.

3.3.1.2 Erhebung von Daten über Terrorverdächtige

(193) Gemäß dem Antiterrorismusgesetz kann der NIS unter Einhaltung der in anderen Gesetzen festgelegten Einschränkungen und Garantien Daten über Terrorverdächtige ([349]) erheben ([350]). Insbesondere kann der NIS Kommunikationsdaten (auf der Grundlage des CPPA) und andere persönliche Daten (durch ein Ersuchen um freiwillige Offenlegung) erhalten ([351]). Für die Erhebung von Kommunikationsdaten (d. h. Kommunikationsinhalts- oder Kommunikationsbestätigungsdaten) gelten die in Abschnitt 3.3.1.1 beschriebenen Einschränkungen und Garantien, einschließlich des Erfordernisses, eine gerichtlich genehmigte Anordnung einzuholen. Bei Ersuchen um freiwillige Offenlegung anderer Arten personenbezogener Daten von Terrorverdächtigen muss der NIS die Anforderungen der Verfassung und des PIPA an die Erforderlichkeit und Verhältnismäßigkeit erfüllen (siehe Erwägungsgrund (164)) ([352]). Datenverantwortliche, die solche Ersuchen erhalten, können diesen unter den im PIPA festgelegten Bedingungen freiwillig nachkommen (z. B. nach dem Grundsatz der Datenminimierung und durch Begrenzung der Auswirkungen auf die Privatsphäre des Einzelnen) ([353]). In diesem Fall müssen sie auch der Anforderung, die betroffene Person zu unterrichten, gemäß der Bekanntmachung Nr. 2021-5 nachkommen (siehe Erwägungsgrund (166)).

([345]) Bei kommunikationsbeschränkenden Maßnahmen müssen solche Aufzeichnungen drei Jahre lang aufbewahrt werden, siehe Artikel 9 Absatz 3 CPPA und Artikel 17 Absatz 2 des CPPA-Durchführungserlasses. In Bezug auf die Kommunikationsbestätigungsdaten müssen die Nachrichtendienste ein Ersuchen um Übermittlung solcher Daten dokumentieren; die entsprechenden Aufzeichnungen und das schriftliche Ersuchen selbst sind aufzubewahren und es ist auch die Einrichtung zu dokumentieren, die sich darauf gestützt hat (Artikel 13 Absatz 5 und Artikel 13-4 Absatz 3 CPPA). Die Telekommunikationsdiensteanbieter müssen Aufzeichnungen sieben Jahre lang aufbewahren und dem Minister für Wissenschaft und IKT zweimal jährlich über die Häufigkeit der Offenlegung Bericht erstatten (Artikel 9 Absatz 3 CPPA in Verbindung mit Artikel 13 Absatz 7 CPPA sowie Artikel 37 Absatz 4 und Artikel 39 des CPPA-Durchführungserlasses).

([346]) Artikel 18 Absatz 3 des CPPA-Durchführungserlasses.

([347]) Artikel 9-2 Absatz 3 und Artikel 13-4 CPPA. Der Benachrichtigung muss zu entnehmen sein: 1) die Tatsache, dass Daten erhoben wurden, 2) die ausführende Behörde und 3) der Durchführungszeitraum.

([348]) Artikel 9-2 Absatz 4 CPPA. In diesem Fall muss die Unterrichtung innerhalb von 30 Tagen nach Wegfall der Aufschiebungsgründe erfolgen, siehe Artikel 13-4 Absatz 2 und Artikel 9-2 Absatz 6 CPPA.

([349]) Das heißt, Mitglieder einer terroristischen Vereinigung (wie von den Vereinten Nationen bezeichnet, siehe Artikel 2 Absatz 2 des Antiterrorismusgesetzes); Personen, die Ideen oder Taktiken einer terroristischen Vereinigung fördern und verbreiten, Gelder für den Terrorismus beschaffen oder zu ihm beitragen oder sich an anderen Aktivitäten zur Vorbereitung, Verschwörung, Propaganda oder Anstiftung zum Terrorismus beteiligen oder Personen, bei denen ein begründeter Verdacht besteht, dass sie solche Aktivitäten durchgeführt haben (Artikel 2 Absatz 3 des Antiterrorismusgesetzes). „Terrorismus" ist in Artikel 2 Absatz 1 des Antiterrorismusgesetzes definiert als eine Handlung zu dem Zweck, die Ausübung der Autorität des Staates, einer lokalen Verwaltung oder einer ausländischen Regierung (einschließlich internationaler Organisationen) zu untergraben, in einer bestimmten Angelegenheit ihr Tätigwerden zu erwirken, zu dem sie nicht verpflichtet sind, oder die Öffentlichkeit zu bedrohen. Dazu gehören beispielsweise die Tötung einer Person, die Gefangennahme, die Entführung oder Geiselnahme einer Person, Entführung oder Kaperung, Zerstörung oder Beschädigung eines Schiffes oder Flugzeugs, Verwendung von biochemischen Waffen, Sprengstoffen oder Brandsätzen in der Absicht, Tod, schwere Verletzungen oder Schäden zu verursachen und der Missbrauch von Kernmaterial oder radioaktiven Stoffen.

([350]) Artikel 9 Absätze 1 und 3 des Antiterrorismusgesetzes.

([351]) Im Antiterrorismusgesetz wird zwar auch auf die Möglichkeit verwiesen, auf der Grundlage des Einwanderungsgesetzes und des Zollgesetzes Informationen über die Ein- und Ausreise in die bzw. aus der Republik Korea zu erheben, doch ist eine solche Ermächtigung in diesen Gesetzen derzeit nicht vorgesehen (siehe Anhang II Abschnitt 3.2.2.1). In jedem Fall würden die Gesetze grundsätzlich nicht für Daten gelten, die auf der Grundlage dieses Beschlusses übermittelt werden, da sie sich in der Regel auf Daten beziehen, die direkt von den koreanischen Behörden erhoben werden (und nicht auf den Zugang zu Daten, die zuvor von der Union an koreanische Datenverantwortliche übermittelt wurden). Darüber hinaus wird das ARUSFTI im Antiterrorismusgesetz als Rechtsgrundlage für die Erhebung von Daten über Finanztransaktionen genannt. Wie in der Fußnote 200 erläutert, fallen die Arten von Daten, die auf der Grundlage dieses Gesetzes erhoben werden könnten, jedoch nicht in den Anwendungsbereich dieses Beschlusses. Schließlich heißt es im Antiterrorismusgesetz auch, dass die NIS Standortdaten durch unverbindliche Anfragen erheben kann, wobei die Anbieter von Standortdaten diese Daten unter den im PIPA (wie in Erwägungsgrund (193) beschrieben) und im Standortdatengesetz festgelegten Voraussetzungen freiwillig weitergeben könnten. Wie jedoch in Fußnote 17 erläutert, würden Standortdaten auf der Grundlage dieses Beschlusses nicht von der Union an koreanische Datenverantwortliche übermittelt, sondern sie würden vielmehr innerhalb Koreas generiert.

([352]) Siehe Anhang II Abschnitt 3.2.2.2.

([353]) Siehe Artikel 58 Absatz 4 PIPA, wonach personenbezogene Daten nur in dem Umfang verarbeitet werden dürfen, der zur Erreichung des beabsichtigten Zwecks erforderlich ist, und Artikel 3 Absatz 6 PIPA, wonach personenbezogene Daten in einer Weise verarbeitet werden müssen, die die Wahrscheinlichkeit einer Verletzung der Privatsphäre des Einzelnen auf ein Mindestmaß beschränkt. Siehe auch Artikel 59 Nummern 2 und 3 PIPA, demzufolge die Datenverantwortlichen nicht befugt sind, personenbezogene Daten an Dritte weiterzugeben.

3.3.1.3 Ersuchen um freiwillige Offenlegung von Teilnehmerdaten

(194) Auf der Grundlage des TBA können Telekommunikationsanbieter einem Ersuchen um freiwillige Offenlegung von Teilnehmerdaten (siehe Erwägungsgrund (163)) nachkommen, den ein Nachrichtendienst an sie richtet, um durch die Erhebung dieser Daten eine Gefahr für die nationale Sicherheit abzuwenden ([354]). Für solche Ersuchen des NIS gelten die gleichen Einschränkungen (die sich aus der Verfassung, dem PIPA und dem TBA ergeben) wie im Bereich der Strafverfolgung (siehe Erwägungsgrund (164)) ([355]). Telekommunikationsanbieter sind nicht verpflichtet, diesen Ersuchen stattzugeben, und können dies nur unter den im PIPA festgelegten Bedingungen tun (insbesondere nach dem Grundsatz der Datenminimierung und durch Begrenzung der Auswirkungen auf die Privatsphäre des Einzelnen, siehe auch Erwägungsgrund (193)). Es gelten die gleichen Anforderungen hinsichtlich der Aufzeichnung und Unterrichtung der betroffenen Person wie im Bereich der Strafverfolgung (siehe Erwägungsgründe (165) und (166)).

3.3.2 *Weitere Verwendung der erhobenen Daten*

(195) Die Verarbeitung personenbezogener Daten, die von koreanischen Behörden für die Zwecke der nationalen Sicherheit erhoben werden, unterliegt den Grundsätzen der Zweckbindung (Artikel 3 Absätze 1 bis 2 PIPA), der Rechtmäßigkeit und der Verarbeitung nach Treu und Glauben (Artikel 3 Absatz 1 PIPA), der Verhältnismäßigkeit bzw. Datenminimierung (Artikel 3 Absätze 1, 6 und 58 PIPA), der Richtigkeit (Artikel 3 Absatz 3 PIPA), der Transparenz (Artikel 3 Absatz 5 PIPA), der Sicherheit (Artikel 58 Absatz 4 PIPA) und der Speicherbegrenzung (Artikel 58 Absatz 4 PIPA) ([356]). Eine etwaige Weitergabe personenbezogener Daten an Dritte (einschließlich Drittländer) kann nur im Einklang mit diesen Grundsätzen (insbesondere Zweckbindung und Datenminimierung) erfolgen, nachdem die Einhaltung der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit (Artikel 37 Absatz 2 der Verfassung) geprüft und die Auswirkungen auf die Rechte der betroffenen Personen berücksichtigt wurden (Artikel 3 Absatz 6 PIPA).

(196) Die Verwendung von Kommunikationsinhalts- und Kommunikationsbestätigungsdaten ist nach dem CPPA auf Gerichtsverfahren beschränkt, wenn sich eine Partei, die von der Kommunikation betroffen ist, bei einer Schadenersatzklage auf diese Daten beruft, oder auf zulässige Verwendungen nach anderen Gesetzen ([357]).

3.3.3 *Aufsicht*

(197) Die Arbeit der koreanischen nationalen Sicherheitsbehörden wird von verschiedenen Stellen überwacht ([358]).

(198) Erstens sind im Antiterrorismusgesetz spezielle Aufsichtsmechanismen für die Terrorismusbekämpfung vorgesehen, einschließlich der Erhebung von Daten über Terrorverdächtige. Auf der Verwaltungsebene werden die Maßnahmen zur Terrorismusbekämpfung von der Kommission für Terrorismusbekämpfung überwacht; ([359]) der Direktor des NIS ist verpflichtet, der Kommission über Ermittlungen und das Aufspüren von Terrorverdächtigen Bericht zu erstatten, um die für die Terrorismusbekämpfung erforderlichen Daten und Materialien zu sammeln ([360]). Darüber hinaus überwacht der Menschenrechtsbeauftragte (Human Rights Protection Officer – HRPO) speziell die Einhaltung der Grundrechte bei der Terrorismusbekämpfung ([361]). Der HRPO wird vom Vorsitzenden der Kommission für Terrorismusbekämpfung aus einem Kreis von Personen ernannt, die bestimmte, im Durchführungserlass zum Antiterrorismusgesetz ([362]) aufgeführte Qualifikationen aufweisen, und zwar für eine (verlängerbare) Amtszeit von zwei Jahren; er kann nur aus bestimmten, begrenzten und berechtigten Gründen seines Amtes enthoben werden ([363]). In Ausübung seiner Aufsichtsfunktion kann der HRPO allgemeine

([354]) Artikel 83 Absatz 3 TBA.
([355]) Siehe auch Anhang II Abschnitt 3.2.3.
([356]) Siehe Anhang II Abschnitt 1.2.
([357]) Artikel 5 Absätze 1 und 2, Artikel 12 und Artikel 13-5 CPPA.
([358]) Siehe Anhang II Abschnitt 3.3.
([359]) Artikel 5 Absatz 3 des Antiterrorismusgesetzes. Die Kommission wird vom Premierminister geleitet und setzt sich aus mehreren Ministern und Leitern von Regierungsstellen zusammen, darunter dem Außenminister, dem Justizminister, dem Verteidigungsminister, dem Minister für Inneres und Sicherheit, dem Direktor des NIS und dem Generalkommissar der nationalen Polizei (Artikel 3 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz).
([360]) Artikel 9 Absatz 4 des Antiterrorismusgesetzes.
([361]) Artikel 7 des Antiterrorismusgesetzes.
([362]) D. h. Rechtsanwälte mit mindestens zehn Jahren Berufserfahrung, Personen mit Fachwissen auf dem Gebiet der Menschenrechte, die zehn Jahre lang (mindestens) die Stelle eines außerordentlichen Professors innehatten, Personen, die als höhere öffentliche Bedienstete in staatlichen Stellen oder lokalen Verwaltungen tätig waren oder die über mindestens zehn Jahre Berufserfahrung im Bereich der Menschenrechte, z. B. in einer Menschenrechtsorganisation verfügen (Artikel 7 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz).
([363]) Zum Beispiel, wenn er in einem Strafverfahren angeklagt ist, das mit seinen Aufgaben zusammenhängt, wenn er vertrauliche Informationen weitergibt oder wenn er langfristig geistig oder körperlich behindert ist (Artikel 7 Absatz 3 des Durchführungserlasses zum Antiterrorismusgesetz).

Empfehlungen zur Verbesserung des Schutzes der Menschenrechte ([364]) und spezifische Empfehlungen für Abhilfemaßnahmen abgeben, wenn eine Menschenrechtsverletzung festgestellt wurde ([365]). Die Behörden sind verpflichtet, den HRPO über die Folgemaßnahmen zu seinen Empfehlungen zu informieren ([366]).

(199) Zweitens überwacht die PIPC die Einhaltung der Datenschutzvorschriften durch die nationalen Sicherheitsbehörden, und zwar sowohl die geltenden Bestimmungen des PIPA (siehe Erwägungsgrund (149)) als auch die Einschränkungen und Garantien, die für die Erhebung personenbezogener Daten nach anderen Gesetzen gelten (CPPA, Antiterrorismusgesetz und TBA, siehe auch Erwägungsgrund (171)) ([367]). Bei der Ausübung dieser Aufsichtsfunktion kann die PIPC von all ihren Untersuchungs- und Abhilfebefugnissen Gebrauch machen, wie in Abschnitt 2.4.2 ausführlich beschrieben.

(200) Drittens unterliegt die Tätigkeit der nationalen Sicherheitsbehörden der unabhängigen Aufsicht der NHRC gemäß den in Erwägungsgrund (172) beschriebenen Verfahren ([368]).

(201) Viertens erstreckt sich die Aufsichtsfunktion des BAI auch auf die nationalen Sicherheitsbehörden, obwohl der NIS unter außergewöhnlichen Umständen bestimmte Daten oder Materialien verweigern kann, z. B. wenn es sich um Staatsgeheimnisse handelt und die Offenlegung ernsthafte Auswirkungen auf die nationale Sicherheit hätte ([369]).

(202) Schließlich wird die parlamentarische Aufsicht über die Tätigkeit des NIS von der Nationalversammlung wahrgenommen (über einen speziellen Geheimdienstausschuss) ([370]). Die Nationalversammlung verfügt nach dem CPPA über eine besondere Aufsichtsfunktion in Bezug auf den Einsatz von kommunikationsbeschränkenden Maßnahmen für die Zwecke der nationalen Sicherheit ([371]). Insbesondere kann die Nationalversammlung Kontrollen vor Ort von Abhörgeräten durchführen und sowohl den NIS als auch die Telekommunikationsanbieter, die Kommunikationsinhaltsdaten weitergegeben haben, auffordern, darüber zu berichten. Die Nationalversammlung kann auch ihre allgemeinen Aufsichtsaufgaben wahrnehmen (in Übereinstimmung mit den in Erwägungsgrund (174) beschriebenen Verfahren). Der Direktor des NIS ist nach dem NIS-Gesetz verpflichtet, unverzüglich zu antworten, wenn der Nachrichtendienstausschuss einen Bericht zu einer bestimmten Angelegenheit anfordert, ([372]) wobei für bestimmte besonders sensible Daten besondere Vorschriften gelten. So kann der Direktor des NIS eine Antwort oder eine Aussage vor dem Ausschuss nur unter außergewöhnlichen Umständen verweigern, d. h. wenn sich das Ersuchen auf Staatsgeheimnisse im Zusammenhang mit militärischen, diplomatischen oder mit nordkoreanischen Angelegenheiten bezieht, wenn deren öffentliches Bekanntwerden schwerwiegende Auswirkungen auf das „Schicksal der Nation" haben könnte ([373]). In diesem Fall kann der Geheimdienstausschuss den Premierminister um eine Erklärung ersuchen, und wenn innerhalb von sieben Tagen keine Erklärung abgegeben wird, darf die Antwort oder Aussage nicht verweigert werden.

3.3.4 *Rechtsbehelfe*

(203) Auch im Bereich der nationalen Sicherheit bietet das koreanische System verschiedene (gerichtliche) Möglichkeiten, Rechtsbehelfe zu erlangen, darunter auch Schadenersatz. Durch diese Mechanismen stehen betroffenen Personen wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung, die es ihnen insbesondere ermöglichen, ihre Rechte durchzusetzen, unter anderem das Auskunftsrecht hinsichtlich ihrer personenbezogenen Daten oder das Recht auf Berichtigung oder Löschung dieser Daten.

(204) Erstens können natürliche Personen gemäß Artikel 3 Absatz 5 und Artikel 4 Absätze 1, 3 und 4 PIPA gegenüber den nationalen Sicherheitsbehörden ihre Rechte auf Auskunft, Berichtigung, Löschung und Aussetzung der Verarbeitung ausüben. In Abschnitt 6 der Bekanntmachung Nr. 2021-5 (Anhang I dieses Beschlusses) wird näher erläutert, wie diese Rechte im Zusammenhang mit der Datenverarbeitung für die Zwecke der nationalen Sicherheit gelten. Insbesondere kann eine nationale Sicherheitsbehörde die Ausübung der Rechte verzögern,

([364]) Artikel 8 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz.

([365]) Artikel 9 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz. Der Menschenrechtsbeauftragte entscheidet eigenständig über den Beschluss von Empfehlungen, ist jedoch verpflichtet, die Empfehlungen dem Vorsitzenden der Kommission für Terrorismusbekämpfung mitzuteilen.

([366]) Artikel 9 Absatz 2 des Durchführungserlasses zum Antiterrorismusgesetz. Laut der offiziellen Erklärung der koreanischen Regierung würde ein Versäumnis bei der Umsetzung einer Empfehlung des HRPO an die Kommission für Terrorismusbekämpfung, einschließlich des Premierministers, weitergeleitet, obwohl es bisher nicht vorgekommen ist, dass die Empfehlungen des HRPO nicht umgesetzt wurden (siehe Abschnitt 3.3.1 des Anhangs II).

([367]) Anhang II Abschnitt 3.3.4.

([368]) Speziell im Hinblick auf den NIS hat die NHRC bereits Untersuchungen von Amts wegen durchgeführt und eine Reihe von Einzelbeschwerden bearbeitet. Siehe z. B. den NHRC-Jahresbericht 2018, S. 128 (abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) und den NHRC-Jahresbericht 2019, S. 70 (abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([369]) Artikel 13 Absatz 1 des NIS-Gesetzes.

([370]) Artikel 36 und Artikel 37 Absatz 1 Nummer 15 des Gesetzes über die Nationalversammlung.

([371]) Artikel 15 CPPA.

([372]) Artikel 15 Absatz 2 des NIS-Gesetzes.

([373]) Artikel 17 Absatz 2 des NIS-Gesetzes. „Staatsgeheimnisse" sind definiert als Tatsachen, Gegenstände oder Kenntnisse, die als Verschlusssachen eingestuft wurden, auf die nur ein begrenzter Personenkreis zugreifen darf und die zur Vermeidung einer schwerwiegenden Beeinträchtigung der nationalen Sicherheit keinem anderen Land und keiner anderen Organisation offengelegt werden dürfen. Siehe Artikel 13 Absatz 4 des NIS-Gesetzes.

beschränken oder ablehnen, nur soweit und solange dies zum Schutz eines wichtigen Ziels von öffentlichem Interesse erforderlich und verhältnismäßig ist (z. B. soweit und solange die Gewährung der Rechte eine laufende Ermittlung oder die nationale Sicherheit gefährden würde), oder wenn die Gewährung der Rechte zur Schädigung eines Dritten an Leib und Leben führen könnte. Die Berufung auf eine solche Einschränkung erfordert daher eine Abwägung der Rechte und Interessen des Einzelnen gegen das betroffene öffentliche Interesse und darf auf keinen Fall das Recht in seinem Wesensgehalt antasten (Artikel 37 Absatz 2 der Verfassung). Wird der Antrag abgelehnt oder die Ausübung der Rechte eingeschränkt, so sind der betroffenen Person unverzüglich die Gründe dafür mitzuteilen.

(205) Zweitens haben Einzelpersonen das Recht, im Rahmen des PIPA Rechtsbehelfe zu erwirken, wenn ihre Daten von einer nationalen Sicherheitsbehörde unter Verstoß gegen das PIPA oder gegen die Einschränkungen und Garantien in anderen Gesetzen, in denen die Erhebung personenbezogener Daten geregelt ist, verarbeitet wurden (insbesondere im CPPA, siehe hierzu Erwägungsgrund (171)) ([374]). Dieses Recht kann durch eine Beschwerde bei der PIPC (auch über das von der koreanischen Internet- und Sicherheitsbehörde betriebene Datenschutz-Callcenter) ausgeübt werden ([375]). Um den Zugang zu Rechtsbehelfen gegen koreanische Sicherheitsbehörden zu erleichtern, können EU-Bürger außerdem eine Beschwerde über ihre nationale Datenschutzbehörde bei der PIPC einreichen ([376]). In solchen Fällen benachrichtigt die PIPC die betroffene Person über die nationale Datenschutzbehörde, sobald die Untersuchung abgeschlossen ist, und unterrichtet sie ggf. über die verhängten Abhilfemaßnahmen. Auf der Grundlage des Gesetzes über die Verwaltungsgerichtsbarkeit können Einzelpersonen darüber hinaus die Entscheidungen oder die Untätigkeit der PIPC anfechten (siehe Erwägungsgrund (132)).

(206) Drittens können Einzelpersonen beim HRPO eine Beschwerde über die Verletzung ihres Rechts auf Privatsphäre/Datenschutz im Rahmen von Terrorismusbekämpfungsmaßnahmen (d. h. gemäß dem Antiterrorismusgesetz) ([377]) einreichen, der Abhilfemaßnahmen empfehlen kann. Da keinerlei Zulässigkeitsvoraussetzungen vor dem Menschenrechtsbeauftragten bestehen, wird eine Beschwerde auch dann bearbeitet, wenn die betroffene Person nicht nachweisen kann, dass sie tatsächlich einen Schaden erlitten hat (z. B. durch die angeblich unrechtmäßige Erhebung ihrer Daten durch eine nationale Sicherheitsbehörde) ([378]). Die zuständige Behörde muss den HRPO über alle Maßnahmen informieren, die sie zur Umsetzung ihrer Empfehlungen ergriffen hat.

(207) Viertens können Einzelpersonen eine Beschwerde über die Erhebung ihrer Daten durch die nationalen Sicherheitsbehörden bei der NHRC einreichen und gemäß dem in Erwägungsgrund (178) beschriebenen Verfahren Rechtsbehelfe erlangen ([379]).

(208) Schließlich stehen verschiedene Rechtsbehelfe zur Verfügung, ([380]) die es dem Einzelnen ermöglichen, sich auf die in Abschnitt 3.3.1 beschriebenen Einschränkungen und Garantien zu berufen, um Rechtsschutz zu erhalten. Insbesondere können Einzelpersonen die Rechtmäßigkeit von Maßnahmen der nationalen Sicherheitsbehörden auf der Grundlage des Gesetzes über die Verwaltungsgerichtsbarkeit (gemäß dem in Erwägungsgrund(181) beschriebenen Verfahren) oder des Verfassungsgerichtsgesetzes (siehe Erwägungsgrund (182)) anfechten. Darüber hinaus können sie Schadenersatz auf der Grundlage des Gesetzes über staatlichen Schadenersatz erhalten (wie in Erwägungsgrund (183) näher beschrieben).

4. SCHLUSSFOLGERUNG

(209) Die Kommission ist der Ansicht, dass in der Republik Korea durch das PIPA, die besonderen Vorschriften für bestimmte Sektoren (wie in Abschnitt 2 analysiert) und die zusätzlichen Garantien in der Bekanntmachung Nr. 2021-5 (Anhang I) ein Schutzniveau für aus der Europäischen Union übermittelte personenbezogene Daten gewährleistet wird, das der Sache nach demjenigen gleichwertig ist, das durch die Verordnung (EU) 2016/679 garantiert wird.

(210) Darüber hinaus ist die Kommission der Auffassung, dass die Aufsichtsmechanismen und Rechtsbehelfe im koreanischen Recht es insgesamt ermöglichen, Verstöße gegen die Datenschutzvorschriften durch Datenverantwortliche in Korea zu erkennen und in der Praxis zu bekämpfen und der betroffenen Person Rechtsbehelfe anzubieten, um Auskunft über ihre personenbezogenen Daten zu erhalten und schließlich die Berichtigung oder Löschung dieser Daten zu erwirken.

([374]) Artikel 58 Absatz 4 und Artikel 4 Absatz 5 PIPA. Siehe Anhang II Abschnitt 3.4.2.
([375]) Artikel 62 und Artikel 63 Absatz 2 PIPA.
([376]) Bekanntmachung Nr. 2021-5 (Anhang I Abschnitt 6).
([377]) Artikel 8 Absatz 1 Nummer 2 des Durchführungserlasses zum Antiterrorismusgesetz.
([378]) Siehe Anhang II Abschnitt 3.4.1.
([379]) Beispielsweise gehen bei der NHRC regelmäßig Beschwerden gegen den nationalen Nachrichtendienst ein, siehe die Angaben im NHRC-Jahresbericht 2019 zur Anzahl der zwischen 2015 und 2019 eingegangenen Beschwerden, S. 70 (abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Siehe Anhang II Abschnitt 3.4.4.

(211) Schließlich ist die Kommission auf der Grundlage der verfügbaren Informationen über die koreanische Rechtsordnung, einschließlich der in Anhang II enthaltenen Erklärungen, Zusicherungen und Pflichten der koreanischen Regierung, der Auffassung, dass jeder Eingriff in die Grundrechte der Personen, deren personenbezogene Daten aus der Europäischen Union an die Republik Korea übermittelt werden, durch koreanischen Behörden aus Gründen des öffentlichen Interesses, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, auf das zur Erreichung des betreffenden berechtigten Ziels unbedingt erforderliche Maß beschränkt ist und dass ein wirksamer Rechtsschutz gegen solche Eingriffe besteht.

(212) In Anbetracht der Feststellungen dieses Beschlusses ist daher zu beschließen, dass die Republik Korea ein angemessenes Schutzniveau im Sinne von Artikel 45 der Verordnung (EU) 2016/679, wie er unter Berücksichtigung der Charta der Grundrechte der Europäischen Union auszulegen ist, für personenbezogene Daten gewährleistet, die aus der Europäischen Union in die Republik Korea an die den Bestimmungen des PIPA unterliegenden Verantwortlichen für personenbezogene Daten in der Republik Korea übermittelt werden, mit Ausnahme religiöser Organisationen, soweit sie personenbezogene Daten für ihre Missionierungstätigkeiten verarbeiten, politischen Parteien, soweit sie personenbezogene Daten im Zusammenhang mit der Nominierung von Kandidaten verarbeiten und Datenverantwortlichen, die der Aufsicht der Finanzdienstleistungskommission über die Verarbeitung personenbezogener Kreditdaten gemäß dem Kreditdatengesetz unterliegen, soweit sie solche Daten verarbeiten.

5. AUSWIRKUNGEN DIESES BESCHLUSSES UND MAßNAHMEN DER DATENSCHUTZBEHÖRDEN

(213) Die Mitgliedstaaten und ihre Organe müssen die notwendigen Maßnahmen treffen, um Rechtsakten der Unionsorgane nachzukommen, da für diese Rechtsakte eine Vermutung der Rechtmäßigkeit gilt, sodass sie Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder infolge eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für ungültig erklärt wurden.

(214) Daher ist ein nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlassener Angemessenheitsbeschluss der Kommission für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. So können insbesondere Übermittlungen von einem Verantwortlichen oder Auftragsverarbeiter in der Europäischen Union an Datenverantwortliche in der Republik Korea ohne weitere Genehmigung vorgenommen werden.

(215) Es sei daran erinnert, dass gemäß Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und wie vom Gerichtshof der Europäischen Union im Urteil in der Rechtssache Schrems ([381]) erläutert Folgendes gilt: Wenn eine nationale Datenschutzbehörde, auch auf eine Beschwerde hin, die Vereinbarkeit eines Angemessenheitsbeschlusses der Kommission mit den Grundrechten des Einzelnen auf Privatsphäre und Datenschutz infrage stellt, muss das nationale Recht Rechtsbehelfe vorsehen, die es der Datenschutzbehörde ermöglichen, diese Rügen vor einem nationalen Gericht geltend zu machen, das gegebenenfalls ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss ([382]).

6. ÜBERWACHUNG UND ÜBERPRÜFUNG DIESES BESCHLUSSES

(216) Nach der Rechtsprechung des Gerichtshofs ([383]) und Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 sollte die Kommission nach Erlass eines Angemessenheitsbeschlusses die relevanten Entwicklungen in dem Drittland fortlaufend überwachen, um festzustellen, ob ein Drittland weiterhin ein im Wesentlichen gleichwertiges Schutzniveau bietet. Eine solche Kontrolle ist auf jeden Fall erforderlich, wenn der Kommission Informationen vorliegen, die Anlass zu begründeten Zweifeln geben.

(217) Daher sollte die Kommission die Situation in der Republik Korea in Bezug auf den Rechtsrahmen und die tatsächliche Praxis bei der Verarbeitung personenbezogener Daten, wie in diesem Beschluss geprüft, fortlaufend überwachen, einschließlich der Einhaltung der in Anhang II enthaltenen Erklärungen, Zusicherungen und Pflichten durch die koreanischen Behörden. Um diesen Prozess zu erleichtern, werden die koreanischen Behörden ersucht, die Kommission umgehend über wesentliche Entwicklungen im Zusammenhang mit diesem Beschluss zu unterrichten, und zwar in Bezug auf die Verarbeitung personenbezogener Daten durch Unternehmer und Behörden sowie hinsichtlich der Einschränkungen und Garantien, die für den Zugriff der Behörden auf personenbezogene Daten gelten.

([381]) Schrems, Rn. 65.
([382]) Schrems, Rn. 65. „Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen."
([383]) Schrems, Rn. 76.

(218) Damit die Kommission ihre Überwachungsfunktion wirksam ausüben kann, sollten die Mitgliedstaaten die Kommission über alle relevanten Maßnahmen der nationalen Datenschutzbehörden informieren, insbesondere über Anfragen oder Beschwerden von betroffenen EU-Bürgern in Bezug auf die Übermittlung personenbezogener Daten aus der Europäischen Union an Datenverantwortliche in der Republik Korea. Ferner sollte die Kommission über jegliche Hinweise darauf informiert werden, dass die Maßnahmen der koreanischen Behörden, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder für die nationale Sicherheit zuständig sind, einschließlich der Aufsichtsbehörden, nicht das erforderliche Schutzniveau gewährleisten.

(219) In Anwendung des Artikels 45 Absatz 3 der Verordnung (EU) 2016/679 ([384]) und angesichts der Tatsache, dass sich das von der koreanischen Rechtsordnung gewährte Schutzniveau ändern könnte, sollte die Kommission nach der Annahme dieses Beschlusses regelmäßig prüfen, ob die Feststellungen über die Angemessenheit des von der Republik Korea gewährleisteten Schutzniveaus noch sachlich und rechtlich gerechtfertigt sind.

(220) Zu diesem Zweck sollte dieser Beschluss innerhalb von drei Jahren nach seinem Inkrafttreten einer ersten Überprüfung unterzogen werden. Nach dieser ersten Überprüfung entscheidet die Kommission in enger Abstimmung mit dem nach Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschuss je nach Ergebnis, ob der Dreijahreszyklus beibehalten werden sollte. In jedem Fall sollten die anschließenden Überprüfungen mindestens alle vier Jahre stattfinden ([385]). Die Überprüfung sollte sich auf alle Aspekte der Funktionsweise dieses Beschlusses erstrecken, insbesondere auf die Anwendung der in Anhang I dieses Beschlusses enthaltenen zusätzlichen Garantien mit besonderem Augenmerk auf den Schutz im Falle der Weiterübertragung, auf die einschlägigen Entwicklungen in der Rechtsprechung, die Vorschriften über die Verarbeitung pseudonymisierter Daten für die Zwecke der Statistik, der wissenschaftlichen Forschung und der Archivierung im öffentlichen Interesse sowie die Anwendung der Ausnahmen nach Artikel 28 Absatz 7 PIPA, die Wirksamkeit der Ausübung der Rechte des Einzelnen, auch vor der kürzlich reformierten PIPC, und auf die Anwendung der Ausnahmen von diesen Rechten, die Anwendung der teilweisen Ausnahmen nach dem PIPA sowie die Einschränkungen und Garantien in Bezug auf den Zugang der Behörden (wie in Anhang II dieses Beschlusses dargelegt), einschließlich der Zusammenarbeit der PIPC mit den EU-Datenschutzbehörden bei individuellen Beschwerden. Sie sollte auch die Wirksamkeit der Aufsicht und Durchsetzung in Bezug auf das PIPA und im Bereich der Strafverfolgung und der nationalen Sicherheit (insbesondere durch die PIPC und die NHRC) umfassen.

(221) Zur Durchführung der Überprüfung sollte die Kommission mit der PIPC zusammenkommen, gegebenenfalls unter Mitwirkung anderer koreanischen Behörden, die für den staatlichen Zugriff zuständig sind, einschließlich der zuständigen Aufsichtsbehörden. Die Teilnahme an diesem Treffen sollte Vertretern der Mitglieder des Europäischen Datenschutzausschusses offenstehen. Im Rahmen der Überprüfung sollte die Kommission die PIPC ersuchen, umfassende Informationen über alle Aspekte, die für die Feststellung der Angemessenheit von Belang sind, vorzulegen, auch über die Einschränkungen und Garantien in Bezug auf den staatlichen Zugriff ([386]). Die Kommission sollte auch Erläuterungen zu allen für diesen Beschluss maßgeblichen, ihr vorliegenden Informationen einholen, einschließlich öffentlicher Berichte von koreanischen Behörden oder anderen Beteiligten in Korea, dem Europäischen Datenschutzausschuss, einzelnen Datenschutzbehörden, zivilgesellschaftlichen Gruppen, Medienberichten oder jeder anderen verfügbaren Informationsquelle.

(222) Auf der Grundlage der Überprüfung sollte die Kommission einen öffentlichen Bericht erstellen, der dem Europäischen Parlament und dem Rat vorgelegt wird.

7. AUSSETZUNG, AUFHEBUNG ODER ÄNDERUNG DIESES BESCHLUSSES

(223) Lassen verfügbare Informationen – insbesondere Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder von den koreanischen Behörden oder der Mitgliedstaaten zur Verfügung gestellt werden – darauf schließen, dass das von der Republik Korea gewährleistete Schutzniveau möglicherweise nicht mehr angemessen ist, sollte die Kommission die zuständigen koreanischen Behörden umgehend davon in Kenntnis setzen und sie ersuchen, innerhalb einer bestimmten, angemessenen Frist geeignete Maßnahmen zu ergreifen.

(224) Falls die zuständigen koreanischen Behörden nach Ablauf dieser Frist keine derartigen Maßnahmen ergriffen haben oder nicht auf andere Weise glaubhaft gemacht haben, dass dieser Beschluss weiterhin auf einem angemessenen Schutzniveau beruht, wird die Kommission das Verfahren gemäß Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 einleiten, um diesen Beschluss teilweise oder vollständig auszusetzen oder aufzuheben.

(225) Alternativ wird die Kommission dieses Verfahren einleiten, um den Beschluss zu ändern, indem sie insbesondere Datenübermittlungen zusätzlichen Bedingungen unterwirft oder den Anwendungsbereich der Angemessenheitsfeststellung auf Datenübermittlungen beschränkt, für die auch weiterhin ein angemessenes Schutzniveau gewährleistet ist.

([384]) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 ist „[i]n dem Durchführungsrechtsakt … ein Mechanismus für eine regelmäßige Überprüfung, … vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird."

([385]) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 muss „mindestens alle vier Jahre eine regelmäßige Überprüfung stattfinden". Siehe auch Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254 Rev. 01.

([386]) Siehe Anhang II des vorliegenden Beschlusses.

(226) Konkret sollte die Kommission das Verfahren zur Aussetzung oder Aufhebung einleiten, wenn Hinweise darauf vorliegen, dass die zusätzlichen Garantien in Anhang I von Unternehmern, die nach diesem Beschluss personenbezogene Daten erhalten, nicht eingehalten und/oder nicht wirksam durchgesetzt werden, oder dass die koreanischen Behörden den Erklärungen, Zusicherungen und Pflichten in Anhang II nicht nachkommen.

(227) Die Kommission sollte ferner die Einleitung des Verfahrens zur Änderung, Aussetzung oder Aufhebung dieses Beschlusses in Betracht ziehen, wenn die zuständigen koreanischen Behörden im Rahmen der Überprüfung oder anderweitig nicht die Informationen oder Erläuterungen liefern, die für die Bewertung des Schutzniveaus für personenbezogene Daten, die aus der Europäischen Union an die Republik Korea übermittelt werden, oder für die Einhaltung dieses Beschlusses erforderlich sind. In diesem Zusammenhang sollte die Kommission Überlegungen dazu anstellen, inwieweit die relevanten Informationen aus anderen Quellen bezogen werden können.

(228) In hinreichend begründeten Fällen äußerster Dringlichkeit wird die Kommission von der Möglichkeit Gebrauch machen, nach dem in Artikel 93 Absatz 3 der Verordnung (EU) 2016/679 genannten Verfahren sofort geltende Durchführungsrechtsakte zur Aussetzung, Aufhebung oder Änderung des Beschlusses zu erlassen.

8. **SCHLUSSBEMERKUNGEN**

(229) Der Europäische Datenschutzausschuss hat seine Stellungnahme ([387]) veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

(230) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 bietet die Republik Korea ein angemessenes Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Rechtsträger in der Republik Korea übermittelt werden, die dem Gesetz zum Schutz personenbezogener Daten, ergänzt durch die in Anhang I aufgeführten zusätzlichen Garantien, in Verbindung mit den offiziellen Erklärungen, Zusicherungen und Pflichten in Anhang II unterliegen.

(2) Dieser Beschluss gilt nicht für personenbezogene Daten, die an Empfänger übermittelt werden, die unter eine der folgenden Kategorien fallen, soweit die Zwecke der Verarbeitung der personenbezogenen Daten ganz oder teilweise einem der dort jeweils aufgeführten Zwecke entsprechen:

a) religiöse Einrichtungen, soweit sie personenbezogene Daten für die Zwecke Missionierungstätigkeiten verarbeiten,

b) politische Parteien, soweit sie personenbezogene Daten im Zusammenhang mit der Nominierung von Kandidaten verarbeiten,

c) Rechtsträger, die der Aufsicht der Finanzdienstleistungskommission über die Verarbeitung personenbezogener Kreditdaten gemäß dem Kreditdatengesetz unterliegen, soweit sie solche Daten verarbeiten.

Artikel 2

Üben die zuständigen Behörden in den Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ihre Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 im Hinblick auf die Übermittlung von Daten im Rahmen des Anwendungsbereichs gemäß Artikel 1 dieses Beschlusses aus, so unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission.

Artikel 3

(1) Um zu prüfen, ob die Republik Korea weiter ein angemessenes Schutzniveau im Sinne des Artikels 1 bietet, überwacht die Kommission fortlaufend die Anwendung des Rechtsrahmens, auf den sich dieser Beschluss stützt, einschließlich der Bedingungen, unter denen Weiterübermittlungen vorgenommen werden, individuelle Rechte ausgeübt werden und die Behörden der Republik Korea Zugang zu Daten haben, die auf der Grundlage dieses Beschlusses übermittelt werden.

([387]) Stellungnahme 32/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Richtlinie (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten in der Republik Korea, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

(2) Die Mitgliedstaaten und die Kommission unterrichten einander über Fälle, in denen die Kommission für den Schutz personenbezogener Daten oder eine andere zuständige koreanische Behörde die Einhaltung des Rechtsrahmens, auf den sich dieser Beschluss stützt, nicht gewährleistet.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über Hinweise darauf, dass Eingriffe koreanischer Behörden in das Recht von Einzelpersonen auf Schutz ihrer personenbezogenen Daten über den unbedingt erforderlichen Umfang hinausgehen oder dass es keinen wirksamen Rechtsschutz gegen solche Eingriffe gibt.

(4) Drei Jahren nach dem Tag der Bekanntgabe dieses Beschlusses an die Mitgliedstaaten und danach mindestens alle vier Jahre evaluiert die Kommission die Feststellung in Artikel 1 Absatz 1 auf der Grundlage aller verfügbaren Informationen, einschließlich der Informationen, die sie im Rahmen der mit den zuständigen koreanischen Behörden durchgeführten Überprüfung erhalten hat.

(5) Liegen der Kommission Hinweise darauf vor, dass ein angemessenes Schutzniveau nicht länger gewährleistet ist, so unterrichtet die Kommission die zuständigen koreanischen Behörden. Erforderlichenfalls kann sie beschließen, diesen Beschluss gemäß Artikel 45 Absatz 5 der Verordnung (EU) 2016/679 auszusetzen, zu ändern oder aufzuheben oder seinen Anwendungsbereich einzuschränken, insbesondere wenn Hinweise darauf vorliegen, dass

a) Datenverantwortliche in Korea, die nach diesem Beschluss personenbezogene Daten aus der Europäischen Union erhalten haben, die in Anhang I festgelegten zusätzlichen Garantien nicht beachten oder Aufsicht und Durchsetzung diesbezüglich unzureichend sind,

b) die koreanischen Behörden den Erklärungen, Zusicherungen und Pflichten in Anhang II nicht nachkommen, unter anderem im Hinblick auf die Voraussetzungen und Einschränkungen für die Erhebung von und den Zugang zu nach diesem Beschluss übermittelten personenbezogenen Daten durch koreanische Behörden für die Zwecke der Strafverfolgung oder der nationalen Sicherheit.

Die Kommission kann solche Maßnahmen auch dann ergreifen, wenn sie aufgrund mangelnder Kooperation der koreanischen Regierung nicht feststellen kann, ob die Republik Korea weiterhin ein angemessenes Schutzniveau gewährleistet.

Artikel 4

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 17. Dezember 2021

Für die Kommission
Didier REYNDERS
Mitglied der Kommission

ANHANG I

ERGÄNZENDE VORSCHRIFTEN FÜR DIE AUSLEGUNG UND ANWENDUNG DES KOREANISCHEN GESETZES ZUM SCHUTZ PERSONENBEZOGENER DATEN IN ZUSAMMENHANG MIT DER VERARBEITUNG VON NACH KOREA ÜBERMITTELTEN PERSONENBEZOGENEN DATEN

Inhalt

I. **Überblick**

Infolge der Angemessenheitsgespräche zwischen Korea und der Europäischen Union (EU) hat die Europäische Kommission festgestellt, dass Korea ein angemessenes Schutzniveau für personenbezogene Daten gemäß Artikel 45 der DSGVO bietet.

Die Kommission für den Schutz personenbezogener Daten (Personal Information Protection Commission, PIPC) hat in diesem Zusammenhang auf der Grundlage des Artikels 5 (Pflichten des Staates usw.) und des Artikels 14 (Internationale Zusammenarbeit) ([1]) des Gesetzes zum Schutz personenbezogener Daten (Personal Information Protection Act, PIPA, im Folgenden auch „Gesetz") die vorliegende Bekanntmachung beschlossen, um die Auslegung, Anwendung und Durchsetzung einiger Bestimmungen des Gesetzes zu klären, u. a. auch in Bezug auf die Verarbeitung personenbezogener Daten, die auf der Grundlage des Angemessenheitsbeschlusses der EU nach Korea übermittelt werden.

Da diese Bekanntmachung den Status einer Verwaltungsvorschrift hat, die die zuständige Verwaltungsbehörde erlässt und bekannt gibt, um die Standards der Auslegung, Anwendung und Durchsetzung des PIPA in der koreanischen Rechtsordnung zu erläutern, ist sie für den Verantwortlichen für die Verarbeitung personenbezogener Daten rechtlich bindend in dem Sinne, dass jeder Verstoß gegen diese Bekanntmachung als Verstoß gegen die einschlägigen Bestimmungen des PIPA betrachtet werden kann. Wenn durch einen Verstoß gegen diese Bekanntmachung persönliche Rechte und Interessen verletzt werden, haben die betroffenen Personen außerdem das Recht, bei der PIPC oder vor Gericht Rechtsbehelfe einzulegen.

Trifft der Verantwortliche, der die nach dem Angemessenheitsbeschluss der EU nach Korea übermittelten personenbezogenen Daten verarbeitet, keine Maßnahmen entsprechend dieser Bekanntmachung, so wird gemäß Artikel 64 Absätze 1 und 2 des Gesetzes davon ausgegangen, „dass wesentliche Gründe für die Annahme bestehen, dass eine Verletzung des Schutzes personenbezogener Daten vorliegt und bei Untätigkeit ein schwer zu behebender Schaden wahrscheinlich

([1]) Gemäß Artikel 14 PIPA ist die koreanische Regierung befugt, Maßnahmen zu ergreifen, um den Schutz personenbezogener Daten im internationalen Umfeld zu verbessern und Verletzungen der Rechte betroffener Personen zu verhindern, die auf die grenzüberschreitende Übermittlung personenbezogener Daten zurückzuführen sind.

ist". In solchen Fällen können die PIPC oder die zuständigen zentralen Verwaltungsbehörden den Verantwortlichen für die Verarbeitung personenbezogener Daten entsprechend der ihnen mit dieser Bestimmung übertragenen Befugnis anweisen, Abhilfemaßnahmen zu ergreifen usw., und je nach Gesetzesverstoß kann auch eine entsprechende Strafe (Sanktionen, Geldbußen usw.) verhängt werden.

II. **Begriffsbestimmungen**

Für die Zwecke dieser Bestimmung bezeichnet der Ausdruck

i. „Gesetz" das Gesetz zum Schutz personenbezogener Daten (Gesetz Nr. 16930, am 4. Februar 2020 geändert und am 5. August 2020 in Kraft getreten),

ii. „Präsidialerlass" den Erlass zur Durchführung des Gesetzes zum Schutz personenbezogener Daten (Präsidialerlass Nr. 30509 vom 3. März 2020, Erlass zur Änderung anderer Rechtsakte),

iii. „betroffene Person" eine natürliche Person, die durch gemäß diesen Vorschriften verarbeitete Daten identifizierbar ist und auf die sich diese Daten beziehen,

iv. „Verantwortlicher für die Verarbeitung personenbezogener Daten" (im Folgenden „Datenverantwortlicher") eine öffentliche Einrichtung, juristische Person, Organisation, natürliche Person usw., die personenbezogene Daten direkt oder indirekt im Rahmen ihrer Tätigkeiten verarbeitet,

v. „EU" die EU (Stand: Ende Februar 2020, 27 Mitgliedstaaten [2]): Belgien, Bulgarien, Tschechien, Dänemark, Deutschland, Estland, Irland, Griechenland, Spanien, Frankreich, Kroatien, Italien, Zypern, Lettland, Litauen, Luxemburg, Ungarn, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Slowenien, Slowakei, Finnland, Schweden) sowie die Länder, die über das EWR-Abkommen mit der EU assoziiert sind (Island, Liechtenstein, Norwegen),

vi. „DSGVO" das allgemeine Datenschutzgesetz der EU, die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679),

vii. „Angemessenheitsbeschluss" einen Beschluss der Europäischen Kommission gemäß Artikel 45 Absatz 3 der DSGVO darüber, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bieten.

III. **Ergänzende Vorschriften**

1. **Beschränkung auf eine zweckgebundene Nutzung und Übermittlung personenbezogener Daten (Artikel 3, 15 und 18 des Gesetzes)**

<Gesetz zum Schutz personenbezogener Daten

(Gesetz Nr. 16930, teilweise geändert am 4. Februar 2020)>

Artikel 3 (Grundsätze des Schutzes personenbezogener Daten) (1) Der Datenverantwortliche gibt ausdrücklich an, für welche Zwecke die personenbezogenen Daten verarbeitet werden, erhebt die personenbezogenen Daten in rechtmäßiger und fairer Weise und nur in dem Ausmaß, wie es für die Verarbeitungszwecke erforderlich ist.

(2) Der Datenverantwortliche verarbeitet die personenbezogenen Daten in geeigneter Weise entsprechend den Erfordernissen für die Zwecke ihrer Verarbeitung und darf sie nicht für andere Zwecke nutzen.

Artikel 15 (Erhebung und Nutzung personenbezogener Daten) (1) Ein Datenverantwortlicher kann unter folgenden Umständen personenbezogene Daten erheben und für den Zweck ihrer Erhebung nutzen:

1. wenn die Einwilligung der betroffenen Personen eingeholt wurde,

2. bei entsprechenden besonderen Bestimmungen in Gesetzen oder wenn dies für die Einhaltung rechtlicher Pflichten unumgänglich ist,

3. wenn eine öffentliche Einrichtung andernfalls ihre Aufgaben in ihrem Zuständigkeitsbereich gemäß den Gesetzen usw. nicht wahrnehmen kann,

4. wenn dies für die Durchführung und Erfüllung eines Vertrags mit einer betroffenen Person unbedingt erforderlich ist,

[2] Bis zum Ende des Übergangszeitraums gehört gemäß den Artikeln 126, 127 und 132 des Abkommens über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft (ABl. C 384 I vom 12.11.2019, S. 1) auch das Vereinigte Königreich dazu.

5. wenn dies als eindeutig erforderlich erachtet wird, um Leib und Leben oder die Eigentumsinteressen der betroffenen Person oder eines Dritten vor unmittelbarer Gefahr zu schützen, sofern die betroffene Person oder ihr gesetzlicher Vertreter nicht zu einer Willensäußerung in der Lage ist oder eine vorherige Einwilligung wegen unbekannter Anschrift usw. nicht eingeholt werden kann,
6. wenn dies für das berechtigte Interesse eines Datenverantwortlichen erforderlich ist, das eindeutig Vorrang vor den Rechten der betroffenen Person hat. In solchen Fällen ist die Verarbeitung nur insoweit zulässig, als sie in einem wesentlichen Zusammenhang mit dem berechtigten Interesse des Datenverantwortlichen steht und nicht über einen angemessenen Umfang hinausgeht.

Artikel 18 (Beschränkung auf eine zweckgebundene Nutzung und Übermittlung personenbezogener Daten) (1) Ein Datenverantwortlicher darf personenbezogene Daten nur in dem Maße nutzen, wie in Artikel 15 Absatz 1 und Artikel 39-3 Absätze 1 und 2 festgelegt ist, und darf sie nur in dem in Artikel 17 Absätze 1 und 3 vorgesehenen Rahmen an Dritte übermitteln.

(2) Unbeschadet des Absatzes 1 kann ein Datenverantwortlicher in den Fällen unter den folgenden Nummern personenbezogene Daten für andere Zwecke nutzen oder einem Dritten übermitteln, es sei denn, dass dadurch die Interessen einer betroffenen Person oder eines Dritten in unfairer Weise verletzt werden. Für Anbieter von Informations- und Kommunikationsdiensten, die personenbezogene Daten von Nutzern verarbeiten, gelten dabei nur die Nummern 1 und 2 („Anbieter von Informations- und Kommunikationsdiensten“ und „Nutzer“ hier und im Folgenden im Sinne des Artikels 2 Absatz 1 Nummer 3 bzw. 4 des Gesetzes zur Förderung der Nutzung von Informations- und Kommunikationsnetzen und des Datenschutzes usw. (Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.)); die Nummern 5 bis 9 gelten nur für öffentliche Einrichtungen:

1. wenn eine zusätzliche Einwilligung der betroffenen Person eingeholt wurde,
2. bei entsprechenden besonderen Bestimmungen in Gesetzen,
3. wenn dies als eindeutig erforderlich erachtet wird, um Leib und Leben oder die Eigentumsinteressen der betroffenen Person oder eines Dritten vor unmittelbarer Gefahr zu schützen, sofern die betroffene Person oder ihr gesetzlicher Vertreter nicht zu einer Willensäußerung in der Lage ist oder wegen unbekannter Anschrift keine vorherige Einwilligung eingeholt werden kann,
4. gestrichen <durch das Gesetz Nr. 16930 vom 4. Februar 2020>
5. wenn die Wahrnehmung der in einem Rechtsakt vorgesehenen Aufgaben im Zuständigkeitsbereich des Datenverantwortlichen nicht möglich ist, es sei denn, dass dieser die personenbezogenen Daten für einen anderen als den vorgesehenen Zweck nutzt oder sie an einen Dritten übermittelt, und wenn die Kommission darüber beraten und einen entsprechenden Entschluss gefasst hat,
6. wenn es für die Durchführung eines Vertrags oder einer anderen internationalen Übereinkunft erforderlich ist, einer ausländischen Regierung oder einer internationalen Organisation personenbezogene Daten zu übermitteln,
7. wenn dies für die Untersuchung einer Straftat, eine Anklage und ein strafrechtliches Verfahren erforderlich ist,
8. wenn dies für ein Gericht erforderlich ist, um verfahrensbezogene Aufgaben wahrzunehmen,
9. wenn dies für die Vollstreckung einer Strafe oder zur Durchsetzung einer Bewährungszeit oder Untersuchungshaft erforderlich ist.

[Absätze 3 und 4 ausgelassen]

(5) Übermittelt ein Datenverantwortlicher einem Dritten in einem der in Absatz 2 beschriebenen Fälle personenbezogene Daten für einen anderen als den vorgesehenen Zweck, so fordert der Datenverantwortliche den Empfänger der personenbezogenen Daten auf, den Zweck und die Art der Nutzung sowie andere erforderliche Aspekte einzuschränken oder die erforderlichen Vorkehrungen zu treffen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Person, die ein solches Ersuchen erhält, trifft die erforderlichen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten.

i) In Artikel 3 Absätze 1 und 2 des Gesetzes wird der Grundsatz dargelegt, dass ein Datenverantwortlicher personenbezogene Daten nur in dem Ausmaß erheben darf, wie es für die rechtmäßige Verarbeitung der personenbezogenen Daten erforderlich ist, und dass er sie nicht für andere Zwecke als den vorgesehenen nutzen darf. ([3])

ii) Nach diesem Grundsatz sieht Artikel 15 Absatz 1 des Gesetzes vor, dass ein Datenverantwortlicher die erhobenen personenbezogenen Daten für den Zweck ihrer Erhebung nutzen darf, und sieht Artikel 18 Absatz 1 vor, dass personenbezogene Daten nicht für einen anderen als den Zweck der Erhebung genutzt oder einem Dritten übermittelt werden dürfen.

([3]) Da in diesen Bestimmungen allgemeine Grundsätze beschrieben werden, die für jede Verarbeitung personenbezogener Daten gelten, einschließlich einer Verarbeitung, die ausdrücklich durch andere Gesetze geregelt wird, gelten die Erläuterungen dieses Abschnitts auch dann, wenn personenbezogene Daten auf der Grundlage anderer Gesetze verarbeitet werden (siehe z. B. Artikel 15 Absatz 1 des Kreditdatengesetzes (Credit Information Act), in dem ausdrücklich auf diese Bestimmungen Bezug genommen wird).

iii) Auch wenn personenbezogene Daten in den Ausnahmefällen ([4]) gemäß den Nummern des Artikels 18 Absatz 2 des Gesetzes für andere Zwecke als den vorgesehenen genutzt oder einem Dritten übermittelt werden dürfen, so ist in diesen Fällen darum zu ersuchen, dass der Zweck oder die Art der Nutzung eingeschränkt werden, damit die personenbezogenen Daten gemäß Absatz 5 sicher verarbeitet werden können, oder dass Maßnahmen getroffen werden, die zur Gewährleistung der Sicherheit der personenbezogenen Daten erforderlich sind.

iv) Die vorstehenden Bestimmungen gelten unabhängig von der Staatsangehörigkeit der betroffenen Person für die Verarbeitung aller personenbezogenen Daten, die im Hoheitsgebiet Koreas aus einem Drittland empfangen werden.

v) Übermittelt beispielsweise ein Verantwortlicher aus der EU personenbezogene Daten gemäß dem Angemessenheitsbeschluss der Europäischen Kommission an einen koreanischen Datenverantwortlichen, so gilt der Zweck, für den der Verantwortliche aus der EU die personenbezogenen Daten übermittelt, als Erhebungszweck des koreanischen Datenverantwortlichen, und dieser darf die personenbezogenen Daten ausschließlich im Rahmen des Erhebungszwecks nutzen oder einem Dritten übermitteln, wenn nicht einer der in den Nummern des Artikels 18 Absatz 2 genannten Ausnahmefälle vorliegt.

2. **Einschränkung der Übermittlung personenbezogener Daten (Artikel 17 Absätze 3 und 4 und Artikel 18 des Gesetzes)**

<Gesetz zum Schutz personenbezogener Daten

(Gesetz Nr. 16930, teilweise geändert am 4. Februar 2020)>

Artikel 17 (Übermittlung personenbezogener Daten) [Absatz 1 ausgelassen]

(2) Ein Datenverantwortlicher informiert die betroffene Person über die folgenden Punkte, wenn er die Einwilligung gemäß Absatz 1 Nummer 1 einholt. Gleiches gilt, wenn sich einer der folgenden Punkte ändert:

1. der Empfänger der personenbezogenen Daten,
2. der Zweck, für den der Empfänger der personenbezogenen Daten diese nutzt,
3. Einzelheiten zu den zu übermittelnden personenbezogenen Daten,
4. der Zeitraum, über den der Empfänger die personenbezogenen Daten speichert und nutzt,
5. die Berechtigung der betroffenen Person, die Einwilligung zu verweigern, und etwaige Nachteile, die sich aus der Verweigerung der Einwilligung ergeben.

(3) Der Datenverantwortliche teilt der betroffenen Person die in Absatz 2 genannten Informationen mit und holt die Einwilligung der betroffenen Person ein, bevor er personenbezogene Daten an einen Dritten im Ausland übermittelt, und er darf keinen Vertrag über die grenzüberschreitende Übermittlung personenbezogener Daten schließen, der gegen dieses Gesetz verstößt.

(4) Ein Datenverantwortlicher kann personenbezogene Daten ohne Einwilligung der betroffenen Person übermitteln, wenn dies in einem angemessenen Zusammenhang mit den Zwecken steht, für die die personenbezogenen Daten ursprünglich erhoben wurden; gemäß den per Präsidialerlass festgelegten Bestimmungen ist dabei zu berücksichtigen, ob der betroffenen Person Nachteile entstehen, ob die erforderlichen Sicherheitsmaßnahmen (z. B. Verschlüsselung) getroffen wurden usw.

[Siehe die Seiten 3, 4 und 5 in Bezug auf Artikel 18.]

<Erlass zur Durchführung des Gesetzes zum Schutz personenbezogener Daten

(Datum des Inkrafttretens: 5. Februar 2021. Präsidialerlass Nr. 30892 vom 4. August 2020, Erlass zur Änderung anderer Rechtsakte)>

Artikel 14-2 (Standards für die zusätzliche Nutzung oder Übermittlung personenbezogener Daten usw.)

(1) Nutzt oder übermittelt ein Datenverantwortlicher gemäß Artikel 15 Absatz 3 des Gesetzes oder Artikel 17 Absatz 4 des Gesetzes personenbezogene Daten ohne Einwilligung der betroffenen Person (im Folgenden „zusätzliche Nutzung oder Übermittlung personenbezogener Daten"), prüft der Datenverantwortliche,

1. ob dies in einem angemessenen Zusammenhang mit dem ursprünglichen Zweck der Erhebung der personenbezogenen Daten steht,
2. ob eine zusätzliche Nutzung oder Übermittlung der personenbezogenen Daten angesichts der Umstände ihrer Erhebung und der Verarbeitungspraxis absehbar ist,
3. ob die zusätzliche Nutzung oder Übermittlung der personenbezogenen Daten die Interessen der betroffenen Person nicht in unfairer Weise verletzt und
4. ob die zur Gewährleistung der Sicherheit erforderlichen Maßnahmen wie Pseudonymisierung oder Verschlüsselung getroffen wurden.

([4]) Für Anbieter von Informations- und Kommunikationsdiensten gelten nur die Nummern 1 und 2 des Artikels 18 Absatz 2. Die Nummern 5 bis 9 gelten nur für öffentliche Einrichtungen.

(2) Der Datenverantwortliche legt vorab in der Datenschutzerklärung die Kriterien für die Bewertung der unter den Nummern des Absatzes 1 genannten Punkte gemäß Artikel 30 Absatz 1 des Gesetzes offen, und der Datenschutzbeauftragte gemäß Artikel 31 Absatz 1 des Gesetzes prüft, ob der Datenverantwortliche die zusätzlichen personenbezogenen Daten nach den einschlägigen Standards nutzt oder übermittelt.

i) Übermittelt der Datenverantwortliche personenbezogene Daten an einen Dritten im Ausland, so muss er den betroffenen Personen vorab alle in Artikel 17 Absatz 2 des Gesetzes genannten Informationen mitteilen und ihre Einwilligung einholen; davon ausgenommen sind die nachfolgend in den Absätzen 1 und 2 beschriebenen Fälle. Es darf kein Vertrag über die grenzüberschreitende Übermittlung personenbezogener Daten abgeschlossen werden, der gegen dieses Gesetz verstößt.

(1) Wenn die Übermittlung der personenbezogenen Daten gemäß Artikel 17 Absatz 4 des Gesetzes in einem angemessenen Zusammenhang mit dem ursprünglichen Zweck der Erhebung steht. Diese Bestimmung kann jedoch nur auf Fälle angewandt werden, in denen die Standards für die zusätzliche Nutzung und Übermittlung personenbezogener Daten gemäß Artikel 14-2 des Durchführungserlasses erfüllt sind. Außerdem muss der Datenverantwortliche prüfen, ob den betroffenen Personen durch die Übermittlung der personenbezogenen Daten Nachteile entstehen könnten, und ob die für die Gewährleistung der Sicherheit erforderlichen Maßnahmen, z. B. Verschlüsselung, getroffen wurden.

(2) Ausnahmefälle gemäß Artikel 18 Absatz 2 des Gesetzes, in denen personenbezogene Daten an Dritte übermittelt werden dürfen (siehe die Seiten 3–5). Selbst in solchen Fällen dürfen die personenbezogenen Daten jedoch nicht an einen Dritten übermittelt werden, wenn eine unfaire Verletzung der Interessen der betroffenen Person oder eines Dritten durch diese Übermittlung wahrscheinlich ist. Darüber hinaus muss der Übermittler der personenbezogenen Daten den Empfänger der personenbezogenen Daten darum ersuchen, den Zweck oder die Art der Nutzung der personenbezogenen Daten einzuschränken oder die erforderlichen Maßnahmen zur Gewährleistung ihrer Sicherheit zu treffen, damit die personenbezogenen Daten sicher verarbeitet werden können.

ii) Werden personenbezogene Daten an einen Dritten im Ausland übermittelt, so wird aufgrund der Unterschiede in den Systemen zum Schutz personenbezogener Daten zwischen verschiedenen Ländern möglicherweise nicht das durch das koreanische Gesetz zum Schutz personenbezogener Daten gewährleistete Schutzniveau erreicht. Dementsprechend werden solche Fälle als „Fälle, in denen der betroffenen Person Nachteile entstehen können“ im Sinne des Artikels 17 Absatz 4 des Gesetzes oder als „Fälle, in denen die Interessen einer betroffenen Person oder eines Dritten in unfairer Weise verletzt werden“ im Sinne des Artikels 18 Absatz 2 des Gesetzes und des Artikels 14-2 des Erlasses zur Durchführung des Gesetzes betrachtet ([5]). Um die Anforderungen dieser Bestimmungen zu erfüllen, müssen der Datenverantwortliche und der Dritte daher ausdrücklich ein dem Gesetz gleichwertiges Schutzniveau gewährleisten, einschließlich der in einem rechtsverbindlichen Dokument, z. B. einem Vertrag, festgelegten Garantie, dass die betroffene Person ihre Rechte auch nach der Übermittlung der personenbezogenen Daten ins Ausland ausüben kann.

3. **Unterrichtung über personenbezogene Daten, die nicht von der betroffenen Person übermittelt wurden (Artikel 20 des Gesetzes)**

<Gesetz zum Schutz personenbezogener Daten

(Gesetz Nr. 16930, teilweise geändert am 4. Februar 2020)>

Artikel 20 (Unterrichtung über die Quellen usw. bei durch Dritte erhobenen personenbezogenen Daten) (1) Wenn ein Datenverantwortlicher personenbezogene Daten verarbeitet, die von Dritten erhoben wurden, erteilt der Datenverantwortliche der betroffenen Person auf deren Anfrage unverzüglich Auskunft über die folgenden Punkte:

1. die Quelle der erhobenen personenbezogenen Daten,
2. den Zweck der Verarbeitung der personenbezogenen Daten,
3. die Berechtigung der betroffenen Person gemäß Artikel 37, die Aussetzung der Verarbeitung der personenbezogenen Daten zu verlangen.

(2) Unbeschadet des Absatzes 1 gilt Folgendes: Wenn ein Datenverantwortlicher, der die per Präsidialerlass festgelegten Kriterien im Hinblick auf die Art und den Umfang der verarbeiteten personenbezogenen Daten, die Zahl der Beschäftigten, die Höhe der Umsätze usw. erfüllt, personenbezogene Daten von Dritten erhebt und gemäß Artikel 17 Absatz 1 Nummer 1 verarbeitet, unterrichtet der Datenverantwortliche die betroffene Person über die in Absatz 1 genannten Punkte, es sei denn, dass die von dem Datenverantwortlichen erhobenen Daten keine personenbezogenen Daten, z. B. Kontaktdaten, enthalten, die die Benachrichtigung der betroffenen Person ermöglichen.

([5]) Gemäß Artikel 18 Absatz 2 Nummer 2 PIPA gilt dies auch, wenn personenbezogene Daten auf der Grundlage von Bestimmungen anderer Gesetze (z. B. des Kreditdatengesetzes) Dritten im Ausland offengelegt werden.

(3) Die nötigen Einzelheiten in Bezug auf den Zeitrahmen, die Art und Weise und das Verfahren der Unterrichtung der betroffenen Person gemäß dem Hauptsatz des Absatzes 2 werden per Präsidialerlass geregelt.

(4) Absatz 1 und der Hauptsatz des Absatzes 2 gelten nicht, wenn einer der folgenden Umstände vorliegt, sofern dieser Umstand eindeutig Vorrang vor den Rechten der betroffenen Personen gemäß diesem Gesetz hat:

1. wenn die personenbezogenen Daten, die das Auskunftsersuchen betrifft, Teil von personenbezogenen Akten gemäß einer der Nummern des Artikels 32 Absatz 2 sind,
2. wenn wahrscheinlich ist, dass die Unterrichtung zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde.

i) Erhält der Datenverantwortliche personenbezogene Daten, die auf der Grundlage des Angemessenheitsbeschlusses der EU aus der EU übermittelt wurden, ([6]) muss er der betroffenen Person unverzüglich, in jedem Fall jedoch innerhalb eines Monats nach der Übermittlung, die folgenden in den Absätzen 1 bis 5 genannten Informationen mitteilen.

(1) Namen und Kontaktdaten der Personen, die die personenbezogenen Daten übermittelt und empfangen haben,

(2) die personenbezogenen Daten oder Kategorien der personenbezogenen Daten, die übermittelt wurden,

(3) den Zweck der Erhebung und Nutzung der personenbezogenen Daten (der gemäß Nummer 1 dieser Bekanntmachung vom Datenexporteur bestimmt wird),

(4) den Zeitraum, für den die personenbezogenen Daten gespeichert werden,

(5) die Rechte der betroffenen Person in Bezug auf die Verarbeitung der personenbezogenen Daten, die Art und Weise und das Verfahren der Ausübung der Rechte sowie etwaige Nachteile, die die Ausübung dieser Rechte mit sich bringt.

ii) Übermittelt der Datenverantwortliche personenbezogene Daten gemäß Ziffer i an einen Dritten in der Republik Korea oder im Ausland, muss er der betroffenen Person außerdem vor der Übermittlung die in den Absätzen 1 bis 5 genannten Informationen mitteilen.

(1) Namen und Kontaktdaten der Personen, die die personenbezogenen Daten übermitteln und empfangen,

(2) die personenbezogenen Daten oder Kategorien der personenbezogenen Daten, die übermittelt werden,

(3) das Land, in das die personenbezogenen Daten übermittelt werden sollen, das geplante Datum und die geplante Art und Weise der Übermittlung (nur wenn die personenbezogenen Daten an einen Dritten im Ausland übermittelt werden sollen),

(4) den Zweck und die Rechtsgrundlage der Übermittlung der personenbezogenen Daten,

(5) die Rechte der betroffenen Person in Bezug auf die Verarbeitung der personenbezogenen Daten, die Art und Weise und das Verfahren der Ausübung der Rechte sowie etwaige Nachteile, die die Ausübung dieser Rechte mit sich bringt.

iii) Der Datenverantwortliche darf Ziffer i oder ii nicht anwenden, wenn einer der in den Absätzen 1 bis 4 genannten Fälle vorliegt.

(1) Wenn die personenbezogenen Daten, über die die betroffene Person zu unterrichten ist, Teil von personenbezogenen Akten gemäß Artikel 32 Absatz 2 des Gesetzes sind, soweit die durch diese Bestimmung geschützten Interessen eindeutig Vorrang vor den Rechten der betroffenen Person haben, und nur so lange, wie die Unterrichtung die Verfolgung der betreffenden Interessen beeinträchtigt, z. B. durch die Gefährdung einer laufenden strafrechtlichen Untersuchung oder der nationalen Sicherheit.

(2) Wenn und solange wahrscheinlich ist, dass die Unterrichtung zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen würde, sofern diese Rechte oder Interessen eindeutig Vorrang vor den Rechten der betroffenen Person haben.

(3) Wenn die betroffene Person bereits über die Informationen verfügt, die ihr der Datenverantwortliche gemäß Ziffer i oder ii mitteilen muss.

(4) Wenn der Datenverantwortliche über keine Kontaktdaten der betroffenen Person verfügt oder übermäßige Anstrengungen erforderlich wären, um mit der betroffenen Person Kontakt aufzunehmen; dies gilt auch für eine Verarbeitung unter den in Abschnitt 3 des PIPA beschriebenen Bedingungen. Bei der Entscheidung darüber, ob die betroffene Person kontaktiert werden kann oder ob dies mit übermäßigen Anstrengungen verbunden ist, sollte die Möglichkeit einer Zusammenarbeit mit dem Datenexporteur aus der EU berücksichtigt werden.

([6]) Die in den Ziffern i, ii und iii vorgesehenen Pflichten gelten auch, wenn der Datenverantwortliche, der auf der Grundlage des Angemessenheitsbeschlusses personenbezogene Daten aus der EU erhält, diese Daten auf der Grundlage anderer Gesetze, z. B. des Kreditdatengesetzes, verarbeitet.

4. **Anwendungsbereich der Sonderregelung für die Verarbeitung pseudonymisierter Daten (Artikel 28-2, 28-3, 28-4, 28-5, 28-6 und 28-7, Artikel 3 und Artikel 58-2 des Gesetzes)**

<Gesetz zum Schutz personenbezogener Daten

(Gesetz Nr. 16930, teilweise geändert am 4. Februar 2020)>

Kapitel III Verarbeitung personenbezogener Daten

ABSCHNITT 3 Sonderfälle bei pseudonymisierten Daten

Artikel 28-2 (Verarbeitung pseudonymisierter Daten) (1) Ein Datenverantwortlicher darf pseudonymisierte Daten ohne Einwilligung der betroffenen Personen für statistische Zwecke, wissenschaftliche Forschungszwecke, Archivierungszwecke im öffentlichen Interesse usw. verarbeiten.

(2) Die pseudonymisierten Daten, die der Datenverantwortliche gemäß Absatz 1 einem Dritten übermittelt, dürfen keine Daten enthalten, mit denen eine natürliche Person identifiziert werden könnte.

Artikel 28-3 (Beschränkung der Verknüpfung pseudonymisierter Daten) (1) Die Verknüpfung pseudonymisierter Daten, die von verschiedenen Datenverantwortlichen für statistische Zwecke, für wissenschaftliche Forschung, zur Aufbewahrung von Aufzeichnungen von öffentlichem Interesse usw. verarbeitet wurden, wird unbeschadet des Artikels 28-2 von einer spezialisierten Einrichtung durchgeführt, die von der PIPC oder dem Leiter der zuständigen zentralen Verwaltungsbehörde benannt wird.

(2) Ein Datenverantwortlicher, der die Daten außerhalb der Organisation, die die Daten miteinander kombiniert hat, freigeben möchte, holt die Genehmigung des Leiters der spezialisierten Einrichtung ein, nachdem die Daten zu pseudonymisierten Daten verarbeitet oder in die in Artikel 58-2 genannte Form gebracht wurden.

(3) Die nötigen Einzelheiten, darunter die Verfahren und Methoden der Verknüpfung gemäß Absatz 1, die Standards und Verfahren für die Benennung oder den Widerruf der Benennung einer spezialisierten Einrichtung, die Leitung und Aufsicht sowie die Standards und Verfahren für den Export und die Genehmigung gemäß Absatz 2, werden per Präsidialerlass geregelt.

Artikel 28-4 (Pflicht zur Durchführung von Sicherheitsmaßnahmen für pseudonymisierte Daten) (1) Bei der Verarbeitung pseudonymisierter Daten trifft der Datenverantwortliche – wie per Präsidialerlass zur Gewährleistung der Sicherheit vorgeschrieben – die gegebenenfalls erforderlichen technischen, organisatorischen und physischen Maßnahmen, z. B. getrennte Speicherung und Verwaltung zusätzlicher Daten, die für die Wiederherstellung des ursprünglichen Zustands benötigt werden, damit die personenbezogenen Daten nicht verloren gehen, gestohlen, offengelegt, gefälscht, verändert oder beschädigt werden können.

(2) Ein Datenverantwortlicher, der pseudonymisierte Daten verarbeiten will, führt zu Verwaltungszwecken Aufzeichnungen über die im Präsidialerlass geregelten Einzelheiten, wie über den Zweck der Verarbeitung der pseudonymisierten Daten und, im Fall ihrer Übermittlung, über den Dritten, der die pseudonymisierten Daten empfängt.

Artikel 28-5 (Verbotene Handlungen bei der Verarbeitung pseudonymisierter Daten) (1) Niemand darf pseudonymisierte Daten zu dem Zweck verarbeiten, eine bestimmte natürliche Person zu identifizieren.

(2) Wenn bei der Verarbeitung pseudonymisierter Daten solche Daten generiert werden, die die Identifizierung einer bestimmten natürlichen Person ermöglichen, stellt der Datenverantwortliche die Verarbeitung der Daten sofort ein, ruft die betreffenden Daten ab und vernichtet sie.

Artikel 28-6 (Verhängung von Geldbußen für die Verarbeitung pseudonymisierter Daten) (1) Die Kommission kann gegen einen Datenverantwortlichen, der unter Verstoß gegen Artikel 28-5 Absatz 1 Daten verarbeitet hat, um eine bestimmte natürliche Person zu identifizieren, eine Geldbuße in Höhe von weniger als drei Hundertsteln seines Gesamtumsatzes verhängen. Falls keine Umsätze vorliegen oder die Berechnung des Ertrags schwierig ist, darf die Geldbuße höchstens 400 Millionen Won oder drei Hundertstel des Kapitalbetrags betragen, je nachdem, welcher Betrag höher ist.

(2) Was die nötigen Einzelheiten der Erhebung und Beitreibung von Geldbußen anbelangt, gilt mutatis mutandis Artikel 34-2 Absätze 3 bis 5.

Artikel 28-7 (Anwendungsbereich) Die Artikel 20, 21 und 27, Artikel 34 Absatz 1, Artikel 35 bis 37, 39-3, 39-4 und 39-6 bis 39-8 gelten nicht für pseudonymisierte Daten.

Kapitel I Allgemeine Bestimmungen

Artikel 3 (Grundsätze des Schutzes personenbezogener Daten) (1) Der Datenverantwortliche gibt ausdrücklich an, für welche Zwecke die personenbezogenen Daten verarbeitet werden, erhebt die personenbezogenen Daten in rechtmäßiger und fairer Weise und nur in dem Ausmaß, wie es für die Verarbeitungszwecke erforderlich ist.

(2) Der Datenverantwortliche verarbeitet die personenbezogenen Daten in geeigneter Weise entsprechend den Erfordernissen für die Zwecke ihrer Verarbeitung und darf sie nicht für andere Zwecke nutzen.

(3) Der Datenverantwortliche stellt sicher, dass die personenbezogenen Daten sachlich richtig, vollständig und auf dem neuesten Stand sind, soweit dies für die Zwecke ihrer Verarbeitung erforderlich ist.

(4) Der Datenverantwortliche verwaltet die personenbezogenen Daten in einer sicheren Weise entsprechend den Verarbeitungsmethoden, der Art usw. der personenbezogenen Daten, wobei er der Möglichkeit einer Verletzung der Rechte der betroffenen Person und der Schwere der einschlägigen Risiken Rechnung trägt.

(5) Der Datenverantwortliche veröffentlicht seine Datenschutzerklärung und andere Informationen in Zusammenhang mit der Verarbeitung personenbezogener Daten und gewährleistet die Rechte der betroffenen Person, wie etwa das Recht auf Auskunft über die sie betreffenden personenbezogenen Daten.

(6) Der Datenverantwortliche verarbeitet die personenbezogenen Daten so, dass die Gefahr einer Verletzung der Privatsphäre der betroffenen Personen so gering wie möglich ist.

(7) Wenn es möglich ist, die Zwecke der Erhebung der personenbezogenen Daten durch die Verarbeitung anonymisierter oder pseudonymisierter personenbezogener Daten zu erfüllen, bemüht sich der Datenverantwortliche um die Verarbeitung anonymisierter personenbezogener Daten, soweit eine Anonymisierung möglich ist, oder die Verarbeitung pseudonymisierter personenbezogener Daten, wenn es bei einer Anonymisierung unmöglich ist, die Zwecke der Erhebung der personenbezogenen Daten zu erfüllen.

(8) Der Datenverantwortliche bemüht sich, das Vertrauen der betroffenen Personen zu erlangen, indem er die in diesem Gesetz und anderen einschlägigen Gesetzen vorgesehenen Aufgaben und Pflichten achtet und wahrnimmt.

Kapitel IX Ergänzende Bestimmungen

Artikel 58-2 (Ausnahme von der Anwendung) Dieses Gesetz gilt nicht für Daten, bei denen unter angemessener Berücksichtigung von Zeit, Kosten, Technologie usw. ausgeschlossen werden kann, dass ihre Verknüpfung mit anderen Daten die Identifizierung einer bestimmten natürlichen Person ermöglicht. <Dieser Artikel wurde durch das Gesetz Nr. 16930 vom 4. Februar 2020 hinzugefügt>

i) Kapitel III, Abschnitt 3 „Sonderfälle bei pseudonymisierten Daten“ (Artikel 28-2 bis Artikel 28-7) sieht Folgendes vor: Die Verarbeitung pseudonymisierter Daten ohne Einwilligung der betroffenen Person ist zum Zweck der Erstellung von Statistiken, der wissenschaftlichen Forschung, der Aufbewahrung öffentlicher Aufzeichnungen usw. erlaubt (Artikel 28-2), in solchen Fällen sind jedoch geeignete Garantien vorzusehen und Verbote einzuhalten, um die Rechte der betroffenen Personen zu schützen (Artikel 28-4 und 28-5), gegen Zuwiderhandelnde können Geldbußen verhängt werden (Artikel 28-6) und bestimmte Garantien, die gemäß dem PIPA in anderen Fällen gelten, sind hier nicht anwendbar (Artikel 28-7).

ii) Diese Bestimmungen gelten nicht für Fälle, in denen pseudonymisierte Daten für andere Zwecke als die Erstellung von Statistiken, wissenschaftliche Forschung, die Aufbewahrung öffentlicher Aufzeichnungen usw. verarbeitet werden. Wenn beispielsweise personenbezogene Daten einer Person aus der EU, die gemäß dem Angemessenheitsbeschluss der Europäischen Kommission nach Korea übermittelt wurden, für andere Zwecke als die Erstellung von Statistiken, wissenschaftliche Forschung, die Aufbewahrung öffentlicher Aufzeichnungen usw. pseudonymisiert werden, finden die besonderen Bestimmungen des Kapitels III Abschnitt 3 keine Anwendung. ([7])

iii) Verarbeitet ein Datenverantwortlicher pseudonymisierte Daten zum Zwecke der Erstellung von Statistiken, der wissenschaftlichen Forschung, der Aufbewahrung öffentlicher Aufzeichnungen usw. und sind die pseudonymisierten Daten nicht vernichtet worden, sobald der spezifische Zweck der Verarbeitung gemäß Artikel 37 der Verfassung und Artikel 3 des Gesetzes (Grundsätze des Schutzes personenbezogener Daten) erfüllt war, muss der Datenverantwortliche die Daten anonymisieren, um gemäß Artikel 58-2 PIPA die Identifizierung einer bestimmten natürlichen Person durch die Daten an sich oder ihre Verknüpfung mit anderen Daten unter angemessener Berücksichtigung von Zeit, Kosten, Technologie usw. auszuschließen.

5. **Abhilfemaßnahmen usw. (Artikel 64 Absätze 1, 2 und 4 des Gesetzes)**

<Gesetz zum Schutz personenbezogener Daten

(Gesetz Nr. 16930, teilweise geändert am 4. Februar 2020)>

Artikel 64 (Abhilfemaßnahmen) (1) Ist die PIPC der Auffassung, dass wesentliche Gründe für die Annahme bestehen, dass eine Verletzung des Schutzes personenbezogener Daten vorliegt und bei Untätigkeit ein schwer zu behebender Schaden wahrscheinlich ist, so kann sie die Person, die gegen dieses Gesetz verstoßen hat, (mit Ausnahme zentraler Verwaltungsbehörden, lokaler Verwaltungen, der Nationalversammlung, des Gerichts, des Verfassungsgerichts und der nationalen Wahlkommission) anweisen, eine der folgenden Maßnahmen zu ergreifen:

1. die Verletzung des Schutzes personenbezogener Daten zu unterbinden,

2. die Verarbeitung personenbezogener Daten vorübergehend auszusetzen,

([7]) Die Ausnahme nach Artikel 40-3 des Kreditdatengesetzes gilt ebenfalls nur für die Verarbeitung pseudonymisierter Kreditdaten zum Zweck der Erstellung von Statistiken, der wissenschaftlichen Forschung und der Aufbewahrung öffentlicher Aufzeichnungen.

3. andere erforderliche Maßnahmen zu treffen, um die personenbezogenen Daten zu schützen und die Verletzung des Schutzes personenbezogener Daten zu verhindern.

(2) Ist der Leiter einer zuständigen zentralen Verwaltungsbehörde der Auffassung, dass wesentliche Gründe für die Annahme bestehen, dass eine Verletzung des Schutzes personenbezogener Daten vorliegt und bei Untätigkeit ein schwer zu behebender Schaden wahrscheinlich ist, so kann er gemäß den Gesetzen, die in die Zuständigkeit dieser zentralen Verwaltungsbehörde fallen, einen Datenverantwortlichen anweisen, eine der in Absatz 1 genannten Maßnahmen zu ergreifen.

(4) Verstößt eine zentrale Verwaltungsbehörde, eine lokale Verwaltung, die Nationalversammlung, das Gericht, das Verfassungsgericht oder die nationale Wahlkommission gegen dieses Gesetz, so kann die PIPC dem Leiter der betreffenden Behörde empfehlen, eine der in Absatz 1 genannten Maßnahmen zu ergreifen. Sobald die Behörde eine solche Empfehlung erhält, muss sie ihr nachkommen, sofern nicht außergewöhnliche Umstände vorliegen.

i) „Schwer zu behebender Schaden" wurde in Präzedenzfällen ([8]) ([9]) als ein Fall ausgelegt, in dem die persönlichen Rechte oder die Privatsphäre einer Person beeinträchtigt werden könnten.

ii) Entsprechend bezieht sich die Formulierung „wesentliche Gründe für die Annahme, dass eine Verletzung des Schutzes personenbezogener Daten vorliegt und bei Untätigkeit ein schwer zu behebender Schaden wahrscheinlich ist" in Artikel 64 Absätze 1 und 2 auf Fälle, in denen davon ausgegangen wird, dass bei einem Verstoß gegen das Gesetz eine Verletzung der Rechte und der Freiheit natürlicher Personen in Bezug auf personenbezogene Daten wahrscheinlich ist. Dies trifft auf alle Fälle zu, in denen gegen die Grundsätze, Rechte und Pflichten verstoßen wird, die Teil des Datenschutzrechts sind ([10]).

iii) Nach Artikel 64 Absatz 4 PIPA ist eine Maßnahme in Bezug auf einen Verstoß „gegen dieses Gesetz", d. h. eine Gegenmaßnahme im Hinblick auf einen Verstoß gegen das PIPA.

Zentrale Verwaltungsbehörden usw. dürfen als an die Rechtsstaatlichkeit gebundene Behörden gegen kein Gesetz verstoßen; in dem Ausnahmefall, dass dennoch eine rechtswidrige Handlung begangen wurde, sind sie verpflichtet, eine Abhilfemaßnahme zu ergreifen, einschließlich der sofortigen Einstellung der betreffenden Handlung, und Schadenersatz zu leisten.

Entsprechend müssen zentrale Verwaltungsbehörden usw. gemäß Artikel 64 Absatz 4 PIPA auch ohne Eingreifen der PIPC eine Abhilfemaßnahme ergreifen, wenn sie Kenntnis von einem Gesetzesverstoß erlangen.

Insbesondere wenn die PIPC eine Abhilfemaßnahme empfohlen hat, dürfte für zentrale Verwaltungsbehörden usw. in der Regel objektive Klarheit darüber bestehen, dass sie gegen das Gesetz verstoßen haben. Um ihre Auffassung zu rechtfertigen, dass eine Empfehlung der PIPC nicht befolgt werden sollte, müssen zentrale Verwaltungsbehörden usw. daher klare Gründe darlegen, um nachzuweisen, dass sie nicht gegen das Gesetz verstoßen haben. Die Empfehlung muss befolgt werden, es sei denn, die PIPC stellt fest, dass tatsächlich kein Gesetzesverstoß vorliegt.

In Anbetracht dessen sind die „außergewöhnlichen Umstände" gemäß Artikel 64 Absatz 4 PIPA streng auf außergewöhnliche Umstände zu beschränken, bei denen zentrale Verwaltungsbehörden usw. anhand klarer Gründe nachweisen können, dass „tatsächlich nicht gegen dieses Gesetz verstoßen wurde", z. B. „Fälle mit außergewöhnlichen (tatsächlichen oder rechtlichen) Umständen", die der PIPC bei der ursprünglichen Empfehlung nicht bekannt waren und die die PIPC zu der Feststellung veranlasst, dass tatsächlich kein Verstoß vorliegt.

6. **Anwendung des PIPA auf die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit, einschließlich der Untersuchung von Verstößen gegen das PIPA und seiner Durchsetzung (Artikel 7-8, 7-9, 58, 3, 4 und 62 PIPA)**

<Gesetz zum Schutz personenbezogener Daten

(Gesetz Nr. 16930, teilweise geändert am 4. Februar 2020)>

Artikel 7-8 (Arbeit der PIPC) (1) Zu den Aufgaben der PIPC gehört Folgendes: […]

3. Aufgaben in Zusammenhang mit der Untersuchung von Verletzungen der Rechte betroffener Personen und den sich daraus ergebenden Verfügungen

4. Bearbeitung von Beschwerden oder Handhabung von Abhilfeverfahren in Zusammenhang mit der Verarbeitung personenbezogener Daten und Schlichtung von Streitigkeiten über personenbezogene Daten

[…]

([8]) Urteil des obersten Gerichtshofs vom 26. Januar 1999, 97Da10215, 10222: Wenn die strafbaren Handlungen des Angeklagten durch die Medien offengelegt werden, kann dadurch nicht nur das Opfer, d. h. der Kläger, einen irreparablen psychischen und physischen Schaden erleiden, sondern auch dessen Familie und andere Menschen in dessen Umfeld.

([9]) Urteil des Seoul High Court vom 16. Januar 2008, 2006NA92006: Wird ein diffamierender Artikel veröffentlicht, so kann die betreffende Person dadurch einen schweren irreparablen Schaden erleiden.

([10]) Die Grundsätze unter Ziffer ii sind auch auf Artikel 45-4 des Kreditdatengesetzes anwendbar.

Artikel 7-9 (Gegenstand der Beratung und Beschlussfassung der PIPC sind) (1) Die PIPC berät und fasst Beschlüsse über folgende Fragen: […]

5. Fragen der Auslegung und Anwendung des Rechts in Zusammenhang mit dem Schutz personenbezogener Daten

[…]

Artikel 58 (Teilweise Ausnahme von der Anwendung) (1) Kapitel III bis VII gelten nicht für folgende personenbezogene Daten:

1. personenbezogene Daten, die gemäß dem Statistikgesetz für die Verarbeitung durch öffentliche Einrichtungen erhoben werden,
2. personenbezogene Daten, die für Datenanalysen in Zusammenhang mit der nationalen Sicherheit erhoben oder angefordert werden,
3. personenbezogene Daten, die vorübergehend verarbeitet werden, wenn sie für die öffentliche Sicherheit, die öffentliche Gesundheit usw. dringend erforderlich sind,
4. personenbezogene Daten, die von der Presse für ihre eigenen Berichterstattungszwecke, für Missionierungstätigkeiten religiöser Organisationen oder für die Aufstellung von Kandidaten durch politische Parteien erhoben oder genutzt werden.

[Absätze 2 und 3 ausgelassen]

(4) Im Falle der Verarbeitung personenbezogener Daten gemäß Absatz 1 beschränkt der Datenverantwortliche die Verarbeitung und den Verarbeitungszeitraum auf das für den verfolgten Zweck notwendige Mindestmaß; außerdem trifft er technische, organisatorische und physische Sicherheitsvorkehrungen, bearbeitet die von natürlichen Personen eingereichten Beschwerden und ergreift weitere Maßnahmen, die für die sichere Verwaltung und angemessene Verarbeitung der personenbezogenen Daten erforderlich sind.

Artikel 3 (Grundsätze des Schutzes personenbezogener Daten) (1) Der Datenverantwortliche gibt ausdrücklich an, für welche Zwecke die personenbezogenen Daten verarbeitet werden, erhebt die personenbezogenen Daten in rechtmäßiger und fairer Weise und nur in dem Ausmaß, wie es für die Verarbeitungszwecke erforderlich ist.

(2) Der Datenverantwortliche verarbeitet die personenbezogenen Daten in geeigneter Weise entsprechend den Erfordernissen für die Zwecke ihrer Verarbeitung und darf sie nicht für andere Zwecke nutzen.

(3) Der Datenverantwortliche stellt sicher, dass die personenbezogenen Daten sachlich richtig, vollständig und auf dem neuesten Stand sind, soweit dies für die Zwecke ihrer Verarbeitung erforderlich ist.

(4) Der Datenverantwortliche verwaltet die personenbezogenen Daten in einer sicheren Weise entsprechend den Verarbeitungsmethoden, der Art usw. der personenbezogenen Daten, wobei er der Möglichkeit einer Verletzung der Rechte der betroffenen Person und der Schwere der einschlägigen Risiken Rechnung trägt.

(5) Der Datenverantwortliche veröffentlicht seine Datenschutzerklärung und andere Informationen in Zusammenhang mit der Verarbeitung personenbezogener Daten und gewährleistet die Rechte der betroffenen Person, wie etwa das Recht auf Auskunft über die sie betreffenden personenbezogenen Daten.

(6) Der Datenverantwortliche verarbeitet die personenbezogenen Daten so, dass die Gefahr einer Verletzung der Privatsphäre der betroffenen Personen so gering wie möglich ist.

(7) Wenn es möglich ist, die Zwecke der Erhebung der personenbezogenen Daten durch die Verarbeitung anonymisierter oder pseudonymisierter personenbezogener Daten zu erfüllen, bemüht sich der Datenverantwortliche um die Verarbeitung anonymisierter personenbezogener Daten, soweit eine Anonymisierung möglich ist, oder die Verarbeitung pseudonymisierter personenbezogener Daten, wenn es bei einer Anonymisierung unmöglich ist, die Zwecke der Erhebung der personenbezogenen Daten zu erfüllen.

(8) Der Datenverantwortliche bemüht sich, das Vertrauen der betroffenen Personen zu erlangen, indem er die in diesem Gesetz und anderen einschlägigen Gesetzen vorgesehenen Aufgaben und Pflichten achtet und wahrnimmt.

Artikel 4 (Rechte der betroffenen Personen) Eine betroffene Person hat in Bezug auf die Verarbeitung der sie betreffenden personenbezogenen Daten folgende Rechte:

1. das Recht, über die Verarbeitung der personenbezogenen Daten unterrichtet zu werden,
2. das Recht, über die Einwilligung und den Umfang der Einwilligung in die Verarbeitung der personenbezogenen Daten zu entscheiden,
3. das Recht, zu erfahren, ob personenbezogene Daten verarbeitet werden, und Auskunft über die sie betreffenden personenbezogenen Daten zu verlangen (hier und im Folgenden einschließlich des Erhalts von Kopien),
4. das Recht auf Aussetzung der Verarbeitung der personenbezogenen Daten und darauf, ihre Berichtigung, Löschung und Vernichtung zu verlangen,
5. das Recht, für Schäden, die sich aus der Verarbeitung der personenbezogenen Daten ergeben, in einem zügigen und fairen Verfahren eine angemessene Wiedergutmachung zu erhalten.

Artikel 62 (Meldung von Verletzungen) (1) Jede Person, deren Rechte oder Interessen in Zusammenhang mit den sie betreffenden personenbezogenen Daten bei der Verarbeitung personenbezogener Daten durch einen Datenverantwortlichen verletzt werden, kann dies der PIPC melden.

(2) Die PIPC kann eine spezialisierte Einrichtung benennen, die die Beschwerden gemäß Absatz 1 wie per Präsidialerlass vorgeschrieben effizient entgegennimmt und bearbeitet Die spezialisierte Einrichtung richtet in diesem Fall ein Callcenter für Verletzungen des Schutzes personenbezogener Daten ein (im Folgenden „Datenschutz-Callcenter") und betreibt dieses.

(3) Das Datenschutz-Callcenter hat folgende Aufgaben:

1. Entgegennahme von Beschwerden und Beratung in Zusammenhang mit der Verarbeitung personenbezogener Daten,
2. Untersuchung und Bestätigung von Vorfällen sowie Anhörung beteiligter Personen,
3. weitere Aufgaben in Zusammenhang mit den unter den Nummern 1 und 2 genannten Aufgaben.

(4) Die PIPC kann bei Bedarf nach Artikel 32-4 des Gesetzes über öffentliche Bedienstete (State Public Officials Act) einen Behördenvertreter in die gemäß Absatz 2 benannte spezialisierte Einrichtung entsenden, um Vorfälle nach Absatz 3 Nummer 2 effizient zu untersuchen und zu bestätigen.

i) Die Erhebung personenbezogener Daten für die Zwecke der nationalen Sicherheit ist durch spezielle Gesetze geregelt, die die zuständigen Behörden (z. B. den nationalen Nachrichtendienst (National Intelligence Service, NIS)) ermächtigen, unter bestimmten Bedingungen und Garantien Kommunikationsvorgänge zu überwachen oder ihre Offenlegung zu verlangen (im Folgenden „Gesetze zur nationalen Sicherheit"). Zu diesen Gesetzen zur nationalen Sicherheit gehören beispielsweise das Gesetz zum Schutz der Privatsphäre bei der Kommunikation (Communications Privacy Protection Act), das Gesetz über die Terrorismusbekämpfung zum Schutz der Bürger und der öffentlichen Sicherheit (Act on Anti-Terrorism for the Protection of Citizens and Public Security) oder das Gesetz über Telekommunikationsunternehmen (Telecommunications Business Act). Außerdem müssen die Erhebung und Weiterverarbeitung personenbezogener Daten den Anforderungen des PIPA entsprechen. Artikel 58 Absatz 1 Nummer 2 PIPA sieht jedoch vor, dass die Kapitel III bis VII nicht für personenbezogene Daten gelten, die für Datenanalysen in Zusammenhang mit der nationalen Sicherheit erhoben oder angefordert werden. Für die Verarbeitung personenbezogener Daten zu Zwecken der nationalen Sicherheit besteht also diese teilweise Ausnahme.
Kapitel I (Allgemeine Bestimmungen), Kapitel II (Festlegung von Strategien zum Schutz personenbezogener Daten usw.), Kapitel VIII (Sammelklagen wegen Verletzungen des Datenschutzes), Kapitel IX (Ergänzende Bestimmungen) und Kapitel X (Sanktionsbestimmungen) des PIPA sind hingegen auf die Verarbeitung solcher personenbezogenen Daten anwendbar. Dies umfasst die allgemeinen Datenschutzgrundsätze gemäß Artikel 3 (Grundsätze des Schutzes personenbezogener Daten) und die individuellen Rechte, die durch Artikel 4 (Rechte der betroffenen Personen) garantiert werden.
Weiterhin sieht Artikel 58 Absatz 4 PIPA vor, dass die Verarbeitung der Daten und der Verarbeitungszeitraum auf das für den verfolgten Zweck notwendige Mindestmaß beschränkt sein müssen und dass der Datenverantwortliche die erforderlichen Maßnahmen für eine sichere Verwaltung und eine angemessene Verarbeitung der Daten treffen muss, z. B. technische, organisatorische und physische Sicherheitsvorkehrungen, sowie Maßnahmen für eine angemessene Bearbeitung der von natürlichen Personen eingereichten Beschwerden.
Darüber hinaus gelten die Bestimmungen über die Aufgaben und Befugnisse der PIPC (darunter die Artikel 60 bis 65 des PIPA über die Bearbeitung von Beschwerden und den Beschluss von Empfehlungen und Abhilfemaßnahmen) sowie die Bestimmungen über verwaltungsrechtliche und strafrechtliche Sanktionen (Artikel 70 ff. PIPA). Diese Untersuchungs- und Abhilfebefugnisse, auch bezüglich der Bearbeitung von Beschwerden, erstrecken sich gemäß Artikel 7-8 Absatz 1 Nummern 3 und 4 und Artikel 7-9 Absatz 1 Nummer 5 PIPA auch auf mögliche Verstöße gegen die Einschränkungs- und Garantiebestimmungen für die Erhebung personenbezogener Daten, die in speziellen Gesetzen, z. B. den Gesetzen zur nationalen Sicherheit, enthalten sind. Da Artikel 3 Absatz 1 PIPA eine rechtmäßige und faire Erhebung personenbezogener Daten vorsieht und solche Verstöße einen Verstoß gegen „dieses Gesetz" im Sinne der Artikel 63 und 64 darstellt, ist die PIPC berechtigt, eine Untersuchung durchzuführen und Abhilfemaßnahmen zu ergreifen ([11]). Die Befugnisse der nationalen Menschenrechtskommission nach dem Gesetz über die nationale Menschenrechtskommission (National Human Rights Commission Act) werden durch die Ausübung dieser Befugnisse durch die PIPC ergänzt, aber nicht ersetzt.
Die Anwendung der Grundsätze, Rechte und Pflichten des PIPA auf die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit ist Ausdruck der in der Verfassung verankerten Garantien für den Schutz des Rechts natürlicher Personen, die eigenen personenbezogenen Daten zu kontrollieren. Wie vom Verfassungsgericht anerkannt, umfasst dies das Recht natürlicher Personen ([12]), „persönlich zu entscheiden, wann, wem bzw. von wem und in welchem Umfang ihre Daten offengelegt oder genutzt werden. Es handelt sich um ein Grundrecht ([13]) […] zum Schutz der persönlichen Entscheidungsfreiheit angesichts des Risikos, das durch die Ausweitung der Funktionen des Staates und der Informations- und Kommunikationstechnologie entsteht." Jede Einschränkung dieses Rechts, z. B. wenn dies zum Schutz der nationalen Sicherheit notwendig ist, erfordert eine Abwägung der Rechte und Interessen des Einzelnen gegen das betreffende öffentliche Interesse und darf das Recht in seinem Wesensgehalt nicht antasten (Artikel 37 Absatz 2 der Verfassung).

([11]) Zu den Abhilfemaßnahmen gemäß Artikel 64 siehe auch Abschnitt 5.
([12]) Urteil des Verfassungsgerichts vom 26. Mai 2005, 99HunMa513, 2004HunMa190.
([13]) Urteil des Verfassungsgerichts vom 21. Juli 2005, 2003HunMa282.

Der Datenverantwortliche (z. B. der NIS) muss daher bei der Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit unter anderem

1) ausdrücklich angeben, für welche Zwecke die personenbezogenen Daten verarbeitet werden, und diese nur in dem Ausmaß erheben, wie es für die angegebenen Zwecke erforderlich ist (Artikel 3 Absatz 1 PIPA); insbesondere darf er die personenbezogenen Daten nur zur Wahrnehmung seiner Aufgaben gemäß den einschlägigen Gesetzen wie dem Gesetz über den nationalen Nachrichtendienst (National Intelligence Service Act) erheben und weiterverarbeiten,

2) die Verarbeitung der personenbezogenen Daten und den Verarbeitungszeitraum auf das für den verfolgten Zweck notwendige Mindestmaß beschränken (Artikel 58 Absatz 4 PIPA); wenn der Zweck der Verarbeitung erfüllt ist, muss der Datenverantwortliche die personenbezogenen Daten vernichten, es sei denn, ihre weitere Speicherung ist ausdrücklich gesetzlich vorgeschrieben; in diesem Fall müssen die betreffenden personenbezogenen Daten getrennt von anderen personenbezogenen Daten gespeichert und verwaltet werden, dürfen nicht für andere als die im Gesetz genannten Zwecke genutzt werden und sind nach Ablauf der Speicherfrist zu vernichten,

3) die personenbezogenen Daten in einer geeigneten und für die Zwecke ihrer Verarbeitung notwendigen Weise verarbeiten und darf sie nicht für andere Zwecke nutzen (Artikel 3 Absatz 2 PIPA),

4) sicherstellen, dass die personenbezogenen Daten sachlich richtig, vollständig und auf dem neuesten Stand sind, soweit dies für die Zwecke ihrer Verarbeitung erforderlich ist (Artikel 3 Absatz 3 PIPA),

5) die personenbezogenen Daten in einer sicheren Weise entsprechend den Verarbeitungsmethoden, der Art usw. der personenbezogene Daten verwalten, wobei er der Möglichkeit einer Verletzung der Rechte der betroffenen Person und der Schwere der einschlägigen Risiken Rechnung trägt (Artikel 3 Absatz 4 PIPA),

6) seine Datenschutzerklärung und andere Informationen in Zusammenhang mit der Verarbeitung personenbezogener Daten veröffentlichen (Artikel 3 Absatz 5 PIPA),

7) die personenbezogenen Daten so verarbeiten, dass die Gefahr einer Verletzung der Privatsphäre der betroffenen Personen so gering wie möglich ist (Artikel 3 Absatz 6 PIPA).

ii) Der Datenverantwortliche (z. B. die für die nationale Sicherheit zuständigen Behörden wie der NIS) muss gemäß Artikel 58 Absatz 4 PIPA die erforderlichen Maßnahmen treffen, z. B. technische, organisatorische und physische Sicherheitsvorkehrungen, um die Einhaltung dieser Grundsätze und eine angemessene Verarbeitung der personenbezogenen Daten zu gewährleisten. Dies kann beispielsweise spezifische Maßnahmen zur Gewährleistung der Sicherheit der personenbezogenen Daten umfassen, z. B. Beschränkungen des Zugangs zu den personenbezogenen Daten, Zugangskontrollen, Protokolle, gezielte Schulungen der Mitarbeiter zum Umgang mit personenbezogenen Daten usw.

Gemäß Artikel 3 Absatz 5 und Artikel 4 PIPA haben die betroffenen Personen unter anderem folgende Rechte in Bezug auf personenbezogene Daten, die für die Zwecke der nationalen Sicherheit verarbeitet werden:

1) das Recht, zu erfahren, ob ihre personenbezogenen Daten verarbeitet werden, sowie auf Auskunft über die Verarbeitung und über die verarbeiteten Daten, einschließlich des Erhalts von Kopien (Artikel 4 Absatz 1 Absatz 3 PIPA),

2) das Recht auf die Aussetzung der Verarbeitung sowie auf die Berichtigung, Löschung und Vernichtung der personenbezogenen Daten (Artikel 4 Absatz 4 PIPA).

iii) Die betroffenen Personen können zur Ausübung dieser Rechte einen Antrag stellen, entweder direkt beim Datenverantwortlichen oder indirekt über die PIPC, und sie können ihren Vertreter zur Einreichung eines solchen Antrags ermächtigen. Wenn eine betroffene Person einen entsprechenden Antrag stellt, muss der Datenverantwortliche das Recht unverzüglich gewähren, wobei er die Gewährung des Rechts jedoch verzögern, einschränken oder ablehnen kann, wenn dies ausdrücklich gesetzlich vorgesehen oder für die Einhaltung anderer Gesetze unumgänglich ist, soweit und solange dies zum Schutz eines wichtigen Ziels von öffentlichem Interesse erforderlich und verhältnismäßig ist (z. B. soweit und solange die Gewährung dieses Rechts eine laufende Untersuchung oder die nationale Sicherheit gefährden würde) oder wenn die Gewährung des Rechts zur Schädigung eines Dritten an Leib und Leben oder zu einer unfairen Beeinträchtigung der Eigentumsinteressen und anderen Interessen eines Dritten führen könnte. Lehnt der Datenverantwortliche den Antrag ab oder kommt er ihm nur eingeschränkt nach, hat er der betroffenen Person unverzüglich die Gründe dafür mitzuteilen. Der Datenverantwortliche muss Vorkehrungen bezüglich der Art und Weise treffen, wie betroffene Personen Anträge einreichen können, und ein entsprechendes Verfahren einrichten und er muss dies öffentlich bekannt geben, damit die betroffenen Personen davon Kenntnis erlangen können.

Die betroffenen Personen haben außerdem das Recht auf Wiedergutmachung gemäß Artikel 58 Absatz 4 PIPA (Pflicht zur Gewährleistung einer angemessenen Bearbeitung der von natürlichen Personen eingereichten Beschwerden) und Artikel 4 Absatz 5 PIPA (Recht, für Schäden, die sich aus der Verarbeitung der personenbezogenen Daten ergeben, in einem zügigen und fairen Verfahren eine angemessene Wiedergutmachung zu erhalten). Dies schließt das Recht ein, einen mutmaßlichen Verstoß beim Zentrum für Datenschutzverletzungen (Personal Information Infringement Report Center) zu melden (gemäß Artikel 62 Absatz 3 PIPA), bei der PIPC gemäß Artikel 62 PIPA eine Beschwerde über eine Verletzung von Rechten oder Interessen in Zusammenhang mit personenbezogenen Daten einzureichen und nach dem Gesetz über die Verwaltungsgerichtsbarkeit (Administrative Litigation Act) einen gerichtlichen Rechtsbehelf gegen die Beschlüsse oder die Untätigkeit der PIPC einzulegen. Darüber hinaus können die betroffenen Personen auch dann einen gerichtlichen Rechtsbehelf nach dem Administrative Litigation Act einlegen, wenn ihre Rechte oder Interessen durch eine Verfügung oder Unterlassung des Datenverantwortlichen verletzt wurden (z. B. durch die unrechtmäßige Erhebung personenbezogener Daten), oder sie können gemäß dem Gesetz über staatlichen Schadenersatz (State Compensation Act) auf Schadenersatz klagen. Diese Rechtsbehelfsmöglichkeiten bestehen bei möglichen Verstößen gegen das PIPA und gegen die Einschränkungs- und Garantiebestimmungen für die Erhebung personenbezogener Daten, die in speziellen Gesetzen wie den Gesetzen zur nationalen Sicherheit enthalten sind.

Natürliche Personen aus der EU können über ihre nationale Datenschutzbehörde eine Beschwerde bei der PIPC einreichen, und die PIPC wird sie über die nationale Datenschutzbehörde benachrichtigen, wenn die Untersuchung und etwaige Abhilfemaßnahmen abgeschlossen sind.

ANHANG II

18. Mai 2021

Seiner Exzellenz dem für Justiz zuständigen Mitglied der Europäischen Kommission Herrn Didier Reynders

Exzellenz,

ich begrüße die konstruktiven Gespräche zwischen Korea und der Europäischen Kommission, die geführt werden, um den Rahmen für die Übermittlung personenbezogener Daten aus der EU nach Korea zu schaffen.

Auf Ersuchen der Europäischen Kommission, gerichtet an die Regierung Koreas, übermittle ich in der Anlage ein Dokument mit einer Übersicht über den rechtlichen Rahmen für den Datenzugriff der Regierung Koreas.

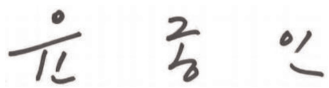
Dieses Dokument betrifft zahlreiche Ministerien und Behörden der koreanischen Regierung. Für den Inhalt der einzelnen Passagen des Dokuments sind die jeweils zuständigen Ministerien und Behörden verantwortlich (die Kommission für den Schutz personenbezogener Daten, das Justizministerium, der nationale Nachrichtendienst, die nationale Menschenrechtskommission Koreas, das nationale Zentrum für Terrorismusbekämpfung, die zentrale Meldestelle Koreas). Die zuständigen Ministerien und Behörden sowie die entsprechenden Unterschriften sind nachstehend aufgeführt.

Die Kommission für den Schutz personenbezogener Daten nimmt alle Fragen zu diesem Dokument entgegen und wird die Einholung der erforderlichen Antworten bei den zuständigen Ministerien und Behörden koordinieren.

Ich hoffe, dass sich dieses Dokument für die Beschlussfassung in der Europäischen Kommission als dienlich erweist.

Für Ihren umfangreichen Beitrag in dieser Angelegenheit bin ich Ihnen sehr verbunden.

Mit ausgezeichneter Hochachtung

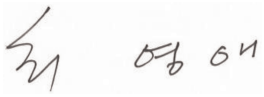


Yoon Jong In
Vorsitzender der Kommission für den Schutz personenbezogener Daten

Dieses Dokument wurde von der Kommission für den Schutz personenbezogener Daten und den folgenden betroffenen Ministerien und Behörden erstellt.

Park Jie Won
Präsident (Direktor) des nationalen Nachrichtendienstes

Lee Jung Soo
Generaldirektor des Justizministeriums



Choi Young Ae
Vorsitzende der nationalen Menschenrechtskommission Koreas

Kim Hyuck Soo
Direktor des nationalen Zentrums für Terrorismusbekämpfung

Kim Jeong Kag
Kommissar der zentralen Meldestelle Koreas

Rechtlicher Rahmen für die Erhebung und Nutzung personenbezogener Daten für die Zwecke der Strafverfolgung und der nationalen Sicherheit durch die koreanischen Behörden

Das folgende Dokument bietet einen Überblick über den rechtlichen Rahmen für die Erhebung und Nutzung personenbezogener Daten für die Zwecke der Strafverfolgung und der nationalen Sicherheit durch die koreanischen Behörden (im Folgenden „staatlicher Zugriff"), insbesondere in Bezug auf die verfügbaren Rechtsgrundlagen, die geltenden Auflagen (Einschränkungen) und Garantien sowie die unabhängige Aufsicht und die möglichen individuellen Rechtsbehelfe.

1. ALLGEMEINE RECHTSGRUNDSÄTZE FÜR DEN STAATLICHEN ZUGRIFF

1.1. Verfassungsrechtlicher Rahmen

In der Verfassung der Republik Korea ist allgemein das Recht auf Privatsphäre (Artikel 17) und insbesondere das Briefgeheimnis (Artikel 18) verankert. Es ist die Aufgabe des Staates, diese Grundrechte zu gewährleisten ([1]). In der Verfassung ist ferner festgelegt, dass die Einschränkung der Rechte und Freiheiten der Bürger nur per Gesetz und nur dann zulässig ist, wenn dies für die nationale Sicherheit oder zur Aufrechterhaltung der öffentlichen Ordnung für das Gemeinwohl erforderlich ist ([2]). Selbst wenn entsprechende Einschränkungen auferlegt werden, dürfen sie den jeweiligen Wesensgehalt der Freiheit oder des Rechts nicht antasten ([3]). Die koreanischen Gerichte haben diese Bestimmungen in Rechtssachen angewandt, in denen es um den Eingriff des Staates in die Privatsphäre ging. Der oberste Gerichtshof stellte beispielsweise fest, dass die Überwachung von Zivilisten eine Verletzung des Grundrechts auf Privatsphäre darstellt, und hob hervor, dass Zivilisten „das Recht auf Selbstbestimmung in Bezug auf personenbezogene Daten" haben ([4]). In einer anderen Rechtssache befand das Verfassungsgericht, dass die Privatsphäre ein Grundrecht ist, das die Bürger in ihrem Privatleben vor dem Eingriff und der Beobachtung durch den Staat schützt ([5]).

Die koreanische Verfassung garantiert ferner, dass außer in den gesetzlich vorgesehenen Fällen niemand festgenommen, verhaftet, durchsucht oder verhört wird und keine Gegenstände beschlagnahmt werden ([6]). Darüber hinaus dürfen Durchsuchungen und Beschlagnahmen nur auf der Grundlage einer richterlichen Anordnung, auf Antrag eines Staatsanwalts und unter Beachtung eines ordnungsgemäßen Verfahrens durchgeführt werden ([7]). In Ausnahmefällen, d. h. wenn ein Verdächtiger bei der Begehung einer Straftat (*in flagrante delicto*) festgenommen wird oder wenn die Gefahr besteht, dass eine Person, die verdächtigt wird, eine mit einer Freiheitsstrafe von drei Jahren oder mehr belegte Straftat begangen zu haben, entkommt oder Beweismaterial vernichtet, können die Untersuchungsbehörden eine Durchsuchung oder Beschlagnahme ohne gerichtliche Anordnung durchführen; die Anordnung muss in solchen Fällen nachträglich beantragt werden ([8]). Diese allgemeinen Grundsätze werden in den speziellen Gesetzen des Strafverfahrensrechts und zum Schutz der Kommunikation genauer ausgeführt (ein detaillierter Überblick folgt weiter unten).

Ausländern garantiert die Verfassung den Status, den sie nach dem Völkerrecht und gemäß internationalen Verträgen haben ([9]). In mehreren internationalen Übereinkommen, die Korea unterzeichnet hat, werden Rechte auf Privatsphäre garantiert. Beispiele hierfür sind der Internationale Pakt über bürgerliche und politische Rechte (Artikel 17), das Übereinkommen über die Rechte von Menschen mit Behinderungen (Artikel 22) und das Übereinkommen über die Rechte des Kindes (Artikel 16). Wenn auch in der Verfassung grundsätzlich auf die Rechte von „Bürgern" Bezug genommen wird, hat das Verfassungsgericht zudem entschieden, dass auch Ausländer über Grundrechte verfügen ([10]). Insbesondere befand das Gericht, dass der Schutz der Würde und des Wertes einer Person als Mensch sowie das Recht, Glück

([1]) Artikel 10 der Verfassung der Republik Korea, verkündet am 17. Juli 1948 (im Folgenden „Verfassung").
([2]) Artikel 37 Absatz 2 der Verfassung.
([3]) Artikel 37 Absatz 2 der Verfassung.
([4]) Entscheidung des obersten Gerichtshofs Koreas vom 24. Juli 1998, 96DA42789.
([5]) Entscheidung des Verfassungsgerichts vom 30. Oktober 2003, 2002Hun-Ma51. Weiterhin erläuterte das Verfassungsgericht in seiner Entscheidung vom 26. Mai 2005, 99Hun-Ma513 und 2004Hun-Ma190 (konsolidiert): „Das Recht, die eigenen personenbezogenen Daten zu kontrollieren, ist das Recht der betroffenen Person, persönlich zu entscheiden, wann, wem bzw. von wem und in welchem Umfang ihre Daten offengelegt oder genutzt werden. Es handelt sich um ein Grundrecht, wenn auch kein in der Verfassung festgelegtes Recht, zum Schutz der persönlichen Entscheidungsfreiheit angesichts des Risikos, das durch die Ausweitung der Funktionen des Staates und der Informations- und Kommunikationstechnologie entsteht."
([6]) Artikel 12 Absatz 1 Satz 1 der Verfassung.
([7]) Artikel 16 und Artikel 12 Absatz 3 der Verfassung.
([8]) Artikel 12 Absatz 3 der Verfassung.
([9]) Artikel 6 Absatz 2 der Verfassung.
([10]) Entscheidung des Verfassungsgerichts vom 29. Dezember 1994, 93Hun-MA120. Siehe außerdem z. B. die Entscheidung des Verfassungsgerichts vom 31. Mai 2018, 2014Hun-Ma346, in der das Gericht feststellte, dass das verfassungsmäßige Recht eines sudanesischen Staatsangehörigen auf Rechtsbeistand am Flughafen verletzt wurde. In einer anderen Rechtssache befand das Verfassungsgericht, dass die freie Wahl einer legalen Beschäftigung eng mit dem Recht auf das Streben nach Glück sowie mit der Würde und dem Wert des Menschen verknüpft ist und daher nicht nur Bürgern vorbehalten ist, sondern auch Ausländern garantiert werden kann, die in der Republik Korea legal beschäftigt sind (Entscheidung des Verfassungsgerichts vom 29. September 2011, 2007Hun-Ma1083).

zu streben, Rechte aller Menschen und nicht nur Rechte von Bürgern sind ([11]). Es stellte außerdem klar, dass das Recht auf Kontrolle der eigenen Daten als Grundrecht gilt, das auf dem Recht auf Würde und das Streben nach Glück und dem Recht auf Achtung des Privatlebens beruht ([12]). Obwohl das Recht auf Privatsphäre nichtkoreanischer Staatsangehöriger bislang nicht explizit Gegenstand der Rechtsprechung war, ist unter Rechtsgelehrten daher weithin anerkannt, dass in den Artikeln 12 bis 22 der Verfassung (die sich unter anderem auf die Privatsphäre und die persönliche Freiheit beziehen) „Menschenrechte" festgelegt sind.

Nicht zuletzt sieht die Verfassung auch das Recht vor, gegenüber Behörden Anspruch auf angemessenen Schadenersatz zu erheben ([13]). Darüber hinaus kann jede Person, deren durch die Verfassung garantierte Grundrechte durch die Ausübung der Staatsgewalt (außer durch Gerichtsurteile) verletzt werden, auf der Grundlage des Gesetzes über das Verfassungsgericht (Constitutional Court Act) Verfassungsbeschwerde beim Verfassungsgericht einlegen ([14]).

1.2. **Allgemeine Datenschutzvorschriften**

Das allgemeine Datenschutzgesetz der Republik Korea, das Gesetz über den Schutz personenbezogener Daten (Personal Information Protection Act, PIPA), gilt sowohl für den privaten als auch für den öffentlichen Sektor. Behörden sind nach dem PIPA ausdrücklich dazu verpflichtet, Strategien auszuarbeiten, um den „Missbrauch personenbezogener Daten, indiskrete Überwachung und Verfolgung usw. zu verhindern und die Achtung der Menschenwürde und der Privatsphäre des Einzelnen zu verbessern." ([15])

Die Verarbeitung personenbezogener Daten für Strafverfolgungszwecke unterliegt sämtlichen Anforderungen des PIPA. Dies bedeutet beispielsweise, dass die Strafverfolgungsbehörden den Pflichten für eine rechtmäßige Verarbeitung nachkommen müssen und sich zur Erhebung, Nutzung oder Übermittlung personenbezogener Daten auf eine der im PIPA aufgeführten Rechtsgrundlagen stützen (Artikel 15–18) sowie die Grundsätze der Zweckbeschränkung (Artikel 3 Absätze 1 und 2), der Verhältnismäßigkeit bzw. Datenminimierung (Artikel 3 Absätze 1 und 6), der begrenzten Datenspeicherung (Artikel 21), der Datensicherheit einschließlich der Meldung von Verletzungen des Schutzes personenbezogener Daten (Artikel 3 Absatz 4, Artikel 29 und Artikel 34) und der Transparenz (Artikel 3 Absätze 1 und 5, Artikel 20, 30 und 32) einhalten müssen. In Bezug auf sensible Informationen gelten besondere Garantien (Artikel 23 PIPA). Darüber hinaus können natürliche Personen gemäß Artikel 3 Absatz 5 und Artikel 4 PIPA sowie den Artikeln 35 bis 39-2 PIPA gegenüber den Strafverfolgungsbehörden ihre Rechte auf Auskunft, Berichtigung, Löschung und Aussetzung der Verarbeitung ausüben.

Während das PIPA für die Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken uneingeschränkt zur Anwendung kommt, enthält er eine Ausnahme für die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit. Artikel 58 Absatz 1 Nummer 2 sieht vor, dass die Artikel 15 bis 50 nicht für personenbezogene Daten gelten, die für Datenanalysen in Zusammenhang mit der nationalen Sicherheit erhoben oder angefordert werden ([16]). Kapitel I (Allgemeine Bestimmungen), Kapitel II (Festlegung von Strategien zum Schutz personenbezogener Daten usw.), Kapitel VIII (Sammelklagen wegen Verletzungen des Datenschutzes), Kapitel IX (Ergänzende Bestimmungen) und Kapitel X (Sanktionsbestimmungen) bleiben hingegen anwendbar. Dies umfasst die allgemeinen Datenschutzgrundsätze gemäß Artikel 3 (Grundsätze des Schutzes personenbezogener Daten) und die individuellen Rechte, die durch Artikel 4 (Rechte der betroffenen Personen) garantiert werden. Die zentralen Grundsätze und Rechte werden also auch in diesem Bereich gewährleistet. Weiterhin sieht Artikel 58 Absatz 4 PIPA vor, dass die Verarbeitung der Daten und der Verarbeitungszeitraum auf das für den verfolgten Zweck notwendige Mindestmaß beschränkt sein müssen und dass der Datenverantwortliche die erforderlichen Maßnahmen für eine sichere Verwaltung und eine angemessene Verarbeitung der Daten treffen muss, z. B. technische, organisatorische und physische Sicherheitsvorkehrungen, sowie Maßnahmen für eine angemessene Bearbeitung der von natürlichen Personen eingereichten Beschwerden.

In der Bekanntmachung Nr. 2021-1 über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten hat die Kommission für den Schutz personenbezogener Daten (Personal Information Protection Commission, PIPC) im Hinblick auf diese teilweise Ausnahme näher erläutert, wie das PIPA auf die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit anzuwenden ist ([17]). Die Ausführungen betreffen insbesondere die Rechte natürlicher Personen (Auskunft, Berichtigung, Aussetzung der Verarbeitung und Löschung) und die Gründe sowie die Grenzen für mögliche Einschränkungen dieser Rechte. Gemäß dieser Bekanntmachung ist die Anwendung der Grundsätze, Rechte und Pflichten des PIPA auf die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit Ausdruck der in der Verfassung vorgesehenen Garantien für den

([11]) Entscheidung des Verfassungsgerichts vom 29. November 2001, 99HeonMa494.
([12]) Siehe z. B. die Entscheidung 99HunMa513 des Verfassungsgerichts.
([13]) Artikel 29 Absatz 1 der Verfassung.
([14]) Artikel 68 Absatz 1 des Gesetzes über das Verfassungsgericht.
([15]) Artikel 5 Absatz 1 PIPA.
([16]) Artikel 58 Absatz 1 Nummer 2 PIPA.
([17]) Abschnitt III, Absatz 6 der Bekanntmachung Nr. 2021-1 der PIPC über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten.

Schutz des Rechts natürlicher Personen, die eigenen personenbezogenen Daten zu kontrollieren. Jede Einschränkung dieses Rechts, z. B. wenn dies zum Schutz der nationalen Sicherheit notwendig ist, erfordert eine Abwägung der Rechte und Interessen des Einzelnen gegen das betreffende öffentliche Interesse und darf das Recht in seinem Wesensgehalt nicht antasten (Artikel 37 Absatz 2 der Verfassung).

2. STAATLICHER ZUGRIFF FÜR STRAFVERFOLGUNGSZWECKE

2.1. Zuständige Behörden im Bereich der Strafverfolgung

Auf der Grundlage des Strafverfahrensgesetzes (Criminal Procedure Act, CPA), des Gesetzes zum Schutz der Privatsphäre bei der Kommunikation (Communications Privacy Protection Act, CPPA) und des Gesetzes über Telekommunikationsunternehmen (Telecommunications Business Act, TBA) können Polizei, Staatsanwälte und Gerichte für Strafverfolgungszwecke personenbezogene Daten erheben. Dem nationalen Nachrichtendienst (National Intelligence Service, NIS) wurde diese Befugnis durch das Gesetz über den nationalen Nachrichtendienst (National Intelligence Service Act, im Folgenden „NIS-Gesetz“) übertragen; er unterliegt in dem dadurch vorgegebenen Maße ebenfalls den oben genannten Gesetzen ([18]). Das Gesetz über die Meldung und Nutzung genau bestimmter Finanztransaktionsdaten (Act on Reporting and Using Specified Financial Transaction Information, ARUSFTI) bildet schließlich die Rechtsgrundlage für die Offenlegung von Daten durch Finanzinstitute gegenüber der zentralen Meldestelle Koreas (Korea Financial Intelligence Unit, KOFIU) zur Prävention der Geldwäsche und der Terrorismusfinanzierung. Diese Spezialbehörde darf die Daten wiederum an die Strafverfolgungsbehörden weiterleiten. Diese Offenlegungspflichten gelten jedoch nur für Datenverantwortliche, die personenbezogene Kreditdaten gemäß dem Kreditdatengesetz verarbeiten und der Aufsicht der Finanzdienstleistungskommission unterliegen. Da die Verarbeitung personenbezogener Kreditdaten durch solche Datenverantwortliche nicht in den Geltungsbereich des Angemessenheitsbeschlusses fällt, werden die Einschränkungen und Garantien nach dem ARUSFTI in diesem Dokument nicht näher beschrieben.

2.2. Rechtsgrundlagen und Einschränkungen

Das CPA (siehe 2.2.1), das CPPA (siehe 2.2.2) und das TBA (siehe 2.2.3) bilden die Rechtsgrundlagen für die Erhebung personenbezogener Daten für Strafverfolgungszwecke und enthalten die geltenden Einschränkungen und Garantien.

2.2.1. *Durchsuchung und Beschlagnahme*

2.2.1.1. Rechtsgrundlage

Staatsanwälte und leitende Beamte der Kriminalpolizei dürfen nur dann Gegenstände inspizieren, Personen durchsuchen oder Gegenstände beschlagnahmen, 1) wenn eine Person einer Straftat verdächtigt wird (Tatverdächtiger), 2) wenn es für die Untersuchung erforderlich ist und 3) wenn angenommen wird, dass die zu inspizierenden Gegenstände, die zu durchsuchenden Personen und die beschlagnahmten Gegenstände mit dem Fall in Verbindung stehen ([19]). Ebenso können Gerichte Durchsuchungen durchführen und Gegenstände beschlagnahmen, die als Beweismaterial verwendet werden sollen oder der Einziehung unterliegen, sofern die betreffenden Gegenstände oder Personen mit einem konkreten Fall in Verbindung gebracht werden ([20]).

2.2.1.2. Einschränkungen und Garantien

Staatsanwälte und Beamte der Kriminalpolizei sind allgemein verpflichtet, die Menschenrechte des Tatverdächtigen und anderer Betroffener zu achten ([21]). Zudem sind Zwangsmaßnahmen zur Erreichung des Zwecks der Untersuchung nur in den Fällen zulässig, die im CPA ausdrücklich vorgesehen sind, und das notwendige Mindestmaß ihrer Anwendung darf nicht überschritten werden ([22]).

Durchsuchungen, Inspektionen oder Beschlagnahmen durch Polizeibeamte oder Staatsanwälte im Rahmen einer strafrechtlichen Untersuchung dürfen nur auf der Grundlage einer gerichtlichen Anordnung erfolgen ([23]). Die Behörde, die eine solche Anordnung beantragt, muss Unterlagen vorlegen, aus denen hervorgeht, warum eine Person einer Straftat verdächtigt wird, dass die Durchsuchung, Inspektion oder Beschlagnahme erforderlich ist und dass die zu beschlagnahmenden Gegenstände existieren ([24]). In der Anordnung sind unter anderem der Name des Tatverdächtigen und die Bezeichnung der Straftat, der Ort, die Person oder die Gegenstände, die durchsucht werden sollen, oder die Gegenstände, die beschlagnahmt werden sollen, das Ausstellungsdatum und die Geltungsdauer zu nennen ([25]). Wenn in einem laufenden Gerichtsverfahren Durchsuchungen und Beschlagnahmen nicht in einem öffentlichen Verfahren durchgeführt werden, muss ebenfalls eine gerichtliche Anordnung eingeholt werden ([26]). Der Betroffene und sein Verteidiger werden im Voraus über die Durchsuchung oder Beschlagnahme unterrichtet und dürfen bei der Vollstreckung der Anordnung anwesend sein ([27]).

([18]) Siehe Artikel 3 des NIS-Gesetzes (Gesetz Nr. 12948), der sich auf strafrechtliche Ermittlungen bei bestimmten Straftaten wie Aufstand, Rebellion und Verbrechen in Zusammenhang mit der nationalen Sicherheit (z. B. Spionage) bezieht. Für Durchsuchungen und Beschlagnahmen gelten die Verfahren des CPA, während das CPPA die Erhebung von Kommunikationsdaten regelt (siehe Teil 3 zu den Bestimmungen über den Zugriff auf Kommunikationsdaten für die Zwecke der nationalen Sicherheit).
([19]) Artikel 215 Absätze 1 und 2 CPA.
([20]) Artikel 106 Absatz 1, Artikel 107 und Artikel 109 CPA.
([21]) Artikel 198 Absatz 2 CPA.
([22]) Artikel 199 Absatz 1 CPA.
([23]) Artikel 215 Absätze 1 und 2 CPA.
([24]) Artikel 108 Absatz 1 der Regulation on Criminal Procedure (Strafverfahrensverordnung).
([25]) Artikel 114 Absatz 1 CPA in Verbindung mit Artikel 219 CPA.
([26]) Artikel 113 CPA.
([27]) Artikel 121 und 122 CPA.

Bei Durchsuchungen oder Beschlagnahmen von Computerfestplatten oder anderen Datenträgern werden grundsätzlich nur die (kopierten oder ausgedruckten) Daten selbst und nicht der gesamte Datenträger beschlagnahmt ([28]). Der Datenträger selbst darf nur beschlagnahmt werden, wenn es als im Wesentlichen unmöglich erachtet wird, die erforderlichen Daten getrennt auszudrucken oder zu kopieren, oder wenn es als im Wesentlichen nicht praktikabel erachtet wird, den Zweck der Durchsuchung auf andere Weise zu erfüllen ([29]). Der Betroffene muss unverzüglich über die Beschlagnahme unterrichtet werden ([30]). Diese Informationspflicht ist nach dem CPA ausnahmslos anzuwenden.

Durchsuchungen, Inspektionen und Beschlagnahmen ohne gerichtliche Anordnung sind nur in bestimmten Fällen zulässig. Dazu gehören erstens Situationen, in denen es aufgrund der Dringlichkeit am Tatort unmöglich ist, eine Anordnung einzuholen ([31]). Dies muss anschließend jedoch unverzüglich nachgeholt werden ([32]). Zweitens kann bei der Festnahme oder Verhaftung eines Tatverdächtigen vor Ort eine Durchsuchung und Inspektion ohne gerichtliche Anordnung erfolgen ([33]). Drittens können Staatsanwälte oder leitende Beamte der Kriminalpolizei einen Gegenstand ohne gerichtliche Anordnung beschlagnahmen, wenn der Gegenstand von einem Tatverdächtigen oder einer dritten Person entsorgt oder freiwillig übergeben wurde ([34]).

Beweismaterial, das unter Verstoß gegen das CPA erhoben wurde, wird als unzulässig betrachtet ([35]). Darüber hinaus ist im Strafgesetz (Criminal Act) festgelegt, dass eine unrechtmäßige Durchsuchung einer Person oder des Wohnorts, eines geschützten Gebäudes, Bauwerks, Kraftfahrzeugs, Schiffs, Flugzeugs oder Zimmers einer Person mit einer Freiheitsstrafe von bis zu drei Jahren geahndet werden kann ([36]). Diese Bestimmung gilt folglich auch für die Beschlagnahme von Gegenständen wie Datenträgern während einer unrechtmäßigen Durchsuchung.

2.2.2. *Erhebung von Kommunikationsdaten*

2.2.2.1. Rechtsgrundlage

Die Erhebung von Kommunikationsdaten wird durch ein spezielles Gesetz, das CPPA, geregelt. Gemäß dem CPPA ist es insbesondere verboten, Post zu zensieren, Telekommunikation abzuhören, Kommunikationsbestätigungsdaten zu übermitteln oder nicht öffentliche Gespräche zwischen anderen Personen aufzuzeichnen oder abzuhören, es sei denn, dies geschieht auf der Grundlage des CPA, des CPPA oder des Militärgerichtsgesetzes (Military Court Act) ([37]). „Kommunikation" im Sinne des CPPA umfasst sowohl gewöhnliche Post als auch Telekommunikation ([38]). In diesem Zusammenhang wird im CPPA zwischen „kommunikationsbeschränkenden Maßnahmen" ([39]) und der Erhebung von „Kommunikationsbestätigungsdaten" unterschieden.

Der Begriff der kommunikationsbeschränkenden Maßnahmen umfasst die „Zensur", d. h. die Erhebung von Inhaltsdaten herkömmlicher Postsendungen sowie das „Abhören", d. h. die direkte Überwachung (Erfassung oder Aufzeichnung) des Inhalts eines Telekommunikationsvorgangs ([40]). Der Begriff der Kommunikationsbestätigungsdaten umfasst folgende „Aufzeichnungsdaten von Telekommunikationsvorgängen": das Datum des Telekommunikationsvorgangs, seine Anfangs- und Endzeit, die Zahl der ausgehenden und eingehenden Anrufe sowie die Rufnummer der anderen Person, die Häufigkeit der Nutzung, Protokolldateien über die Nutzung von Telekommunikationsdiensten und Standortdaten (z. B. von den Sendemasten, die die Signale empfangen) ([41]).

([28]) Artikel 106 Absatz 3 CPA.
([29]) Artikel 106 Absatz 3 CPA.
([30]) Artikel 219 CPA in Verbindung mit Artikel 106 Absatz 4 CPA.
([31]) Artikel 216 Absatz 3 CPA.
([32]) Artikel 216 Absatz 3 CPA.
([33]) Artikel 216 Absätze 1 und 2 CPA.
([34]) Artikel 218 CPA. In Bezug auf personenbezogene Daten gilt dies nur für die freiwillige Übergabe durch die betroffene Person selbst, nicht für die Übergabe durch einen Datenverantwortlichen, der über diese Daten verfügt (Letzteres würde nach dem PIPA eine spezielle Rechtsgrundlage erfordern). Freiwillig übergebene Gegenstände werden nur dann als Beweismaterial in einem Gerichtsverfahren zugelassen, wenn kein begründeter Zweifel an der Freiwilligkeit der Übergabe besteht, was der Staatsanwalt nachweisen muss. Siehe die Entscheidung des obersten Gerichtshofs vom 10. März 2016, 2013Do11233.
([35]) Artikel 308-2 CPA.
([36]) Artikel 321 des Strafgesetzes.
([37]) Artikel 3 CPPA. Das Militärgerichtsgesetz regelt grundsätzlich die Erhebung von Daten über militärisches Personal und ist nur in einigen wenigen Fällen auf Zivilisten anwendbar (beispielsweise kann ein Militärgericht angerufen werden, wenn militärisches Personal und Zivilisten gemeinsam eine Straftat begehen oder wenn eine Straftat gegen das Militär begangen wird, siehe Artikel 2 des Militärgerichtsgesetzes). Die allgemeinen Bestimmungen über Durchsuchungen und Beschlagnahmen ähneln denen des CPA, siehe z. B. die Artikel 146–149 und 153–156 des Militärgerichtsgesetzes. Beispielsweise dürfen Postdaten nur erhoben werden, wenn dies für eine Untersuchung erforderlich ist und wenn eine Anordnung des Militärgerichts vorliegt. Für die Erhebung der Daten elektronischer Kommunikation gelten die Einschränkungen und Garantien des CPPA.
([38]) Das heißt „die Übertragung oder der Empfang aller Arten von Geräuschen, Wörtern, Symbolen oder Bildern über Kabel, Funk, Glasfaserkabel oder andere elektromagnetische Systeme, einschließlich Telefon, E-Mail, Mitgliederinformationsdienste, Telefax und Funkrufsysteme" (Artikel 2 Absatz 1 CPPA).
([39]) Artikel 2 Absatz 7 und Artikel 3 Absatz 2 CPPA.
([40]) „Zensur" ist definiert als „das Öffnen von Post ohne Zustimmung des Betroffenen oder die Aneignung von Wissen über ihren Inhalt, die Aufzeichnung oder die Vorenthaltung ihres Inhalts auf anderem Wege" (Artikel 2 Absatz 6 CPPA). „Abhören" bezeichnet „die Erfassung oder Aufzeichnung des Inhalts von Telekommunikation durch Abhören oder Mitlesen der Geräusche, Wörter, Symbole oder Bilder eines Kommunikationsvorgangs mittels elektronischer und mechanischer Geräte ohne Einwilligung des Betroffenen oder die Störung der Übertragung und des Empfangs" (Artikel 2 Absatz 7 CPPA).
([41]) Artikel 2 Absatz 11 CPPA.

Im CPPA sind die Einschränkungen und Garantien für die Erhebung beider Arten von Daten festgelegt, und mehrere dieser Anforderungen sind bei Nichteinhaltung mit strafrechtlichen Sanktionen belegt ([42]).

2.2.2.2. Einschränkungen und Garantien für die Erhebung von Kommunikationsinhaltsdaten (kommunikationsbeschränkende Maßnahmen)

Die Erhebung von Kommunikationsinhaltsdaten darf nur als zusätzliches Mittel zur Erleichterung einer strafrechtlichen Untersuchung (d. h. als letztes Mittel) erfolgen, und es müssen Anstrengungen unternommen werden, um Eingriffe in die Kommunikationsgeheimnisse der Menschen auf ein Mindestmaß zu beschränken ([43]). Nach diesem allgemeinen Grundsatz dürfen kommunikationsbeschränkende Maßnahmen nur dann ergriffen werden, wenn es schwierig ist, auf andere Weise die Begehung einer Straftat zu verhindern, den Straftäter festzunehmen oder Beweismaterial zu sammeln ([44]). Damit die Verletzung der Privatsphäre bei der Kommunikation so gering wie möglich ist, müssen Strafverfolgungsbehörden die Erhebung von Kommunikationsdaten unverzüglich einstellen, sobald die Fortsetzung des Zugriffs nicht mehr für notwendig erachtet wird ([45]).

Darüber hinaus dürfen kommunikationsbeschränkende Maßnahmen nur dann angewandt werden, wenn wesentliche Gründe für den Verdacht vorliegen, dass bestimmte im CPPA ausdrücklich aufgeführte schwere Straftaten geplant sind, begangen werden oder begangen wurden. Zu diesen Straftaten gehören etwa Aufstände, Drogenkriminalität oder Sprengstoffkriminalität sowie Straftaten in Zusammenhang mit der nationalen Sicherheit, den diplomatischen Beziehungen oder Militärstützpunkten und -anlagen ([46]). Ziel einer kommunikationsbeschränkenden Maßnahme müssen bestimmte Postsendungen oder Telekommunikationsnachrichten sein, die der Verdächtige sendet oder empfängt, oder die Postsendungen oder Telekommunikationsnachrichten, die der Verdächtige während eines bestimmten Zeitraums sendet oder empfängt ([47]).

Selbst wenn diese Anforderungen erfüllt sind, darf die Erhebung von Inhaltsdaten nur auf der Grundlage einer gerichtlichen Anordnung erfolgen. Ein Staatsanwalt kann das Gericht ersuchen, die Erhebung von Inhaltsdaten in Bezug auf den Verdächtigen oder den Beschuldigten zu genehmigen ([48]). Ebenso kann ein Beamter der Kriminalpolizei bei einem Staatsanwalt eine Genehmigung beantragen, der wiederum eine gerichtliche Anordnung beantragen kann ([49]). Der Antrag auf Anordnung ist schriftlich zu stellen und muss konkrete Angaben enthalten. Insbesondere sind darin folgende Punkte darzulegen: 1) die wesentlichen Gründe für den Verdacht, dass eine der aufgeführten Straftaten geplant ist, begangen wird oder begangen wurde, sowie alle Unterlagen, die einen Prima-facie-Fall begründen, 2) die kommunikationsbeschränkenden Maßnahmen sowie ihr Ziel, Umfang, Zweck und der Durchführungszeitraum und 3) der Ort, an dem die Maßnahmen durchgeführt werden sollen, und die Art und Weise ihrer Durchführung ([50]).

Sind die gesetzlichen Voraussetzungen erfüllt, so kann das Gericht schriftlich die Genehmigung zur Durchführung kommunikationsbeschränkender Maßnahmen in Bezug auf den Verdächtigen oder den Beschuldigten erteilen ([51]). In der entsprechenden Anordnung werden die Arten der Maßnahmen sowie ihr Ziel, Umfang und Durchführungszeitraum, der Ort und die Art und Weise ihrer Durchführung festgelegt ([52]).

Kommunikationsbeschränkende Maßnahmen dürfen nur über einen Zeitraum von zwei Monaten durchgeführt werden ([53]). Wird das Ziel der Maßnahmen innerhalb dieses Zeitraums früher erreicht, müssen die Maßnahmen unverzüglich eingestellt werden. Sind hingegen die erforderlichen Voraussetzungen noch erfüllt, kann innerhalb der Zweimonatsfrist ein Antrag auf Verlängerung des Durchführungszeitraums der kommunikationsbeschränkenden Maßnahmen gestellt werden. Ein solcher Antrag muss Unterlagen enthalten, die im Hinblick auf die Verlängerung der Maßnahmen einen Prima-facie-Fall begründen ([54]). Der verlängerte Zeitraum darf insgesamt ein Jahr bzw. drei Jahre bei bestimmten besonders schweren Straftaten (z. B. Verbrechen in Zusammenhang mit Aufständen, Angriffen aus dem Ausland, der nationalen Sicherheit usw.) nicht überschreiten ([55]).

Die Strafverfolgungsbehörden können die Unterstützung der Anbieter von Kommunikationsdiensten erzwingen, indem sie ihnen die schriftliche Genehmigung des Gerichts vorlegen ([56]). Die Anbieter sind in diesem Fall zur Zusammenarbeit verpflichtet und müssen die ihnen vorgelegte Genehmigung in ihren Akten aufbewahren ([57]). Sie können die Zusammenarbeit jedoch verweigern, wenn die schriftliche Genehmigung des Gerichts falsche Angaben zu der Zielperson (z. B. eine falsche Telefonnummer) enthält. Darüber hinaus ist es ihnen unter allen Umständen untersagt, für die Telekommunikation verwendete Passwörter offenzulegen ([58]).

([42]) Artikel 16 und 17 CPPA. Dies gilt z. B. für Beschlagnahmen ohne Anordnung, das Versäumnis, Aufzeichnungen zu führen, das Versäumnis, die Beschlagnahme einzustellen, wenn keine Dringlichkeit mehr besteht, oder das Versäumnis, die betroffene Person zu benachrichtigen.
([43]) Artikel 3 Absatz 2 CPPA.
([44]) Artikel 5 Absatz 1 CPPA.
([45]) Artikel 2 des CPPA-Durchführungserlasses.
([46]) Artikel 5 Absatz 1 CPPA.
([47]) Artikel 5 Absatz 2 CPPA.
([48]) Artikel 6 Absatz 1 CPPA.
([49]) Artikel 6 Absatz 2 CPPA.
([50]) Artikel 6 Absatz 4 CPPA und Artikel 4 Absatz 1 des CPPA-Durchführungserlasses.
([51]) Artikel 6 Absätze 5 und 8 CPPA.
([52]) Artikel 6 Absatz 6 CPPA.
([53]) Artikel 6 Absatz 7 CPPA.
([54]) Artikel 6 Absatz 7 CPPA.
([55]) Artikel 6 Absatz 8 CPPA.
([56]) Artikel 9 Absatz 2 CPPA.
([57]) Artikel 15-2 CPPA und Artikel 12 des CPPA-Durchführungserlasses.
([58]) Artikel 9 Absatz 4 CPPA.

Wer kommunikationsbeschränkende Maßnahmen ausführt oder zur Zusammenarbeit aufgefordert wird, muss Aufzeichnungen über die Zwecke der Maßnahmen, ihre Ausführung, das Datum der Zusammenarbeit und das Ziel führen ([59]). Auch die Strafverfolgungsbehörden, die kommunikationsbeschränkende Maßnahmen ergreifen, haben Aufzeichnungen zu führen, in denen die Einzelheiten der Maßnahmen und die erzielten Ergebnisse dokumentiert werden ([60]). Nach Abschluss einer Untersuchung muss die Kriminalpolizei dem Staatsanwalt einen Bericht mit diesen Informationen vorlegen ([61]).

Wenn ein Staatsanwalt in einem Fall, in dem kommunikationsbeschränkende Maßnahmen angewandt wurden, Anklage erhebt oder verfügt, dass die betroffene Person nicht angeklagt oder festgenommen wird (im Unterschied zu einer Aussetzung der Strafverfolgung), hat der Staatsanwalt die Person, gegen die die kommunikationsbeschränkenden Maßnahmen verhängt wurden, über die Durchführung der kommunikationsbeschränkenden Maßnahmen, die durchführende Behörde und den Durchführungszeitraum zu unterrichten. Diese Benachrichtigung muss schriftlich innerhalb von 30 Tagen nach der Verfügung erfolgen ([62]). Die Benachrichtigung kann aufgeschoben werden, wenn wahrscheinlich ist, dass sie eine ernsthafte Gefährdung der nationalen Sicherheit, eine Beeinträchtigung der öffentlichen Sicherheit und Ordnung oder eine wesentliche Schädigung Dritter an Leib und Leben nach sich ziehen würde ([63]). Will der Staatsanwalt oder ein Beamter der Kriminalpolizei die Benachrichtigung aufschieben, muss er die Genehmigung des Leiters der Bezirksstaatsanwaltschaft einholen ([64]). Wenn die Gründe für den Aufschub nicht mehr bestehen, hat die Benachrichtigung innerhalb von 30 Tagen zu erfolgen ([65]).

Im CPPA ist auch ein spezielles Verfahren festgelegt, das die Erhebung von Kommunikationsinhaltsdaten in dringenden Fällen regelt. Strafverfolgungsbehörden können Kommunikationsinhaltsdaten erheben, wenn sich die Planung oder Durchführung eines organisierten Verbrechens oder einer anderen schweren Straftat abzeichnet, die unmittelbar zum Tod oder zu schweren Verletzungen führen kann, und wenn es aufgrund der Dringlichkeit der Situation unmöglich ist, das oben beschriebene reguläre Verfahren zu durchlaufen ([66]). In einem solchen dringenden Fall kann ein Polizeibeamter oder Staatsanwalt ohne vorherige gerichtliche Genehmigung kommunikationsbeschränkende Maßnahmen ergreifen, wobei die gerichtliche Genehmigung jedoch unmittelbar nach deren Durchführung zu beantragen ist. Liegt der Strafverfolgungsbehörde nicht innerhalb von 36 Stunden nach Durchführung der Eilmaßnahmen eine gerichtliche Genehmigung vor, so ist die Erhebung unverzüglich einzustellen, in der Regel gefolgt von der Vernichtung der erhobenen Daten ([67]). Führen Polizeibeamte in einem dringenden Fall eine Überwachung durch, unterliegen sie dabei der Kontrolle eines Staatsanwalts oder müssen, falls die Unterweisung durch den Staatsanwalt aufgrund des dringenden Handlungsbedarf vorab nicht möglich ist, unmittelbar nach Durchführungsbeginn die Genehmigung eines Staatsanwalts einholen ([68]). Die oben dargelegten Bestimmungen über die Benachrichtigung der betroffenen Person gelten auch für die Erhebung von Kommunikationsinhaltsdaten in dringenden Fällen.

Die Datenerhebung in dringenden Fällen hat stets gemäß einer „Erklärung über die Dringlichkeit von Zensur- oder Abhörmaßnahmen“ zu erfolgen und die Behörde, die die Erhebung durchführt, muss ein Eilmaßnahmenregister führen ([69]). Dem bei einem Gericht gestellten Antrag auf Genehmigung von Eilmaßnahmen ist ein schriftliches Dokument beizufügen, das folgende Informationen enthält: die erforderlichen kommunikationsbeschränkenden Maßnahmen, Ziel, Angelegenheit, Umfang, Zeitraum, Durchführungsort und -art sowie eine Erklärung, inwiefern in Bezug auf die betreffenden kommunikationsbeschränkenden Maßnahmen die Anforderungen des Artikels 5 Absatz 1 CPPA erfüllt sind ([70]); entsprechende Nachweise sind beizufügen.

In Fällen, in denen eine Eilmaßnahme innerhalb kurzer Zeit abgeschlossen wird, sodass eine gerichtliche Genehmigung ausgeschlossen ist (z. B. wenn der Verdächtige unmittelbar nach Überwachungsbeginn festgenommen und die Überwachung beendet wird), unterrichtet der Leiter der zuständigen Staatsanwaltschaft das zuständige Gericht in einer entsprechenden Mitteilung über die Eilmaßnahme ([71]). In der Mitteilung sind Zweck, Ziel, Umfang, Zeitraum, Ort und Art der Erhebung anzugeben sowie die Gründe zu nennen, warum kein Antrag auf gerichtliche Genehmigung gestellt wurde ([72]). Die Mitteilung ermöglicht dem empfangenden Gericht die Prüfung der Rechtmäßigkeit der Erhebung und ist in einem Eilmaßnahmenregister zu erfassen.

([59]) Artikel 9 Absatz 3 CPPA.
([60]) Artikel 18 Absatz 1 des CPPA-Durchführungserlasses.
([61]) Artikel 18 Absatz 2 des CPPA-Durchführungserlasses.
([62]) Artikel 9-2 Absatz 1 CPPA.
([63]) Artikel 9-2 Absatz 4 CPPA.
([64]) Artikel 9-2 Absatz 5 CPPA.
([65]) Artikel 9-2 Absatz 6 CPPA.
([66]) Artikel 8 Absatz 1 CPPA.
([67]) Artikel 8 Absatz 2 CPPA.
([68]) Artikel 8 Absatz 3 CPPA und Artikel 16 Absatz 3 des CPPA-Durchführungserlasses.
([69]) Artikel 8 Absatz 4 CPPA.
([70]) Das heißt, dass wesentliche Gründe für den Verdacht vorliegen, dass bestimmte schwere Straftaten geplant sind, begangen werden oder begangen wurden und es nicht praktikabel ist, auf andere Weise die Begehung einer Straftat zu verhindern, den Straftäter festzunehmen oder Beweismaterial zu sammeln.
([71]) Artikel 8 Absatz 5 CPPA.
([72]) Artikel 8 Absätze 6 und 7 CPPA.

Allgemein gilt, dass der Inhalt eines Kommunikationsvorgangs, der durch die Durchführung von kommunikationsbeschränkenden Maßnahmen auf der Grundlage des CPPA erfasst wurde, nur in folgenden Fällen genutzt werden darf: zur Untersuchung, Verfolgung oder Verhütung der oben genannten spezifischen Straftaten, in Disziplinarverfahren wegen derselben Straftaten, in Zusammenhang mit einem Schadenersatzanspruch, der von einem der Kommunikationspartner erhoben wird, oder wenn dies nach anderen Gesetzen erlaubt ist ([73]).

Besondere Garantien gelten, wenn über das Internet übermittelte Telekommunikationsdaten erhoben werden ([74]). Diese Daten dürfen nur zur Untersuchung der in Artikel 5 Absatz 1 CPPA aufgeführten schweren Straftaten genutzt werden. Zur Speicherung der Daten ist eine entsprechende Genehmigung des Gerichts einzuholen, das auch die kommunikationsbeschränkenden Maßnahmen genehmigt hat ([75]). Jeder Antrag auf Datenspeicherung muss Angaben zu den kommunikationsbeschränkenden Maßnahmen, eine Zusammenfassung der Ergebnisse der Maßnahmen, die Gründe für die Speicherung (mit Belegen) und die Informationen über die zu speichernden Telekommunikationsdaten enthalten ([76]). Ohne einen solchen Antrag sind die erhobenen Telekommunikationsdaten innerhalb von 14 Tagen nach Beendigung der kommunikationsbeschränkenden Maßnahmen zu löschen ([77]). Wird der Antrag abgelehnt, müssen die Telekommunikationsdaten innerhalb von sieben Tagen vernichtet werden ([78]). Werden die Telekommunikationsdaten gelöscht, so ist dem Gericht, das die kommunikationsbeschränkenden Maßnahmen genehmigt hat, innerhalb von sieben Tagen ein Bericht vorzulegen, in dem die Gründe für die Löschung sowie die Einzelheiten und der Zeitpunkt der Löschung angegeben sind.

Allgemein gilt, dass Daten, die auf unrechtmäßige Weise durch kommunikationsbeschränkende Maßnahmen erhoben wurden, nicht als Beweismaterial in Gerichts- oder Disziplinarverfahren zugelassen werden ([79]). Personen, die kommunikationsbeschränkende Maßnahmen ergreifen, ist es nach dem CPPA außerdem verboten, im Zuge der Durchführung dieser Maßnahmen eingeholte vertrauliche Informationen offenzulegen und zu nutzen, um den Ruf der von den Maßnahmen betroffenen Personen zu schädigen ([80]).

2.2.2.3. Einschränkungen und Garantien für die Erhebung von Kommunikationsbestätigungsdaten

Auf der Grundlage des CPPA können Strafverfolgungsbehörden Telekommunikationsdiensteanbieter auffordern, ihnen Kommunikationsbestätigungsdaten zu übermitteln, wenn dies für eine Untersuchung oder die Vollstreckung einer Strafe erforderlich ist ([81]). Anders als bei der Erhebung von Inhaltsdaten ist die Möglichkeit, Kommunikationsbestätigungsdaten einzuholen, nicht auf bestimmte spezifische Straftaten beschränkt. Wie bei Inhaltsdaten erfordert die Erhebung von Kommunikationsbestätigungsdaten jedoch eine vorherige schriftliche Genehmigung eines Gerichts, für die die oben beschriebenen Voraussetzungen erfüllt sein müssen ([82]). Wenn es aus Dringlichkeitsgründen nicht möglich ist, eine gerichtliche Genehmigung zu erhalten, können die Kommunikationsbestätigungsdaten ohne Anordnung erhoben werden; in diesem Fall muss die Genehmigung unmittelbar nach der Anforderung der Daten eingeholt und dem Telekommunikationsdiensteanbieter übermittelt werden ([83]). In Ermangelung einer nachträglichen Genehmigung sind die erhobenen Daten zu vernichten ([84]).

Staatsanwälte, Polizeibeamte und Gerichte müssen Aufzeichnungen über die Anträge zur Erhebung von Kommunikationsbestätigungsdaten führen ([85]). Telekommunikationsdiensteanbieter müssen zudem zweimal jährlich dem Minister für Wissenschaft und IKT über die Offenlegung von Kommunikationsbestätigungsdaten Bericht erstatten, entsprechende Aufzeichnungen führen und diese ab dem Zeitpunkt der Offenlegung der Daten sieben Jahre lang aufbewahren ([86]).

Natürliche Personen werden grundsätzlich darüber unterrichtet, dass Kommunikationsbestätigungsdaten erhoben wurde ([87]). Der Zeitpunkt dieser Benachrichtigung hängt von den Umständen der Untersuchung ab ([88]). Sobald eine Entscheidung für (oder gegen) die Strafverfolgung getroffen wurde, muss die Benachrichtigung innerhalb von 30 Tagen erfolgen. Wird dagegen die Anklage aufgeschoben, ist die betroffene Person innerhalb von 30 Tagen zu unterrichten, nachdem ein Jahr seit dieser Entscheidung vergangen ist. In jedem Fall muss die Benachrichtigung innerhalb von 30 Tagen erfolgen, nachdem ein Jahr seit der Erhebung der Daten vergangen ist.

Die Benachrichtigung kann aufgeschoben werden, wenn sie 1) die Gefährdung der nationalen Sicherheit und der öffentlichen Sicherheit und Ordnung, 2) Tod oder Körperverletzung, 3) die Behinderung eines fairen

([73]) Artikel 12 CPPA.
([74]) Artikel 12-2 CPPA.
([75]) Der Staatsanwalt oder der Polizeibeamte, der die kommunikationsbeschränkenden Maßnahmen durchführt, muss innerhalb von 14 Tagen nach Beendigung der Maßnahmen die zu speichernden Telekommunikationsdaten auswählen und die gerichtliche Genehmigung beantragen (Polizeibeamte haben den Antrag an einen Staatsanwalt zu richten, der wiederum den Antrag bei Gericht einreicht), siehe Artikel 12-2 Absätze 1 und 2 CPPA.
([76]) Artikel 12-2 Absatz 3 CPPA.
([77]) Artikel 12-2 Absatz 5 CPPA.
([78]) Artikel 12-2 Absatz 5 CPPA.
([79]) Artikel 4 CPPA.
([80]) Artikel 11 Absatz 2 des CPPA-Durchführungserlasses.
([81]) Artikel 13 Absatz 1 CPPA.
([82]) Artikel 6 und 13 CPPA.
([83]) Artikel 13 Absatz 2 CPPA. Wie bei dringenden kommunikationsbeschränkenden Maßnahmen ist ein Dokument zu erstellen, in dem die Einzelheiten des Falls (der Verdächtige, die zu ergreifenden Maßnahmen, die mutmaßliche Straftat sowie die Dringlichkeit) dargelegt werden. Siehe Artikel 37 Absatz 5 des CPPA-Durchführungserlasses.
([84]) Artikel 13 Absatz 3 CPPA.
([85]) Artikel 13 Absätze 5 und 6 CPPA.
([86]) Artikel 13 Absatz 7 CPPA.
([87]) Siehe Artikel 13-3 Absatz 7 CPPA in Verbindung mit Artikel 9-2 CPPA.
([88]) Artikel 13-3 Absatz 1 CPPA.

Gerichtsverfahrens (z. B. durch die Vernichtung von Beweismaterial oder die Bedrohung von Zeugen) oder 4) die Verleumdung des Verdächtigen, der Opfer oder anderer mit dem Fall in Verbindung stehender Personen oder die Verletzung ihrer Privatsphäre nach sich ziehen kann ([89]). Liegt einer dieser Gründe vor, muss die Benachrichtigung vom Leiter der zuständigen Bezirksstaatsanwaltschaft genehmigt werden ([90]). Wenn die Gründe für den Aufschub nicht mehr bestehen, hat die Benachrichtigung innerhalb von 30 Tagen zu erfolgen ([91]).

Benachrichtigte Personen können beim Staatsanwalt oder dem betreffenden Beamten der Kriminalpolizei schriftlich die Gründe für die Erhebung der Kommunikationsbestätigungsdaten erfragen ([92]). In diesem Fall muss der Staatsanwalt oder Beamte der Kriminalpolizei die Gründe innerhalb von 30 Tagen nach Empfang der Anfrage schriftlich darlegen, es sei denn, es liegt einer der oben genannten Gründe vor (Ausnahmen für den Aufschub der Benachrichtigung) ([93]).

2.2.3. *Freiwillige Offenlegung durch Telekommunikationsdiensteanbieter*

Nach Artikel 83 Absatz 3 TBA können Telekommunikationsdiensteanbieter freiwillig einem Ersuchen eines Gerichts, Staatsanwalts oder des Leiters einer Untersuchungsbehörde um Offenlegung von „Kommunikationsdaten" entsprechen, das zur Unterstützung eines Strafverfahrens, einer Untersuchung oder der Strafvollstreckung an sie gerichtet wird. Im Sinne des TBA umfassen „Kommunikationsdaten" den Namen, die Melderegisterzahl, die Anschrift und die Telefonnummer von Nutzern, das jeweilige Datum, an dem die Nutzer ihren Vertrag abgeschlossen oder beendet haben, sowie Nutzeridentifikationscodes (d. h. Codes, die zur Identifizierung des rechtmäßigen Nutzers von Computersystemen oder Kommunikationsnetzen verwendet werden) ([94]). Für die Zwecke des TBA gelten als Nutzer nur natürliche Personen, die einen direkten Vertrag über Dienste eines koreanischen Telekommunikationsdiensteanbieters abgeschlossen haben ([95]). Folglich dürfte es nur sehr selten vorkommen, dass natürliche Personen aus der EU, deren Daten in die Republik Korea übermittelt wurden, unter die Nutzerdefinition des TBA fallen, da sie normalerweise keinen direkten Vertrag mit einem koreanischen Telekommunikationsdiensteanbieter abschließen würden.

Jedes Ersuchen um Offenlegung von Kommunikationsdaten auf der Grundlage des TBA muss schriftlich erfolgen und Ausführungen über die Gründe für das Ersuchen, die Verbindung zu dem betreffenden Nutzer und den Umfang der angeforderten Daten enthalten ([96]). Ist wegen Dringlichkeit ein schriftliches Ersuchen nicht möglich, so muss dieses vorgelegt werden, sobald der Grund für die Dringlichkeit nicht mehr besteht ([97]). Telekommunikationsdiensteanbieter, die den Ersuchen um Offenlegung von Kommunikationsdaten nachkommen, müssen Bücher führen, die Aufzeichnungen über die Übermittlung von Kommunikationsdaten sowie die betreffenden Unterlagen, wie z. B. das schriftliche Ersuchen, enthalten ([98]). Darüber hinaus müssen sie dem Minister für Wissenschaft und IKT zweimal jährlich über die Übermittlung von Kommunikationsdaten Bericht erstatten ([99]).

Telekommunikationsdiensteanbieter sind nicht verpflichtet, einem Ersuchen um Offenlegung von Kommunikationsdaten auf der Grundlage des TBA nachzukommen. Jedes Ersuchen muss daher hinsichtlich der geltenden Datenschutzanforderungen des PIPA vom Anbieter geprüft werden. Insbesondere muss der Telekommunikationsdiensteanbieter die Interessen der betroffenen Person berücksichtigen und darf die Daten nicht offenlegen, wenn es wahrscheinlich ist, dass dadurch die Interessen der betroffenen Person oder eines Dritten in unfairer Weise verletzt würden ([100]). Gemäß der Bekanntmachung Nr. 2021-1 über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten ist die betroffene Person zudem über die Offenlegung zu unterrichten. In Ausnahmesituationen kann diese Benachrichtigung aufgeschoben werden, insbesondere wenn und solange dadurch eine laufende strafrechtliche Untersuchung gefährdet würde oder die Schädigung eines Dritten an Leib und Leben wahrscheinlich ist, sofern diese Rechte oder Interessen eindeutig Vorrang vor den Rechten der betroffenen Person haben ([101]).

Im Jahr 2016 stellte der oberste Gerichtshof fest, dass durch die freiwillige Übermittlung von Kommunikationsdaten durch Telekommunikationsunternehmen, die ohne Anordnung auf der Grundlage des TBA erfolgt, nicht an sich das Recht des betreffenden Nutzers des Telekommunikationsdienstes auf informationelle Selbstbestimmung verletzt wird. Das Gericht erläuterte jedoch, dass eine Verletzung vorliegt, wenn offensichtlich ist, dass eine Behörde mit einem Ersuchen um Offenlegung von Kommunikationsdaten ihre Autorität missbraucht hat, wodurch die Interessen der betroffenen Person oder eines Dritten verletzt werden ([102]). Allgemein muss jedes Ersuchen einer Strafverfolgungsbehörde um freiwillige Offenlegung den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit entsprechen, die aus der koreanischen Verfassung hervorgehen (Artikel 12 Absatz 1 und Artikel 37 Absatz 2).

([89]) Artikel 13-3 Absatz 2 CPPA.
([90]) Artikel 13-3 Absatz 3 CPPA.
([91]) Artikel 13-3 Absatz 4 CPPA.
([92]) Artikel 13-3 Absatz 5 CPPA.
([93]) Artikel 13-3 Absatz 6 CPPA.
([94]) Artikel 83 Absatz 3 TBA.
([95]) Artikel 2 Absatz 9 TBA.
([96]) Artikel 83 Absatz 4 TBA.
([97]) Artikel 83 Absatz 4 TBA.
([98]) Artikel 83 Absatz 5 TBA.
([99]) Artikel 83 Absatz 6 TBA.
([100]) Artikel 18 Absatz 2 PIPA.
([101]) Abschnitt III Absatz 2 Ziffer iii der Bekanntmachung Nr. 2021-1 der PIPC über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten.
([102]) Entscheidung des obersten Gerichtshofs vom 10. März 2016, 2012Da105482.

2.3. **Aufsicht**

Die Aufsicht über die Strafverfolgungsbehörden wird über verschiedene Mechanismen gewährleistet; sie erfolgt sowohl intern als auch durch externe Stellen.

2.3.1. *Eigenprüfung*

Mit dem Gesetz über Prüfungen im öffentlichen Sektor (Act on Public Sector Audits) werden Behörden aufgefordert, ein internes Gremium für die Eigenprüfung einzurichten, das unter anderem die Aufgabe hat, Rechtmäßigkeitskontrollen durchzuführen ([103]). Den Leitern dieser Prüfungsgremien ist weitestgehende Unabhängigkeit zu garantieren ([104]). Sie werden von Personen außerhalb der betreffenden Behörde (z. B. von ehemaligen Richtern oder Professoren) für einen Zeitraum von zwei bis fünf Jahren ernannt und können nur aus berechtigten Gründen abberufen werden (z. B. wenn sie aufgrund einer geistigen oder körperlichen Behinderung nicht in der Lage sind, ihr Amt auszuüben, oder wenn Disziplinarmaßnahmen gegen sie verhängt wurden) ([105]). Auch für die Ernennung der Prüfer sind in dem Gesetz spezifische Bedingungen festgelegt ([106]). Die Prüfberichte können Empfehlungen oder Aufforderungen zu Schadenersatz oder Abhilfemaßnahmen sowie Verwarnungen und Empfehlungen oder Aufforderungen bezüglich Disziplinarmaßnahmen enthalten ([107]). Sie werden dem Leiter der geprüften Behörde sowie dem Rechnungshof (siehe Abschnitt 2.3.2) innerhalb von 60 Tagen nach Abschluss der Prüfung übermittelt ([108]). Die betroffene Behörde muss die geforderten Maßnahmen umsetzen und dem Rechnungshof über die Ergebnisse Bericht erstatten ([109]). Außerdem werden die Prüfungsergebnisse in der Regel der Öffentlichkeit zugänglich gemacht ([110]). Die Verweigerung oder Behinderung einer Eigenprüfung kann mit einer Geldbuße geahndet werden ([111]). Im Bereich der Strafverfolgung betreibt die nationale Polizei zur Einhaltung der genannten Rechtsvorschriften ein Generalinspekteur-System für interne Prüfungen, auch in Bezug auf mögliche Menschenrechtsverletzungen ([112]).

2.3.2. *Rechnungshof*

Der Rechnungshof (Board of Audit and Inspection – BAI) kann die Tätigkeiten von Behörden kontrollieren und auf der Grundlage solcher Kontrollen Empfehlungen aussprechen, Disziplinarmaßnahmen verlangen oder Strafanzeige erstatten ([113]). Der Rechnungshof ist dem Präsidenten der Republik Korea unterstellt, hat in Bezug auf seine Aufgaben jedoch eine unabhängige Stellung inne ([114]). Das Gesetz zur Errichtung des Rechnungshofes sieht außerdem vor, dass der Rechnungshof auch in Bezug auf die Einstellung, Entlassung und Organisation seines Personals sowie die Aufstellung seines Haushaltsplans weitestgehende Unabhängigkeit genießen soll ([115]). Der Vorsitzende des Rechnungshofs wird mit der Zustimmung der Nationalversammlung vom Präsidenten ernannt ([116]). Die sechs übrigen Mitglieder des Prüfungsausschusses werden auf Empfehlung des Vorsitzenden für eine Amtszeit von vier Jahren vom Präsidenten ernannt ([117]). Die Mitglieder des Prüfungsausschusses (einschließlich des Vorsitzenden) müssen bestimmte gesetzlich festgelegte Voraussetzungen erfüllen ([118]) und dürfen nur in folgenden Fällen abberufen werden: im Fall der Amtsenthebung, bei einer Verurteilung zu einer Freiheitsstrafe oder weil sie wegen langfristiger geistiger oder körperlicher Schwäche nicht in der Lage sind, ihre Aufgaben wahrzunehmen ([119]). Darüber hinaus sind den Mitgliedern des Prüfungsausschusses politische Tätigkeiten und das gleichzeitige Innehaben von Ämtern in der Nationalversammlung, in Verwaltungsbehörden, in den vom Rechnungshof geprüften und kontrollierten Organisationen oder von sonstigen vergüteten Ämtern oder Positionen untersagt ([120]).

Der Rechnungshof führt jährlich eine allgemeine Prüfung durch, kann aber auch Sonderprüfungen zu Fragen von besonderem Interesse vornehmen. Bei einer Kontrolle kann der Rechnungshof die Vorlage von Unterlagen verlangen und Personen vorladen ([121]). Gegenstand einer Prüfung sind zunächst die Einnahmen und Ausgaben des Staates, doch der Rechnungshof prüft auch die allgemeine Einhaltung der Pflichten von Behörden und öffentlichen Bediensteten,

([103]) Artikel 3 und 5 des Gesetzes über Prüfungen im öffentlichen Sektor.
([104]) Artikel 7 des Gesetzes über Prüfungen im öffentlichen Sektor.
([105]) Artikel 8 bis 11 des Gesetzes über Prüfungen im öffentlichen Sektor.
([106]) Artikel 16 ff. des Gesetzes über Prüfungen im öffentlichen Sektor.
([107]) Artikel 23 Absatz 2 des Gesetzes über Prüfungen im öffentlichen Sektor.
([108]) Artikel 23 Absatz 1 des Gesetzes über Prüfungen im öffentlichen Sektor.
([109]) Artikel 23 Absatz 3 des Gesetzes über Prüfungen im öffentlichen Sektor.
([110]) Artikel 26 des Gesetzes über Prüfungen im öffentlichen Sektor.
([111]) Artikel 41 des Gesetzes über Prüfungen im öffentlichen Sektor.
([112]) Siehe insbesondere die Abteilungen, die dem Generaldirektor für Prüfungen und Kontrollen (Director General for Audit and Inspection) unterstehen: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Artikel 24 und 31–35 des Gesetzes über den Rechnungshof (Board of Audit and Inspection Act, im Folgenden „BAI-Gesetz“).
([114]) Artikel 2 Absatz 1 des BAI-Gesetzes.
([115]) Artikel 2 Absatz 2 des BAI-Gesetzes.
([116]) Artikel 4 Absatz 1 des BAI-Gesetzes.
([117]) Artikel 5 Absatz 1 und Artikel 6 des BAI-Gesetzes.
([118]) Beispielsweise müssen sie mindestens zehn Jahre als Richter, Staatsanwalt oder Rechtsanwalt gearbeitet haben, mindestens acht Jahren als Beamter oder als Professor oder Inhaber einer höheren Stelle an einer Hochschule tätig gewesen sein oder mindestens zehn Jahre lang in einem börsennotierten Unternehmen oder einer staatlich finanzierten Einrichtung gearbeitet haben (davon mindestens fünf Jahre als Geschäftsführer), siehe Artikel 7 des BAI-Gesetzes.
([119]) Artikel 8 des BAI-Gesetzes.
([120]) Artikel 9 des BAI-Gesetzes.
([121]) Siehe z. B. Artikel 27 des BAI-Gesetzes.

um die Funktionsweise der öffentlichen Verwaltung zu verbessern ([122]). Seine Aufsicht erstreckt sich somit über Haushaltsaspekte hinaus und umfasst auch eine Rechtmäßigkeitskontrolle.

2.3.3. *Nationalversammlung*

Die Nationalversammlung kann Behörden Untersuchungen und Kontrollen unterziehen ([123]). Im Rahmen einer Untersuchung oder Kontrolle kann die Nationalversammlung die Offenlegung von Dokumenten verlangen und Zeugen vorladen ([124]). Wer während einer Untersuchung der Nationalversammlung einen Meineid leistet, wird strafrechtlich belangt (Freiheitsstrafe von bis zu zehn Jahren) ([125]). Das Verfahren und die Ergebnisse der Kontrollen können der Öffentlichkeit zugänglich gemacht werden ([126]). Stellt die Nationalversammlung unrechtmäßige oder missbräuchliche Tätigkeiten fest, so kann sie die betreffende Behörde auffordern, Abhilfemaßnahmen zu treffen; dazu zählen die Gewährung von Schadenersatz, Disziplinarmaßnahmen und die Verbesserung der internen Verfahren ([127]). Auf eine solche Aufforderung hin muss die Behörde unverzüglich tätig werden und der Nationalversammlung über das Ergebnis Bericht erstatten ([128]).

2.3.4. *Kommission für den Schutz personenbezogener Daten*

Die Kommission für den Schutz personenbezogener Daten (Personal Information Protection Commission, PIPC), überwacht, ob die Verarbeitung personenbezogener Daten durch die Strafverfolgungsbehörden mit dem PIPA im Einklang steht. Außerdem erstreckt sich die Aufsicht der PIPC gemäß Artikel 7-8 Absätze 3 und 4 und Artikel 7-9 Absatz 5 PIPA auch auf mögliche Verstöße gegen Einschränkungs- und Garantiebestimmungen in Bezug auf die Erhebung personenbezogener Daten, einschließlich derjenigen, die in den speziellen Gesetzen über die Sammlung von (elektronischem) Beweismaterial für die Zwecke der Strafverfolgung enthalten sind (siehe Abschnitt 2.2). Artikel 3 Absatz 1 PIPA sieht eine rechtmäßige und faire Erhebung personenbezogener Daten vor, und ein Verstoß gegen diese Anforderung stellt einen Verstoß gegen das PIPA dar, der die PIPC berechtigt, eine Untersuchung durchzuführen und Abhilfemaßnahmen zu ergreifen ([129]).

Bei der Wahrnehmung ihrer Aufsichtsfunktion hat die PIPC Zugriff auf alle zweckdienlichen Informationen ([130]). Die PIPC kann Strafverfolgungsbehörden beraten, wie diese bei ihren Verarbeitungstätigkeiten den Schutz personenbezogener Daten verbessern können, sie kann ihnen Abhilfemaßnahmen auferlegen (z. B. die Aussetzung der Datenverarbeitung oder das Ergreifen der zum Schutz der personenbezogenen Daten erforderlichen Maßnahmen) oder die Einleitung von Disziplinarmaßnahmen empfehlen ([131]). Für bestimmte Verstöße gegen das PIPA (beispielsweise wenn personenbezogene Daten auf unrechtmäßige Weise genutzt oder Dritten offengelegt oder sensible Daten auf unrechtmäßige Weise verarbeitet werden) sind auch strafrechtliche Sanktionen vorgesehen ([132]). Zu diesem Zweck kann die PIPC die Angelegenheit an die zuständige Untersuchungsbehörde (auch an einen Staatsanwalt) verweisen ([133]).

2.3.5. *Nationale Menschenrechtskommission*

Die nationale Menschenrechtskommission (National Human Rights Commission, NHRC) – eine unabhängige Stelle für den Schutz und die Förderung der Grundrechte ([134]) – ist befugt, Verstöße gegen die Artikel 10 bis 22 der Verfassung zu untersuchen und Abhilfe zu schaffen; dies bedeutet, dass sie auch für Verletzungen des Rechts auf Privatsphäre und des Briefgeheimnisses zuständig ist. Die NHRC besteht aus elf Mitgliedern, die auf Vorschlag der Nationalversammlung (vier), des Präsidenten (vier) und des obersten Gerichtshofs (drei) ernannt werden ([135]). In die Kommission berufen werden können Personen, die 1) mindestens zehn Jahre lang und mindestens als außerordentlicher Professor an einer Universität oder einem zugelassenen Forschungsinstitut gearbeitet haben, 2) mindestens zehn Jahre als Richter, Staatsanwalt oder Rechtsanwalt tätig gewesen sind, 3) mindestens zehn Jahre im Bereich der Menschenrechte gearbeitet haben (z. B. für eine gemeinnützige Organisation, eine Nichtregierungsorganisation oder eine internationale Organisation) oder 4) von zivilgesellschaftlichen Gruppen empfohlen worden sind ([136]). Der Vorsitzende wird vom Präsidenten aus dem Kreis

([122]) Artikel 20 und 24 des BAI-Gesetzes.
([123]) Artikel 128 des Gesetzes über die Nationalversammlung (National Assembly Act) und Artikel 2, 3 und 15 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung (Act on the Inspection and Investigation of State Administration). Es werden jährliche allgemeine Kontrollen der Regierungsangelegenheiten sowie Untersuchungen zu spezifischen Fragen durchgeführt.
([124]) Artikel 10 Absatz 1 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung. Siehe auch die Artikel 128 und 129 des Gesetzes über die Nationalversammlung.
([125]) Artikel 14 des Gesetzes über Zeugenaussagen, Begutachtungen usw. vor der Nationalversammlung (Act on Testimony, Appraisal, etc. before the National Assembly).
([126]) Artikel 12-2 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([127]) Artikel 16 Absatz 2 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([128]) Artikel 16 Absatz 3 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([129]) Siehe Bekanntmachung Nr. 2021-1 der PIPC über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten.
([130]) Artikel 63 PIPA.
([131]) Artikel 61 Absatz 2, Artikel 65 Absätze 1 und 2 und Artikel 64 Absatz 4 PIPA.
([132]) Artikel 70–74 PIPA.
([133]) Artikel 65 Absatz 1 PIPA.
([134]) Artikel 1 des Gesetzes über die nationale Menschenrechtskommission (National Human Rights Commission Act, im Folgenden „NHRC-Gesetz“).
([135]) Artikel 5 Absätze 1 und 2 des NHRC-Gesetzes.
([136]) Artikel 5 Absatz 3 des NHRC-Gesetzes.

der Kommissionsmitglieder ernannt und muss von der Nationalversammlung bestätigt werden ([137]). Die Kommissionsmitglieder (einschließlich des Vorsitzenden) werden für eine verlängerbare Amtszeit von drei Jahren ernannt und dürfen nur abberufen werden, wenn sie zu einer Freiheitsstrafe verurteilt wurden oder wegen anhaltender körperlicher oder geistiger Schwäche nicht mehr in der Lage sind, ihre Aufgaben wahrzunehmen (in diesem Fall müssen zwei Drittel der Kommissionsmitglieder der Abberufung zustimmen) ([138]). Den Mitgliedern der NHRC ist es untersagt, gleichzeitig ein Amt in der Nationalversammlung, in einem Gemeinderat oder in einer anderen Regierung oder Verwaltung auf nationaler oder lokaler Ebene (als öffentlicher Bediensteter) auszuüben ([139]).

Die NHRC kann von sich aus oder auf der Grundlage einer Petition einer natürlichen Person eine Untersuchung einleiten. Im Rahmen ihrer Untersuchungen kann die NHRC die Vorlage von sachdienlichen Unterlagen verlangen, Inspektionen durchführen und Personen zur Anhörung vorladen ([140]). Im Anschluss an eine Untersuchung kann die NHRC Empfehlungen zur Verbesserung oder Korrektur bestimmter Strategien und Vorgehensweisen aussprechen und veröffentlichen ([141]). Die Behörden müssen der NHRC innerhalb von 90 Tagen nach Erhalt der Empfehlungen einen Plan für deren Umsetzung mitteilen ([142]). Im Falle der Nichtumsetzung einer Empfehlung hat die betreffende Behörde die Kommission davon in Kenntnis setzen ([143]). Die NHRC kann wiederum die Nationalversammlung und/oder die Öffentlichkeit über die Nichtumsetzung unterrichten. Die Behörden kommen den Empfehlungen der NHRC in der Regel nach und haben einen starken Anreiz dazu, da dies in die allgemeine Bewertung durch das Amt für die Abstimmung der Regierungspolitik (Office for Government Policy Coordination) einfließt, das dem Büro des Premierministers untersteht.

2.4. **Individuelle Rechtsbehelfe**

2.4.1. *Rechtsbehelfsmechanismen nach dem PIPA*

Natürliche Personen können in Bezug auf personenbezogene Daten, die von Strafverfolgungsbehörden verarbeitet werden, ihre Rechte auf Auskunft, Berichtigung, Löschung und Aussetzung der Verarbeitung gemäß dem PIPA ausüben. Ein Auskunftsersuchen kann direkt an die betreffende Behörde gerichtet werden oder indirekt über die PIPC erfolgen ([144]). Die zuständige Behörde darf die Auskunft nur beschränken oder verweigern, wenn dies gesetzlich vorgesehen ist, wenn andernfalls die Schädigung eines Dritten an Leib und Leben oder eine ungerechtfertigte Verletzung der Eigentumsinteressen und anderen Interessen eines Dritten wahrscheinlich wäre (d. h. wenn die Interessen des Dritten schwerer wiegen als die Interessen der Person, die den Antrag gestellt hat) ([145]). Wird ein Auskunftsersuchen abgelehnt, so muss die betroffene Person darüber unterrichtet werden, welche Gründe für die Ablehnung vorliegen und wie sie einen Rechtsbehelf einlegen kann ([146]). Auch ein Antrag auf Berichtigung oder Löschung kann abgelehnt werden, wenn dies in anderen Gesetzen vorgesehen ist, wobei die betroffene Person über die Gründe für die Ablehnung und die Möglichkeit, einen Rechtsbehelf einzulegen, zu unterrichten ist ([147]).

Was die möglichen Rechtsbehelfe anbelangt, so können natürliche Personen bei der PIPC Beschwerde einlegen, unter anderem über das von der koreanischen Internet- und Sicherheitsbehörde (Korea Internet & Security Agency) betriebene Datenschutz-Callcenter ([148]). Außerdem haben sie die Möglichkeit der Schlichtung vor einem speziellen Schlichtungsausschuss für Streitigkeiten in Zusammenhang mit personenbezogenen Daten (Personal Information Dispute Mediation Committee) ([149]). Diese Rechtsbehelfe sind verfügbar bei möglichen Verstößen gegen das PIPA und gegen die in einschlägigen Gesetzen enthaltenen Einschränkungs- und Garantiebestimmungen für die Erhebung personenbezogener Daten (Abschnitt 2.2). Darüber hinaus können die Beschlüsse oder die Untätigkeit der PIPC gemäß dem Gesetz über die Verwaltungsgerichtsbarkeit angefochten werden (siehe Abschnitt 2.4.3).

([137]) Artikel 5 Absatz 5 des NHRC-Gesetzes.
([138]) Artikel 7 Absatz 1 und Artikel 8 des NHRC-Gesetzes.
([139]) Artikel 10 des NHRC-Gesetzes.
([140]) Artikel 36 des NHRC-Gesetzes. Gemäß Artikel 36 Absatz 7 des Gesetzes darf die Vorlage von Unterlagen oder Gegenständen verweigert werden, wenn dies die Vertraulichkeit von Staatsangelegenheiten beeinträchtigen würde und wesentliche negative Auswirkungen auf die Staatssicherheit oder die diplomatischen Beziehungen haben könnte oder wenn es ein schwerwiegendes Hindernis für eine strafrechtliche Untersuchung oder ein anhängiges Gerichtsverfahren darstellen würde. In solchen Fällen kann die Kommission den Leiter der zuständigen Behörde erforderlichenfalls um weitere Informationen bitten, um zu prüfen, ob die Verweigerung der Auskunftserteilung gerechtfertigt ist, und der Behördenleiter muss diesem Ersuchen nach Treu und Glauben nachkommen.
([141]) Artikel 25 Absatz 1 des NHRC-Gesetzes.
([142]) Artikel 25 Absatz 3 des NHRC-Gesetzes.
([143]) Artikel 25 Absatz 4 des NHRC-Gesetzes.
([144]) Artikel 35 Absatz 2 PIPA.
([145]) Artikel 35 Absatz 4 PIPA.
([146]) Artikel 42 Absatz 2 des PIPA-Durchführungserlasses.
([147]) Artikel 36 Absätze 1 und 2 PIPA und Artikel 43 Absatz 3 des PIPA-Durchführungserlasses.
([148]) Artikel 62 PIPA.
([149]) Artikel 40 bis 50 PIPA und Artikel 48-2 bis 57 des PIPA-Durchführungserlasses.

2.4.2. *Rechtsbehelf über die nationale Menschenrechtskommission*

Die NHRC bearbeitet Beschwerden natürlicher Personen (koreanischer wie auch ausländischer Staatsangehöriger) über Menschenrechtsverletzungen, die von Behörden begangen wurden ([150]). Die Einreichung einer Beschwerde bei der NHRC ist nicht an Voraussetzungen gebunden ([151]). Folglich wird eine Beschwerde auch dann von der NHRC bearbeitet, wenn die betroffene Person bei der Zulässigkeitsprüfung keine tatsächliche Schädigung nachweisen kann. Im Zusammenhang der Erhebung personenbezogener Daten für Strafverfolgungszwecke muss eine natürliche Person daher nicht nachweisen, dass koreanische Behörden tatsächlich auf ihre personenbezogenen Daten zugegriffen haben, damit die Beschwerde bei der NHRC zulässig ist. Außerdem kann zur Beilegung einer Beschwerde ein Schlichtungsverfahren beantragt werden ([152]).

Zur Prüfung einer Beschwerde kann die NHRC von ihren Untersuchungsbefugnissen Gebrauch machen und unter anderem die Vorlage zweckdienlicher Unterlagen verlangen, Inspektionen durchführen und Personen zur Anhörung vorladen ([153]). Ergibt die Prüfung, dass ein Verstoß gegen einschlägige Gesetze vorliegt, so kann die NHRC die Umsetzung von Abhilfemaßnahmen oder die Korrektur oder Verbesserung einschlägiger Gesetze, Einrichtungen, Strategien oder Vorgehensweisen empfehlen ([154]). Die vorgeschlagenen Abhilfemaßnahmen können ein Schlichtungsverfahren, die Abstellung der Menschenrechtsverletzung, Schadenersatz und Maßnahmen zur Verhütung eines erneuten Vorkommens der gleichen oder ähnlicher Verletzungen umfassen ([155]). Im Falle einer nach den geltenden Vorschriften unrechtmäßigen Erhebung personenbezogener Daten kann auch die Löschung der erhobenen personenbezogenen Daten eine Abhilfemaßnahme sein. Wird es als sehr wahrscheinlich erachtet, dass der Verstoß andauert, und wird davon ausgegangen, dass bei Untätigkeit schwer zu behebende Schäden verursacht würden, kann die NHRC Sofortmaßnahmen ergreifen ([156]).

Die NHRC hat zwar keine Zwangsbefugnisse, doch ihre Beschlüsse (z. B. der Beschluss, die Untersuchung einer Beschwerde nicht fortzusetzen) ([157]) und ihre Empfehlungen können nach dem Gesetz über die Verwaltungsgerichtsbarkeit vor den koreanischen Gerichten angefochten werden (siehe Abschnitt 2.4.3) ([158]). Wenn die NHRC feststellt, dass eine Behörde auf unrechtmäßige Weise personenbezogene Daten erhoben hat, kann die betroffene Person außerdem vor den koreanischen Gerichten weitere Rechtsbehelfe gegen diese Behörde einlegen; Beispiele sind die Anfechtung der Erhebung nach dem Gesetz über die Verwaltungsgerichtsbarkeit, eine Verfassungsbeschwerde nach dem Gesetz über das Verfassungsgericht oder ein Antrag auf Schadenersatz nach dem Gesetz über staatlichen Schadenersatz (siehe Abschnitt 2.4.3).

2.4.3. *Gerichtliche Rechtsbehelfe*

Natürliche Personen können sich auf die in den vorherigen Abschnitten beschriebenen Einschränkungen und Garantien berufen und auf unterschiedlichen Wegen Rechtsbehelfe vor den koreanischen Gerichten einlegen.

Das CPA sieht vor, dass die betroffene Person und ihr Rechtsbeistand bei der Vollstreckung einer angeordneten Durchsuchung oder Beschlagnahme anwesend sein dürfen, sodass sie zum Zeitpunkt der Vollstreckung Widerspruch erheben können ([159]). Weiterhin sieht das CPA einen sogenannten Quasi-Beschwerdemechanismus vor, der es natürlichen Personen ermöglicht, beim zuständigen Gericht die Aufhebung oder Änderung einer eine Beschlagnahme betreffenden staatsanwaltlichen oder polizeilichen Verfügung zu beantragen ([160]). Auf diese Weise können die Maßnahmen angefochten werden, die zur Vollstreckung einer Beschlagnahmeverfügung getroffen wurden.

([150]) Obwohl in Artikel 4 des NHRC-Gesetzes auf Bürger und in der Republik Korea ansässige Ausländer Bezug genommen wird, ist der Begriff der Ansässigkeit eher in Zusammenhang mit der Zuständigkeit und nicht territorial zu verstehen. Wenn daher die Grundrechte eines Ausländers außerhalb Koreas von nationalen Einrichtungen in Korea verletzt werden, kann die betroffene Person eine Beschwerde bei der NHRC einreichen. Siehe beispielsweise die entsprechende Frage auf der Seite der NHRC zu häufig gestellten Fragen, abrufbar unter https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Dies wäre der Fall, wenn koreanische Behörden auf unrechtmäßige Weise auf nach Korea übermittelte personenbezogene Daten eines Ausländers zugreifen.

([151]) Jede Beschwerde ist grundsätzlich innerhalb eines Jahres nach der Menschenrechtsverletzung einzureichen; allerdings kann die NHRC beschließen, eine Beschwerde zu untersuchen, die nach Ablauf dieser Frist eingereicht wird, solange die straf- oder zivilrechtliche Verjährungsfrist noch nicht verstrichen ist (Artikel 32 Absatz 1 Nummer 4 des NHRC-Gesetzes).

([152]) Artikel 42 ff. des NHRC-Gesetzes.

([153]) Artikel 36 und 37 des NHRC-Gesetzes.

([154]) Artikel 44 des NHRC-Gesetzes.

([155]) Artikel 42 Absatz 4 des NHRC-Gesetzes.

([156]) Artikel 48 des NHRC-Gesetzes.

([157]) Wenn die NHRC ausnahmsweise nicht in der Lage ist, bestimmte Unterlagen einzusehen oder Einrichtungen zu inspizieren, weil diese in Zusammenhang mit Staatsgeheimnissen stehen, die erhebliche Auswirkungen auf die Staatssicherheit oder die diplomatischen Beziehungen haben könnten, oder wenn die Einsichtnahme oder Inspektion ein schwerwiegendes Hindernis für eine strafrechtliche Untersuchung oder ein anhängiges Gerichtsverfahren darstellen würde (siehe Fußnote 166), sodass die NHRC eine Untersuchung, die erforderlich ist, um die Begründetheit einer Petition zu beurteilen, nicht durchführen kann, muss sie der betroffenen Person gemäß Artikel 39 des NHRC-Gesetzes die Gründe für die Ablehnung der Beschwerde mitteilen. In diesem Fall kann die betroffene Person die Entscheidung der NHRC nach dem Gesetz über die Verwaltungsgerichtsbarkeit anfechten.

([158]) Siehe z. B. die Entscheidung des Seoul High Court vom 18. April 2008, 2007NU27259, bestätigt durch die Entscheidung des obersten Gerichtshofs vom 9. Oktober 2008, 2008Du7854, sowie die Entscheidung des Seoul High Court vom 2. Februar 2018, 2017NU69382.

([159]) Artikel 121 und 219 CPA.

([160]) Artikel 417 CPA in Verbindung mit Artikel 414 Absatz 2 CPA. Siehe auch die Entscheidung des obersten Gerichtshofs vom 29. September 1997, 97Mo66.

Darüber hinaus können natürliche Personen vor den koreanischen Gerichten auf Schadenersatz klagen. Auf der Grundlage des Gesetzes über staatlichen Schadenersatz (State Compensation Act) können sie Anspruch auf Schadenersatz für Schäden erheben, die ihnen öffentliche Bedienstete unter Verstoß gegen das Gesetz bei der Ausübung ihres Amtes zugefügt haben ([161]). Ein Anspruch nach dem Gesetz über staatlichen Schadenersatz kann bei einem speziellen „Schadenersatzrat" (Compensation Council) oder direkt vor den koreanischen Gerichten erhoben werden ([162]). Handelt es sich bei dem Opfer um einen Ausländer, findet das Gesetz über staatlichen Schadenersatz Anwendung, sofern das Herkunftsland koreanischen Staatsangehörigen ebenfalls staatlichen Schadenersatz gewährleistet ([163]). Gemäß der Rechtsprechung ist diese Bedingung erfüllt, wenn die Anforderungen an Schadenersatzansprüche in dem anderen Land „nicht so gestaltet sind, dass eine wesentliche Unausgewogenheit zwischen Korea und dem anderen Land besteht" und wenn sie „allgemein nicht strenger als die Anforderungen in Korea sind, zu denen sie keinen wesentlichen Unterschied aufweisen" ([164]). Die staatliche Schadenersatzhaftung ist im Zivilgesetz (Civil Act) geregelt und erstreckt sich somit auch auf immaterielle Schäden (z. B. seelisches Leid) ([165]).

Für Verstöße gegen die Datenschutzvorschriften sieht das PIPA einen zusätzlichen Rechtsbehelf vor. Nach Artikel 39 PIPA kann jede natürliche Person, die durch einen Verstoß gegen das PIPA oder durch Verlust, Diebstahl, Verbreitung, Fälschung, Veränderung oder Schädigung ihrer personenbezogenen Daten geschädigt wird, vor Gericht auf Schadenersatz klagen. Ein Gegenseitigkeitserfordernis wie nach dem Gesetz über staatlichen Schadenersatz besteht in diesem Fall nicht.

Neben dem Anspruch auf Schadenersatz kann gemäß dem Gesetz über die Verwaltungsgerichtsbarkeit verwaltungsrechtlich gegen Maßnahmen oder Unterlassungen von Verwaltungsbehörden vorgegangen werden. Jede natürliche Person hat die Möglichkeit, eine Verfügung (die Ausübung oder Verweigerung der Ausübung öffentlicher Gewalt in einem bestimmten Fall) oder eine Unterlassung (das längere Versäumnis einer Verwaltungsbehörde, eine bestimmte Verfügung zu erlassen, das einer entsprechenden rechtlichen Pflicht zuwiderläuft) anzufechten, was den Widerruf oder die Änderung einer rechtswidrigen Verfügung, die Feststellung der Nichtigkeit (die Feststellung, dass eine Verfügung keine Rechtswirkung hat oder in der Rechtsordnung nicht vorhanden ist) oder die Feststellung der Rechtswidrigkeit einer Unterlassung zur Folge haben kann ([166]). Damit eine verwaltungsrechtliche Verfügung angefochten werden kann, muss sie sich unmittelbar auf die bürgerlichen Rechte und Pflichten auswirken ([167]). Dies ist bei Maßnahmen zur Erhebung personenbezogener Daten der Fall, unabhängig davon, ob die Erhebung direkt erfolgt (z. B. durch die Überwachung von Kommunikationsvorgängen) oder über ein Offenlegungsersuchen (z. B. an einen Diensteanbieter).

Entsprechende Ansprüche können vor dem Verwaltungsbeschwerdeausschuss bestimmter Behörden (z. B. NIS, NHRC) erhoben werden, oder vor dem zentralen Verwaltungsbeschwerdeausschuss, der der Kommission für Korruptionsbekämpfung und bürgerliche Rechte (Anti-Corruption & Civil Rights Commission) unterstellt ist ([168]). Eine solche Verwaltungsbeschwerde ist ein alternativer, weniger formeller Weg der Anfechtung einer Verfügung oder Unterlassung einer Behörde. Allerdings kann nach dem Gesetz über die Verwaltungsgerichtsbarkeit auch direkt vor den koreanischen Gerichten geklagt werden.

Ein Antrag auf Widerruf oder Änderung einer Verfügung nach dem Gesetz über die Verwaltungsgerichtsbarkeit kann von jeder Person gestellt werden, die ein rechtliches Interesse daran hat, den Widerruf oder die Änderung zu verfolgen oder – falls die Verfügung nicht mehr wirksam ist – sich durch den Widerruf oder die Änderung wieder in ihre Rechte einsetzen zu lassen ([169]). Eine Nichtigkeitsfeststellungsklage kann ihrerseits von jeder Person erhoben werden, die ein rechtliches Interesse an dieser Feststellung hat, während eine Klage zur Feststellung der Rechtswidrigkeit einer Unterlassung von jeder Person eingereicht werden kann, die eine Verfügung beantragt und ein rechtliches Interesse daran hat, dass die Rechtswidrigkeit der Unterlassung festgestellt wird ([170]). Nach der Rechtsprechung des obersten Gerichtshofs wird ein „rechtliches Interesse" als „rechtlich geschütztes Interesse" ausgelegt, d. h. als ein unmittelbares und konkretes Interesse, das durch Gesetze und Vorschriften, auf denen verwaltungsrechtliche Verfügungen beruhen, geschützt ist (im Unterschied zu einem allgemeinen, mittelbaren und abstrakten öffentlichen Interesse) ([171]). Natürliche Personen haben also ein rechtliches Interesse, wenn Verstöße gegen die Einschränkungen und Garantien für die Erhebung ihrer personenbezogenen Daten zu Strafverfolgungszwecken (nach speziellen Gesetzen oder gemäß dem PIPA) begangen werden. Ein rechtskräftiges Urteil nach dem Gesetz über die Verwaltungsgerichtsbarkeit ist für die Parteien bindend ([172]).

Ein Antrag auf Widerruf oder Änderung einer Verfügung und ein Antrag auf Feststellung der Rechtswidrigkeit einer Unterlassung müssen innerhalb von 90 Tagen ab dem Tag eingereicht werden, an dem die Person von der Verfügung

([161]) Artikel 2 Absatz 1 des Gesetzes über staatlichen Schadenersatz.
([162]) Artikel 9 und 12 des Gesetzes über staatlichen Schadenersatz. Mit dem Gesetz wurden entsprechende Bezirksräte eingerichtet (unter dem Vorsitz des stellvertretenden Staatsanwalts der entsprechenden Staatsanwaltschaft) sowie ein Zentralrat (unter dem Vorsitz des stellvertretenden Justizministers) und ein Sonderrat (unter dem Vorsitz des stellvertretenden Verteidigungsministers), in dessen Zuständigkeit Schadenersatzansprüche für Schäden fallen, die durch militärisches Personal oder Zivilbeschäftigte des Militärs verursacht wurden. Grundsätzlich werden Schadenersatzansprüche von den Bezirksräten bearbeitet, die einen Fall unter bestimmten Umständen an den Zentral-/Sonderrat verweisen müssen, z. B. wenn der Schadenersatz einen bestimmten Betrag übersteigt oder wenn die betroffene Person eine erneute Beratung beantragt. Die Mitglieder aller Räte werden vom Justizminister ernannt (es handelt sich z. B. um öffentliche Bedienstete des Justizministeriums, Justizbeamten, Rechtsanwälte und Experten für staatlichen Schadenersatz) und sie unterliegen besonderen Vorschriften über Interessenkonflikte (siehe Artikel 7 des Durchführungserlassen zum Gesetz über staatlichen Schadenersatz).
([163]) Artikel 7 des Gesetzes über staatlichen Schadenersatz.
([164]) Entscheidung des obersten Gerichtshofs vom 11. Juni 2015, 2013Da208388.
([165]) Siehe Artikel 8 des Gesetzes über staatlichen Schadenersatz sowie Artikel 751 des Zivilgesetzes.
([166]) Artikel 2 und 4 des Gesetzes über die Verwaltungsgerichtsbarkeit.
([167]) Entscheidung des obersten Gerichtshofs vom 22. Oktober 1999, 98Du18435, Entscheidung des obersten Gerichtshofs vom 8. September 2000, 99Du1113, Entscheidung des obersten Gerichtshofs vom 27. September 2012, 2010Du3541.
([168]) Artikel 6 des Verwaltungsbeschwerdegesetzes (Administrative Appeals Act) und Artikel 18 Absatz 1 des Gesetzes über die Verwaltungsgerichtsbarkeit.
([169]) Artikel 12 des Gesetzes über die Verwaltungsgerichtsbarkeit.
([170]) Artikel 35 und 36 des Gesetzes über die Verwaltungsgerichtsbarkeit.
([171]) Entscheidung des obersten Gerichtshofs vom 26. März 2006, 2006Du330.
([172]) Artikel 30 Absatz 1 des Gesetzes über die Verwaltungsgerichtsbarkeit.

bzw. Unterlassung Kenntnis erlangt, und grundsätzlich nicht später als ein Jahr nach Erlass der Verfügung bzw. nach der Unterlassung, es sei denn, es liegen berechtigte Gründe vor ([173]). Nach der Rechtsprechung des obersten Gerichtshofs ist der Begriff „berechtigte Gründe" weit auszulegen und muss unter Berücksichtigung aller Umstände des Falles geprüft werden, ob die Zulassung einer verspäteten Klage gesellschaftlich akzeptabel ist ([174]). Berechtigte Gründe sind beispielsweise (aber nicht ausschließlich) Verzögerungsgründe, die die betroffene Partei nicht zu verantworten hat, (d. h. Situationen, die sich der Kontrolle des Klägers entziehen, z. B. wenn dieser nicht über die Erhebung seiner personenbezogenen Daten unterrichtet wurde) oder höhere Gewalt (z. B. Naturkatastrophen, Kriege).

Darüber hinaus besteht auch die Möglichkeit, eine Verfassungsbeschwerde beim Verfassungsgericht einreichen ([175]). Auf der Grundlage des Gesetzes über das Verfassungsgericht kann jede Person, deren durch die Verfassung garantierte Grundrechte durch die Ausübung oder Nichtausübung der Staatsgewalt (außer durch Gerichtsurteile) verletzt wurden, einen Antrag auf Entscheidung über eine Verfassungsbeschwerde stellen. Etwaige andere verfügbare Rechtsbehelfe müssen zuvor erschöpft worden sein. Ausländer können nach der Rechtsprechung des Verfassungsgerichts Verfassungsbeschwerde einlegen, soweit ihre Grundrechte in der koreanischen Verfassung anerkannt werden (siehe die Erläuterungen in Abschnitt 1.1) ([176]). Verfassungsbeschwerden müssen innerhalb von 90 Tagen, nachdem die Person Kenntnis von der Verletzung ihrer Rechte erlangt hat, und innerhalb eines Jahres nach der Verletzung selbst eingereicht werden. Da auf Rechtsstreitigkeiten nach dem Gesetz über das Verfassungsgericht das Verfahren des Gesetzes über die Verwaltungsgerichtsbarkeit angewandt wird ([177]), ist eine Klage andernfalls trotzdem zulässig, wenn „berechtigte Gründe" nach der Auslegung der Rechtsprechung des obersten Gerichtshofs vorliegen (siehe oben).

Wenn zunächst andere Rechtsbehelfe zu erschöpfen sind, muss die Verfassungsbeschwerde innerhalb von 30 Tagen nach der rechtskräftigen Entscheidung über einen solchen Rechtsbehelf eingelegt werden ([178]). Das Verfassungsgericht kann die Ausübung der Staatsgewalt, die zu der Verletzung geführt hat, für ungültig erklären oder feststellen, dass eine bestimmte Unterlassung verfassungswidrig ist ([179]). In diesem Fall ist die betreffende Behörde verpflichtet, Maßnahmen zu ergreifen, um der Entscheidung des Gerichts zu entsprechen.

3. STAATLICHER ZUGRIFF FÜR DIE ZWECKE DER NATIONALEN SICHERHEIT

3.1. Zuständige Behörden im Bereich der nationalen Sicherheit

Die Republik Korea verfügt über zwei spezielle Nachrichtendienste: den NIS und das Defense Security Support Command. Darüber hinaus können auch Polizei und Staatsanwaltschaft personenbezogene Daten für die Zwecke der nationalen Sicherheit erheben.

Der NIS wurde durch das NIS-Gesetz gegründet und untersteht unmittelbar der Verantwortung und Aufsicht des Präsidenten ([180]). Die Aufgaben des NIS sind die Beschaffung, Zusammenstellung und Weiterleitung von Informationen über das Ausland (und Nordkorea) ([181]), von Nachrichten in Zusammenhang mit der Abwehr von Spionage (einschließlich Militär- und Industriespionage), Terrorismus und den Tätigkeiten internationaler Verbrechersyndikate, von Nachrichten über bestimmte Arten von Straftaten gegen die öffentliche und nationale Sicherheit (z. B. Aufstände im Inland, Angriffe aus dem Ausland) und von Nachrichten in Zusammenhang mit der Gewährleistung der Cybersicherheit und der Prävention oder Abwehr von Cyberangriffen und -bedrohungen ([182]). Das NIS-Gesetz zur Gründung des NIS und zur Festlegung seiner Aufgaben enthält auch allgemeine Grundsätze, die den Rahmen alle Tätigkeiten des NIS bilden. Grundsätzlich muss der NIS politische Neutralität wahren und die Freiheit und die Rechte natürlicher Personen schützen ([183]). Der Präsident des NIS ist dafür verantwortlich, allgemeine Leitlinien aufzustellen, in denen die Grundsätze, der Umfang und die Verfahren zur Erfüllung der Aufgaben des NIS in Zusammenhang mit der Erhebung und Nutzung von Daten festgelegt sind, und der Nationalversammlung über diese Leitlinien Bericht zu erstatten ([184]). Die Nationalversammlung kann (über ihren Geheimdienstausschuss) veranlassen, dass die Leitlinien korrigiert oder ergänzt werden, wenn sie der Ansicht ist, dass sie rechtswidrig oder ungerecht sind. Allgemein dürfen der Direktor und die NIS-Mitarbeiter bei der Wahrnehmung ihrer Aufgaben Einrichtungen, Organisationen oder natürliche Personen nicht zu etwas zwingen, zu dem diese nicht verpflichtet sind, und niemanden durch Missbrauch ihrer öffentlichen Gewalt bei der Ausübung seiner Rechte behindern ([185]). Darüber hinaus müssen die Zensur der Post, die Überwachung der Telekommunikation, die Erhebung von Standortdaten oder Kommunikationsbestätigungsdaten oder die Aufzeichnung oder das Abhören privater Kommunikation durch den NIS mit dem CPPA, dem Gesetz über den Schutz, die Nutzung usw. von Standortdaten (Act on the Protection, Use, etc. of Location Information, im Folgenden „Standortdatengesetz") oder

([173]) Artikel 20 des Gesetzes über die Verwaltungsgerichtsbarkeit. Diese Frist gilt auch für einen Antrag auf Feststellung der Rechtswidrigkeit einer Unterlassung (siehe Artikel 38 Absatz 2 des Gesetzes über die Verwaltungsgerichtsbarkeit).
([174]) Entscheidung des obersten Gerichtshofs vom 28. Juni 1991, 90Nu6521
([175]) Artikel 68 Absatz 1 des Gesetzes über das Verfassungsgericht.
([176]) Entscheidung des Verfassungsgerichts vom 29. November 2001, 99HeonMa194.
([177]) Artikel 40 des Gesetzes über das Verfassungsgericht.
([178]) Artikel 69 des Gesetzes über das Verfassungsgericht.
([179]) Artikel 75 Absatz 3 des Gesetzes über das Verfassungsgericht.
([180]) Artikel 2 und Artikel 4 Absatz 2 des NIS-Gesetzes.
([181]) Keine Informationen über natürliche Personen, sondern allgemeine Informationen über das Ausland (Trends, Entwicklungen) und über die Tätigkeiten staatlicher Akteure aus anderen Ländern.
([182]) Artikel 3 Absatz 1 des NIS-Gesetzes.
([183]) Artikel 3 Absatz 1, Artikel 6 Absatz 2, Artikel 11 und Artikel 21 des NIS-Gesetzes. Siehe auch die Vorschriften über Interessenkonflikte, insbesondere die Artikel 10 und 12.
([184]) Artikel 4 Absatz 2 des NIS-Gesetzes.
([185]) Artikel 13 des NIS-Gesetzes.

dem CPA im Einklang stehen ([186]). Machtmissbrauch oder die Erhebung von Daten unter Verstoß gegen diese Gesetze ist strafbar ([187]).

Das Defense Security Support Command (Unterstützungskommando für Sicherheit im Verteidigungsbereich) ist ein dem Verteidigungsministerium unterstellter Nachrichtendienst. Es ist für Sicherheitsfragen beim Militär, für militärstrafrechtliche Untersuchungen (nach dem Militärgerichtsgesetz) und für militärische Nachrichten zuständig. Im Allgemeinen überwacht das Defense Security Support Command keine Zivilisten, es sei denn, dies ist für die Wahrnehmung seiner militärischen Aufgaben erforderlich. Untersuchungen können sich gegen militärisches Personal, Zivilbeschäftigte des Militärs, Personen in militärischer Ausbildung, Reservisten oder Rekrutierer sowie Kriegsgefangene richten ([188]). Bei der Erhebung von Kommunikationsdaten für die Zwecke der nationalen Sicherheit unterliegt das Defense Security Support Command den Einschränkungen und Garantien, die im CPPA und in dem entsprechenden Durchführungserlass festgelegt sind.

3.2. **Rechtsgrundlagen und Einschränkungen**

Das CPPA, das Gesetz über die Terrorismusbekämpfung zum Schutz der Bürger und der öffentlichen Sicherheit (Act on Anti-Terrorism for the Protection of Citizens and Public Security, im Folgenden „Antiterrorismusgesetz") und das TBA bilden die Rechtsgrundlagen für die Erhebung personenbezogener Daten für die Zwecke der nationalen Sicherheit und sehen Einschränkungen und Garantien vor ([189]). Durch diese Einschränkungen und Garantien, die in den nächsten Abschnitten beschrieben werden, ist sichergestellt, dass die Erhebung und Verarbeitung von Daten auf das Maß beschränkt wird, das unbedingt erforderlich ist, um ein legitimes Ziel zu erreichen. Eine massenhafte und wahllose Erhebung personenbezogener Daten für die Zwecke der nationalen Sicherheit ist dadurch ausgeschlossen.

3.2.1. *Erhebung von Kommunikationsdaten*

3.2.1.1. Erhebung von Kommunikationsdaten durch die Nachrichtendienste

3.2.1.1.1. Rechtsgrundlage

Das CPPA ermächtigt die Nachrichtendienste, Kommunikationsdaten zu erheben, und verpflichtet Kommunikationsanbieter zur Zusammenarbeit bei Anfragen der Nachrichtendienste ([190]). Wie in Abschnitt 2.2.2.1 beschrieben, wird im CPPA zwischen der Erhebung von Kommunikationsinhaltsdaten („kommunikationsbeschränkende Maßnahmen" wie das „Abhören" oder „Zensur" ([191])) und der Erhebung von „Kommunikationsbestätigungsdaten" unterschieden ([192]).

Die Schwelle für die Erhebung dieser beiden Arten von Daten ist unterschiedlich, die anzuwendenden Verfahren und Garantien sind jedoch weitgehend identisch ([193]). Kommunikationsbestätigungsdaten (oder Metadaten) dürfen für den Zweck der Abwendung von Gefahren für die nationale Sicherheit erhoben werden ([194]). Eine höhere Schwelle gilt für die Durchführung von kommunikationsbeschränkenden Maßnahmen (d. h. für die Erhebung von Kommunikationsinhaltsdaten), die nur dann zulässig ist, wenn von einer ernsthaften Gefahr für die nationale Sicherheit ausgegangen wird und die Beschaffung von Nachrichten erforderlich ist, um diese Gefahr zu abzuwenden ([195]). Darüber hinaus darf der Zugriff auf den Inhalt eines Kommunikationsvorgangs nur das letzte Mittel zur Gewährleistung der nationalen Sicherheit sein und es müssen Anstrengungen unternommen werden, um die Verletzung der Privatsphäre bei der Kommunikation so gering wie möglich zu halten ([196]). Selbst wenn die entsprechende Genehmigung eingeholt wurde, müssen diese Maßnahmen, sobald sie nicht mehr erforderlich sind, unverzüglich eingestellt werden, damit sichergestellt ist, dass jede Verletzung der Kommunikationsgeheimnisse natürlicher Personen auf ein Mindestmaß beschränkt wird ([197]).

3.2.1.1.2. Einschränkungen und Garantien für die Erhebung von Kommunikationsdaten, die mindestens einen koreanischen Staatsangehörigen betreffen

Kommunikationsdaten (Inhalts- und Metadaten), bei denen eine oder beide an der Kommunikation beteiligte Personen koreanische Staatsangehörige sind, dürfen nur mit der Genehmigung eines leitenden Richters des obersten Gerichtshofs

([186]) Artikel 14 des NIS-Gesetzes.
([187]) Artikel 22 und 23 des NIS-Gesetzes.
([188]) Artikel 1 des Militärgerichtsgesetzes.
([189]) Bei der Untersuchung von Straftaten in Zusammenhang mit der nationalen Sicherheit handeln die Polizei und der NIS auf der Grundlage des CPA, während das Defense Security Support Command dem Militärgerichtsgesetz unterliegt.
([190]) Artikel 15-2 CPPA.
([191]) Artikel 2 Absätze 6 und 7 CPPA.
([192]) Artikel 2 Absatz 11 CPPA.
([193]) Siehe auch Artikel 13-4 Absatz 2 CPPA und Artikel 37 Absatz 4 des CPPA-Durchführungserlasses, in denen festgelegt ist, dass die Verfahren für die Erhebung von Kommunikationsinhaltsdaten mutatis mutandis auch für die Erhebung von Kommunikationsbestätigungsdaten gelten.
([194]) Artikel 13-4 CPPA.
([195]) Artikel 7 Absatz 1 CPPA.
([196]) Artikel 3 Absatz 2 CPPA.
([197]) Artikel 2 des CPPA-Durchführungserlasses.

erhoben werden ([198]). Der entsprechende Antrag des Nachrichtendienstes ist schriftlich an einen Staatsanwalt oder an die Oberstaatsanwaltschaft zu richten ([199]). Der Antrag muss die Gründe für die Erhebung enthalten (d. h., dass von einer ernsthaften Gefahr für die nationale Sicherheit ausgegangen wird oder dass die Erhebung zur Abwendung von Gefahren für die nationale Sicherheit erforderlich ist) – Belege, die einen Prima-facie-Fall begründen, sind beizufügen –, sowie entsprechende Einzelheiten (d. h. Zwecke, Zielperson(en) Umfang, Erhebungszeitraum, Art und Ort der Erhebung) ([200]). Der Staatsanwalt bzw. die Oberstaatsanwaltschaft beantragt wiederum die Genehmigung eines leitenden Richters des High Court ([201]). Der leitende Richter darf seine schriftliche Genehmigung nur erteilen, wenn er den Antrag für gerechtfertigt erachtet; hält er ihn für unbegründet, lehnt er den Antrag ab ([202]). In der entsprechenden Anordnung werden Art, Zweck, Ziel, Umfang und Erhebungszeitraum festgelegt und es wird angegeben, wo und wie die Erhebung erfolgen darf ([203]).

Besondere Vorschriften gelten für den Fall, dass die Maßnahme auf Ermittlungen über eine die nationale Sicherheit gefährdende Verschwörung abzielt und Dringlichkeit besteht, sodass es unmöglich ist, die genannten Verfahren zu durchlaufen ([204]). Sind diese Voraussetzungen erfüllt, können die Nachrichtendienste Überwachungsmaßnahmen ohne vorherige gerichtliche Genehmigung durchführen ([205]). Die gerichtliche Genehmigung ist dann jedoch unmittelbar nach Durchführung der Eilmaßnahmen vom Nachrichtendienst einzuholen. Liegt sie nicht innerhalb von 36 Stunden ab dem Zeitpunkt der Ergreifung der Maßnahmen vor, so müssen diese unverzüglich eingestellt werden ([206]). Die Datenerhebung in dringenden Fällen hat stets gemäß einer „Erklärung über die Dringlichkeit von Zensur- oder Abhörmaßnahmen" zu erfolgen und der Nachrichtendienst, der die Erhebung durchführt, muss ein Eilmaßnahmenregister führen ([207]).

In Fällen, in denen die Überwachung innerhalb kurzer Zeit abgeschlossen wird, sodass das Einholen einer gerichtlichen Genehmigung ausgeschlossen ist, muss der Leiter der zuständigen Oberstaatsanwaltschaft den Vorsitzenden des zuständigen Gerichts, der das Eilmaßnahmenregister führt, in einer entsprechenden Mitteilung über die Eilmaßnahme unterrichten ([208]). Dies ermöglicht dem Gericht, die Rechtmäßigkeit der Erhebung zu prüfen.

3.2.1.1.3. Einschränkungen und Garantien für die Erhebung von Kommunikationsdaten, die ausschließlich nichtkoreanische Staatsangehörige betreffen

Um Daten über Kommunikationsvorgänge zwischen ausschließlich nichtkoreanischen Staatsangehörigen zu erheben, müssen die Nachrichtendienste die vorherige schriftliche Genehmigung des Präsidenten einholen ([209]). Solche Daten werden nur dann für die Zwecke der nationalen Sicherheit erhoben, wenn die Kommunikation in eine der aufgeführten Kategorien fällt: Kommunikation zwischen Staatsbediensteten oder anderen natürlichen Personen aus Ländern, die der Republik Korea feindlich gesinnt sind, Kommunikation zwischen ausländischen Behörden, Organisationen oder Staatsangehörigen, die antikoreanischer Aktivitäten ([210]) verdächtigt werden, oder Kommunikation zwischen Mitgliedern von Organisationen auf der koreanischen Halbinsel, die faktisch nicht unter die Staatshoheit der Republik Korea fallen, und der im Ausland sitzender Dachorganisation ([211]). Ist hingegen ein Kommunikationspartner ein koreanischer Staatsangehöriger und der andere ein nichtkoreanischer Staatsangehöriger, so ist eine gerichtliche Genehmigung nach dem in Abschnitt 3.2.1.1.2 beschriebenen Verfahren erforderlich.

Der Leiter des Nachrichtendienstes muss dem Direktor des NIS eine Planung über die beabsichtigten Maßnahmen vorlegen ([212]). Der Direktor des NIS prüft, ob die Planung angemessen ist, und legt sie, falls dies der Fall ist, dem Präsidenten zur Genehmigung vor ([213]). Die Informationen, die die Planung enthalten muss, entsprechen den Pflichtangaben eines Antrags auf gerichtliche Genehmigung der Erhebung von Daten koreanischer Staatsangehöriger (siehe oben) ([214]). Insbesondere muss die Planung die Gründe für die Erhebung enthalten (d. h., dass von einer ernsthaften Gefahr für die nationale Sicherheit ausgegangen wird oder dass die Erhebung zur Abwendung von Gefahren für die nationale Sicherheit erforderlich ist), die Hauptgründe für den Verdacht – Belege, die einen Prima-facie-Fall begründen, sind beizufügen –, sowie entsprechende Einzelheiten (d. h. Zwecke, Zielpersonen(en) Umfang, Erhebungszeitraum, Art

([198]) Artikel 7 Absatz 1 Nummer 1 CPPA. Das zuständige Gericht ist der High Court, in dessen Zuständigkeit der Wohnsitz oder Sitz einer oder beider überwachter Personen fällt.
([199]) Artikel 7 Absatz 3 des CPPA-Durchführungserlasses.
([200]) Artikel 7 Absatz 3 und Artikel 6 Absatz 4 CPPA.
([201]) Artikel 7 Absatz 4 des CPPA-Durchführungserlasses. Der Antrag des Staatsanwalts an das Gericht muss die Hauptgründe für den Verdacht und, wenn gleichzeitig mehrere Genehmigungen beantragt werden, die Begründung dafür enthalten (siehe Artikel 4 des CPPA-Durchführungserlasses).
([202]) Artikel 7 Absatz 3 und Artikel 6 Absätze 5 und 9 CPPA.
([203]) Artikel 7 Absatz 3 und Artikel 6 Absatz 6 CPPA.
([204]) Artikel 8 CPPA.
([205]) Artikel 8 Absatz 1 CPPA.
([206]) Artikel 8 Absatz 2 CPPA.
([207]) Artikel 8 Absatz 4 CPPA. Zu Eilmaßnahmen im Rahmen der Strafverfolgung siehe Abschnitt 2.2.2.2.
([208]) Artikel 8 Absätze 5 und 7 CPPA. In der Mitteilung sind Zweck, Ziel, Umfang, Zeitraum, Ort und Art der Erhebung anzugeben sowie die Gründe zu nennen, warum vor der Durchführung der Maßnahme kein entsprechender Antrag gestellt wurde (Artikel 8 Absatz 6 CPPA).
([209]) Artikel 7 Absatz 1 Nummer 2 CPPA.
([210]) Dies bezieht sich auf Aktivitäten, die eine Gefahr für den Fortbestand und die Sicherheit der Nation, die demokratische Ordnung oder das Überleben und die Freiheit der Bevölkerung darstellen.
([211]) Wenn ein Kommunikationspartner eine Person im Sinne des Artikels 7 Absatz 1 Nummer 2 CPPA ist und der andere nicht bekannt ist oder nicht genauer bestimmt werden kann, findet das Verfahren des Artikels 7 Absatz 1 Nummer 2 Anwendung.
([212]) Artikel 8 Absatz 1 des CPPA-Durchführungserlasses. Der Direktor des NIS wird nach Bestätigung durch das Parlament vom Präsidenten ernannt (Artikel 7 des NIS-Gesetzes).
([213]) Artikel 8 Absatz 2 des CPPA-Durchführungserlasses.
([214]) Artikel 8 Absatz 3 des CPPA-Durchführungserlasses in Verbindung mit Artikel 6 Absatz 4 CPPA.

und Ort der Erhebung). Werden mehrere Genehmigungen gleichzeitig beantragt, sind außerdem der damit beabsichtigte Zweck und die Gründe dafür zu nennen ([215]).

In dringenden Fällen ([216]) ist vorab die Genehmigung des Ministers einzuholen, dem der jeweilige Nachrichtendienst untersteht. In solchen Fällen muss der Nachrichtendienst jedoch unmittelbar nach Ergreifen der Eilmaßnahmen die Genehmigung des Präsidenten beantragen. Liegt die Genehmigung dem Nachrichtendienst nicht innerhalb von 36 Stunden nach der Antragstellung vor, so muss die Erhebung unverzüglich eingestellt werden ([217]). Die erhobenen Daten sind in solchen Fällen stets zu vernichten.

3.2.1.1.4. Einschränkungen und Garantien

Wenn die Nachrichtendienste private Unternehmen um ihre Zusammenarbeit ersuchen, müssen sie ihnen die gerichtliche Anordnung oder die Genehmigung des Präsidenten oder eine Kopie des Deckblatts einer Erklärung über die Dringlichkeit von Zensurmaßnahmen vorlegen, die das betreffende Unternehmen in seinen Akten aufbewahren muss ([218]). Unternehmen, die auf der Grundlage des CPPA Daten an einen Nachrichtendienst übermitteln sollen, dürfen dies verweigern, wenn in der Genehmigung oder Erklärung über die Dringlichkeit von Zensurmaßnahmen eine falsche Kennung genannt wird (z. B. eine Telefonnummer, die einer anderen als der angegebenen natürlichen Person zugeordnet ist). Außerdem dürfen in keinem Fall Passwörter offengelegt werden, die für den Zweck der Kommunikation verwendet werden ([219]).

Die Nachrichtendienste können eine Poststelle oder einen Telekommunikationsdiensteanbieter (im Sinne des TBA) mit der Durchführung von kommunikationsbeschränkenden Maßnahmen oder der Erhebung von Kommunikationsbestätigungsdaten beauftragen ([220]). Sowohl der betreffende Nachrichtendienst als auch der Telekommunikationsdiensteanbieter, der ein Ersuchen um Zusammenarbeit erhält, müssen ein Register mit Aufzeichnungen über den Zweck der Aufforderung zur Durchführung der Maßnahmen, das Datum der Durchführung oder der Zusammenarbeit und den Gegenstand der Maßnahmen (z. B. Post, Telefon, E-Mail) führen, die drei Jahre lang aufzubewahren sind ([221]). Telekommunikationsdiensteanbieter, die Kommunikationsbestätigungsdaten übermitteln, müssen in ihren Akten Aufzeichnungen über die Häufigkeit der Datenerhebung führen und sieben Jahre lang aufbewahren sowie zweimal jährlich dem Minister für Wissenschaft und IKT Bericht erstatten ([222]).

Die Nachrichtendienste haben dem Direktor des NIS über die von ihnen gesammelten Informationen und die Ergebnisse der Überwachungstätigkeit Bericht zu erstatten ([223]). In Bezug auf die Erhebung von Kommunikationsbestätigungsdaten ist ein Ersuchen um Übermittlung solcher Daten zu dokumentieren, die entsprechenden Aufzeichnungen und das schriftliche Ersuchen selbst sind aufzubewahren und es ist auch die Einrichtung zu dokumentieren, die sich darauf gestützt hat ([224]).

Sowohl Kommunikationsinhaltsdaten als auch Kommunikationsbestätigungsdaten dürfen nur über einen Zeitraum von höchstens vier Monate erhoben werden und die Erhebung muss unverzüglich eingestellt werden, wenn das verfolgte Ziel früher erreicht wird ([225]). Bestehen die Voraussetzungen für die Genehmigung fort, kann die Frist mit Erlaubnis des Gerichts oder Genehmigung des Präsidenten verlängert werden. In dem schriftlich zu stellenden Antrag auf Genehmigung der Verlängerung der Überwachungsmaßnahmen sind die Gründe für die Verlängerung zu nennen und es sind Belege beizufügen ([226]).

Je nach Rechtsgrundlage der Erhebung werden natürliche Personen in der Regel benachrichtigt, wenn ihre Kommunikationsdaten erhoben werden. Unabhängig davon, ob die erhobenen Daten den Inhalt eines Kommunikationsvorgangs betreffen oder ob es sich um Kommunikationsbestätigungsdaten handelt und unabhängig davon, ob die Daten im ordentlichen Verfahren oder in einem dringenden Fall erhobenen wurden, muss der Leiter des Nachrichtendienstes die betroffene Person innerhalb von 30 Tagen nach Beendigung der Überwachungsmaßnahme schriftlich über die Überwachungsmaßnahme unterrichten ([227]). Der Benachrichtigung muss zu entnehmen sein: 1) die Tatsache, dass Daten erhoben wurden, 2) die ausführende Behörde und 3) der Durchführungszeitraum. Ist es jedoch wahrscheinlich, dass

([215]) Artikel 8 Absatz 3 und Artikel 4 des CPPA-Durchführungserlasses.
([216]) Das heißt in Fällen, in denen die Maßnahme wegen einer die nationale Sicherheit gefährdenden Verschwörung getroffen wird, nicht genügend Zeit bleibt, um die Genehmigung des Präsidenten einzuholen und die Unterlassung von Eilmaßnahmen zu einer Beeinträchtigung der nationalen Sicherheit führen könnte (Artikel 8 Absatz 8 CPPA).
([217]) Artikel 8 Absatz 9 CPPA.
([218]) Artikel 9 Absatz 2 CPPA und Artikel 12 des CPPA-Durchführungserlasses.
([219]) Artikel 9 Absatz 4 CPPA.
([220]) Artikel 13 des CPPA-Durchführungserlasses.
([221]) Artikel 9 Absatz 3 CPPA und Artikel 17 Absatz 2 des CPPA-Durchführungserlasses. Dieser Zeitraum gilt nicht für Kommunikationsbestätigungsdaten (siehe Artikel 39 des CPPA-Durchführungserlasses).
([222]) Artikel 13 Absatz 7 CPPA und Artikel 39 des CPPA-Durchführungserlasses.
([223]) Artikel 18 Absatz 3 des CPPA-Durchführungserlasses.
([224]) Artikel 13 Absatz 5 und Artikel 13-4 Absatz 3 CPPA.
([225]) Artikel 7 Absatz 2 CPPA.
([226]) Artikel 7 Absatz 2 CPPA und Artikel 5 des CPPA-Durchführungserlasses.
([227]) Artikel 9-2 Absatz 3 CPPA. Gemäß Artikel 13-4 CPPA gilt dies sowohl für die Erhebung von Kommunikationsinhaltsdaten als auch für die Erhebung von Kommunikationsbestätigungsdaten.

die Benachrichtigung zu einer Gefährdung der nationalen Sicherheit oder zu Schäden an Leib und Leben führen würde, darf sie aufgeschoben werden ([228]). Sobald die Gründe für den Aufschub nicht mehr bestehen, muss die Benachrichtigung innerhalb von 30 Tagen erfolgen ([229]).

Diese Informationspflicht gilt jedoch nur für Datenerhebungen, bei denen mindestens ein Kommunikationspartner ein koreanischer Staatsangehöriger ist. Folglich werden nichtkoreanische Staatsangehörige nur dann benachrichtigt, wenn Daten über ihre Kommunikation mit koreanischen Staatsangehörigen erhoben wurden. Es besteht keine Informationspflicht, wenn Daten über Kommunikation zwischen ausschließlich nichtkoreanischen Staatsangehörigen erhoben werden.

Kommunikationsinhaltsdaten sowie Kommunikationsbestätigungsdaten, die durch Überwachung auf der Grundlage des CPPA erhoben wurden, dürfen nur 1) für die Untersuchung, Verfolgung oder Verhütung bestimmter Straftaten, 2) für Disziplinarverfahren, 3) für Gerichtsverfahren, bei denen sich eine Person für einen Schadenersatzanspruch auf sie beruft, oder 4) auf der Grundlage anderer Gesetze genutzt werden ([230]).

3.2.1.2. Erhebung von Kommunikationsdaten durch die Polizei oder Staatsanwälte für die Zwecke der nationalen Sicherheit

Die Polizei bzw. der Staatsanwalt darf unter den in Abschnitt 3.2.1.1 beschriebenen Bedingungen Kommunikationsdaten (sowohl Kommunikationsinhaltsdaten als auch Kommunikationsbestätigungsdaten) für die Zwecke der nationalen Sicherheit erheben. In dringenden Fällen ([231]) gilt das zuvor beschriebene Verfahren für dringende Fälle, in denen Kommunikationsinhaltsdaten für Strafverfolgungszwecke erhoben werden müssen (Artikel 8 CPPA).

3.2.2. *Erhebung von Daten über Terrorverdächtige*

3.2.2.1. Rechtsgrundlage

Das Antiterrorismusgesetz ermächtigt den Direktor des NIS zur Erhebung von Daten über Terrorverdächtige ([232]). Ein „Terrorverdächtiger" ist definiert als ein Mitglied einer terroristischen Vereinigung ([233]), eine Person, die (durch die Bekanntmachung und Verbreitung von Ideen oder Taktiken einer terroristischen Vereinigung) zum Wachstum einer terroristischen Vereinigung beigetragen hat, Gelder für Terrorismus ([234]) gesammelt oder beigesteuert hat oder im Terrorismuskontext an anderen Tätigkeiten der Vorbereitung, Verschwörung, Propaganda oder Anstiftung beteiligt gewesen ist, oder eine Person, gegen die im Hinblick auf solche Tätigkeiten ein begründeter Verdacht besteht ([235]). Allgemein muss jeder öffentliche Bedienstete bei der Durchführung des Antiterrorismusgesetzes die in der koreanischen Verfassung verankerten Grundrechte achten ([236]).

Im Antiterrorismusgesetz selbst sind keine spezifischen Befugnisse, Einschränkungen und Garantien für die Erhebung von Daten über Terrorverdächtige festgelegt; stattdessen wird auf die Verfahren in anderen Gesetzen verwiesen. Der Direktor des NIS kann auf der Grundlage des Antiterrorismusgesetzes 1) Daten über die Einreise und Ausreise in die bzw. aus der Republik Korea, 2) Finanztransaktionsdaten und 3) Kommunikationsdaten erheben. Je nach Art der zu erhebenden Daten gelten die Verfahrensvorschriften des Einwanderungsgesetzes (Immigration Act) und des Zollgesetzes (Customs Act), des ARUSFTI bzw. des CPPA ([237]). Hinsichtlich der Erhebung von Daten über die Einreise nach Korea und die Ausreise aus Korea wird im Antiterrorismusgesetz auf die im Einwanderungsgesetz und im Zollgesetz festgelegten Verfahren hingewiesen. Diese Gesetze sehen jedoch derzeit keine entsprechenden Befugnisse vor. Bezüglich der Erhebung von Kommunikationsdaten wird im Antiterrorismusgesetz auf die Einschränkungen und Garantien im CPPA hingewiesen (die im Folgenden näher ausgeführt werden), bezüglich der Erhebung von Finanztransaktionsdaten auf

([228]) Artikel 9-2 Absatz 4 CPPA.
([229]) Artikel 13-4 Absatz 2 und Artikel 9-2 Absatz 6 CPPA.
([230]) Artikel 5 Absätze 1 und 2, Artikel 12 und Artikel 13-5 CPPA.
([231]) Das heißt in Fällen, in denen die Maßnahme wegen einer die nationale Sicherheit gefährdenden Verschwörung getroffen wird und Dringlichkeit besteht, sodass es unmöglich ist, das ordentliche Genehmigungsverfahren zu durchlaufen (Artikel 8 Absatz 1 CPPA).
([232]) Artikel 9 Antiterrorismusgesetz.
([233]) Eine „terroristische Vereinigung" ist definiert als eine Vereinigung von Terroristen, die von den Vereinten Nationen als solche benannt wurde (Artikel 2 Absatz 2 des Antiterrorismusgesetzes).
([234]) „Terrorismus" ist in Artikel 2 Absatz 1 des Antiterrorismusgesetzes definiert als eine Handlung, die zu dem Zweck erfolgt, die Ausübung der Autorität des Staates, einer lokalen Verwaltung oder einer ausländischen Regierung (einschließlich lokaler Verwaltungen und internationaler Organisationen) zu untergraben, in einer bestimmten Angelegenheit ihr Tätigwerden zu erwirken, zu dem sie nicht verpflichtet sind, oder die Öffentlichkeit zu bedrohen. Dazu gehören a) die Tötung einer Person oder die Gefährdung des Lebens einer Person durch Körperverletzung oder die Gefangennahme, das Gefangenhalten, die Entführung oder Geiselnahme einer Person, b) bestimmte Handlungen, die auf ein Luftfahrzeug abzielen (z. B. Verursachung des Absturzes, Entführung oder Beschädigung eines im Flug befindlichen Luftfahrzeugs), c) bestimmte Handlungen in Zusammenhang mit einem Schiff (z. B. Kaperung eines in Betrieb befindlichen Schiffes oder Meeresbauwerks, Zerstörung eines in Betrieb befindlichen Schiffes oder Meeresbauwerks oder dessen Beschädigung in einem Ausmaß, das dessen Sicherheit gefährdet, einschließlich der Beschädigung der Ladung eines in Betrieb befindlichen Schiffs oder Meeresbauwerks), d) das Platzieren, Zünden oder anderweitige Verwenden einer biochemischen Waffe, eines Spreng- oder Brandsatzes mit der Absicht, zu töten oder schwere Verletzungen, erhebliche Sachschäden oder entsprechende Schäden an bestimmten Arten von Fahrzeugen oder Einrichtungen (z. B. Züge, Straßenbahnen, Kraftfahrzeuge, öffentliche Parks und Bahnhöfe, Strom-, Gas- und Telekommunikationsanlagen usw.) zu verursachen, e) bestimmte Handlungen in Zusammenhang mit Kernmaterial, radioaktivem Material oder kerntechnischen Anlagen (z. B. Schädigung an Leib und Leben oder von Eigentum oder sonstige Beeinträchtigung der öffentlichen Sicherheit durch die Zerstörung eines Kernreaktors oder die rechtswidrige Handhabung radioaktiver Stoffe usw.).
([235]) Artikel 2 Absatz 3 des Antiterrorismusgesetzes.
([236]) Artikel 3 Absatz 3 des Antiterrorismusgesetzes.
([237]) Artikel 9 Absatz 1 des Antiterrorismusgesetzes.

die Einschränkungen und Garantien im ARUSFTI (das, wie in Abschnitt 2.1 erläutert, für die Bewertung des Angemessenheitsbeschlusses nicht relevant ist).

Darüber hinaus sieht Artikel 9 Absatz 3 des Antiterrorismusgesetzes vor, dass der Direktor des NIS personenbezogene Daten oder Standortdaten eines Terrorverdächtigen von einem Datenverantwortlichen ([238]) oder Standortdatenanbieter ([239]) anfordern kann. Diese Möglichkeit beschränkt sich auf das Ersuchen um freiwillige Zusammenarbeit, dem die Datenverantwortlichen und Standortdatenanbieter nicht nachkommen müssen, und in jedem Fall nur im Einklang mit dem PIPA und dem Standortdatengesetz (siehe Abschnitt 3.2.2.2) nachkommen dürfen.

3.2.2.2. Einschränkungen und Garantien für die freiwillige Offenlegung nach dem PIPA und dem Standortdatengesetz

Das Ersuchen um freiwillige Zusammenarbeit nach dem Antiterrorismusgesetz muss sich auf Daten zu Terrorverdächtigen beschränken (siehe Abschnitt 3.2.2.1). Ein solches Ersuchen des NIS muss mit den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit der koreanischen Verfassung (Artikel 12 Absatz 1 und Artikel 37 Absatz 2) ([240]) sowie mit den Anforderungen des PIPA für die Erhebung personenbezogener Daten (Artikel 3 Absatz 1 PIPA, siehe Abschnitt 1.2 dieses Dokuments) im Einklang stehen. Das NIS-Gesetz sieht weiterhin vor, dass der NIS Einrichtungen, Organisationen oder natürliche Personen nicht zu etwas zwingen darf, zu dem sie nicht verpflichtet sind, und niemanden durch Missbrauch der öffentlichen Gewalt bei der Ausübung seiner Rechte behindern darf ([241]). Ein Verstoß gegen dieses Verbot kann mit strafrechtlichen Sanktionen geahndet werden ([242]).

Datenverantwortliche und Standortdatenanbieter, die ein Ersuchen des NIS auf der Grundlage des Antiterrorismusgesetzes erhalten, müssen diesem nicht nachkommen. Die Zusammenarbeit ist freiwillig, muss jedoch im Einklang mit dem PIPA und dem Standortdatengesetz stehen. Zur Einhaltung des PIPA muss der Datenverantwortliche insbesondere die Interessen der betroffenen Person berücksichtigen und darf die Daten nicht offenlegen, wenn es wahrscheinlich ist, dass dadurch die Interessen der betroffenen Person oder eines Dritten in unfairer Weise verletzt würden ([243]). Gemäß der Bekanntmachung Nr. 2021-1 über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten ist die betroffene Person zudem über die Offenlegung zu unterrichten. In Ausnahmesituationen kann diese Benachrichtigung aufgeschoben werden, insbesondere wenn und solange dadurch eine laufende strafrechtliche Untersuchung gefährdet würde oder die Schädigung eines Dritten an Leib und Leben wahrscheinlich ist, sofern diese Rechte oder Interessen eindeutig Vorrang vor den Rechten der betroffenen Person haben ([244]).

3.2.2.3. Einschränkungen und Garantien nach dem CPPA

Auf der Grundlage des Antiterrorismusgesetzes dürfen Nachrichtendienste nur dann Kommunikationsdaten (Kommunikationsinhaltsdaten wie auch Kommunikationsbestätigungsdaten) erheben, wenn dies für Maßnahmen zur Terrorismusbekämpfung, d. h. Maßnahmen in Zusammenhang mit der Prävention und Bekämpfung von Terrorismus, erforderlich ist. Für die Erhebung von Kommunikationsdaten zur Terrorismusbekämpfung gelten die in Abschnitt 3.2.1 beschriebenen Verfahren des CPPA.

3.2.3. *Freiwillige Offenlegung durch Telekommunikationsdiensteanbieter*

Auf der Grundlage des TBA können Telekommunikationsdiensteanbieter einem Ersuchen um Offenlegung von „Kommunikationsdaten“ nachkommen, den ein Nachrichtendienst an sie richtet, um durch die Erhebung dieser Daten eine Gefahr für die nationale Sicherheit abzuwenden ([245]). Ein solches Ersuchen muss mit den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit der koreanischen Verfassung (Artikel 12 Absatz 1 und Artikel 37 Absatz 2) ([246]) sowie mit den Anforderungen des PIPA für die Erhebung personenbezogener Daten (Artikel 3 Absatz 1 PIPA, siehe Abschnitt 1.2 dieses Dokuments) im Einklang stehen. Darüber hinaus gelten dieselben Einschränkungen und Garantien wie für die freiwillige Offenlegung zu Strafverfolgungszwecken (siehe Abschnitt 2.2.3) ([247]).

([238]) Laut der Definition in Artikel 2 PIPA handelt es sich hierbei um eine öffentliche Einrichtung, juristische Person, Organisation, natürliche Person usw., die personenbezogene Daten direkt oder indirekt verarbeitet, um die personenbezogenen Akten zu geschäftlichen Zwecken zu nutzen.

([239]) Laut der Definition in Artikel 5 des Standortdatengesetzes ist dies jede Person, die von der koreanischen Kommunikationskommission (Korea Communications Commission) die Erlaubnis erhalten hat, ein Geschäft mit Standortdaten zu betreiben.

([240]) Siehe auch Artikel 3 Absätze 2 und 3 des Antiterrorismusgesetzes.

([241]) Artikel 11 Absatz 1 des NIS-Gesetzes.

([242]) Artikel 19 des NIS-Gesetzes.

([243]) Artikel 18 Absatz 2 PIPA.

([244]) Abschnitt III Absatz 2 Ziffer iii der Bekanntmachung Nr. 2021-1 der PIPC über ergänzende Vorschriften für die Auslegung und Anwendung des Gesetzes über den Schutz personenbezogener Daten.

([245]) Artikel 83 Absatz 3 TBA.

([246]) Siehe auch Artikel 3 Absätze 2 und 3 des Antiterrorismusgesetzes.

([247]) Das Ersuchen muss schriftlich erfolgen und Ausführungen über die Gründe für das Ersuchen, die Verbindung zu dem betreffenden Nutzer und den Umfang der angeforderten Daten enthalten, und der Telekommunikationsdiensteanbieter muss entsprechende Aufzeichnungen führen und zweimal jährlich dem Minister für Wissenschaft und IKT Bericht erstatten.

Die Telekommunikationsdiensteanbieter sind nicht verpflichtet, dem Ersuchen nachzukommen; die Zusammenarbeit ist freiwillig und muss im Einklang mit dem PIPA stehen. In diesem Zusammenhang unterliegen Telekommunikationsdiensteanbieter denselben Pflichten, einschließlich in Bezug auf die Benachrichtigung der betroffenen Person, wie bei Ersuchen von Strafverfolgungsbehörden (näher erläutert in Abschnitt 2.2.3).

3.3. **Aufsicht**

Die Tätigkeiten der koreanischen Nachrichtendienste werden von verschiedenen Stellen überwacht. Die Aufsicht über das Defense Security Support Command erfolgt durch das Verteidigungsministerium gemäß dessen Richtlinie über die Umsetzung der internen Prüfung. Der NIS unterliegt der Aufsicht durch die Exekutive, die Nationalversammlung und andere unabhängige Stellen, wie nachstehend näher erläutert wird.

3.3.1. *Menschenrechtsbeauftragter*

Für die Erhebung von Daten über Terrorverdächtige durch die Nachrichtendienste sieht das Antiterrorismusgesetz die Aufsicht durch die Kommission für Terrorismusbekämpfung und den Menschenrechtsbeauftragten vor ([248]).

Die Aufgaben der Kommission für Terrorismusbekämpfung sind unter anderem die Entwicklung von Strategien zur Terrorismusbekämpfung und die Überwachung der Durchführung von Maßnahmen zur Terrorismusbekämpfung sowie der Tätigkeiten der verschiedenen zuständigen Behörden in diesem Bereich ([249]). Die Kommission wird vom Premierminister geleitet und setzt sich aus mehreren Ministern und Leitern von Regierungsstellen zusammen, darunter der Außenminister, der Justizminister, der Verteidigungsminister, der Minister für Inneres und Sicherheit, der Direktor des NIS, der Generalkommissar der nationalen Polizei und der Vorsitzende der Finanzdienstleistungskommission ([250]). Bei der Durchführung von Untersuchungen im Bereich der Terrorismusbekämpfung und der Überwachung von Terrorverdächtigen zur Sammlung von Informationen oder Unterlagen, die für entsprechende Gegenmaßnahmen erforderlich sind, muss der Direktor des NIS dem Vorsitzenden der Kommission für Terrorismusbekämpfung (d. h. dem Premierminister) Bericht erstatten ([251]).

Das Antiterrorismusgesetz bildet außerdem die Grundlage für die Ernennung eines Menschenrechtsbeauftragten zum Schutz vor Grundrechtsverletzungen im Zuge der Terrorismusbekämpfung ([252]). Der Menschenrechtsbeauftragte wird vom Vorsitzenden der Kommission für Terrorismusbekämpfung aus einem Kreis von Personen ernannt, die die im Durchführungserlass zum Antiterrorismusgesetz aufgeführten Voraussetzungen erfüllen (d. h. Rechtsanwälte mit mindestens zehn Jahren Berufserfahrung, Personen mit Fachwissen auf dem Gebiet der Menschenrechte, die mindestens zehn Jahre lang (mindestens) die Stelle eines außerordentlichen Professors innehatten, Personen, die als höhere öffentliche Bedienstete in staatlichen Stellen oder lokalen Verwaltungen tätig waren oder die über mindestens zehn Jahre Berufserfahrung im Bereich der Menschenrechte, z. B. in einer Menschenrechtsorganisation verfügen) ([253]). Der Menschenrechtsbeauftragte wird für eine (verlängerbare) Amtszeit von zwei Jahren ernannt und kann nur aus wenigen wichtigen Gründen seines Amtes enthoben werden, z. B. wenn er in einem Strafverfahren in Zusammenhang mit seinen Aufgaben angeklagt wird, wenn er vertrauliche Informationen weitergegeben hat oder wegen Unfähigkeit aufgrund einer langfristigen geistigen oder körperlichen Einschränkung ([254]).

Was die Befugnisse des Menschenrechtsbeauftragten anbelangt, so kann dieser Empfehlungen dazu abgeben, wie die im Bereich der Terrorismusbekämpfung tätigen Behörden den Schutz der Menschenrechte verbessern können. Außerdem bearbeitet der Menschenrechtsbeauftragte Petitionen der Zivilgesellschaft (siehe Abschnitt 3.4.3) ([255]). Wird nach vernünftigem Ermessen festgestellt, dass es bei der Ausübung amtlicher Aufgaben zu einer Menschenrechtsverletzung gekommen ist, so kann der Menschenrechtsbeauftragte dem Leiter der betreffenden Behörde empfehlen, Abhilfe zu schaffen ([256]). Die betreffende Behörde muss dem Menschenrechtsbeauftragten mitteilen, welche Maßnahmen zur Umsetzung dieser Empfehlung ergriffen wurden ([257]). Sollte die Behörde eine Empfehlung des Menschenrechtsbeauftragten nicht umsetzen, wird die Angelegenheit an die Kommission für Terrorismusbekämpfung und ihren Vorsitzenden, den Premierminister, verwiesen. Es ist bisher nicht vorgekommen, dass die Empfehlungen des Menschenrechtsbeauftragten nicht umgesetzt wurden.

3.3.2. *Nationalversammlung*

Wie in Abschnitt 2.3.2 beschrieben, kann die Nationalversammlung Untersuchungen und Kontrollen von Behörden durchführen und in diesem Zusammenhang die Offenlegung von Dokumenten verlangen und Zeugen vorladen. In Angelegenheiten, die in die Zuständigkeit des NIS fallen, obliegt diese parlamentarische Kontrolle dem Geheimdienstausschuss der Nationalversammlung ([258]). Der Direktor des NIS, der die Arbeit der Behörde überwacht, erstattet

([248]) Artikel 7 Antiterrorismusgesetz.
([249]) Artikel 5 Absatz 3 des Antiterrorismusgesetzes.
([250]) Artikel 3 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz.
([251]) Artikel 9 Absatz 4 des Antiterrorismusgesetzes.
([252]) Artikel 7 Antiterrorismusgesetz.
([253]) Artikel 7 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz.
([254]) Artikel 7 Absatz 3 des Durchführungserlasses zum Antiterrorismusgesetz.
([255]) Artikel 8 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz.
([256]) Artikel 9 Absatz 1 des Durchführungserlasses zum Antiterrorismusgesetz. Der Menschenrechtsbeauftragte entscheidet eigenständig über den Beschluss von Empfehlungen, ist jedoch verpflichtet, die Empfehlungen dem Vorsitzenden der Kommission für Terrorismusbekämpfung mitzuteilen.
([257]) Artikel 9 Absatz 2 des Durchführungserlasses zum Antiterrorismusgesetz.
([258]) Artikel 36 und Artikel 37 Absatz 1 Nummer 16 des Gesetzes über die Nationalversammlung.

dem Geheimdienstausschuss (sowie dem Präsidenten) darüber Bericht ([259]). Der Geheimdienstausschuss kann außerdem seinerseits einen Bericht über eine bestimmte Angelegenheit anfordern, worauf der Direktor des NIS unverzüglich reagieren muss ([260]). Der Direktor kann eine Antwort oder eine Aussage vor dem Geheimdienstausschuss nur in Zusammenhang mit Staatsgeheimnissen in militärischen, diplomatischen oder nordkoreanischen Angelegenheiten verweigern, wenn deren öffentliches Bekanntwerden schwerwiegende Auswirkungen auf das Schicksal der Nation haben könnte ([261]). In solchen Fällen kann der Geheimdienstausschuss den Premierminister um eine Erklärung bitten. Wird diese Erklärung nicht innerhalb von sieben Tagen vorgelegt, so kann die Antwort oder Aussage nicht mehr verweigert werden.

Stellt die Nationalversammlung unrechtmäßige oder missbräuchliche Tätigkeiten fest, so kann sie die betreffende Behörde auffordern, Abhilfemaßnahmen zu treffen; dazu zählen die Gewährung von Schadenersatz, Disziplinarmaßnahmen und die Verbesserung der internen Verfahren ([262]). Auf eine solche Aufforderung hin muss die Behörde unverzüglich tätig werden und der Nationalversammlung über das Ergebnis Bericht erstatten. Für die Anwendung von kommunikationsbeschränkenden Maßnahmen (d. h. die Erhebung von Kommunikationsinhaltsdaten) nach dem CCPA gelten besondere Vorschriften hinsichtlich der parlamentarischen Kontrolle ([263]). Die Nationalversammlung kann die Leiter der Nachrichtendienste um einen Bericht über jede kommunikationsbeschränkende Maßnahme bitten. Sie kann außerdem vor Ort Inspektionen von Abhörgeräten durchführen. Darüber hinaus müssen die Nachrichtendienste, wenn sie für die Zwecke der nationalen Sicherheit Inhaltsdaten erhoben haben, und Anbieter, die für diese Zwecke Inhaltsdaten offengelegt haben, auf Anfrage der Nationalversammlung über diese Offenlegung Bericht erstatten.

3.3.3. *Rechnungshof*

Der Rechnungshof übt in Bezug auf die Nachrichtendienste die gleichen Aufsichtsfunktionen aus wie im Bereich der Strafverfolgung (siehe Abschnitt 2.3.2) ([264]).

3.3.4. *Kommission für den Schutz personenbezogener Daten*

Die Verarbeitung, einschließlich der Erhebung, von Daten für die Zwecke der nationalen Sicherheit unterliegt zusätzlich der Aufsicht durch die PIPC. Wie in Abschnitt 1.2 näher erläutert, bezieht sich diese Aufsicht auf die in Artikel 3 und Artikel 58 Absatz 4 PIPA festgelegten allgemeinen Grundsätze und Pflichten sowie die Ausübung der durch Artikel 4 PIPA garantierten individuellen Rechte. Darüber hinaus erstreckt sich die Aufsicht der PIPC gemäß Artikel 7-8 Absätze 3 und 4 und Artikel 7-9 Absatz 5 PIPA auch auf mögliche Verstöße gegen die Einschränkungs- und Garantiebestimmungen für die Erhebung personenbezogener Daten, die in speziellen Gesetzen wie dem CPPA, dem Antiterrorismusgesetz und dem TBA enthalten sind. Angesichts der in Artikel 3 Absatz 1 PIPA festgelegten Anforderung einer rechtmäßigen und fairen Erhebung personenbezogener Daten stellt jeder Verstoß gegen diese Gesetze einen Verstoß gegen das PIPA dar. Die Befugnisse der PIPC umfassen somit die Untersuchung ([265]) von Verstößen gegen Gesetze, die den Datenzugriff für die Zwecke der nationalen Sicherheit regeln, sowie gegen die Verarbeitungsbestimmungen des PIPA, die Formulierung von Verbesserungsvorschlägen, das Verhängen von Abhilfemaßnahmen, die Empfehlung von Disziplinarmaßnahmen und die Weiterleitung von Fällen möglicher Straftaten an die zuständigen Untersuchungsbehörden ([266]).

3.3.5. *Nationale Menschenrechtskommission*

Die Nachrichtendienste stehen wie andere Regierungsstellen unter der Aufsicht der NHRC (siehe Abschnitt 2.3.2).

3.4. **Individuelle Rechtsbehelfe**

3.4.1. *Rechtsbehelf über den Menschenrechtsbeauftragten*

Eine spezielle Rechtsbehelfsmöglichkeit in Bezug auf die Erhebung personenbezogener Daten im Rahmen der Terrorismusbekämpfung bietet der der Kommission für Terrorismusbekämpfung unterstellte Menschenrechtsbeauftragte. Der Menschenrechtsbeauftragte bearbeitet Petitionen der Zivilgesellschaft, die Menschenrechtsverletzungen infolge von Maßnahmen der Terrorismusbekämpfung betreffen ([267]). Er kann entsprechende Abhilfemaßnahmen empfehlen, und die betreffende Behörde muss ihm über die zur Umsetzung dieser Empfehlung ergriffenen Maßnahmen Bericht erstatten. Die Einreichung einer Beschwerde beim Menschenrechtsbeauftragten ist nicht an Voraussetzungen gebunden. Folglich wird eine Beschwerde vom Menschenrechtsbeauftragten auch dann bearbeitet, wenn die betroffene Person bei der Zulässigkeitsprüfung keine tatsächliche Schädigung nachweisen kann.

([259]) Artikel 18 des NIS-Gesetzes.
([260]) Artikel 15 Absatz 2 des NIS-Gesetzes.
([261]) Artikel 17 Absatz 2 des NIS-Gesetzes. „Staatsgeheimnisse" sind definiert als „Tatsachen, Gegenstände oder Kenntnisse, die als Verschlusssachen eingestuft wurden, auf die nur ein begrenzter Personenkreis zugreifen darf und die zur Vermeidung einer schwerwiegenden Beeinträchtigung der nationalen Sicherheit keinem anderen Land und keiner anderen Organisation offengelegt werden dürfen", siehe Artikel 13 Absatz 4 des NIS-Gesetzes.
([262]) Artikel 16 Absatz 2 des Gesetzes über die Kontrolle und Untersuchung der staatlichen Verwaltung.
([263]) Artikel 15 CPPA.
([264]) Wie bei Anfragen des Nachrichtendienstausschusses der Nationalversammlung kann der Direktor des NIS eine Antwort an den Rechnungshof nur in Angelegenheiten verweigern, die Staatsgeheimnisse darstellen, und deren öffentliches Bekanntwerden schwerwiegende Auswirkungen auf die nationale Sicherheit hätte (Artikel 13 Absatz 1 des NIS-Gesetzes).
([265]) Artikel 63 PIPA.
([266]) Artikel 61 Absatz 2, Artikel 65 Absätze 1 und 2 und Artikel 64 Absatz 4 PIPA.
([267]) Artikel 8 Absatz 1 Nummer 2 des Durchführungserlasses zum Antiterrorismusgesetz.

3.4.2. *Rechtsbehelfsmechanismen nach dem PIPA*

Natürliche Personen können in Bezug auf personenbezogene Daten, die für die Zwecke der nationalen Sicherheit verarbeitet werden, ihre Rechte auf Auskunft, Berichtigung, Löschung und Aussetzung der Verarbeitung gemäß dem PIPA ausüben ([268]). Ein Antrag zur Ausübung dieser Rechte kann direkt bei dem betreffenden Nachrichtendienst oder indirekt über die PIPC gestellt werden. Der Nachrichtendienst kann die Ausübung der Rechte jedoch verzögern, einschränken oder ablehnen, soweit und solange dies zum Schutz eines wichtigen Ziels von öffentlichem Interesse erforderlich und verhältnismäßig ist (z. B. soweit und solange die Gewährung der Rechte eine laufende Untersuchung oder die nationale Sicherheit gefährden würde), oder wenn die Gewährung der Rechte zur Schädigung eines Dritten an Leib und Leben führen könnte. Wird der Antrag abgelehnt oder die Ausübung der Rechte eingeschränkt, so sind der betroffenen Person unverzüglich die Gründe dafür mitzuteilen.

Natürliche Personen haben außerdem das Recht auf Wiedergutmachung gemäß Artikel 58 Absatz 4 PIPA (Pflicht zur Gewährleistung einer angemessenen Bearbeitung der von natürlichen Personen eingereichten Beschwerden) und Artikel 4 Absatz 5 PIPA (Recht, für Schäden, die sich aus der Verarbeitung der personenbezogenen Daten ergeben, in einem zügigen und fairen Verfahren eine angemessene Wiedergutmachung zu erhalten). Dies schließt das Recht ein, mutmaßliche Verstöße bei dem von der koreanischen Internet- und Sicherheitsbehörde betriebenen Datenschutz-Callcenter zu melden und eine Beschwerde bei der PIPC einzureichen ([269]). Diese Rechtsbehelfsmöglichkeiten bestehen bei möglichen Verstößen gegen das PIPA und gegen die in speziellen Gesetzen enthaltenen Einschränkungs- und Garantiebestimmungen in Bezug auf die Erhebung personenbezogener Daten für die Zwecke der nationalen Sicherheit. Natürliche Personen aus der EU können über ihre nationale Datenschutzbehörde eine Beschwerde bei der PIPC einreichen, wie in der Bekanntmachung Nr. 2021-1 dargelegt wird. In solchen Fällen benachrichtigt die PIPC die betroffene Person über die nationale Datenschutzbehörde, sobald die Untersuchung abgeschlossen ist, und unterrichtet sie ggf. über die verhängten Abhilfemaßnahmen. Die Beschlüsse oder die Untätigkeit der PIPC können nach dem Gesetz über die Verwaltungsgerichtsbarkeit vor den koreanischen Gerichten angefochten werden.

3.4.3. *Rechtsbehelf über die nationale Menschenrechtskommission*

Die Möglichkeit, einen Rechtsbehelf bei der NHRC einzureichen, besteht in Bezug auf die Nachrichtendienste genauso wie gegenüber anderen Regierungsstellen (siehe Abschnitt 2.4.2).

3.4.4. *Gerichtliche Rechtsbehelfe*

Bei Verstößen gegen die oben genannten Einschränkungen und Garantien können natürliche Personen auf verschiedenen Wegen gerichtliche Rechtsbehelfe gegen die Nachrichtendienste einlegen, wie es auch in Bezug auf die Tätigkeiten der Strafverfolgungsbehörden der Fall ist.

Erstens können natürliche Personen auf Schadenersatz nach dem Gesetz über staatlichen Schadenersatz klagen. So wurde in einem Fall Schadenersatz für die unrechtmäßige Überwachung durch das Defense Support Command (den Vorgänger des Defense Security Support Command) gewährt ([270]).

Zweitens haben natürliche Personen nach dem Gesetz über die Verwaltungsgerichtsbarkeit die Möglichkeit, Verfügungen und Unterlassungen von Verwaltungsbehörden, einschließlich der Nachrichtendienste, anzufechten ([271]).

Drittens können natürliche Personen beim Verfassungsgericht eine Verfassungsbeschwerde gegen Geheimdienstmaßnahmen auf der Grundlage des Gesetzes über das Verfassungsgericht einlegen.

([268]) Artikel 3 Absatz 5 und Artikel 4 Absätze 1, 3 und 4 PIPA.
([269]) Artikel 62 und Artikel 63 Absatz 2 PIPA.
([270]) Entscheidung des obersten Gerichtshofs vom 24. Juli 1998, 96Da42789.
([271]) Artikel 3 und 4 des Gesetzes über die Verwaltungsgerichtsbarkeit.

ISSN 1977-0642 (elektronische Ausgabe)
ISSN 1725-2539 (Papierausgabe)

Amt für Veröffentlichungen der Europäischen Union
L-2985 Luxemburg
LUXEMBURG

DE