II

*(Rechtsakte ohne Gesetzescharakter)*

# BESCHLÜSSE

## DURCHFÜHRUNGSBESCHLUSS (EU) 2019/419 DER KOMMISSION

**vom 23. Januar 2019**

**nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen**

*(Bekanntgegeben unter Aktenzeichen K(2019) 304)*

**(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]) (im Folgenden „DSGVO"), insbesondere auf Artikel 45 Absatz 3,

nach Anhörung des Europäischen Datenschutzbeauftragten,

### 1. EINLEITUNG

(1) Die Verordnung (EU) 2016/679 enthält die Vorschriften für die Übermittlung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter in der Europäischen Union an Drittländer und internationale Organisationen, soweit die betreffenden Übermittlungen in ihren Anwendungsbereich fallen. Die Vorschriften für internationale Übermittlungen personenbezogener Daten sind in Kapitel V der genannten Verordnung, insbesondere in den Artikeln 44 bis 50, festgelegt. Der Fluss personenbezogener Daten in Drittländer und aus Drittländern ist für die Ausweitung der internationalen Zusammenarbeit und des internationalen Handels notwendig und gewährleistet gleichzeitig, dass das Schutzniveau für personenbezogene Daten in der Europäischen Union nicht beeinträchtigt wird.

(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 ohne weitere Genehmigung an dieses Drittland, dieses Gebiet, diesen Sektor oder diese internationale Organisation übermittelt werden.

(3) Wie in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 festgelegt, muss der Erlass 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 Beschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten. Im Rahmen der Prüfung ist festzustellen, 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). Der Gerichtshof der Europäischen Union hat klargestellt, dass es dazu keines identischen Schutzniveaus bedarf ([2]). Insbesondere können sich die Mittel, auf die das betreffende Drittland zurückgreift, von denen unterscheiden, die in der Europäischen Union herangezogen werden, sofern sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten ([3]). Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung

([1]) ABl. L 119 vom 4.5.2016, S. 1.
([2]) Maximilian Schrems/Data Protection Commissioner („Schrems"), C-362/14, ECLI:EU:C:2015:650, Rn. 73.
([3]) Schrems, Rn. 74.

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 ([4]).

(4) Die Kommission hat Recht und Praxis in Japan sorgfältig analysiert. Ausgehend von den Feststellungen in den Erwägungsgründen 6 bis 175 kommt die Kommission zu dem Schluss, dass Japan ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die an Organisationen übermittelt werden, die in den Anwendungsbereich des Gesetzes über den Schutz personenbezogener Informationen ([5]) fallen und den in diesem Beschluss genannten zusätzlichen Bedingungen unterliegen. Diese Bedingungen sind in den Ergänzenden Vorschriften (Anhang I) enthalten, die von der Kommission für den Schutz personenbezogener Informationen (*Personal Information Protection Commission* — PPC) ([6]) erlassen wurden, sowie in den offiziellen Erklärungen, Zusicherungen und Verpflichtungen der japanischen Regierung gegenüber der Europäischen Kommission (Anhang II).

(5) Dieser Beschluss hat zur Folge, dass Übermittlungen an solche Organisationen in Japan von einem Verantwortlichen oder Auftragsverarbeiter im Europäischen Wirtschaftsraum (EWR) ([7]) ohne weitere Genehmigung vorgenommen werden können. Dieser Beschluss hat keine Auswirkungen auf die unmittelbare Anwendung der Verordnung (EU) 2016/679 auf diese Organisationen, wenn die Voraussetzungen von deren Artikel 3 erfüllt sind.

## 2. DIE VORSCHRIFTEN FÜR DIE DATENVERARBEITUNG DURCH UNTERNEHMER

### 2.1. Der japanische Rechtsrahmen für den Datenschutz

(6) Das Rechtssystem für den Schutz der Privatsphäre und den Datenschutz in Japan wurzelt in der im Jahr 1946 verkündeten Verfassung.

(7) In Artikel 13 der Verfassung heißt es:

„Jeder Bürger wird als Einzelperson geachtet. Sein Recht auf Leben, Freiheit und das Streben nach Glück wird, soweit es das Gemeinwohl nicht beeinträchtigt, bei der Gesetzgebung und in allen übrigen Staatsangelegenheiten an oberster Stelle berücksichtigt."

(8) Auf der Grundlage dieses Artikels hat der Oberste Gerichtshof Japans die Rechte von Einzelpersonen in Bezug auf den Schutz personenbezogener Informationen präzisiert. In einer Entscheidung aus dem Jahr 1969 erkannte er das Recht auf Privatsphäre und Datenschutz als verfassungsmäßiges Recht an ([8]). Insbesondere hob der Gerichtshof hervor, dass „jeder Einzelne die Freiheit hat, seine personenbezogenen Informationen vor der Offenlegung gegenüber Dritten und der Veröffentlichung ohne triftigen Grund zu schützen". Zudem stellte der Oberste Gerichtshof in einer Entscheidung vom 6. März 2008 („Juki-Net") ([9]) fest, dass „die Freiheit der Bürger im Privatleben vor der Ausübung öffentlicher Gewalt geschützt ist und davon ausgegangen werden kann, dass eine der Freiheiten des Einzelnen im Privatleben darin besteht, seine personenbezogenen Informationen vor der Offenlegung gegenüber Dritten und der Veröffentlichung ohne triftigen Grund zu schützen" ([10]).

(9) Am 30. Mai 2003 erließ Japan eine Reihe von Gesetzen im Bereich des Datenschutzes:

— das Gesetz über den Schutz personenbezogener Informationen (*Act on the Protection of Personal Information* — APPI),

— das Gesetz über den Schutz personenbezogener Informationen bei Verwaltungsorganen (*Act on the Protection of Personal Information Held by Administrative Organs* — APPIHAO),

— das Gesetz über den Schutz personenbezogener Informationen bei Selbstverwaltungskörperschaften (*Act on the Protection of Personal Information Held by Incorporated Administrative Agencies* — APPI-IAA).

([4]) 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).
([5]) *Act on the Protection of Personal Information* (Gesetz Nr. 57, 2003).
([6]) Weitere Informationen zur PPC sind über den folgenden Link abrufbar: https://www.ppc.go.jp/en/ (einschließlich Kontaktdaten für Fragen und Beschwerden: https://www.ppc.go.jp/en/contactus/access/).
([7]) 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.
([8]) Oberster Gerichtshof, Urteil der Großen Kammer vom 24. Dezember 1969, Keishu Vol. 23, Nr. 12, S. 1625.
([9]) Oberster Gerichtshof, Urteil vom 6. März 2008, Minshu Vol. 62, Nr. 3, S. 665.
([10]) Oberster Gerichtshof, Urteil vom 6. März 2008, Minshu Vol. 62, Nr. 3, S. 665.

(10) Die beiden letztgenannten (2016 geänderten) Gesetze enthalten Bestimmungen für den Schutz personenbezogener Informationen durch öffentliche Stellen. Die Datenverarbeitung, die in den Anwendungsbereich dieser Gesetze fällt, ist nicht Gegenstand der Angemessenheitsfeststellung in diesem Beschluss, die sich auf den Schutz personenbezogener Informationen durch „personenbezogene Informationen handhabende Unternehmer" (*Personal Information Handling Business Operators* — PIHBO) im Sinne des APPI beschränkt.

(11) Das APPI ist in den letzten Jahren reformiert worden. Das geänderte APPI wurde am 9. September 2015 verkündet und ist am 30. Mai 2017 in Kraft getreten. Durch die Einführung neuer und die Verstärkung bestehender Garantien im Rahmen der Änderung näherte sich das japanische Datenschutzsystem dem europäischen an. So wurde eine Reihe durchsetzbarer Rechte des Einzelnen eingeführt und eine unabhängige Aufsichtsbehörde (die PPC) eingerichtet, die mit der Aufsicht und Durchsetzung des APPI betraut ist.

(12) Die Verarbeitung personenbezogener Informationen, die in den Anwendungsbereich dieses Beschlusses fallen, unterliegt nicht nur dem APPI, sondern auch den auf der Grundlage des APPI erlassenen Durchführungsvorschriften. Dazu gehören eine Änderung der Kabinettsverordnung zur Durchsetzung des Gesetzes über den Schutz personenbezogener Informationen vom 5. Oktober 2016 und von der PPC erlassene sogenannte Durchsetzungsvorschriften zum Gesetz über den Schutz personenbezogener Informationen ([11]). Die beiden rechtlich verbindlichen und durchsetzbaren Regelungen sind zeitgleich mit der Änderung des APPI in Kraft getreten.

(13) Darüber hinaus hat das japanische Kabinett (bestehend aus dem Premierminister und den Ministern, die seine Regierung bilden) am 28. Oktober 2016 eine „Grundlegende Richtlinie" verabschiedet, um „Maßnahmen zum Schutz personenbezogener Informationen umfassend und ganzheitlich zu fördern". Nach Artikel 7 APPI wird die „Grundlegende Richtlinie" in Form eines Kabinettsbeschlusses erlassen und enthält politische Leitvorstellungen für die Durchsetzung des APPI, die sowohl an die Zentralregierung als auch an die lokalen Regierungen gerichtet sind.

(14) Unlängst hat die japanische Regierung die „Grundlegende Richtlinie" durch Kabinettsbeschluss vom 12. Juni 2018 geändert. Zur Erleichterung internationaler Datenübermittlungen wird mit dem genannten Kabinettsbeschluss der PPC als der für die Verwaltung und Durchführung des APPI zuständigen Behörde die Befugnis übertragen, „auf der Grundlage des Artikels 6 des Gesetzes die notwendigen Maßnahmen zu treffen, um die Unterschiede zwischen den Systemen und Abläufen in Japan und in dem betreffenden anderen Land zu überbrücken, damit eine angemessene Handhabung der aus diesem Land erhaltenen personenbezogenen Informationen gewährleistet werden kann". Der Kabinettsbeschluss sieht vor, dass dies auch die Befugnis umfasst, den Schutz im Wege des Erlasses strengerer Vorschriften durch die PPC zu verbessern, die die Vorschriften des APPI und der Kabinettsverordnung ergänzen und darüber hinausgehen. Nach dem genannten Beschluss sind diese strengeren Vorschriften für japanische Unternehmer verbindlich und durchsetzbar.

(15) Auf der Grundlage des Artikels 6 APPI und des genannten Kabinettsbeschlusses hat die PPC am 15. Juni 2018 „Ergänzende Vorschriften nach dem Gesetz über den Schutz personenbezogener Informationen für die Handhabung von auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelten personenbezogenen Daten" (im Folgenden „Ergänzende Vorschriften") erlassen, um den Schutz personenbezogener Informationen, die auf der Grundlage des vorliegenden Angemessenheitsbeschlusses aus der Europäischen Union nach Japan übermittelt werden, zu verbessern. Die Ergänzenden Vorschriften sind für japanische Unternehmer rechtlich verbindlich und können von der PPC und den Gerichten in gleicher Weise wie die Bestimmungen des APPI durchgesetzt werden, die durch die strengeren und/oder ausführlicheren Bestimmungen der Vorschriften ergänzt werden ([12]). Da japanische Unternehmer, die personenbezogene Daten aus der Europäischen Union erhalten und/oder weiterverarbeiten, zur Einhaltung der Ergänzenden Vorschriften rechtlich verpflichtet sind, müssen sie — z. B. mit technischen (Markierung) oder organisatorischen Mitteln (Speicherung in einer eigenen Datenbank) — dafür sorgen, dass sie solche personenbezogenen Daten während deren gesamten „Lebenszyklus" erkennen können ([13]). In den folgenden Abschnitten wird der Inhalt jeder Ergänzenden Vorschrift im Rahmen der Prüfung des Artikels des APPI, der durch die betreffende Vorschrift ergänzt wird, analysiert.

(16) Anders als vor der Gesetzesänderung von 2015, als dies in bestimmten Sektoren in die Zuständigkeit verschiedener japanischer Ministerien fiel, ist nach dem APPI die PPC ermächtigt, „Leitlinien" zu verabschieden, um nach den Datenschutzvorschriften „die ordnungsgemäße und wirksame Umsetzung der von einem Unternehmer zu treffenden Maßnahmen sicherzustellen". Mit ihren Leitlinien stellt die PPC eine verbindliche Auslegung dieser Vorschriften

([11]) Abrufbar unter: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Siehe Ergänzende Vorschriften (einleitender Abschnitt).

([13]) Dies wird durch die allgemeine Pflicht, Aufzeichnungen (nur) während eines bestimmten Zeitraums aufzubewahren, nicht infrage gestellt. Auch wenn die Herkunft der Daten zu den Informationen gehört, die der erwerbende PIHBO nach Artikel 26 Absatz 1 APPI bestätigen muss, betrifft die Verpflichtung nach Artikel 26 Absatz 4 APPI in Verbindung mit Artikel 18 der PPC-Vorschriften nur eine bestimmte Form der Aufzeichnung (siehe Artikel 16 der PPC-Vorschriften) und hindert den PIHBO nicht daran, für eine längere Kennzeichnung der Daten zu sorgen. Dies wurde von der PPC bestätigt, die erklärt hat, dass die „Informationen über die Herkunft der EU-Daten von dem PIHBO so lange aufbewahrt werden müssen, wie dies für die Einhaltung der Ergänzenden Vorschriften erforderlich ist".

und insbesondere des APPI zur Verfügung. Nach Auskunft der PPC sind diese Leitlinien Bestandteil des Rechtsrahmens und in Verbindung mit dem Wortlaut des APPI, der Kabinettsverordnung, den PPC-Vorschriften und einem von der PPC erstellten Fragen-Antworten-Katalog ([14]) zu lesen. Sie sind daher „für Unternehmer verbindlich". Wenn die Leitlinien einem Unternehmer etwas vorschreiben oder verbieten, sieht die PPC die Nichteinhaltung der einschlägigen Bestimmungen als Gesetzesverstoß an ([15]).

### 2.2. **Sachlicher und persönlicher Anwendungsbereich**

(17) Der Anwendungsbereich des APPI wird durch die definierten Begriffe „personenbezogene Informationen", „personenbezogene Daten" und „personenbezogene Informationen handhabender Unternehmer" bestimmt. Gleichzeitig sieht das APPI einige wichtige Ausnahmen von seinem Anwendungsbereich vor, insbesondere für anonym verarbeitete personenbezogene Daten und für besondere Arten der Verarbeitung durch bestimmte Unternehmer. Das APPI verwendet jedoch nicht den Begriff „Verarbeitung", sondern den gleichwertigen Begriff „Handhabung", der nach Auskunft der PPC „jede an personenbezogenen Daten vorgenommene Handlung" umfasst, darunter Erwerb, Eingabe, Anhäufung, Organisation, Speicherung, Aufbereitung/Bearbeitung, Erneuerung, Löschung, Ausgabe, Verwendung und Bereitstellung personenbezogener Informationen.

#### 2.2.1. *Definition „personenbezogene Informationen"*

(18) Mit Blick auf seinen sachlichen Anwendungsbereich unterscheidet das APPI zwischen personenbezogenen Informationen und personenbezogenen Daten, wobei für die erste Kategorie nur einige der Bestimmungen des Gesetzes gelten. Nach Artikel 2 Absatz 1 APPI umfasst der Begriff „personenbezogene Informationen" alle Informationen über eine lebende Einzelperson, die die Identifizierung dieser Person ermöglichen. In der Definition werden zwei Kategorien personenbezogener Informationen unterschieden: i) Codes zur Personenidentifizierung und ii) sonstige personenbezogene Informationen, anhand deren eine bestimmte Einzelperson identifiziert werden kann. Zur zweiten Kategorie gehören auch Informationen, die zwar für sich allein keine Identifizierung ermöglichen, die aber mit anderen Informationen „leicht zu verknüpfen" sind und dann die Identifizierung einer bestimmten Einzelperson möglich machen. Ob Informationen als „leicht zu verknüpfen" angesehen werden können, ist nach den PPC-Leitlinien ([16]) im Einzelfall unter Berücksichtigung der tatsächlichen Umstände („Verhältnisse") des Unternehmers zu entscheiden. Dies wird vermutet, wenn eine solche Verknüpfung von einem durchschnittlichen („normalen") Unternehmer mit den ihm zur Verfügung stehenden Mitteln vorgenommen wird (oder vorgenommen werden kann). Beispielsweise sind Informationen nicht mit anderen Informationen „leicht zu verknüpfen", wenn ein Unternehmer außerordentliche Anstrengungen unternehmen oder gegen das Gesetz verstoßen muss, um sich die zu verknüpfenden Informationen bei einem oder mehreren anderen Unternehmern zu beschaffen.

#### 2.2.2. *Definition „personenbezogene Daten"*

(19) Nur bestimmte Formen personenbezogener Informationen fallen nach dem APPI unter den Begriff „personenbezogene Daten". Denn „personenbezogene Daten" sind definiert als „personenbezogene Informationen, die eine Datenbank mit personenbezogenen Informationen bilden", d. h. als „kollektiver Informationsbestand", der personenbezogene Informationen umfasst, die „systematisch so organisiert sind, dass mithilfe eines Computers nach bestimmten personenbezogenen Informationen gesucht werden kann" ([17]) oder die „aufgrund einer Kabinettsverordnung systematisch so organisiert sein müssen, dass leicht nach bestimmten personenbezogenen Informationen gesucht werden kann", jedoch „mit Ausnahme derjenigen, bei denen nach den Feststellungen in einer Kabinettsverordnung kaum die Möglichkeit besteht, dass unter Berücksichtigung der Verwendungsmethode Rechte und Interessen einer Einzelperson beeinträchtigt werden" ([18]).

(20) Diese Ausnahme wird in Artikel 3 Absatz 1 der Kabinettsverordnung näher konkretisiert, nach dem die drei folgenden Voraussetzungen kumulativ erfüllt sein müssen: i) der kollektive Informationsbestand muss „zu dem Zweck erstellt worden sein, an eine große Zahl nicht näher bestimmter Personen verkauft zu werden, und seine

([14]) PPC, Fragen und Antworten, 16. Februar 2017 (geändert am 30. Mai 2017), abrufbar über folgendem Link: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. In dem Fragen-Antworten-Katalog werden anhand von praktischen Beispielen Themen erörtert, die in den Leitlinien behandelt werden, z. B. der Begriff „sensible personenbezogene Daten", die Auslegung der Einwilligung im Einzelfall, Übermittlungen an Dritte im Rahmen von Cloud-Computing oder die Aufzeichnungspflicht bei grenzüberschreitenden Übermittlungen. Der Fragen-Antworten-Katalog liegt nur in japanischer Sprache vor.

([15]) Auf Anfrage hat die PPC dem Europäischen Datenschutzausschuss mitgeteilt, dass „die japanischen Gerichte ihre Auslegung bei der Anwendung des APPI und der PPC-Vorschriften in den von ihnen zu entscheidenden Rechtssachen auf die PPC-Leitlinien stützen und in ihren Urteilen unmittelbar auf deren Wortlaut Bezug nehmen. Daher sind die PPC-Leitlinien auch unter diesem Gesichtspunkt für Unternehmer verbindlich. Der PPC ist nicht bekannt, dass Gerichte schon einmal von den Leitlinien abgewichen wären." In diesem Zusammenhang hat die PPC die Kommission auf ein Urteil im Bereich des Datenschutzes hingewiesen, in dem sich das Gericht bei seinen Feststellungen ausdrücklich auf Leitlinien stützt (siehe Bezirksgericht Osaka, Urteil vom 19. Mai 2006, Hanrei Jiho, Vol. 1948, S. 122, in dem das Gericht entschied, dass der Unternehmer nach den Leitlinien verpflichtet war, eine Sicherheitskontrolle vorzunehmen).

([16]) PPC-Leitlinien (General Rule Edition), S. 6.

([17]) Damit sind auch elektronische Dateisysteme erfasst. Die PPC-Leitlinien (General Rule Edition, S. 17) enthalten konkrete Beispiele, etwa eine in der E-Mail-Client-Software gespeicherte E-Mail-Adressenliste.

([18]) Artikel 2 Absätze 4 und 6 APPI.

Erstellung darf nicht gegen die Bestimmungen eines Gesetzes oder einer darauf gestützten Verordnung verstoßen", ii) er muss „jederzeit von einer großen Zahl nicht näher bestimmter Personen erworben werden können", und iii) die darin enthaltenen personenbezogenen Daten müssen „für ihren ursprünglichen Zweck bereitgestellt werden, ohne andere Informationen über eine lebende Einzelperson hinzuzufügen". Wie die PPC erläutert hat, wurde diese enge Ausnahme eingeführt, um Telefonbücher und ähnliche Verzeichnisse auszuschließen.

(21) Die Unterscheidung zwischen „personenbezogenen Informationen" und „personenbezogenen Daten" ist für in Japan erhobene Daten von Bedeutung, da solche Informationen möglicherweise nicht immer Teil einer „Datenbank mit personenbezogenen Informationen" sind (z. B. ein einzelner manuell erhobener und verarbeiteter Datensatz), sodass die Bestimmungen des APPI, die sich nur auf personenbezogene Daten beziehen ([19]), keine Anwendung finden.

(22) Für personenbezogene Daten, die auf der Grundlage eines Angemessenheitsbeschlusses aus der Europäischen Union nach Japan importiert werden, ist diese Unterscheidung dagegen nicht von Belang. Da diese Daten typischerweise auf elektronischem Wege übermittelt werden (was im digitalen Zeitalter die übliche Form des Datenaustausches ist, insbesondere über eine so große Entfernung wie zwischen der EU und Japan) und dadurch Teil des elektronischen Dateisystems des Datenimporteurs werden, fallen diese EU-Daten nach dem APPI unter die Kategorie „personenbezogene Daten". Selbst wenn personenbezogene Daten ausnahmsweise einmal auf anderem Wege (z. B. in Papierform) aus der EU übermittelt werden sollten, würden sie dennoch unter das APPI fallen, sofern sie nach der Übermittlung Teil eines „kollektiven Informationsbestands" werden, der systematisch so organisiert ist, dass leicht nach bestimmten Informationen gesucht werden kann (Artikel 2 Absatz 4 Ziffer ii APPI). Nach Artikel 3 Absatz 2 der Kabinettsverordnung ist dies der Fall, wenn die Informationen „nach einer bestimmten Regel" geordnet sind und die Datenbank zur Erleichterung der Suche Hilfsmittel wie ein Inhaltsverzeichnis oder einen Index enthält. Dies entspricht der Definition des Dateisystems im Sinne des Artikels 2 Absatz 1 DSGVO.

2.2.3. *Definition „gespeicherte personenbezogene Daten"*

(23) Einige Bestimmungen des APPI, insbesondere die Artikel 27 bis 30 über die Rechte des Einzelnen, gelten nur für eine bestimmte Kategorie personenbezogener Daten, nämlich für „gespeicherte personenbezogene Daten". Diese sind in Artikel 2 Absatz 7 APPI als personenbezogene Daten definiert, die nicht zu denjenigen gehören, bei denen i) „nach den Feststellungen in einer Kabinettsverordnung die Wahrscheinlichkeit besteht, dass sie der Öffentlichkeit oder anderen Interessen schaden, wenn ihr Vorhandensein oder Fehlen bekannt wird" oder die ii) „innerhalb einer durch Kabinettsverordnung festgelegten Frist von höchstens einem Jahr zu löschen sind".

(24) Die erste dieser beiden Gruppen wird in Artikel 4 der Kabinettsverordnung erläutert und umfasst vier Ausnahmen ([20]). Mit diesen Ausnahmen werden ähnliche Ziele verfolgt wie mit Artikel 23 Absatz 1 der Verordnung (EU) 2016/679, insbesondere der Schutz der betroffenen Person (des „Betroffenen" in der Terminologie des APPI) und die Freiheit anderer, die nationale Sicherheit, die öffentliche Sicherheit, die Strafverfolgung oder andere wichtige Ziele von allgemeinem öffentlichem Interesse. Darüber hinaus folgt aus dem Wortlaut des Artikels 4 Absatz 1 Ziffern i bis iv der Kabinettsverordnung, dass ihre Anwendung immer ein bestimmtes Risiko für eines der geschützten wichtigen Interessen voraussetzt ([21]).

(25) Die zweite Gruppe wird in Artikel 5 der Kabinettsverordnung näher konkretisiert. In Verbindung mit Artikel 2 Absatz 7 APPI werden personenbezogene Daten, die innerhalb einer Frist von sechs Monaten „zu löschen sind", vom Anwendungsbereich des Begriffs der gespeicherten personenbezogenen Daten und damit von den im APPI verankerten Rechten des Einzelnen ausgenommen. Die PPC hat erläutert, dass diese Ausnahme einen Anreiz für Unternehmer bieten soll, Daten während eines möglichst kurzen Zeitraums zu speichern und zu verarbeiten. Dies würde jedoch bedeuten, dass betroffene Personen in der EU allein wegen der Dauer der Speicherung ihrer Daten durch den betreffenden Unternehmer nicht in der Lage wären, wichtige Rechte geltend zu machen.

(26) Um Abhilfe zu schaffen, müssen aus der Europäischen Union übermittelte personenbezogene Daten nach der Ergänzenden Vorschrift 2 „als gespeicherte personenbezogene Daten im Sinne des Artikels 2 Absatz 7 des Gesetzes gehandhabt werden, und zwar unabhängig davon, innerhalb welcher Frist sie zu löschen sind". Die Speicherfrist hat daher keinen Einfluss auf die Rechte, die betroffenen Personen in der EU gewährt werden.

([19]) Zum Beispiel Artikel 23 APPI über die Voraussetzungen für die Weitergabe personenbezogener Daten an Dritte.

([20]) Nämlich i) personenbezogene Daten, „bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens dem Leben, der körperlichen Unversehrtheit oder dem Vermögen eines Betroffenen oder eines Dritten schaden würde", ii) personenbezogene Daten, „bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens eine rechtswidrige oder ungerechte Handlung fördern oder veranlassen würde", iii) personenbezogene Daten, „bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens die nationale Sicherheit beeinträchtigen, ein Vertrauensverhältnis zu einem anderen Land oder einer internationalen Organisation zerstören oder bei Verhandlungen mit einem anderen Land oder einer internationalen Organisation Nachteile mit sich bringen würde", und iv) personenbezogene Daten, „bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung behindern würde, zum Beispiel die Verhütung, Bekämpfung oder Untersuchung einer Straftat".

([21]) Unter diesen Voraussetzungen ist keine Benachrichtigung des Einzelnen erforderlich. Dies entspricht Artikel 23 Absatz 2 Buchstabe h DSGVO, nach dem betroffene Personen nicht über die Beschränkung unterrichtet werden müssen, sofern dies „dem Zweck der Beschränkung abträglich ist".

2.2.4. *Definition „anonym verarbeitete personenbezogene Informationen"*

(27) Die Anforderungen, die für anonym verarbeitete personenbezogene Informationen im Sinne des Artikels 2 Absatz 9 APPI gelten, sind in Kapitel IV Abschnitt 2 des Gesetzes („Pflichten eines anonym verarbeitete Informationen handhabenden Unternehmers") festgelegt. Dagegen finden auf diese Informationen nicht die Bestimmungen des Kapitels IV Abschnitt 1 des APPI Anwendung, zu denen die Artikel gehören, in denen die Datenschutzgarantien und -rechte bei der Verarbeitung personenbezogener Daten nach dem Gesetz festgelegt sind. Somit unterliegen „anonym verarbeitete personenbezogene Informationen" zwar nicht den (in Kapitel IV Abschnitt 1 und in Artikel 42 APPI aufgeführten) „Standard"-Datenschutzvorschriften, sie fallen jedoch in den Anwendungsbereich des APPI und insbesondere der Artikel 36 bis 39.

(28) Nach Artikel 2 Absatz 9 APPI sind „anonym verarbeitete personenbezogene Informationen" Informationen über eine Einzelperson, die mithilfe der im APPI (Artikel 36 Absatz 1) vorgeschriebenen und in den PPC-Vorschriften (Artikel 19) im Einzelnen festgelegten Maßnahmen „aus personenbezogenen Informationen hergestellt wurden", sodass es unmöglich geworden ist, eine bestimmte Einzelperson zu identifizieren oder die personenbezogenen Informationen wiederherzustellen.

(29) Wie auch die PPC bestätigt hat, ergibt sich aus diesen Bestimmungen, dass der Vorgang der „Anonymisierung" der personenbezogenen Informationen nicht technisch irreversibel sein muss. Nach Artikel 36 Absatz 2 APPI sind Unternehmer, die „anonym verarbeitete personenbezogene Informationen" handhaben, lediglich verpflichtet, eine erneute Identifizierung zu verhindern, indem sie Maßnahmen treffen, um die Sicherheit „der Beschreibungen usw. und der Codes zur Personenidentifizierung, die aus den personenbezogenen Informationen gelöscht wurden, um die anonym verarbeiteten Informationen herzustellen, sowie der Informationen über die Verarbeitungsmethode" zu gewährleisten.

(30) Da „anonym verarbeitete personenbezogene Informationen" im Sinne des APPI Daten enthalten, mit deren Hilfe eine erneute Identifizierung der Einzelperson noch möglich ist, könnte dies bedeuten, dass aus der Europäischen Union übermittelte personenbezogene Daten einen Teil des verfügbaren Schutzes durch einen Vorgang verlieren könnten, der nach der Verordnung (EU) 2016/679 nicht als „Anonymisierung", sondern als eine Form der „Pseudonymisierung" angesehen würde (durch die sich ihr Charakter als personenbezogene Daten nicht ändert).

(31) Um Abhilfe zu schaffen, sind in den Ergänzenden Vorschriften zusätzliche Bestimmungen vorgesehen, die nur für personenbezogene Daten gelten, die nach diesem Beschluss aus der Europäischen Union übermittelt werden. Nach der Ergänzenden Vorschrift 5 werden solche personenbezogenen Informationen nur dann als „anonym verarbeitete personenbezogene Informationen" im Sinne des APPI angesehen, „wenn der personenbezogene Informationen handhabende Unternehmer Maßnahmen trifft, die die Deidentifizierung der Einzelperson für jedermann irreversibel machen, etwa durch Löschung der Informationen über die Verarbeitungsmethode usw.". Bei diesen Informationen handelt es sich nach den Ergänzenden Vorschriften um die Informationen über die Beschreibungen und die Codes zur Personenidentifizierung, die aus den personenbezogenen Informationen gelöscht wurden, um die „anonym verarbeiteten personenbezogenen Informationen" herzustellen, sowie um die Informationen über die Verarbeitungsmethode, die beim Löschen dieser Beschreibungen und Codes zur Personenidentifizierung angewendet wurde. Mit anderen Worten sind Unternehmer, die „anonym verarbeitete personenbezogene Informationen" herstellen, nach den Ergänzenden Vorschriften verpflichtet, den „Schlüssel" zu zerstören, der eine erneute Identifizierung der Daten ermöglicht. Dies bedeutet, dass aus der Europäischen Union stammende personenbezogene Daten nur dann unter die APPI-Bestimmungen über „anonym verarbeitete personenbezogene Informationen" fallen, wenn sie auch nach der Verordnung (EU) 2016/679 als anonyme Informationen angesehen würden ([22]).

2.2.5. *Definition „personenbezogene Informationen handhabender Unternehmer" (PIHBO)*

(32) Der persönliche Anwendungsbereich des APPI umfasst nur PIHBO. Ein PIHBO ist in Artikel 2 Absatz 5 APPI definiert als „Person, die eine Datenbank mit personenbezogenen Informationen usw. zur Verwendung im Geschäft bereitstellt", mit Ausnahme der Regierung und der Verwaltungsstellen auf zentraler und lokaler Ebene.

(33) Nach den PPC-Leitlinien ist „Geschäft" jedes „Verhalten, das darauf abzielt, zu einem bestimmten Zweck, mit oder ohne Gewinnerzielungsabsicht, wiederholt und kontinuierlich ein gesellschaftlich anerkanntes Gewerbe zu betreiben". Organisationen ohne Rechtspersönlichkeit (z. B. nicht rechtsfähige Vereine) und Einzelpersonen werden als PIHBO angesehen, wenn sie eine Datenbank mit personenbezogenen Informationen usw. für ihr Geschäft bereitstellen (verwenden) ([23]). Der Begriff „Geschäft" im APPI ist demnach sehr weit, da er Tätigkeiten aller Arten von Organisationen und Einzelpersonen nicht nur mit, sondern auch ohne Gewinnerzielungsabsicht einschließt. Zudem umfasst die „Verwendung im Geschäft" auch personenbezogene Informationen, die nicht in den (externen) Geschäftsbeziehungen des Unternehmers, sondern intern, z. B. bei der Verarbeitung von Arbeitnehmerdaten, verwendet werden.

([22]) Siehe Verordnung (EU) 2016/679, Erwägungsgrund 26.
([23]) PPC-Leitlinien (General Rule Edition), S. 18.

(34) Bei den Begünstigten des im APPI festgelegten Schutzes unterscheidet das Gesetz nicht nach Staatsangehörigkeit, Wohnsitz oder Aufenthalt. Dies gilt auch für die Rechtsschutzmöglichkeiten von Einzelpersonen bei der PPC und bei Gericht.

2.2.6. *Begriffe „Verantwortlicher" und „Auftragsverarbeiter"*

(35) Im APPI wird keine besondere Unterscheidung zwischen den Pflichten des Verantwortlichen und des Auftragsverarbeiters getroffen. Das Fehlen dieser Unterscheidung hat keinen Einfluss auf das Schutzniveau, da alle PIHBO allen Bestimmungen des Gesetzes unterliegen. Für einen PIHBO, der einen Treuhänder (der einem Auftragsverarbeiter nach der DSGVO entspricht) mit der Handhabung personenbezogener Daten betraut, gelten hinsichtlich der diesem anvertrauten Daten weiterhin die Pflichten nach dem APPI und den Ergänzenden Vorschriften. Zusätzlich ist er nach Artikel 22 APPI verpflichtet, die „erforderliche und angemessene Aufsicht" über den Treuhänder auszuüben. Der Treuhänder selbst unterliegt, wie die PPC bestätigt hat, allen Pflichten nach dem APPI und den Ergänzenden Vorschriften.

2.2.7. *Sektorspezifische Ausnahmen*

(36) Nach Artikel 76 APPI sind bestimmte Arten der Datenverarbeitung von der Anwendung des Kapitels IV des Gesetzes ausgenommen, das die zentralen Datenschutzbestimmungen enthält (Grundsätze, Pflichten der Unternehmer, Rechte des Einzelnen, Aufsicht durch die PPC). Eine Verarbeitung, die unter eine sektorspezifische Ausnahme nach Artikel 76 fällt, ist nach Artikel 43 Absatz 2 APPI auch von den Durchsetzungsbefugnissen der PPC ausgenommen ([24]).

(37) Die einschlägigen Kategorien für die sektorspezifischen Ausnahmen nach Artikel 76 APPI sind durch Anwendung eines doppelten Kriteriums definiert, das auf der Art des die personenbezogenen Informationen verarbeitenden PIHBO und dem Zweck der Verarbeitung basiert. Unter die Ausnahme fallen insbesondere i) Rundfunkanstalten, Zeitungsverlage, Kommunikationsagenturen und andere Presseorganisationen (einschließlich Personen, die im Rahmen ihrer Geschäftstätigkeit Presseaktivitäten ausüben), soweit sie personenbezogene Informationen für Pressezwecke verarbeiten, ii) Personen, die professionell schreiben, soweit dies personenbezogene Informationen umfasst, iii) Hochschulen und andere Organisationen oder Gruppen, die sich mit wissenschaftlichen Studien befassen, und Personen, die einer solchen Organisation angehören, soweit sie personenbezogene Informationen für die Zwecke wissenschaftlicher Studien verarbeiten, iv) religiöse Einrichtungen, soweit sie personenbezogene Informationen für die Zwecke religiöser Aktivitäten (einschließlich aller damit verbundenen Aktivitäten) verarbeiten, und v) politische Einrichtungen, soweit sie personenbezogene Informationen für die Zwecke ihrer politischen Aktivitäten (einschließlich aller damit verbundenen Aktivitäten) verarbeiten. Die Verarbeitung personenbezogener Informationen für einen der in Artikel 76 aufgeführten Zwecke durch andere Arten von PIHBO sowie die Verarbeitung personenbezogener Informationen durch einen der aufgeführten PIHBO für andere Zwecke, z. B. im Rahmen der Beschäftigung, fallen weiterhin unter die Bestimmungen von Kapitel IV.

(38) Um ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten, die aus der Europäischen Union an Unternehmer in Japan übermittelt werden, sollte dieser Beschluss nur Verarbeitungen personenbezogener Informationen erfassen, die in den Anwendungsbereich des Kapitels IV des APPI fallen, d. h. die von einem PIHBO vorgenommen werden, soweit nicht eine der sektorspezifischen Ausnahmen gilt. Sein Anwendungsbereich sollte daher an den des APPI angepasst werden. Wenn ein unter diesen Beschluss fallender PIHBO später den Verwendungszweck ändert (soweit dies zulässig ist) und dann eine der sektorspezifischen Ausnahmen nach Artikel 76 gilt, würde dies nach Auskunft der PPC als internationale Übermittlung angesehen (da in diesen Fällen die Verarbeitung der personenbezogenen Informationen nicht länger unter Kapitel IV des APPI fällt und somit außerhalb von dessen Anwendungsbereich erfolgt). Dies gilt auch, wenn ein PIHBO personenbezogene Informationen für eine unter Artikel 76 APPI fallende Stelle zur Verwendung für einen der in dieser Bestimmung aufgeführten Verarbeitungszwecke bereitstellt. Im Falle von aus der Europäischen Union übermittelten personenbezogenen Daten würde dies daher eine Weiterübermittlung darstellen, für die die entsprechenden Garantien (insbesondere nach Artikel 24 APPI und der Ergänzenden Vorschrift 4) gelten. Wenn sich der PIHBO auf die Einwilligung ([25]) der betroffenen Person stützt, muss er ihr alle erforderlichen Informationen zur Verfügung stellen und sie unter anderem darauf hinweisen, dass die personenbezogenen Informationen nicht länger durch das APPI geschützt sind.

([24]) Andere Unternehmer darf die PPC bei der Ausübung ihrer Ermittlungs- und Durchsetzungsbefugnisse nicht an der Ausübung der Meinungsfreiheit, der akademischen Freiheit, der Religionsfreiheit und des Recht auf politische Tätigkeit hindern (Artikel 43 Absatz 1 APPI).

([25]) Wie die PPC erläutert hat, wird die Einwilligung in den PPC-Leitlinien als „Willenserklärung eines Betroffenen" ausgelegt, „mit der er akzeptiert, dass seine personenbezogenen Informationen gegebenenfalls nach einer von einem personenbezogene Informationen handhabenden Unternehmen angegebenen Methode gehandhabt werden". In den PPC-Leitlinien (General Rule Edition, S. 24) sind die Formen der Einwilligung aufgeführt, die als „in Japan übliche Geschäftspraxis" angesehen werden, nämlich mündliche Zustimmung, Rücksendung von Formularen oder anderen Unterlagen, Zustimmung per E-Mail, Ankreuzen eines Kästchens auf einer Webseite, Klicken auf eine Startseite, Anklicken einer Schaltfläche „Einwilligung", Antippen eines berührungsempfindlichen Displays usw. Alle diese Methoden stellen eine ausdrückliche Form der Einwilligung dar.

### 2.3. **Garantien, Rechte und Pflichten**

#### 2.3.1. *Zweckbindung*

(39) Personenbezogene Daten sollten für einen bestimmten Zweck verarbeitet und anschließend nur verwendet werden, soweit dies mit dem Zweck der Verarbeitung nicht unvereinbar ist. Dieser Datenschutzgrundsatz wird durch die Artikel 15 und 16 APPI gewährleistet.

(40) Das APPI stützt sich auf den Grundsatz, dass ein Unternehmer den Verwendungszweck „so eindeutig wie möglich" (Artikel 15 Absatz 1) anzugeben hat und dann bei der Verarbeitung der Daten an diesen Zweck gebunden ist.

(41) In diesem Zusammenhang sieht Artikel 15 Absatz 2 APPI vor, dass der ursprüngliche Zweck vom PIHBO nur in dem Umfang geändert werden darf, dass „der vor der Änderung geltende Verwendungszweck angemessen relevant bleibt", was in den PPC-Leitlinien dahin gehend ausgelegt wird, dass er dem entsprechen muss, was die betroffene Person aufgrund „geltender gesellschaftlicher Konventionen" ([26]) objektiv erwarten kann.

(42) Zudem dürfen PIHBO nach Artikel 16 Absatz 1 APPI personenbezogene Informationen nicht über den in Artikel 15 genannten „für die Erreichung eines Verwendungszwecks erforderlichen Umfang" hinaus handhaben, ohne vorher die Einwilligung der betroffenen Person einzuholen, es sei denn, eine der Ausnahmeregelungen des Artikels 16 Absatz 3 ([27]) findet Anwendung.

(43) Bei einem Erwerb personenbezogener Informationen von einem anderen Unternehmer steht es dem PIHBO grundsätzlich frei, einen neuen Verwendungszweck festzulegen ([28]). Um sicherzustellen, dass ein solcher Empfänger im Falle einer Übermittlung aus der Europäischen Union an den Zweck gebunden ist, für den die Daten übermittelt wurden, schreibt die Ergänzende Vorschrift 3 vor, dass in Fällen, „in denen ein [PIHBO] auf der Grundlage eines Angemessenheitsbeschlusses personenbezogene Daten aus der EU erhält" oder ein solcher Unternehmer „von einem anderen [PIHBO] personenbezogene Daten erhält, die zuvor auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt wurden" (Weitergabe), der Empfänger „den Zweck der Verwendung dieser personenbezogenen Daten im Rahmen desjenigen Verwendungszwecks angeben muss, für den die Daten ursprünglich oder später empfangen wurden". Mit anderen Worten gewährleistet diese Vorschrift, dass der nach der Verordnung (EU) 2016/679 festgelegte Zweck im Falle der Übermittlung weiterhin für die Verarbeitung maßgebend ist und dass eine Änderung dieses Zwecks in irgendeiner Phase der Verarbeitungskette in Japan die Einwilligung der betroffenen Person in der EU erfordern würde. Da die Einholung dieser Einwilligung eine Kontaktaufnahme mit der betroffenen Person voraussetzt, muss, wenn dies nicht möglich ist, der ursprüngliche Zweck beibehalten werden.

#### 2.3.2. *Rechtmäßigkeit der Verarbeitung und Verarbeitung nach Treu und Glauben*

(44) Der in Erwägungsgrund 43 genannte zusätzliche Schutz ist umso wichtiger, als das japanische System durch den Grundsatz der Zweckbindung auch dafür sorgt, dass personenbezogene Daten rechtmäßig und nach Treu und Glauben verarbeitet werden.

(45) Das APPI schreibt vor, bei der Erhebung personenbezogener Informationen durch einen PIHBO den Verwendungszweck der personenbezogenen Informationen detailliert anzugeben ([29]) und die betroffene Person umgehend über diesen Verwendungszweck zu informieren (oder diesen öffentlich bekannt zu machen) ([30]). Zudem darf ein PIHBO nach Artikel 17 APPI personenbezogene Informationen nicht durch Täuschung oder andere unzulässige Mittel erlangen. Bestimmte Datenkategorien, z. B. personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen, können nur mit Einwilligung der betroffenen Person erworben werden (Artikel 17 Absatz 2 APPI).

([26]) Der von der PPC herausgegebene Fragen-Antworten-Katalog enthält eine Reihe von Beispielen, die diesen Begriff veranschaulichen. Zu den Beispielen für Fälle, in denen die Änderung in einem angemessen relevanten Rahmen bleibt, gehört insbesondere die Verwendung personenbezogener Informationen, die im Rahmen einer geschäftlichen Transaktion von Käufern von Waren oder Dienstleistungen erworben wurden, um diese Käufer über andere einschlägige Waren oder Dienstleistungen zu informieren (z. B. der Betreiber eines Fitnessclubs, der die E-Mail-Anschriften von Mitgliedern erfasst, um diese über Kurse und Programme zu informieren). Der Fragen-Antworten-Katalog enthält auch ein Beispiel für einen Fall, in dem die Änderung des Verwendungszwecks nicht zulässig ist, nämlich wenn ein Unternehmen Informationen über seine Waren und Dienstleistungen an E-Mail-Anschriften versendet, die es ursprünglich erfasst hatte, um vor Betrug zu warnen oder auf den Diebstahl einer Mitgliedskarte hinzuweisen.

([27]) Diese Ausnahmen können sich aus anderen Gesetzen und Verordnungen ergeben oder Fälle betreffen, in denen die Handhabung personenbezogener Informationen erforderlich ist: i) zum „Schutz von Menschenleben, körperlicher Unversehrtheit oder Eigentum", ii) „zur Verbesserung des öffentlichen Gesundheitswesens oder zur Förderung des Wachstums gesunder Kinder" oder iii) „für die Zusammenarbeit mit Regierungsstellen, Behörden oder ihren Vertretern" bei der Erfüllung ihrer gesetzlichen Aufgaben. Zudem finden die Ziffern i und ii nur dann Anwendung, wenn es schwierig ist, die Einwilligung der betroffenen Person einzuholen, und Ziffer iii nur dann, wenn die Gefahr besteht, dass die Einholung der Einwilligung der betroffenen Person die Erfüllung der betreffenden Aufgaben behindern würde.

([28]) Allerdings ist nach Artikel 23 Absatz 1 APPI für die Offenlegung von Daten gegenüber einem Dritten grundsätzlich die Einwilligung der betroffenen Person erforderlich. Auf diese Weise kann diese eine gewisse Kontrolle über die Verwendung ihrer Daten durch einen anderen Unternehmer ausüben.

([29]) Nach Artikel 15 Absatz 1 APPI muss diese Angabe „so eindeutig wie möglich" sein.

([30]) Artikel 18 Absatz 1 APPI.

(46) Wie in den Erwägungsgründen 41 und 42 erläutert, darf der PIHBO die personenbezogenen Informationen später nicht zu anderen Zwecken verarbeiten, es sei denn, die betroffene Person willigt in die betreffende Verarbeitung ein oder eine der Ausnahmeregelungen nach Artikel 16 Absatz 3 APPI findet Anwendung.

(47) Und schließlich wird die Weitergabe personenbezogener Informationen an Dritte ([31]) durch Artikel 23 Absatz 1 APPI auf bestimmte Fälle beschränkt, in denen in der Regel die vorherige Einwilligung der betroffenen Person erforderlich ist ([32]). Artikel 23 Absätze 2, 3 und 4 APPI sieht Ausnahmen von der Pflicht zur Einholung der Einwilligung vor. Diese Ausnahmen gelten jedoch nur für nicht sensible Daten und setzen voraus, dass der Unternehmer die betroffenen Personen im Voraus über seine Absicht, ihre personenbezogenen Informationen einem Dritten gegenüber offenzulegen, und über die Möglichkeit, jeder weiteren Offenlegung zu widersprechen, informiert ([33]).

(48) Bei Übermittlungen aus der Europäischen Union müssen die personenbezogenen Daten zuerst in der EU nach der Verordnung (EU) 2016/679 erhoben und verarbeitet worden sein. Dies umfasst stets zum einen die Erhebung und Verarbeitung — auch für die Übermittlung aus der Europäischen Union nach Japan — auf einer der in Artikel 6 Absatz 1 der Verordnung aufgeführten Rechtsgrundlagen und zum anderen die Erhebung für einen festgelegten, eindeutigen und legitimen Zweck sowie das Verbot der Weiterverarbeitung — auch im Wege der Übermittlung — in einer mit einem solchen in Artikel 5 Absatz 1 Buchstabe b und Artikel 6 Absatz 4 der Verordnung genannten Zweck nicht zu vereinbarenden Weise.

(49) Nach der Übermittlung muss der PIHBO, der die Daten erhält, nach der Ergänzenden Vorschrift 3 den der Übermittlung zugrunde liegenden Zweck (d. h. den nach der Verordnung (EU) 2016/679 festgelegten Zweck) „bestätigen" und die Daten diesem Zweck entsprechend weiterverarbeiten ([34]). Dies bedeutet, dass nicht nur der erste Erwerber dieser personenbezogenen Daten in Japan, sondern auch jeder künftige Empfänger der Daten (auch ein Treuhänder) an den nach der Verordnung festgelegten Zweck gebunden ist.

(50) Ferner muss der PIHBO, falls er den Zweck, der zuvor nach der Verordnung (EU) 2016/679 festgelegt wurde, nach Artikel 16 Absatz 1 APPI ändern möchte, grundsätzlich die Einwilligung der betroffenen Person einholen. Ohne diese Einwilligung würde eine Datenverarbeitung, die über den für die Erreichung dieses Verwendungszwecks erforderlichen Umfang hinausgeht, einen Verstoß gegen Artikel 16 Absatz 1 darstellen, der von der PPC und den Gerichten geahndet werden könnte.

(51) Da die Übermittlung also nach der Verordnung (EU) 2016/679 eine gültige Rechtsgrundlage und einen festgelegten Zweck voraussetzt, die sich in dem nach dem APPI „bestätigten" Verwendungszweck widerspiegeln, wird die weitere Rechtmäßigkeit der Verarbeitung von EU-Daten in Japan durch die einschlägigen Bestimmungen des APPI in Verbindung mit der Ergänzenden Vorschrift 3 gewährleistet.

2.3.3. *Richtigkeit der Daten und Datenminimierung*

(52) 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.

(53) Diese Grundsätze werden im japanischen Recht durch Artikel 16 Absatz 1 APPI gewährleistet, der die Handhabung personenbezogener Informationen über den „für die Erreichung eines Verwendungszwecks erforderlichen Umfang" hinaus verbietet. Wie die PPC erläutert hat, schließt dies nicht nur die Verwendung nicht angemessener Daten und die übermäßige Verwendung von Daten (über den für die Erreichung des Verwendungszwecks erforderlichen Umfang hinaus) aus, sondern beinhaltet auch das Verbot, Daten zu handhaben, die für die Erreichung des Verwendungszwecks nicht relevant sind.

([31]) Treuhänder fallen zwar für die Zwecke der Anwendung des Artikels 23 nicht unter den Begriff „Dritte" (siehe Absatz 5), dieser Ausschluss gilt jedoch nur, soweit der Treuhänder personenbezogene Informationen im Rahmen der Betrauung („in dem für die Erreichung eines Verwendungszwecks erforderlichen Umfang") handhabt, also als Auftragsverarbeiter handelt.

([32]) Ausnahmen gelten für i) die Bereitstellung personenbezogener Informationen „auf der Grundlage von Gesetzen und Verordnungen", ii) Fälle, „in denen es notwendig ist, ein Menschenleben, die körperliche Unversehrtheit oder ein Vermögen zu schützen, und in denen es schwierig ist, die Einwilligung des Betroffenen einzuholen", iii) Fälle, „in denen es in besonderem Maße notwendig ist, das öffentliche Gesundheitswesen zu verbessern oder die Förderung gesunder Kinder zu unterstützen, und in denen es schwierig ist, die Einwilligung des Betroffenen einzuholen", und iv) Fälle, „in denen es notwendig ist, mit einer zentralen Regierungsorganisation oder einer lokalen Regierung oder einer von ihr beauftragten Person, die ihr durch Gesetze und Verordnungen übertragene Aufgaben erfüllt, zusammenzuarbeiten, und in denen die Möglichkeit besteht, dass die Einholung der Einwilligung des Betroffenen die Erfüllung der genannten Aufgaben behindern würde".

([33]) Zu den bereitzustellenden Informationen gehören insbesondere die Kategorien personenbezogener Daten, die an einen Dritten weitergegeben werden sollen, und die Form der Übermittlung. Darüber hinaus muss der PIHBO die betroffene Person darüber informieren, dass und wie sie der Übermittlung widersprechen kann.

([34]) Nach Artikel 26 Absatz 1 Ziffer ii APPI ist ein PIHBO verpflichtet, beim Empfang personenbezogener Daten von einem Dritten die „Einzelheiten des Erwerbs der personenbezogenen Daten durch den Dritten" zu „bestätigen" (zu überprüfen), einschließlich des Zwecks dieses Erwerbs. Artikel 26 sieht zwar nicht ausdrücklich vor, dass der PIHBO dann diesen Zweck verfolgen muss, dies ist aber durch die Ergänzende Vorschrift 3 eindeutig vorgeschrieben.

(54) In Bezug auf die Verpflichtung, die Richtigkeit und Aktualität der Daten zu gewährleisten, verlangt Artikel 19 APPI, dass sich der PIHBO „bemüht sicherzustellen, dass personenbezogene Daten in dem für die Erreichung eines Verwendungszwecks erforderlichen Umfang sachlich richtig und auf dem neuesten Stand sind". Diese Bestimmung ist in Verbindung mit Artikel 16 Absatz 1 APPI zu lesen. Wie die PPC erläutert hat, wird die Verarbeitung der personenbezogenen Informationen, wenn ein PIHBO die vorgeschriebenen Anforderungen an die Richtigkeit nicht erfüllt, nicht als Erreichung des Verwendungszwecks angesehen, sodass ihre Handhabung nach Artikel 16 Absatz 1 rechtswidrig wird.

2.3.4. *Speicherbegrenzung*

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

(56) Nach Artikel 19 APPI müssen sich PIHBO „um die unverzügliche Löschung der personenbezogenen Daten bemühen, wenn die betreffende Verwendung nicht mehr erforderlich ist". Diese Bestimmung muss in Verbindung mit Artikel 16 Absatz 1 APPI gelesen werden, der die Handhabung personenbezogener Informationen über den „für die Erreichung eines Verwendungszwecks erforderlichen Umfang" hinaus verbietet. Sobald der Verwendungszweck erreicht ist, kann die Verarbeitung personenbezogener Informationen nicht mehr als erforderlich angesehen und darf daher nicht fortgesetzt werden (es sei denn, der PIHBO holt die Einwilligung der betroffenen Person hierzu ein).

2.3.5. *Datensicherheit*

(57) Personenbezogene Daten müssen in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Zu diesem Zweck müssen Unternehmer geeignete technische oder organisatorische Maßnahmen treffen, um personenbezogene Daten vor möglichen Bedrohungen zu schützen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik und der damit verbundenen Kosten bewertet werden.

(58) Dieser Grundsatz ist im japanischen Recht durch Artikel 20 APPI umgesetzt, der vorsieht, dass ein PIHBO „erforderliche und angemessene Maßnahmen zur Kontrolle der Sicherheit personenbezogener Daten trifft, um unter anderem die unerlaubte Veröffentlichung, den Verlust oder die Beschädigung der von ihm gehandhabten personenbezogenen Daten zu verhindern". Die zu treffenden Maßnahmen werden in den PPC-Leitlinien erläutert, einschließlich der Methoden für die Festlegung von grundlegenden Richtlinien, Vorschriften für die Datenhandhabung und verschiedenen „Kontrollmaßnahmen" (in Bezug auf die organisatorische Sicherheit sowie die menschliche, physische und technologische Sicherheit) ([35]). Darüber hinaus enthalten die PPC-Leitlinien und eine von der PPC veröffentlichte besondere Bekanntmachung (Anlage 8 „Inhalt der zu treffenden Maßnahmen für das Sicherheitsmanagement") weitere Einzelheiten zu Maßnahmen bei Sicherheitsvorfällen, die beispielsweise die unerlaubte Veröffentlichung personenbezogener Informationen betreffen, als Teil der von PIHBO treffenden Maßnahmen für das Sicherheitsmanagement ([36]).

(59) Ferner muss, wenn personenbezogene Informationen von Arbeitnehmern oder Subunternehmern gehandhabt werden, nach den Artikeln 20 und 21 APPI die „erforderliche und angemessene Aufsicht" zu Sicherheitskontrollzwecken gewährleistet sein. Außerdem kann die vorsätzliche unerlaubte Veröffentlichung oder der Diebstahl personenbezogener Informationen nach Artikel 83 APPI mit einer Freiheitsstrafe von bis zu einem Jahr geahndet werden.

2.3.6. *Transparenz*

(60) Die betroffenen Personen müssen über die Hauptmerkmale der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden.

(61) Nach Artikel 18 Absatz 1 APPI muss der PIHBO der betroffenen Person Informationen über den Verwendungszweck der erworbenen personenbezogenen Informationen zur Verfügung stellen, außer in „Fällen, in denen ein Verwendungszweck vorher öffentlich bekannt gemacht wurde". Dieselbe Pflicht besteht im Falle einer zulässigen Änderung des Verwendungszwecks (Artikel 18 Absatz 3). Damit ist auch gewährleistet, dass die betroffene Person von der Erhebung ihrer Daten erfährt. Das APPI verlangt zwar nicht generell, dass der PIHBO die betroffene Person in der Erhebungsphase über die voraussichtlichen Empfänger der personenbezogenen Informationen unterrichtet, eine solche Unterrichtung ist aber eine notwendige Voraussetzung für jede spätere Offenlegung von Informationen gegenüber einem Dritten (Empfänger) nach Artikel 23 Absatz 2, wenn dies also ohne vorherige Einwilligung der betroffenen Person geschieht.

([35]) PPC-Leitlinien (General Rule Edition), S. 41 und S. 86 bis 98.

([36]) Nach Abschnitt 3-3-2 der PPC-Leitlinien ist der PIHBO im Falle der unerlaubten Veröffentlichung, der Beschädigung oder des Verlustes von Daten verpflichtet, die erforderlichen Ermittlungen durchzuführen und insbesondere das Ausmaß der Verletzung der Rechte und Interessen der Person sowie Art und Umfang der betroffenen personenbezogenen Informationen festzustellen.

(62) Hinsichtlich „gespeicherter personenbezogener Daten“ sieht Artikel 27 APPI vor, dass der PIHBO die betroffene Person über seine Identität (Kontaktdaten), den Verwendungszweck und die Verfahren für die Beantwortung einer Anfrage bezüglich der individuellen Rechte der betroffenen Person nach den Artikeln 28, 29 und 30 APPI unterrichten muss.

(63) Da aus der Europäischen Union übermittelte personenbezogene Daten nach den Ergänzenden Vorschriften unabhängig von ihrer Speicherfrist als „gespeicherte personenbezogene Daten“ angesehen werden (sofern für sie keine Ausnahme gilt), unterliegen sie stets den Transparenzanforderungen der beiden oben genannten Bestimmungen.

(64) Die Anforderungen des Artikels 18 und die Pflicht zur Unterrichtung über den Verwendungszweck nach Artikel 27 APPI unterliegen den gleichen Ausnahmen, denen zumeist Erwägungen des öffentlichen Interesses und der Schutz der Rechte und Interessen der betroffenen Person, Dritter und des Verantwortlichen zugrunde liegen ([37]). Nach der in den PPC-Leitlinien entwickelten Auslegung gelten diese Ausnahmen in ganz bestimmten Fällen, etwa wenn Informationen über den Verwendungszweck legitime Maßnahmen des Unternehmers zum Schutz bestimmter Interessen (z. B. Bekämpfung von Betrug, Industriespionage oder Sabotage) gefährden könnten.

2.3.7. *Besondere Kategorien von Daten*

(65) Wenn „besondere Kategorien“ von Daten verarbeitet werden, müssen besondere Garantien vorhanden sein.

(66) „Personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen“ sind in Artikel 2 Absatz 3 APPI definiert. Diese Bestimmung bezieht sich auf „personenbezogene Informationen, die die Rasse, den Glauben, den sozialen Status, die Krankengeschichte, die Vorstrafen des Betroffenen, die Tatsache, dass er durch eine Straftat einen Schaden erlitten hat, oder andere Beschreibungen usw. umfassen und deren Handhabung aufgrund einer Kabinettsverordnung einer besonderen Sorgfalt bedarf, damit keine unfaire Diskriminierung und keine Vorurteile oder sonstigen Nachteile zulasten des Betroffenen verursacht werden“. Diese Kategorien entsprechen zu einem großen Teil den in den Artikeln 9 und 10 der Verordnung (EU) 2016/679 aufgeführten sensiblen Daten. So entspricht die „Krankengeschichte“ den Gesundheitsdaten, während die „Vorstrafen“ und die „Tatsache, dass er durch eine Straftat einen Schaden erlitten hat“, im Wesentlichen den in Artikel 10 der Verordnung (EU) 2016/679 genannten Kategorien entsprechen. Die in Artikel 2 Absatz 3 APPI genannten Kategorien werden in der Kabinettsverordnung und den PPC-Leitlinien weiter ausgelegt. In Abschnitt 2.3 Nummer 8 der PPC-Leitlinien werden die in Artikel 2 Ziffern ii und iii der Kabinettsverordnung ausführlich behandelten Unterkategorien der „Krankengeschichte“ dahin gehend ausgelegt, dass sie genetische und biometrische Daten umfassen. Die Liste enthält zwar nicht ausdrücklich die Begriffe „ethnische Herkunft“ und „politische Meinung“, verweist jedoch auf „Rasse“ und „Glauben“. Wie in Abschnitt 2.3 Nummern 1 und 2 der PPC-Leitlinien erläutert, bezieht sich der Verweis auf die „Rasse“ auf „ethnische Bindungen oder Bindungen an einen bestimmten Teil der Welt“, während „Glauben“ sowohl religiöse als auch politische Überzeugungen umfasst.

(67) Der Wortlaut der Bestimmung verdeutlicht, dass es sich nicht um eine geschlossene Liste handelt, da weitere Kategorien von Daten hinzugefügt werden können, soweit deren Verarbeitung die Gefahr von „unfairer Diskriminierung, Vorurteilen oder sonstigen Nachteilen zulasten des Betroffenen“ birgt.

(68) Vor dem Hintergrund, dass der Begriff der „sensiblen“ Daten naturgemäß ein gesellschaftliches Konstrukt ist, da es unter anderem auf kulturellen und rechtlichen Traditionen, moralischen Erwägungen und politischen Entscheidungen einer bestimmten Gesellschaft beruht, und angesichts der Bedeutung angemessener Garantien für sensible Daten bei der Übermittlung an Unternehmer in Japan hat die Kommission erreicht, dass der besondere Schutz, der nach japanischem Recht für „personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen“, gewährt wird, auf alle in der Verordnung (EU) 2016/679 als „sensible Daten“ anerkannten Kategorien ausgeweitet wird. Zu diesem Zweck sieht die Ergänzende Vorschrift 1 vor, dass aus der Europäischen Union übermittelte Daten über das Sexualleben, die sexuelle Orientierung oder die Gewerkschaftszugehörigkeit einer Person von PIHBO „in gleicher Weise wie personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen, im Sinne des Artikels 2 Absatz 3 [APPI]“ verarbeitet werden müssen.

([37]) Dies sind i) Fälle, in denen die Möglichkeit besteht, dass die Unterrichtung der betroffenen Person über den Verwendungszweck oder dessen öffentliche Bekanntmachung „das Leben, die körperliche Unversehrtheit, das Vermögen oder andere Rechte und Interessen eines Betroffenen oder Dritten“ oder „die Rechte oder berechtigten Interessen des PIHBO“ schädigen, ii) Fälle, in denen „es notwendig ist, mit einer zentralen Regierungsorganisation oder einer lokalen Regierung“ bei der Erfüllung ihrer gesetzlichen Aufgaben zusammenzuarbeiten, wenn eine solche Unterrichtung oder Bekanntmachung diese „Angelegenheiten“ behindern würde, iii) Fälle, in denen der Verwendungszweck aufgrund der Umstände, unter denen die Daten erworben wurden, klar ist.

(69) Was die zusätzlichen materiellen Garantien betrifft, die für personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen, gelten, so ist es PIHBO nach Artikel 17 Absatz 2 APPI mit wenigen Ausnahmen ([38]) nicht erlaubt, diese Art von Daten ohne vorherige Einwilligung der betroffenen Person zu erwerben. Ferner besteht bei dieser Kategorie personenbezogener Informationen nicht die Möglichkeit, sie Dritten gegenüber nach dem Verfahren des Artikels 23 Absatz 2 APPI offenzulegen (nach dem die Übermittlung von Daten an Dritte ohne vorherige Einwilligung der betroffenen Person zulässig ist).

2.3.8. *Rechenschaftspflicht*

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

(71) Wie in Fußnote 34 (Erwägungsgrund 49) erwähnt, sind PIHBO nach Artikel 26 Absatz 1 APPI verpflichtet, die Identität eines Dritten, der ihnen personenbezogene Daten zur Verfügung stellt, und die „Umstände" zu überprüfen, unter denen diese Daten von dem Dritten erworben wurden (im Falle personenbezogener Daten, die unter diesen Beschluss fallen, umfassen diese Umstände nach dem APPI und der Ergänzenden Vorschrift 3 die Tatsache, dass die Daten aus der Europäischen Union stammen, und den Zweck der ursprünglichen Datenübermittlung). Diese Maßnahme zielt unter anderem darauf ab, die Rechtmäßigkeit der Datenverarbeitung in der gesamten Kette der PIHBO, die die personenbezogenen Daten handhaben, zu gewährleisten. Ferner sind PIHBO nach Artikel 26 Absatz 3 APPI verpflichtet, das Empfangsdatum und die von dem Dritten nach Absatz 1 erhaltenen (vorgeschriebenen) Informationen sowie den Namen der betroffenen Person, die Kategorien der verarbeiteten Daten und, soweit relevant, die Tatsache zu dokumentieren, dass die betroffene Person in die Weitergabe ihrer personenbezogenen Daten eingewilligt hat. Nach Artikel 18 der PPC-Leitlinien müssen diese Aufzeichnungen je nach den Umständen mindestens ein bis drei Jahre aufbewahrt werden. Im Rahmen der Erfüllung ihrer Aufgaben kann die PPC die Vorlage dieser Aufzeichnungen verlangen ([39]).

(72) PIHBO müssen Beschwerden betroffener Personen über die Verarbeitung ihrer personenbezogenen Informationen umgehend und angemessen bearbeiten. Um die Bearbeitung von Beschwerden zu erleichtern, müssen sie ein „für die Erreichung [dieses] Zwecks erforderliches System" einrichten, was voraussetzt, dass sie innerhalb ihrer Organisation geeignete Verfahren einführen (z. B. Zuweisung von Verantwortlichkeiten oder Einrichtung einer Anlaufstelle).

(73) Außerdem schafft das APPI einen Rahmen für die Beteiligung von Branchenverbänden an der Sicherstellung eines hohen Konformitätsniveaus (siehe Kapitel IV Abschnitt 4). Die Rolle dieser akkreditierten Organisationen für den Schutz personenbezogener Informationen ([40]) besteht darin, den Schutz personenbezogener Informationen zu fördern, indem sie Unternehmen mit ihrem Fachwissen unterstützen, aber auch zur Umsetzung von Garantien beizutragen, insbesondere durch die Bearbeitung einzelner Beschwerden und die Unterstützung bei der Lösung damit zusammenhängender Konflikte. Zu diesem Zweck können sie die beteiligten PIHBO gegebenenfalls auffordern, die notwendigen Maßnahmen durchzuführen ([41]). Ferner müssen PHIBO im Falle von Datenschutzverletzungen oder anderen Sicherheitsvorfällen grundsätzlich die PPC und die betroffene Person (oder die Öffentlichkeit) informieren und die notwendigen Maßnahmen treffen, um unter anderem den Schaden zu minimieren und ähnliche Vorfälle zu verhindern ([42]). Obwohl es sich hierbei um freiwillige Regelungen handelt, waren am 10. August 2017 44 Organisationen bei der PPC gelistet, von denen die größte das Japan Information Processing and

([38]) Diese Ausnahmen sind i) „Fälle auf der Grundlage von Gesetzen und Verordnungen", ii) „Fälle, in denen es notwendig ist, ein Menschenleben, die körperliche Unversehrtheit oder ein Vermögen zu schützen, und in denen es schwierig ist, die Einwilligung des Betroffenen einzuholen", iii) „Fälle, in denen es in besonderem Maße notwendig ist, das öffentliche Gesundheitswesen zu verbessern oder die Förderung gesunder Kinder zu unterstützen, und in denen es schwierig ist, die Einwilligung des Betroffenen einzuholen", iv) „Fälle, in denen es notwendig ist, mit einer zentralen Regierungsorganisation oder einer lokalen Regierung oder einer von ihr beauftragten Person, die ihr durch Gesetze und Verordnungen übertragene Aufgaben erfüllt, zusammenzuarbeiten, und in denen die Möglichkeit besteht, dass die Einholung der Einwilligung des Betroffenen die Erfüllung der genannten Aufgaben behindern würde", und v) Fälle, in denen die genannten personenbezogenen Informationen, die einer besonderen Sorgfalt bedürfen, von einer betroffenen Person, einer Regierungsorganisation, einer lokalen Regierung, einer Person, die unter eine der Kategorien des Artikels 76 Absatz 1 fällt, oder anderen Personen, die in Vorschriften der PPC festgelegt sind, der Öffentlichkeit gegenüber offengelegt werden. Eine weitere Kategorie betrifft „andere Fälle, die durch Kabinettsverordnung den vorstehend genannten Fällen gleichgestellt sind", und umfasst nach der geltenden Kabinettsverordnung insbesondere augenfällige Merkmale einer Person (z. B. einen sichtbaren Gesundheitszustand), sofern die sensiblen Daten (unbeabsichtigt) durch visuelle Beobachtung, durch Film- oder Fotoaufnahmen der betroffenen Person, z. B. durch Überwachungskameras, erworben wurden.

([39]) Nach Artikel 40 Absatz 1 APPI kann die PPC, soweit dies für die Umsetzung der einschlägigen Bestimmungen des APPI erforderlich ist, von einem PIHBO verlangen, die erforderlichen Informationen oder Materialien im Zusammenhang mit der Handhabung personenbezogener Informationen vorzulegen.

([40]) Das APPI enthält unter anderem Vorschriften für die Akkreditierung solcher Organisationen; siehe die Artikel 47 bis 50 APPI.

([41]) Artikel 52 APPI.

([42]) PPC-Bekanntmachung Nr. 1/2017 „Maßnahmen, die zu treffen sind, wenn der Schutz personenbezogener Daten verletzt worden ist oder sich ein ähnlicher Vorfall ereignet hat".

Development Center (JIPDEC) war, dem allein 15 436 teilnehmende Unternehmer ([43]) angehören. Akkreditiert sind auch Branchenverbände wie die Japan Securities Dealers Association, die Japan Association of Car Driving Schools oder die Association of Marriage Brokers ([44]).

(74) Die akkreditierten Organisationen für den Schutz personenbezogener Informationen müssen jährlich Bericht über ihre Tätigkeit erstatten. Nach der von der PPC veröffentlichten „Übersicht über den Stand der Umsetzung des APPI im Geschäftsjahr 2015" gingen bei den akkreditierten Organisationen für den Schutz personenbezogener Informationen insgesamt 442 Beschwerden ein; sie verlangten 123 Erklärungen von Unternehmern in ihrem Zuständigkeitsbereich, forderten in 41 Fällen Unterlagen von diesen Unternehmern an, gaben 181 Anweisungen und sprachen zwei Empfehlungen aus ([45]).

2.3.9. *Beschränkungen für Weiterübermittlungen*

(75) Das Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an Unternehmer in Japan übermittelt werden, darf nicht durch die Weiterübermittlung dieser Daten an Empfänger in einem Drittland außerhalb Japans beeinträchtigt werden. Solche Weiterübermittlungen, die aus Sicht des japanischen Unternehmers internationale Übermittlungen aus Japan darstellen, sollten nur dann zulässig sein, wenn der spätere Empfänger außerhalb Japans selbst Vorschriften unterliegt, die ein ähnliches Schutzniveau gewährleisten, wie es in der japanischen Rechtsordnung garantiert ist.

(76) Eine erste Schutzmaßnahme ist in Artikel 24 APPI verankert, der die Übermittlung personenbezogener Daten an einen Dritten außerhalb des Hoheitsgebiets Japans ohne vorherige Einwilligung der betroffenen Person grundsätzlich verbietet. Durch die Ergänzende Vorschrift 4 wird sichergestellt, dass diese Einwilligung bei Datenübermittlungen aus der Europäischen Union in voller Kenntnis der Sachlage gegeben wird, da der betroffenen Person „die Informationen über die Umstände der Übermittlung zur Verfügung gestellt werden, die erforderlich sind, damit der Betroffene eine Entscheidung über seine Einwilligung treffen kann". Auf dieser Grundlage ist die betroffene Person davon in Kenntnis zu setzen, dass die Daten ins Ausland (außerhalb des Anwendungsbereichs des APPI) übermittelt werden, und über das jeweilige Bestimmungsland zu informieren. Dies ermöglicht es ihr, das mit der Übermittlung verbundene Risiko für die Privatsphäre zu bewerten. Wie aus Artikel 23 APPI abgeleitet werden kann (siehe Erwägungsgrund 47), sollten die für den Betroffenen bereitgestellten Informationen auch die in Absatz 2 vorgeschriebenen Angaben umfassen, nämlich die Kategorien personenbezogener Daten, die einem Dritten zur Verfügung gestellt werden, und die Offenlegungsmethode.

(77) Artikel 24 APPI sieht in Verbindung mit Artikel 11-2 der PPC-Leitlinien mehrere Ausnahmen von dieser auf Einwilligung beruhenden Vorschrift vor. Zudem gelten die Ausnahmeregelungen des Artikels 23 Absatz 1 APPI nach Artikel 24 auch für internationale Datenübermittlungen ([46]).

(78) Um die Kontinuität des Schutzes im Falle der Übermittlung personenbezogener Daten aus der Europäischen Union nach Japan auf der Grundlage dieses Beschlusses zu gewährleisten, wird mit der Ergänzenden Vorschrift 4 das Schutzniveau für Weiterübermittlungen dieser Daten durch den PIHBO an einen Empfänger in einem Drittland erhöht. Dies geschieht durch Beschränkung und Präzisierung der Grundlagen für internationale Übermittlungen, die der PIHBO als Alternative zur Einwilligung nutzen kann. So können nach diesem Beschluss übermittelte personenbezogene Daten unbeschadet der Ausnahmeregelungen des Artikels 23 Absatz 1 APPI nur in zwei Fällen ohne Einwilligung (weiter)übermittelt werden: i) wenn die Daten in ein Drittland übermittelt werden, dessen Datenschutzniveau von der PPC nach Artikel 24 APPI als dem in Japan garantierten Schutzniveau gleichwertig eingestuft wurde ([47]), oder ii) wenn der PIHBO und der Dritte (Empfänger) gemeinsam durch Vertrag, andere Formen verbindlicher Vereinbarungen oder verbindliche Regelungen innerhalb einer Unternehmensgruppe Maßnahmen getroffen haben, die ein Schutzniveau bieten, das dem des APPI in Verbindung mit den Ergänzenden Vorschriften gleichwertig ist. Die zweite Kategorie entspricht den Instrumenten, die nach der Verordnung (EU) 2016/679 verwendet werden, um für geeignete Garantien zu sorgen (insbesondere Vertragsklauseln und verbindliche interne Datenschutzvorschriften). Zudem unterliegt die Übermittlung, wie die PPC bestätigt hat, auch in diesen Fällen weiterhin den allgemeinen Vorschriften, die für die Bereitstellung personenbezogener Daten für einen Dritten nach dem APPI gelten (d. h. Pflicht zur Einholung der Einwilligung nach Artikel 23 Absatz 1 oder alternativ Informationspflicht mit der Möglichkeit, eine Ausnahmeregelung in Anspruch zu nehmen, nach

([43]) Nach den auf der PrivacyMark-Website des JIPDEC am 2. Oktober 2017 veröffentlichten Zahlen.
([44]) PPC, Verzeichnis der akkreditierten Organisationen für den Schutz personenbezogener Informationen, im Internet abrufbar unter: https://www.ppc.go.jp/personal/nintei/list/ oder https://www.ppc.go.jp/files/pdf/nintei_list.pdf
([45]) PPC, Übersicht über den Stand der Umsetzung des APPI im Geschäftsjahr 2015 (Oktober 2016), im Internet (nur in japanischer Sprache) abrufbar unter: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf
([46]) Siehe Fußnote 32.
([47]) Nach Artikel 11 der PPC-Leitlinien erfordert dies nicht nur materielle Standards, die denen des APPI gleichwertig sind und von einer unabhängigen Durchsetzungsbehörde wirksam überwacht werden, sondern auch, dass die Umsetzung der einschlägigen Vorschriften im Drittland gewährleistet ist.

Artikel 23 Absatz 2 APPI). Falls die betroffene Person nicht zu erreichen ist, um sie um Einwilligung zu ersuchen oder ihr die erforderlichen Vorabinformationen nach Artikel 23 Absatz 2 APPI zur Verfügung zu stellen, darf die Übermittlung nicht stattfinden.

(79) Abgesehen von den Fällen, in denen die PPC festgestellt hat, dass das betreffende Drittland ein dem Schutzniveau des APPI gleichwertiges Schutzniveau gewährleistet ([48]), schließen die in der Ergänzenden Vorschrift 4 festgelegten Anforderungen daher den Einsatz von Übermittlungsinstrumenten aus, die keine rechtsverbindlichen Beziehungen zwischen dem japanischen Datenexporteur und dem Datenimporteur des Drittlands begründen und nicht das erforderliche Schutzniveau gewährleisten. Dies ist beispielsweise beim System grenzüberschreitender Vorschriften zur Wahrung der Privatsphäre (*Cross Border Privacy Rules (CBPR) System*) der APEC der Fall, an dem Japan beteiligt ist ([49]), da der Schutz sich in diesem System nicht aus einer Regelung ergibt, die den Exporteur und den Importeur im Rahmen ihrer bilateralen Beziehungen bindet, und sich eindeutig auf einem niedrigeren Niveau bewegt sind als dem, das durch das APPI im Verbindung mit den Ergänzenden Vorschriften gewährleistet ist ([50]).

(80) Und schließlich ergibt sich aus den Artikeln 20 und 22 APPI eine weitere Garantie im Falle von (Weiter-)Übermittlungen. Nach diesen Bestimmungen muss der PIHBO (Datenexporteur), wenn ein Drittlandunternehmer (Datenimporteur) in seinem Namen — d. h. als (Unter-)Verarbeiter — handelt, die Aufsicht über den Drittlandunternehmer in Bezug auf die Sicherheit der Datenverarbeitung gewährleisten.

2.3.10. *Rechte des Einzelnen*

(81) Wie das EU-Datenschutzrecht gewährt auch das APPI Einzelpersonen eine Reihe durchsetzbarer Rechte. Hierzu gehören das Recht auf Auskunft („Offenlegung"), Berichtigung und Löschung sowie das Recht auf Widerspruch („Beendigung der Verwendung").

(82) Erstens hat die betroffene Person nach Artikel 28 Absätze 1 und 2 APPI das Recht, von einem PIHBO zu verlangen, „gespeicherte personenbezogene Daten, anhand deren sie identifiziert werden kann, offenzulegen", und der PIHBO muss nach Eingang eines solchen Antrags der betroffenen Person die „gespeicherten personenbezogenen Daten offenlegen". Artikel 29 (Recht auf Berichtigung) und 30 (Recht auf Beendigung der Verwendung) sind wie Artikel 28 aufgebaut.

(83) Nach Artikel 9 der Kabinettsverordnung muss die Offenlegung personenbezogener Informationen nach Artikel 28 Absatz 2 APPI schriftlich erfolgen, es sei denn, der PIHBO und die betroffene Person haben etwas anderes vereinbart.

(84) Für diese Rechte gelten drei Arten von Beschränkungen; sie betreffen die Rechte und Interessen des Einzelnen oder Dritter ([51]), eine erhebliche Beeinträchtigung des Geschäftsbetriebs des PIHBO ([52]) sowie Fälle, in denen die Offenlegung gegen andere Gesetze oder Verordnungen verstoßen würde ([53]). Die Situationen, in denen diese Beschränkungen Anwendung finden, ähneln einigen der Ausnahmen, die nach Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 gelten, dem zufolge Beschränkungen der Rechte des Einzelnen im Hinblick auf „den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen" oder „den Schutz sonstiger wichtiger Ziele

([48]) Bisher hat die PPC noch keine Beschlüsse nach Artikel 24 APPI erlassen, mit denen das Schutzniveau eines Drittlands als dem in Japan garantierten Schutzniveau gleichwertig anerkannt wird. Der einzige Beschluss, dessen Erlass sie derzeit prüft, betrifft den EWR. Im Hinblick auf mögliche weitere Beschlüsse wird die Kommission die Lage genau beobachten und erforderlichenfalls geeignete Maßnahmen treffen, um etwaigen nachteiligen Auswirkungen auf die Kontinuität des Schutzes zu begegnen (siehe unten die Erwägungsgründe 176, 177 und 184 sowie Artikel 3 Absatz 1).

([49]) Allerdings sind nur zwei japanische Unternehmen nach dem CBPR-System der APEC zertifiziert (siehe https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Außerhalb Japans sind die einzigen anderen Unternehmer, die nach diesem System zertifiziert sind, einige wenige (23) US-Unternehmen (siehe https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) So gibt es beispielsweise keine Definition und keinen besonderen Schutz für sensible Daten und keine Verpflichtung zur Begrenzung der Datenspeicherung. Siehe auch Artikel-29-Datenschutzgruppe, Stellungnahme 02/2014 zu einer Referenzgrundlage für Anforderungen an verbindliche unternehmensinterne Vorschriften, die den nationalen Datenschutzbehörden in der EU vorgelegt wurden, sowie grenzüberschreitende Vorschriften zur Wahrung der Privatsphäre, die den CBPR-Rechenschaftspflichtigen der APEC vorgelegt wurden, 6. März 2014.

([51]) Laut PPC können nur solche Interessen eine Beschränkung rechtfertigen, die „rechtlich schutzwürdig" sind. Diese Bewertung muss im Einzelfall vorgenommen werden, und zwar „unter Berücksichtigung des Eingriffs in das Grundrecht auf Privatsphäre einschließlich des Datenschutzes, wie es in der Verfassung und der Rechtsprechung anerkannt worden ist". Zu den geschützten Interessen können unter anderem Betriebs- oder sonstige Geschäftsgeheimnisse gehören.

([52]) Der Begriff der „erheblichen Beeinträchtigung des ordnungsgemäßen Geschäftsbetriebs des Unternehmers" wird in den PPC-Leitlinien durch verschiedene Beispiele veranschaulicht, z. B. identische komplexe Anträge, die von derselben Person wiederholt gestellt werden, wenn solche Anträge für den Unternehmer eine erhebliche Belastung darstellen und seine Fähigkeit beeinträchtigen, andere Anträge zu beantworten (PPC-Leitlinien (General Rule Edition) S. 62). Ganz allgemein hat die PPC bestätigt, dass sich diese Kategorie auf Ausnahmefälle beschränkt, die über eine bloße Unannehmlichkeit hinausgehen. Insbesondere darf ein PIHBO die Offenlegung nicht allein deshalb verweigern, weil eine große Menge Daten angefordert wird.

([53]) Wie die PPC bestätigt hat, müssen solche Gesetze das in der Verfassung verankerte Recht auf Privatsphäre achten und somit „eine erforderliche und angemessene Beschränkung" darstellen.

des allgemeinen öffentlichen Interesses“ zulässig sind. Die Kategorie der Fälle, in denen die Offenlegung gegen „andere Gesetze oder Verordnungen“ verstoßen würde, mag zwar weit gefasst erscheinen, die Gesetze und Verordnungen, die entsprechende Beschränkungen vorsehen, müssen jedoch das verfassungsmäßige Recht auf Privatsphäre achten und dürfen Beschränkungen nur auferlegen, soweit die Ausübung des betreffenden Rechts „das Gemeinwohl beeinträchtigen“ würde ([54]). Dies erfordert eine Abwägung der betroffenen Interessen.

(85) Nach Artikel 28 Absatz 3 APPI ist die betroffene Person unverzüglich zu informieren, wenn die angeforderten Daten nicht vorhanden sind oder wenn der betreffende PIHBO beschließt, keine Auskunft über die gespeicherte Daten zu erteilen.

(86) Zweitens hat die betroffene Person nach Artikel 29 Absätze 1 und 2 APPI das Recht, die Berichtigung, Ergänzung oder Löschung ihrer gespeicherten personenbezogenen Daten zu verlangen, wenn die Daten unrichtig sind. Nach Erhalt eines solchen Antrags muss der PIHBO „die notwendige Untersuchung durchführen“ und auf der Grundlage des Ergebnisses dieser Untersuchung „eine Berichtigung usw. des Inhalts der gespeicherten Daten vornehmen“.

(87) Drittens hat die betroffene Person nach Artikel 30 Absätze 1 und 2 APPI das Recht, von einem PIHBO die Beendigung der Verwendung personenbezogener Informationen oder die Löschung dieser Informationen zu verlangen, wenn sie unter Verstoß gegen Artikel 16 (Zweckbindung) gehandhabt oder unter Verstoß gegen Artikel 17 APPI in unzulässiger Weise (durch Täuschung, andere unzulässige Mittel oder, im Falle sensibler Daten, ohne Einwilligung) erworben wurden. Ebenso hat die Person nach Artikel 30 Absätze 3 und 4 APPI das Recht, vom PIHBO zu verlangen, die Weitergabe der Informationen an einen Dritten zu beenden, wenn diese gegen Artikel 23 Absatz 1 oder Artikel 24 APPI (Weitergabe an Dritte, einschließlich internationaler Übermittlungen) verstößt.

(88) Wenn der Antrag begründet ist, hat der PIHBO unverzüglich die Verwendung der Daten oder die Weitergabe an Dritte einzustellen, soweit dies zur Behebung der Verletzung erforderlich ist, oder, wenn ein Fall unter eine Ausnahme fällt (insbesondere wenn die Einstellung der Verwendung besonders hohe Kosten verursachen würde) ([55]), die notwendigen alternativen Maßnahmen zum Schutz der Rechte und Interessen der betroffenen Person zu ergreifen.

(89) Anders als das EU-Recht enthalten das APPI und die einschlägigen untergesetzlichen Vorschriften keine gesetzlichen Bestimmungen, die sich speziell mit der Möglichkeit befassen, der Verarbeitung für Direktwerbungszwecke zu widersprechen. Eine solche Verarbeitung wird nach diesem Beschluss jedoch im Zusammenhang mit einer Übermittlung personenbezogener Daten erfolgen, die zuvor in der Europäischen Union erhoben wurden. Nach Artikel 21 Absatz 2 der Verordnung (EU) 2016/679 hat die betroffene Person jederzeit die Möglichkeit, Widerspruch gegen eine Übermittlung von Daten für den Zweck der Verarbeitung für die Direktwerbung einzulegen. Wie in Erwägungsgrund 43 dargelegt, ist ein PIHBO nach der Ergänzenden Vorschrift 3 zudem verpflichtet, die auf der Grundlage des Beschlusses erhaltenen Daten zu dem gleichen Zweck zu verarbeiten, zu dem sie aus der Europäischen Union übermittelt wurden, es sei denn, die betroffene Person willigt in eine Änderung des Verwendungszwecks ein. Ist die Übermittlung zu einem anderen Zweck als dem der Direktwerbung erfolgt, so ist es einem PIHBO in Japan also untersagt, die Daten ohne Einwilligung der betroffenen Person aus der EU zum Zwecke der Direktwerbung zu verarbeiten.

(90) In allen in den Artikeln 28 und 29 APPI genannten Fällen ist der PIHBO verpflichtet, die betroffene Person unverzüglich über das Ergebnis ihrer Anfrage zu informieren und darüber hinaus jede (vollständige oder teilweise) Ablehnung aufgrund der in den Artikeln 27 bis 30 vorgesehenen gesetzlichen Ausnahmen zu begründen (Artikel 31 APPI).

([54]) Artikel 13 der Verfassung wurde vom Obersten Gerichtshof dahin gehend ausgelegt, dass er ein Recht auf Privatsphäre vorsieht (siehe oben die Erwägungsgründe 7 und 8). Zwar kann dieses Recht in Fällen beschränkt werden, in denen es „das Gemeinwohl beeinträchtigt“, der Oberste Gerichtshof hat jedoch in seinem Urteil vom 6. März 2008 (siehe Erwägungsgrund 8) klargestellt, dass jede Beschränkung (die es in dem betreffenden Fall einer Behörde gestattete, personenbezogene Daten zu erheben und zu verarbeiten) gegen das Recht auf Privatsphäre abgewogen werden muss, wobei Faktoren wie die Art der betroffenen Daten, die mit der Verarbeitung dieser Daten verbundenen Risiken für den Einzelnen, die geltenden Garantien und die aus der Verarbeitung erwachsenden Vorteile von öffentlichem Interesse zu berücksichtigen sind. Dies ähnelt sehr der Art der Abwägung, die nach EU-Recht auf der Grundlage der Grundsätze der Erforderlichkeit und der Angemessenheit vorzunehmen ist, wenn es um die Zulässigkeit einer Beschränkung von Datenschutzrechten und -garantien geht.

([55]) Zu weiteren Erläuterungen dieser Ausnahmen siehe Professor Katsuya Uga, *Article by Article Commentary of the revised Act on the Protection of Personal Information*, 2015, S. 217. Ein Beispiel für einen Antrag, der „hohe Kosten“ verursacht, ist der Fall, dass nur einige Namen auf einer langen Liste (z. B. in einem Verzeichnis) unter Verletzung des Zweckbindungsgrundsatzes verarbeitet werden und das Verzeichnis bereits zum Verkauf angeboten wird, sodass der Rückruf dieser Exemplare und das Ersetzen durch neue sehr kostspielig wäre. In diesem Beispiel, bei dem bereits viele Exemplare des Verzeichnisses verkauft wurden und es unmöglich ist, sie alle zurückzuholen, wäre es ebenfalls „schwierig, eine Beendigung der Verwendung durchzusetzen“. In diesen Szenarien könnte etwa die Veröffentlichung oder Verbreitung einer Berichtigungsbekanntmachung zu den „notwendigen alternativen Maßnahmen“ zählen. Durch eine solche Maßnahme werden andere Formen des (gerichtlichen) Rechtsschutzes nicht ausgeschlossen, die bei Verletzung von Persönlichkeitsrechten, bei durch die Veröffentlichung verursachter Rufschädigung (Diffamierung) oder bei Verletzung anderer Interessen in Anspruch genommen werden können.

(91) Was die Voraussetzungen für die Einreichung einer Anfrage betrifft, so ist es dem PIHBO nach Artikel 32 APPI (in Verbindung mit der Kabinettsverordnung) gestattet, geeignete Verfahren festzulegen, auch im Hinblick auf die Informationen, die zur Identifizierung der gespeicherten personenbezogenen Daten erforderlich sind. Nach Absatz 4 des genannten Artikels dürfen die PIHBO jedoch „einem Betroffenen keine übermäßige Belastung" auferlegen. In bestimmten Fällen können die PIHBO auch Gebühren erheben, solange der Betrag „in dem Rahmen bleibt, der unter Berücksichtigung der tatsächlichen Kosten als angemessen angesehen wird" (Artikel 33 APPI).

(92) Schließlich kann die Person gegen die Weitergabe ihrer personenbezogenen Informationen an einen Dritten nach Artikel 23 Absatz 2 APPI Widerspruch einlegen oder die Einwilligung nach Artikel 23 Absatz 1 verweigern (wodurch die Offenlegung verhindert wird, falls keine andere Rechtsgrundlage verfügbar ist). Ebenso kann die betroffene Person die Verarbeitung von Daten zu einem anderen Zweck unterbinden, indem sie sich weigert, die Einwilligung nach Artikel 16 Absatz 1 APPI zu erteilen.

(93) Anders als das EU-Recht enthalten das APPI und die entsprechenden untergesetzlichen Vorschriften 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. Diese Frage wird jedoch in bestimmten in Japan geltenden sektorspezifischen Vorschriften behandelt, die für diese Art der Verarbeitung besonders relevant sind. Dazu gehören auch Sektoren, in denen Unternehmen mit hoher Wahrscheinlichkeit auf die automatisierte Verarbeitung personenbezogener Daten zurückgreifen, um Entscheidungen zu fällen, die Einzelpersonen betreffen (z. B. der Finanzsektor). So wird beispielsweise im Rahmen der im Juni 2017 überarbeiteten „Umfassenden Leitlinien für die Aufsicht über Großbanken" verlangt, dass dem Betreffenden konkrete Erläuterungen zu den Gründen für die Ablehnung eines Antrags auf Abschluss eines Kreditvertrags vorgelegt werden. Diese Vorschriften bieten somit Schutz in den wahrscheinlich eher seltenen Fällen, in denen automatisierte Entscheidungen vom „importierenden" japanischen Unternehmer selbst (und nicht vom „exportierenden" Verantwortlichen in der EU) getroffen werden.

(94) In jedem Fall wird bei personenbezogenen Daten, die in der Europäischen Union erhoben wurden, 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 ([56]). Dazu gehören auch Übermittlungsszenarien, bei denen die Verarbeitung von einem ausländischen (z. B. japanischen) Unternehmer vorgenommen wird, der als Beauftragter (Auftragsverarbeiter) im Namen des Verantwortlichen in der EU (oder als Unter-Auftragsverarbeiter 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 APPI das Schutzniveau der nach diesem Beschluss übermittelten personenbezogenen Daten beeinträchtigt.

### 2.4. **Aufsicht und Durchsetzung**

#### 2.4.1. *Unabhängige Aufsicht*

(95) Um sicherzustellen, dass auch 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.

(96) In Japan ist die Behörde, die für die Überwachung und Durchsetzung des APPI zuständig ist, die PPC. Sie besteht aus einem Vorsitzenden und acht Kommissionsmitgliedern, die vom Premierminister mit Zustimmung der beiden Häuser des Parlaments ernannt werden. Die Amtszeit des Vorsitzenden und der einzelnen Kommissionsmitglieder beträgt fünf Jahre; eine Wiederernennung ist möglich (Artikel 64 APPI). Die Kommissionsmitglieder können nur aus wichtigem Grund in einer begrenzten Zahl von Ausnahmefällen ([57]) entlassen werden und dürfen sich nicht aktiv politisch betätigen. Zudem dürfen die auf Vollzeitbasis tätigen Kommissionsmitglieder nach dem APPI keine anderen vergüteten Tätigkeiten oder Geschäftstätigkeiten ausüben. Alle Kommissionsmitglieder unterliegen auch internen Vorschriften, die ihnen im Falle eines möglichen Interessenkonflikts die Teilnahme an den Beratungen untersagen. Die PPC wird von einem Sekretariat unterstützt, das von einem Generalsekretär geleitet wird und zur Erfüllung der ihr übertragenen Aufgaben eingerichtet wurde (Artikel 70 APPI). Sowohl die Kommissionsmitglieder als auch alle Beamten des Sekretariats sind an strenge Geheimhaltungsregeln gebunden (Artikel 72 und 82 APPI).

([56]) Hingegen wird dies in dem Ausnahmefall, dass der japanische 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 japanischen Unternehmer selbst die Verordnung (EU) 2016/679 (Artikel 3 Absatz 2), sodass er das EU-Datenschutzrecht unmittelbar einhalten muss.

([57]) Nach Artikel 65 APPI ist eine Entlassung gegen den Willen des betreffenden Kommissionsmitglieds nur aus einem der folgenden Gründe möglich: i) Eröffnung eines Insolvenzverfahrens, ii) Verurteilung wegen Verstoßes gegen das APPI oder den „Numbers Use Act", iii) Verurteilung zu einer Freiheitsstrafe ohne Zwangsarbeit oder zu einer noch härteren Strafe, iv) Unfähigkeit aufgrund von psychischen oder physischen Störungen oder Fehlverhalten, die ihm übertragenen Aufgaben zu erfüllen.

(97) Die Befugnisse der PPC, die diese in vollständiger Unabhängigkeit ausübt ([58]), sind im Wesentlichen in den Artikeln 40, 41 und 42 APPI geregelt. Nach Artikel 40 kann die PPC die PIHBO auffordern, über die Verarbeitungsprozesse Bericht zu erstatten oder Unterlagen einzureichen, und auch Kontrollen sowohl vor Ort als auch von Büchern oder anderen Dokumenten durchführen. Soweit es für die Durchsetzung des APPI erforderlich ist, kann die PPC den PIHBO ferner Orientierungshilfen oder Empfehlungen in Bezug auf die Handhabung personenbezogener Informationen zur Verfügung stellen. Von dieser Befugnis nach Artikel 41 APPI hat die PPC bereits nach den Enthüllungen rund um Facebook/Cambridge Analytica Gebrauch gemacht und Orientierungshilfen an Facebook gerichtet.

(98) Insbesondere ist die PPC im Einzelfall befugt, aufgrund einer Beschwerde oder von Amts wegen zur Durchsetzung des APPI und anderer verbindlicher Vorschriften (einschließlich der Ergänzenden Vorschriften) Empfehlungen auszusprechen und Anordnungen zu erlassen. Diese Befugnisse sind in Artikel 42 APPI festgelegt. Während die Absätze 1 und 2 einen zweistufigen Mechanismus vorsehen, nach dem die PPC eine Anordnung (nur) erlassen kann, wenn ihr eine Empfehlung vorausgeht, ermöglicht Absatz 3 in dringenden Fällen den direkten Erlass einer Anordnung.

(99) Obgleich nicht alle Bestimmungen des Kapitels IV Abschnitt 1 des APPI in Artikel 42 Absatz 1 aufgeführt sind — der auch den Anwendungsbereich von Artikel 42 Absatz 2 regelt —, kann dies damit begründet werden, dass einige dieser Bestimmungen keine Verpflichtungen des PIHBO ([59]) betreffen und dass alle wesentlichen Schutzmaßnahmen bereits durch andere Bestimmungen gewährleistet sind, die in dieser Liste enthalten sind. So wird zwar z. B. Artikel 15 (wonach der PIHBO verpflichtet ist, den Verwendungszweck festzulegen und die relevanten personenbezogenen Informationen ausschließlich in diesem Umfang zu verarbeiten) nicht erwähnt, die Nichtbeachtung dieser Bestimmung kann jedoch zu einer Empfehlung führen, die auf einem Verstoß gegen Artikel 16 Absatz 1 beruht (wonach es dem PIHBO untersagt ist, personenbezogene Informationen über das für die Erreichung des Verwendungszwecks erforderliche Maß hinaus zu verarbeiten, es sei denn, er holt die Zustimmung der betroffenen Person ein) ([60]). Eine weitere Bestimmung, die nicht in Artikel 42 Absatz 1 aufgeführt ist, ist Artikel 19 APPI über Datengenauigkeit und -speicherung. Die Nichteinhaltung dieser Bestimmung kann entweder als Verstoß gegen Artikel 16 Absatz 1 oder als Verstoß gegen Artikel 29 Absatz 2 geltend gemacht werden, wenn die betroffene Person die Berichtigung oder Löschung fehlerhafter oder unverhältnismäßig umfangreicher Daten verlangt und der PIHBO sich weigert, dieser Anfrage nachzukommen. Was die *Rechte* der betroffenen Person nach Artikel 28 Absatz 1, Artikel 29 Absatz 1 und Artikel 30 Absatz 1 betrifft, so wird die Aufsicht durch die PPC dadurch gewährleistet, dass ihr Durchsetzungsbefugnisse im Hinblick auf die entsprechenden in diesen Artikeln festgelegten *Pflichten* des PIHBO übertragen werden.

(100) Nach Artikel 42 Absatz 1 APPI kann die PPC, wenn sie einen „Schutzbedarf für die Rechte und Interessen des Einzelnen in Fällen feststellt, in denen ein" PIHBO gegen bestimmt Bestimmungen des APPI „verstoßen hat", eine Empfehlung zur „Unterlassung der Verletzung aussprechen oder andere notwendige Maßnahmen zur Behebung der Verletzung ergreifen". Eine solche Empfehlung ist nicht verbindlich, gibt jedoch den Weg frei für eine verbindliche Anordnung nach Artikel 42 Absatz 2 APPI. Wird der Empfehlung „ohne berechtigten Grund" nicht nachgekommen und stellt die PPC „fest, dass eine schwerwiegende Verletzung der Rechte und Interessen einer Person unmittelbar bevorsteht", kann sie den PIHBO anweisen, im Einklang mit der Empfehlung tätig zu werden.

(101) In den Ergänzenden Vorschriften sind die Durchsetzungsbefugnisse der PPC genauer ausgeführt und umfangreicher gestaltet. Insbesondere wird die PPC in Fällen, in denen es sich um aus der Europäischen Union importierte Daten handelt, die Nichtbeachtung einer Empfehlung seitens des PIHBO nach Artikel 42 Absatz 1 ohne berechtigten Grund immer als schwerwiegende, unmittelbare Verletzung der Rechte und Interessen einer Person im Sinne des Artikels 42 Absatz 2 betrachten und damit als Verletzung, die die Erteilung einer verbindlichen Anordnung rechtfertigt. Darüber hinaus akzeptiert die PPC als „berechtigten Grund" für die Nichtbeachtung einer Empfehlung nur ein „außergewöhnliches Ereignis, [das die Einhaltung verhindert] und außerhalb der Kontrolle des [PIHBO] liegt und nicht in zumutbarer Weise vorhergesehen werden kann (z. B. Naturkatastrophen)", oder Fälle, in denen die Notwendigkeit, im Zusammenhang mit einer Empfehlung Maßnahmen zu ergreifen, „nicht mehr besteht, weil der [PIHBO] alternative Maßnahmen ergriffen hat, mit denen die Verletzung vollständig behoben wurde".

([58]) Siehe Artikel 62 APPI.

([59]) So betreffen einige Bestimmungen beispielsweise freiwillige Maßnahmen des PIHBO (Artikel 32, 33 APPI) oder Verpflichtungen „nach bestmöglichem Bemühen", die an sich nicht durchsetzbar sind (Artikel 31, 35 und 36 Absatz 6 sowie Artikel 39 APPI). Einige Bestimmungen sind nicht an den PIHBO gerichtet, sondern an andere Akteure. Dies ist beispielsweise in Bezug auf Artikel 23 Absatz 4, Artikel 26 Absatz 2 und Artikel 34 APPI der Fall (die Durchsetzung von Artikel 26 Absatz 2 APPI wird jedoch durch die Möglichkeit strafrechtlicher Sanktionen nach Artikel 88 Ziffer i APPI gewährleistet).

([60]) Darüber hinaus wird, wie oben in Erwägungsgrund 48 erläutert, der „Verwendungszweck" in einem Übermittlungskontext vom europäischen Datenexporteur festgelegt, der diesbezüglich an die Verpflichtung nach Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 gebunden ist. Diese Verpflichtung ist durch die zuständige Datenschutzbehörde in der Europäischen Union durchsetzbar.

(102) Die Nichtbeachtung einer Anordnung der PPC gilt nach Artikel 84 APPI als Straftat, und ein für schuldig befundener PIHBO kann mit einem mit Zwangsarbeit verbundenen Freiheitsentzug von bis zu sechs Monaten oder einer Geldstrafe von bis zu 300 000 Yen belegt werden. Darüber hinaus kann nach Artikel 85 Ziffer i APPI die mangelnde Zusammenarbeit mit der PPC oder die Behinderung ihrer Ermittlungen mit einer Geldstrafe von bis zu 300 000 Yen geahndet werden. Diese strafrechtlichen Sanktionen werden zusätzlich zu den Sanktionen angewendet, die wegen erheblicher Verstöße gegen das APPI verhängt werden können (siehe Erwägungsgrund 108).

2.4.2. *Gerichtlicher Rechtsschutz*

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

(104) Vor oder anstelle der Geltendmachung eines behördlichen oder gerichtlichen Rechtsbehelfs kann sich eine Einzelperson dazu entschließen, eine Beschwerde über die Verarbeitung ihrer personenbezogenen Daten an den Verantwortlichen selbst zu richten. Auf der Grundlage des Artikels 35 APPI müssen sich die PIHBO bemühen, solche Beschwerden „angemessen und umgehend" zu bearbeiten, und interne Systeme für die Bearbeitung von Beschwerden einrichten, um dieses Ziel zu erreichen. Darüber hinaus ist die PPC nach Artikel 61 Ziffer ii APPI für „die notwendige Mediation in Bezug auf eine eingereichte Beschwerde und die Zusammenarbeit, die dem die Beschwerde bearbeitenden Unternehmer angeboten wird", verantwortlich, was in beiden Fällen auch für Beschwerden von Ausländern gilt. In diesem Zusammenhang hat der japanische Gesetzgeber auch die Zentralregierung mit der Aufgabe betraut, die „notwendigen Maßnahmen" zu treffen, um die Beilegung von Streitigkeiten durch PIHBO zu ermöglichen und zu erleichtern (Artikel 9), während die lokalen Regierungen in solchen Fällen für eine Mediation sorgen müssen (Artikel 13). In diesem Zusammenhang können Einzelpersonen eine Beschwerde bei einem der mehr als 1 700 Verbraucherzentren einreichen, die von den lokalen Regierungen auf der Grundlage des „Consumer Safety Act" ([61]) eingerichtet wurden; hinzu kommt die Möglichkeit, eine Beschwerde beim National Consumer Affairs Centre of Japan einzureichen. Eine solche Beschwerde ist auch im Zusammenhang mit einem Verstoß gegen das APPI möglich. Nach Artikel 19 des „Basic Consumer Act" ([62]) müssen sich die lokalen Regierungen bemühen, bei Beschwerden eine Mediation einzuleiten und den Parteien das erforderliche Fachwissen zur Verfügung zu stellen. Diese Mechanismen zur Schlichtung von Streitigkeiten scheinen mit einer Schlichtungsrate von 91,2 % für mehr als 75 000 Beschwerdefälle im Jahr 2015 sehr effektiv zu sein.

(105) Verstöße eines PIHBO gegen die Bestimmungen des APPI können zivilrechtliche Klagen sowie Strafverfahren und Sanktionen nach sich ziehen. Erstens kann eine Person, wenn sie der Ansicht ist, dass ihre Rechte nach den Artikeln 28, 29 und 30 APPI verletzt wurden, Unterlassungsansprüche geltend machen, indem sie das Gericht auffordert, einen PIHBO anzuweisen, ihrem Antrag nach einer dieser Bestimmungen nachzukommen, d. h. gespeicherte personenbezogene Daten offenzulegen (Artikel 28), falsche gespeicherte personenbezogene Daten zu berichtigen (Artikel 29) oder die rechtswidrige Verarbeitung oder Weitergabe an Dritte einzustellen (Artikel 30). Eine solche Klage kann ohne Bezugnahme auf Artikel 709 des Bürgerlichen Gesetzbuches ([63]) oder auf das Deliktsrecht ([64]) erhoben werden. Das bedeutet insbesondere, dass der Einzelne keinen Schaden nachweisen muss.

(106) Zweitens kann die betroffene Person, wenn eine mutmaßliche Verletzung nicht die Rechte des Einzelnen nach den Artikeln 28, 29 und 30, sondern allgemeine Datenschutzgrundsätze oder -pflichten des PIHBO betrifft, eine Zivilklage gegen den Unternehmer auf der Grundlage der deliktsrechtlichen Bestimmungen des japanischen Bürgerlichen Gesetzbuches, insbesondere des Artikels 709, einreichen. Zwar ist für eine Klage nach Artikel 709 neben dem Verschulden (Vorsatz oder Fahrlässigkeit) ein Nachweis für einen Schaden erforderlich, dieser kann jedoch nach Artikel 710 des Bürgerlichen Gesetzbuches sowohl materiell als auch immateriell sein. Die Höhe des Schadensersatzes ist nicht begrenzt.

(107) Was die verfügbaren Rechtsbehelfe betrifft, so ist in Artikel 709 des japanischen Bürgerlichen Gesetzbuches eine finanzielle Entschädigung vorgesehen. In der japanischen Rechtsprechung wurde dieser Artikel jedoch so ausgelegt, dass er auch das Recht verleiht, eine einstweilige Verfügung zu erwirken ([65]). Wenn eine betroffene Person somit eine Klage nach Artikel 709 des Bürgerlichen Gesetzbuches einreicht und geltend macht, dass ihre Rechte oder Interessen durch einen Verstoß des Beklagten gegen eine Bestimmung des APPI verletzt wurden, kann diese Klage neben einem Schadensersatzanspruch auch einen Antrag auf Unterlassung umfassen, insbesondere mit dem Ziel, jede rechtswidrige Verarbeitung zu unterbinden.

([61]) Gesetz Nr. 50 vom 5. Juni 2009.
([62]) Gesetz Nr. 60 vom 22. August 2012.
([63]) Artikel 709 des Bürgerlichen Gesetzbuches ist der Hauptklagegrund in Zivilprozessen, in denen Schadensersatzansprüche geltend gemacht werden. Nach dieser Bestimmung ist „eine Person, die vorsätzlich oder fahrlässig Rechte Dritter oder rechtlich geschützte Interessen Dritter verletzt hat, zum Ersatz der daraus resultierenden Schäden verpflichtet".
([64]) Oberstes Gericht Tokyo, Urteil vom 20. Mai 2015 (nicht veröffentlicht); Bezirksgericht Tokyo, Urteil vom 8. September 2014, Westlaw Japan 2014WLJPCA09088002. Siehe auch Artikel 34 Absätze 1 und 3 APPI.
([65]) Siehe Oberster Gerichtshof, Urteil vom 24. September 2002 (Hanrei Times Vol. 1106, S. 72).

(108) Drittens hat eine betroffene Person neben zivilrechtlichen (deliktsrechtlichen) Rechtsbehelfen auch die Möglichkeit, bei einem Staatsanwalt oder einem Kriminalbeamten Beschwerde gegen APPI-Verletzungen einzureichen, die zu strafrechtlichen Sanktionen führen können. Kapitel VII des APPI enthält eine Reihe von strafrechtlichen Bestimmungen. Die wichtigste dieser Bestimmungen (Artikel 84) betrifft die Nichtbeachtung von Anordnungen der PPC nach Artikel 42 Absätze 2 und 3 durch den PIHBO. Kommt ein Unternehmer einer Anordnung der PPC nicht nach, kann der PPC-Vorsitzende (sowie jeder andere Regierungsbeamte) ([66]) den Fall an die Staatsanwaltschaft oder die Kriminalpolizei weiterleiten und so die Einleitung eines Strafverfahrens anstoßen. Ein Verstoß gegen eine Anordnung der PPC wird mit einem mit Zwangsarbeit verbundenen Freiheitsentzug von bis zu sechs Monaten oder mit einer Geldstrafe von bis zu 300 000 Yen geahndet. Weitere Bestimmungen des APPI, die Sanktionen bei APPI-Verstößen im Hinblick auf die Rechte und Interessen von betroffenen Personen vorsehen, sind Artikel 83 APPI (über die „Weitergabe oder heimliche Verwendung" einer Datenbank mit personenbezogenen Informationen „zum Zwecke der Erzielung … illegaler Gewinne") und Artikel 88 Ziffer i APPI (über die Unterlassung einer ordnungsgemäßen Unterrichtung des PIHBO durch einen Dritten, wenn dieser nach Artikel 26 Absatz 1 APPI personenbezogene Daten erhält, insbesondere über die Einzelheiten des vorherigen eigenen Erwerbs dieser Daten durch den Dritten). Das anwendbare Strafmaß für solche Verstöße gegen das APPI sind jeweils ein mit Zwangsarbeit verbundener Freiheitsentzug von bis zu einem Jahr oder eine Geldstrafe von bis zu 500 000 Yen (im Falle von Artikel 83) oder eine Geldbuße von bis zu 100 000 Yen (im Falle von Artikel 88 Ziffer i). Zwar dürfte bereits die Androhung einer strafrechtlichen Sanktion eine starke abschreckende Wirkung auf die die Verarbeitungsvorgänge des PIHBO leitende Geschäftsführung und die die Daten handhabenden Einzelpersonen haben, jedoch stellt Artikel 87 APPI klar, dass, wenn ein Vertreter, Arbeitnehmer oder sonstiger Mitarbeiter einer juristischen Person einen Verstoß nach den Artikeln 83 bis 85 APPI begangen hat, „der Täter bestraft und eine in den einschlägigen Artikeln festgelegte Geldstrafe gegen die genannte juristische Person verhängt wird". In diesem Fall kann sowohl der Arbeitnehmer als auch das Unternehmen mit Sanktionen bis zum vollen Höchstbetrag belegt werden.

(109) Schließlich können Einzelpersonen auch Rechtsbehelfe gegen die Handlungen oder Unterlassungen der PPC einlegen. In dieser Hinsicht bietet das japanische Recht mehrere Möglichkeiten der behördlichen und gerichtlichen Rechtsbehelfe.

(110) Ist eine Einzelperson mit der Vorgehensweise der PPC nicht einverstanden, so kann sie nach dem Verwaltungsbeschwerdeprüfungsgesetz ([67]) einen verwaltungsbehördlichen Rechtsbehelf einlegen. Umgekehrt kann eine Einzelperson, wenn die PPC ihrer Ansicht nach hätte handeln sollen, dies aber nicht getan hat, die PPC nach Artikel 36-3 dieses Gesetzes ersuchen, eine Anordnung zu erlassen oder eine behördliche Richtlinie bereitzustellen, wenn sie der Ansicht ist, dass „eine Anordnung oder eine behördliche Richtlinie, die für die Behebung der Verletzung erforderlich ist, nicht erlassen oder durchgesetzt worden ist".

(111) Was Rechtsbehelfe angeht, so kann eine Einzelperson, die mit einer behördlichen Verfügung der PPC nicht einverstanden ist, nach dem Verwaltungsrechtsstreitigkeitengesetz eine Mandamus-Klage ([68]) erheben, mit der sie das Gericht ersucht, die PPC anzuweisen, weitere Maßnahmen zu treffen ([69]). In bestimmten Fällen kann das Gericht auch eine einstweilige Anordnung im Mandamus-Verfahren erlassen, um einen nicht wiedergutzumachenden Schaden zu verhindern ([70]). Darüber hinaus kann eine Einzelperson nach demselben Gesetz die Aufhebung eines Beschlusses der PPC beantragen ([71]).

(112) Schließlich kann eine Person auch eine Klage auf staatlichen Schadensersatz gegen die PPC nach Artikel 1 Absatz 1 des Staatshaftungsgesetzes erheben, wenn ihr ein Schaden entstanden ist, weil eine von der PPC an einen Unternehmer gerichtete Anordnung rechtswidrig war oder die PPC ihre Befugnisse nicht ausgeübt hat.

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

(113) Die Kommission hat auch die Beschränkungen und Garantien bewertet, einschließlich der Kontrollmechanismen und der Rechtsbehelfe für den Einzelnen, die nach japanischem Recht in Bezug auf die Erhebung und nachfolgende Verwendung personenbezogener Daten, die Unternehmern in Japan von Behörden im öffentlichen Interesse übermittelt werden, insbesondere zur Strafverfolgung und zur nationalen Sicherheit (im Folgenden „staatlicher Zugriff"), verfügbar sind. In diesem Zusammenhang hat die japanische Regierung der Kommission offizielle Erklärungen, Zusicherungen und Verpflichtungen zukommen lassen, die auf höchster Minister- und Behördenebene unterzeichnet wurden und in Anhang II dieses Beschlusses enthalten sind.

([66]) Artikel 239 Absatz 2 Strafprozessordnung.
([67]) Gesetz Nr. 160 aus dem Jahr 2014.
([68]) Artikel 37-2 des Verwaltungsrechtsstreitigkeitengesetzes.
([69]) Nach Artikel 3 Absatz 6 des Verwaltungsrechtsstreitigkeitengesetzes bezeichnet der Begriff „Mandamus-Klage" eine Klage, mit der eine Anordnung des Gerichts gegen eine Verwaltungsbehörde beantragt wird, eine originäre Verwaltungsentscheidung zu treffen, die sie hätte treffen „sollen", jedoch nicht getroffen hat.
([70]) Artikel 37-5 des Verwaltungsrechtsstreitigkeitengesetzes.
([71]) Kapitel II Abschnitt 1 des Verwaltungsrechtsstreitigkeitengesetzes.

### 3.1. **Allgemeiner Rechtsrahmen**

(114) Als eine Form der Ausübung öffentlicher Gewalt muss der staatliche Zugriff in Japan in voller Übereinstimmung mit dem Gesetz erfolgen (Legalitätsprinzip). In diesem Zusammenhang enthält die japanische Verfassung Bestimmungen, die die Erhebung personenbezogener Daten durch Behörden beschränken und präzisieren. Wie bereits in Bezug auf die Verarbeitung durch Unternehmer erwähnt, hat der japanische Oberste Gerichtshof, gestützt auf Artikel 13 der Verfassung, der unter anderem das Recht auf Freiheit schützt, das Recht auf Privatsphäre und Datenschutz anerkannt ([72]). Ein wichtiger Aspekt dieses Rechts ist, dass personenbezogene Informationen nicht ohne Zustimmung des Betroffenen an Dritte weitergegeben werden dürfen ([73]). Daraus ergibt sich ein Recht auf den wirksamen Schutz personenbezogener Daten vor Missbrauch und (insbesondere) rechtswidrigem Zugriff. Zusätzlicher Schutz wird durch Artikel 35 der Verfassung über das Recht aller Personen auf die Sicherheit ihrer Häuser, Papiere und Güter gewährleistet, der von den Behörden verlangt, für sämtliche „Durchsuchungen und Beschlagnahmen" einen Gerichtsbeschluss zu erwirken, der aus „hinreichendem Grund" ([74]) erlassen wird. In seinem Urteil vom 15. März 2017 (Rechtssache GPS) hat der Oberste Gerichtshof präzisiert, dass ein solcher Gerichtsbeschluss immer dann erforderlich ist, wenn der Staat in einer Weise in die Privatsphäre eingreift („eindringt"), die den Willen des Einzelnen unterdrückt, wenn also „Zwangsermittlungen" durchgeführt werden. Ein Richter darf einen solchen Beschluss nur aufgrund eines konkreten Verdachts auf Straftaten erlassen, d. h. wenn ihm Beweismittel vorgelegt wurden, auf deren Grundlage davon ausgegangen werden kann, dass die von den Ermittlungen betroffene Person eine Straftat begangen hat ([75]). Folglich haben die japanischen Behörden keine rechtliche Befugnis, personenbezogene Informationen mittels Zwangsmaßnahmen zu erheben, wenn noch kein Gesetzesverstoß vorliegt ([76]), z. B. um eine Straftat oder eine andere Sicherheitsgefährdung zu verhindern (wie dies bei Ermittlungen aus Gründen der nationalen Sicherheit der Fall ist).

(115) Unter dem Vorbehalt des Rechtsprinzips muss jede Datenerhebung im Rahmen obligatorischer Ermittlungen gesondert gesetzlich genehmigt werden (wie z. B. in Artikel 197 Absatz 1 der Strafprozessordnung („StPO") über die Zwangserhebung von Informationen zum Zwecke strafrechtlicher Ermittlungen vorgesehen). Diese Anforderung gilt auch für den Zugriff auf elektronische Informationen.

(116) Darüber hinaus garantiert Artikel 21 Absatz 2 der Verfassung die Geheimhaltung sämtlicher Kommunikationsmittel, wobei Beschränkungen nur durch Rechtsvorschriften aus Gründen des öffentlichen Interesses zulässig sind. Nach Artikel 4 des „Telecommunications Business Act", wonach die Vertraulichkeit der von einem Telekommunikationsdiensteanbieter verwalteten Kommunikation nicht verletzt werden darf, wird diese Geheimhaltungspflicht auf der Ebene des geltenden Rechts umgesetzt. Dies wurde als Verbot der Offenlegung von Kommunikationsinformationen ausgelegt, sofern nicht die Zustimmung der Nutzer oder eine der ausdrücklichen Ausnahmen von der strafrechtlichen Haftung nach dem Strafgesetzbuch vorliegt ([77]).

(117) Die Verfassung garantiert ferner das Recht auf Zugang zu den Gerichten (Artikel 32) und das Recht, den Staat auf Schadensersatz zu verklagen, wenn eine Person durch die rechtswidrige Handlung eines Beamten Schaden erlitten hat (Artikel 17).

(118) Was insbesondere das Recht auf Datenschutz betrifft, so sind in Kapitel III, Abschnitte 1, 2 und 3 des APPI allgemeine Grundsätze festgelegt, die alle Sektoren umfassen, unter anderem auch den öffentlichen Sektor. So sieht insbesondere Artikel 3 APPI vor, dass alle personenbezogenen Informationen in Übereinstimmung mit dem Grundsatz der Achtung der Persönlichkeit des Einzelnen zu handhaben sind. Sobald personenbezogene Informationen, auch als Teil elektronischer Aufzeichnungen, von Behörden ([78]) erfasst („empfangen") wurden, unterliegt ihre

([72]) Siehe z. B. Oberster Gerichtshof, Urteil vom 12. September 2003, Az. 1656 (2002 (Ju)). Insbesondere hob der Oberste Gerichtshof hervor, dass „jeder Einzelne die Freiheit hat, seine personenbezogenen Informationen vor der Offenlegung gegenüber Dritten und der Veröffentlichung ohne triftigen Grund zu schützen".

([73]) Oberster Gerichtshof, Urteil vom 6. März 2008 (Juki-net).

([74]) Ein „hinreichender Grund" liegt nur dann vor, wenn davon ausgegangen wird, dass die betroffene Person (Verdächtiger, Angeklagter) eine Straftat begangen hat und die Durchsuchung und Beschlagnahme für die Strafverfolgung erforderlich ist. Siehe Oberster Gerichtshof, Urteil vom 18. März 1969, Az. 100 (1968 (Shi)).

([75]) Siehe Artikel 156 Absatz 1 Strafprozessordnung.

([76]) Es sei jedoch darauf hingewiesen, dass das Gesetz über die Bekämpfung der organisierten Kriminalität und die Überwachung illegal erworbener Vermögenswerte (Act on Punishment of Organized Crimes and Control of Crime Proceeds) vom 15. Juni 2017 einen neuen Straftatbestand schafft, der die Vorbereitung von Terrorakten und bestimmte andere Formen der organisierten Kriminalität unter Strafe stellt. Ermittlungen dürfen nur eingeleitet werden, wenn der konkrete, auf Beweisen beruhende Verdacht besteht, dass alle drei notwendigen Tatbestandsmerkmale (Beteiligung einer Gruppe der organisierten Kriminalität, „Planung" und „Vorbereitung für die Umsetzung" der Straftat) erfüllt sind. Siehe auch z. B. die Artikel 38-40 des Gesetzes zur Prävention subversiver Aktivitäten (Subversive Activities Prevention Act) (Gesetz Nr. 240 vom 21. Juli 1952).

([77]) Artikel 15 Absatz 8 der Leitlinien über den Schutz personenbezogener Informationen im Telekommunikationssektor.

([78]) Verwaltungsorgane im Sinne des Artikels 2 Absatz 1 APPIHAO. Nach Auskunft der der japanischen Regierung fallen alle Behörden, mit Ausnahme der Präfekturpolizei, unter die Definition der Verwaltungsorgane. Gleichzeitig arbeitet die Präfekturpolizei innerhalb des Rechtsrahmens, der durch die Präfekturverordnungen zum Schutz personenbezogener Informationen festgelegt ist (siehe Artikel 11 APPI und die „Grundlegende Richtlinie"); diese enthalten Bestimmungen zum Schutz personenbezogener Informationen, die denen des APPIHAO gleichwertig sind. Siehe Anhang II Abschnitt I Buchstabe B. Wie die PPC erläutert hat, müssen diese Verordnungen nach der „Grundlegenden Richtlinie" auf der Grundlage des Inhalts des APPIHAO erlassen werden und gibt das MIC Bekanntmachungen heraus, in denen den lokalen Regierungen die hierfür erforderlichen Anweisungen erteilt werden. Die PPC weist mit Nachdruck darauf hin, dass „innerhalb dieser Grenzen die Verordnung zum Schutz personenbezogener Informationen in jeder Präfektur auf der Grundlage der ‚Grundlegenden Richtlinie' und des Inhalts der Bekanntmachungen zu erlassen ist."

Verarbeitung dem APPIHAO ([79]). Dazu gehört grundsätzlich ([80]) auch die Verarbeitung personenbezogener Informationen zu strafrechtlichen Zwecken oder zur Wahrung der nationalen Sicherheit. Das APPIHAO sieht unter anderem vor, dass Behörden i) personenbezogene Informationen nur insoweit speichern dürfen, als dies für die Erfüllung ihrer Aufgaben erforderlich ist, ii) diese Informationen nicht ohne Begründung zu einem „ungerechtfertigten" Zweck verwenden oder an Dritte weitergeben dürfen, iii) den Zweck angeben und diesen nicht über das Maß hinaus ändern dürfen, das vernünftigerweise als relevant für den ursprünglichen Zweck angesehen werden kann (Zweckbindung), iv) die gespeicherten personenbezogenen Informationen grundsätzlich nicht zu anderen Zwecken verwenden oder einem Dritten zur Verfügung stellen dürfen und, wenn sie dies für erforderlich halten, den Zweck oder die Art der Verwendung durch Dritte beschränken, v) sich bemühen, die Richtigkeit der Informationen zu gewährleisten (Datenqualität), vi) die erforderlichen Maßnahmen für die ordnungsgemäße Verwaltung der Informationen und zur Vermeidung von Veröffentlichung, Verlust oder Beschädigung (Datensicherheit) ergreifen, und vii) sich bemühen, alle Beschwerden über die Verarbeitung der Informationen ordnungsgemäß und zügig zu bearbeiten ([81]).

### 3.2. **Zugriff und Verwendung durch japanische Behörden für Strafverfolgungszwecke**

(119) Das japanische Recht enthält eine Reihe von Beschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten für Strafverfolgungszwecke sowie Aufsichts- und Rechtsbehelfsverfahren, die ausreichende Garantien bieten, damit diese Daten wirksam vor unrechtmäßigen Eingriffen und Missbrauch geschützt werden können.

#### 3.2.1. *Rechtsgrundlage und anwendbare Beschränkungen/Garantien*

(120) Im japanischen Rechtsrahmen ist die Erhebung elektronischer Informationen für Strafverfolgungszwecke auf der Grundlage eines Gerichtsbeschlusses (Zwangserhebung) oder eines Ersuchens um freiwillige Offenlegung zulässig.

##### 3.2.1.1. Zwangsermittlungen auf der Grundlage eines Gerichtsbeschlusses

(121) Wie in Erwägungsgrund 115 dargelegt, muss jede Datenerhebung im Rahmen von Zwangsermittlungen gesondert gesetzlich genehmigt sein und darf nur auf der Grundlage eines Gerichtsbeschlusses erfolgen, der „aus hinreichendem Grund erlassen wurde" (Artikel 35 der Verfassung). Was Ermittlungen in Strafsachen betrifft, so spiegelt sich diese Anforderung in den Bestimmungen der StPO wider. Nach Artikel 197 Absatz 1 StPO sind Zwangsmaßnahmen „nur dann anzuwenden, wenn in der StPO besondere Bestimmungen vorgesehen sind". In Bezug auf die Erfassung elektronischer Informationen sind die einzigen relevanten ([82]) Rechtsgrundlagen in dieser Hinsicht Artikel 218 StPO (Durchsuchung und Beschlagnahme) und Artikel 222-2 StPO, wonach Zwangsmaßnahmen zur Abhörung der elektronischen Kommunikation ohne Zustimmung einer der Parteien auf der Grundlage anderer Gesetze, nämlich des Gesetzes über die Abhörung zur Strafverfolgung („Abhörgesetz"), durchgeführt werden. In beiden Fällen ist ein Gerichtsbeschluss erforderlich.

(122) So kann nach Artikel 218 Absatz 1 StPO ein Staatsanwalt, ein Staatsanwaltsgehilfe oder ein Kriminalbeamter, wenn dies für die Aufklärung einer Straftat erforderlich ist, eine Durchsuchung oder Beschlagnahme (auch von Aufzeichnungen) nach einem von einem Richter im Voraus ausgestellten Gerichtsbeschluss durchführen ([83]). Ein solcher Beschluss muss unter anderem den Namen des Verdächtigen oder Beschuldigten, Angaben zur vorgeworfenen Straftat ([84]), zu den zu beschlagnahmenden elektromagnetischen Aufzeichnungen und zu dem/den zu durchsuchenden „Ort oder Gegenständen" enthalten (Artikel 219 Absatz 1 StPO).

([79]) Personenbezogene Informationen, die von Beamten eines Verwaltungsorgans bei der Ausübung ihrer Aufgaben erlangt und von diesem Verwaltungsorgan zu organisatorischen Zwecken gespeichert werden, sind „gespeicherte personenbezogene Informationen" im Sinne des Artikels 2 Absatz 3 APPIHAO, sofern sie in „Verwaltungsdokumenten" erfasst sind. Dazu gehören auch elektronische Informationen, die von diesen Stellen erhoben und dann weiterverarbeitet werden, da die Definition von „Verwaltungsdokumenten" in Artikel 2 Absatz 2 APPIHAO (Gesetz Nr. 42 aus dem Jahr 1999) elektromagnetische Aufzeichnungen umfasst.

([80]) Nach Artikel 53-2 StPO ist Kapitel IV des APPIHAO jedoch nicht für „Dokumente über Gerichtsverfahren" vorgesehen, die nach den erhaltenen Informationen elektronische Informationen umfassen, die aufgrund von Gerichtsbeschlüssen oder Ersuchen um freiwillige Zusammenarbeit im Rahmen strafrechtlicher Ermittlungen erlangt wurden. Auch in Bezug auf Informationen, die im Rahmen der nationalen Sicherheit erfasst werden, können Einzelpersonen ihre Rechte aus dem APPIHAO nicht erfolgreich geltend machen, wenn der Leiter der Behörde „berechtigte Gründe" hat, davon auszugehen, dass die Offenlegung „der nationalen Sicherheit schaden könnte" (siehe Artikel 14 Ziffer iv). Allerdings müssen die Behörden nach Möglichkeit zumindest eine teilweise Offenlegung gewähren (Artikel 15).

([81]) Siehe die konkreten Hinweise auf das APPIHAO in Anhang II Abschnitt II Buchstabe A Nummer 1 Buchstabe b Nummer 2.

([82]) Obgleich nach Artikel 220 StPO eine Durchsuchung und Beschlagnahme „vor Ort" ohne Gerichtsbeschluss zulässig ist, wenn ein Staatsanwalt, ein Staatsanwaltsgehilfe oder ein Kriminalbeamter einen verdächtigen/offenkundigen Straftäter festnimmt, ist dies im Rahmen einer Übermittlung und damit im Sinne dieses Beschlusses nicht von Belang.

([83]) Nach Artikel 222 Absatz 1 in Verbindung mit Artikel 110 StPO ist demjenigen, der sich der Maßnahme unterziehen soll, der Gerichtsbeschluss für die Durchsuchung bzw. Beschlagnahme von Aufzeichnungen vorzulegen.

([84]) Siehe auch Artikel 189 Absatz 2 StPO, wonach ein Kriminalbeamter den Täter und Beweise für die Tat ermitteln muss, „wenn er der Meinung ist, dass eine Straftat begangen wurde". Ebenso sieht Artikel 155 Absatz 1 der japanischen Strafprozessordnung vor, dass ein schriftliches Ersuchen um einen Gerichtsbeschluss unter anderem die „vorgeworfene Straftat" und eine „Zusammenfassung der Fakten der Straftat" enthalten muss.

(123) Was das das Abfangen von Kommunikation betrifft, so erlaubt Artikel 3 des Abhörgesetzes solche Maßnahmen nur unter strengen Auflagen. Insbesondere müssen die Behörden vorab einen Gerichtsbeschluss erwirken, der nur für die Aufklärung bestimmter schwerer Straftaten (die im Anhang des Gesetzes aufgeführt sind) ([85]) und nur dann erlassen werden darf, wenn es „äußerst schwierig ist, auf andere Weise den Täter zu ermitteln bzw. die Situation/Details der Begehung zu klären" ([86]). Nach Artikel 5 des Abhörgesetzes wird der Gerichtsbeschluss für einen begrenzten Zeitraum erlassen und kann vom Richter mit zusätzlichen Auflagen versehen werden. Darüber hinaus sind im Abhörgesetz weitere Garantien vorgesehen, zum Beispiel die notwendige Anwesenheit von Zeugen (Artikel 12 und 20), das Verbot, die Kommunikation bestimmter privilegierter Gruppen (wie Ärzte oder Rechtsanwälte) abzuhören (Artikel 15), die Pflicht, die Abhörmaßnahmen auch vor Ablauf der Geltungsdauer des Gerichtsbeschlusses zu beenden, wenn sie nicht mehr gerechtfertigt sind (Artikel 18), oder die allgemeine Pflicht, innerhalb von dreißig Tagen nach Beendigung der Abhörmaßnahmen die betroffene Einzelperson zu unterrichten und ihr Zugang zu den Aufzeichnungen zu gewähren (Artikel 23 und 24).

(124) Bei allen Zwangsermittlungen auf der Grundlage eines Gerichtsbeschlusses darf die Durchsuchung nur in dem Umfang durchgeführt werden, der „für die Erreichung ihres Ziels erforderlich ist" — wenn also die mit der Durchsuchung verfolgten Ziele nicht auf andere Weise erreicht werden können (Artikel 197 Absatz 1 StPO). Zwar sind die Kriterien für die Beurteilung der Notwendigkeit im Gesetz nicht weiter spezifiziert, der japanische Oberste Gerichtshof hat jedoch entschieden, dass der Richter, der einen Gerichtsbeschluss erlässt, eine Gesamtbewertung vornehmen sollte, bei der insbesondere Folgendes zu berücksichtigen ist: i) die Schwere der Straftat und die Art ihrer Begehung, ii) der Wert und die Bedeutung der als Beweismittel zu beschlagnahmenden Objekte, iii) die Wahrscheinlichkeit (das Risiko), dass Beweise versteckt oder vernichtet werden, und iv) das Ausmaß, in dem die Beschlagnahme zu einem Schaden für die betroffene Person führen könnte ([87]).

#### 3.2.1.2. Ersuchen um freiwillige Offenlegung auf der Grundlage eines „Anfrageformulars"

(125) Im Rahmen ihrer Zuständigkeit können Behörden elektronische Informationen auch auf der Grundlage von Ersuchen um freiwillige Offenlegung erheben. Hierbei handelt es sich um eine nicht obligatorische Form der Zusammenarbeit, bei der das Ersuchen nicht gerichtlich durchgesetzt werden kann ([88]), sodass die Behörden von der Pflicht befreit sind, einen Gerichtsbeschluss zu erwirken.

(126) Soweit sich ein solches Ersuchen an einen Unternehmer richtet und personenbezogene Informationen betrifft, muss der Unternehmer die Anforderungen des APPI erfüllen. Nach Artikel 23 Absatz 1 APPI dürfen Unternehmer personenbezogene Informationen nur in bestimmten Fällen ohne Einwilligung des Betroffenen Dritten gegenüber offenlegen, unter anderem, wenn die Offenlegung „auf Gesetzen und Verordnungen beruht" ([89]). Im Bereich der Strafverfolgung ist Rechtsgrundlage für solche Anfragen Artikel 197 Absatz 2 StPO, nach dem „private Organisationen aufgefordert werden können, über wesentliche Aspekte der Ermittlungen Bericht zu erstatten." Da ein solches „Anfrageformular" nur im Rahmen strafrechtlicher Ermittlungen zulässig ist, wird dabei stets ein konkreter Verdacht auf eine bereits begangene Straftat vorausgesetzt ([90]). Da solche Ermittlungen in der Regel von der Präfekturpolizei durchgeführt werden, gelten darüber hinaus die Beschränkungen nach Artikel 2 Absatz 2 des Polizeigesetzes ([91]). Danach sind die Tätigkeiten der Polizei „streng begrenzt" auf die Erfüllung ihrer Aufgaben und Pflichten (d. h. die Verhütung, Bekämpfung und Aufklärung von Straftaten). Darüber hinaus muss die Polizei bei der Erfüllung ihrer Aufgaben unparteiisch, unvoreingenommen und fair handeln und darf ihre Befugnisse niemals „in einer Weise missbrauchen, die den in der japanischen Verfassung garantierten Rechten und Freiheiten des Einzelnen zuwiderläuft" (zu denen, wie bereits erwähnt, das Recht auf Privatsphäre und Datenschutz gehört) ([92]).

(127) Insbesondere im Hinblick auf Artikel 197 Absatz 2 StPO hat die Nationale Polizeibehörde (*National Police Agency* — NPA) als unter anderem für alle die Kriminalpolizei betreffenden Angelegenheiten zuständige

([85]) Der Anhang sieht neun Arten von Straftaten vor, z. B. Straftaten im Zusammenhang mit Drogen und Schusswaffen, Menschenhandel und organisiertem Mord. Es sei darauf hingewiesen, dass der neu eingeführte Straftatbestand der „Vorbereitung von Terrorakten und anderen Formen der organisierten Kriminalität" (siehe Fußnote 76) nicht in diese abschließende Liste aufgenommen wurde.

([86]) Darüber hinaus muss die Ermittlungsbehörde nach Artikel 23 des Abhörgesetzes die Person, deren Kommunikation abgehört (und damit in das Abhörprotokoll aufgenommen) wurde, schriftlich über diese Tatsache informieren.

([87]) Siehe Anhang II Abschnitt I Buchstabe A Nummer 1 Buchstabe b Nummer 1.

([88]) Nach den vorliegenden Informationen haben Unternehmer, die nicht kooperieren, nach keinem Gesetz negative Folgen (einschließlich Sanktionen) zu befürchten. Siehe Anhang II Abschnitt II Buchstabe A Nummer 2 Buchstabe a.

([89]) Nach den PPC-Leitlinien (General Rule Edition) bildet Artikel 23 Absatz 1 Ziffer i die Grundlage für die Offenlegung personenbezogener Informationen aufgrund eines Gerichtsbeschlusses (Artikel 218 StPO) und eines „Anfrageformulars" (Artikel 197 Absatz 2 StPO).

([90]) Dies bedeutet, dass das „Anfrageformular" nur zur Erhebung von Informationen im Einzelfall verwendet werden darf, nicht aber zur Erhebung personenbezogener Daten in großem Umfang. Siehe auch Anhang II Abschnitt I Buchstabe A Nummer 2 Buchstabe b Nummer 1.

([91]) Sowie die Vorschriften der Präfekturkommission für öffentliche Sicherheit, siehe Artikel 189 Absatz 1 StPO.

([92]) Siehe auch Artikel 3 des Polizeigesetzes, wonach der von allen Polizeibeamten geleistete Amtseid besagt, dass sie „der Verpflichtung zur Verteidigung und Aufrechterhaltung der Verfassung und der Gesetze Japans treu sind und ihre Aufgaben unparteiisch, gerecht, fair und unvoreingenommen erfüllen".

Zentralbehörde der Präfekturpolizei ([93]) Weisungen zur „ordnungsgemäßen Verwendung schriftlicher Anfragen in Ermittlungsangelegenheiten“ erteilt. Nach dieser Mitteilung müssen Anfragen anhand eines vorher festgelegten Formulars („Formular Nr. 49“ bzw. „Anfrageformular“) ([94]) gestellt werden und Aufzeichnungen „über bestimmte Ermittlungen“ betreffen; die angeforderten Informationen müssen „für [diese] Ermittlungen unbedingt erforderlich“ sein. In jedem Fall muss der leitende Ermittler „die Notwendigkeit, den Inhalt usw. [der] jeweiligen Anfrage in vollem Umfang prüfen“ und die interne Zustimmung eines hochrangigen Beamten einholen.

(128) Darüber hinaus hat der japanische Oberste Gerichtshof in zwei Urteilen aus den Jahren 1969 und 2008 ([95]) Beschränkungen in Bezug auf nicht obligatorische Maßnahmen festgelegt, die einen Eingriff in das Recht auf Privatsphäre darstellen ([96]). Der Gerichtshof war insbesondere der Ansicht, dass derartige Maßnahmen „angemessen“ sein und sich innerhalb „allgemein zulässiger Grenzen“ bewegen müssen, d. h. sie müssen für die Ermittlung eines Verdächtigen (Beweisaufnahme) notwendig sein und „mit geeigneten Methoden zur Erreichung des Zwecks [der] Ermittlungen durchgeführt werden“ ([97]). Die Urteile zeigen, dass dies eine Prüfung der Verhältnismäßigkeit unter Berücksichtigung aller Umstände des Falles erfordert (z. B. des Ausmaßes des Eingriffs in das Recht auf Privatsphäre, einschließlich der Erwartungen hinsichtlich der Privatsphäre, der Schwere der Straftat, der Wahrscheinlichkeit, verwertbare Beweise zu erhalten, der Relevanz dieser Beweise, möglicher alternativer Untersuchungsmethoden usw.) ([98]).

(129) Abgesehen von diesen Beschränkungen für die Ausübung der öffentlichen Gewalt wird von Unternehmern erwartet, dass sie selbst die Notwendigkeit und „Rationalität“ der Weitergabe an einen Dritten überprüfen („bestätigen“) ([99]). Dazu gehört auch die Frage, ob ihnen die Zusammenarbeit dem Gesetz nach untersagt ist. Derart widersprüchliche rechtliche Verpflichtungen können sich insbesondere aus Geheimhaltungsverpflichtungen wie etwa nach Artikel 134 Strafgesetzbuch (über das Verhältnis zwischen einem Arzt, Anwalt, Priester usw. und seinem Gegenüber) ergeben. Ferner muss „jede Person, die im Telekommunikationsbereich tätig ist, während ihrer Tätigkeit die Geheimnisse anderer wahren, die ihr in Bezug auf die vom Telekommunikationsdiensteanbieter verwaltete Kommunikation bekannt geworden sind“ (Artikel 4 Absatz 2 des Telekommunikationsgesetzes). Diese Verpflichtung wird durch die in Artikel 179 des Telekommunikationsgesetzes festgelegte Sanktion gestützt, nach dem jede Person, die gegen den Grundsatz der Geheimhaltung von Kommunikation, die von einem Telekommunikationsdiensteanbieter verwaltet wird, verstoßen hat, sich einer Straftat schuldig macht und mit einem mit Zwangsarbeit verbundenen Freiheitsentzug von bis zu zwei Jahren oder mit einer Geldstrafe von bis zu einer Million Yen bestraft werden muss ([100]). Auch wenn diese Vorschrift nicht uneingeschränkt gilt und insbesondere Maßnahmen erlaubt, die gegen die Geheimhaltung von Kommunikation verstoßen, wenn es sich um „gerechtfertigte Handlungen“ im Sinne des Artikels 35 Strafgesetzbuch ([101]) handelt, so gilt diese Ausnahme jedoch nicht für die Beantwortung nicht obligatorischer Ersuchen von Behörden um Offenlegung elektronischer Informationen nach Artikel 197 Absatz 2 StPO.

3.2.1.3. Weitere Verwendung der erhobenen Daten

(130) Nach der Erhebung durch die japanischen Behörden fallen personenbezogene Informationen in den Anwendungsbereich des APPIHAO. Dieses Gesetz regelt die Handhabung (Verarbeitung) „gespeicherter personenbezogener

([93]) Nach Artikel 30 Absatz 1 und Artikel 31 Absatz 2 des Polizeigesetzes „leitet und beaufsichtiget“ der Generaldirektor der Regionalen Polizeibüros (lokale Dienststellen der NPA) die Präfekturpolizei.

([94]) Auf dem Anfrageformular müssen auch die Kontaktinformationen des „Bearbeiters“ („Name der Abteilung [Position], Name des Bearbeiters, Telefonnummer des Büros, Durchwahl usw.“) angegeben werden.

([95]) Oberster Gerichtshof, Urteil vom 24. Dezember 1969 (1965(A) 1187); Urteil vom 15. April 2008 (2007(A) 839).

([96]) Zwar betrafen diese Urteile nicht die Erhebung elektronischer Informationen, die japanische Regierung hat jedoch präzisiert, dass sich die Anwendung der vom Obersten Gerichtshof entwickelten Kriterien auf alle Eingriffe von Behörden in das Recht auf Privatsphäre erstreckt, auch auf „freiwillige Ermittlungen“, und dass die Kriterien somit für die japanischen Behörden auch verbindlich sind, wenn sie um freiwillige Offenlegung von Informationen ersuchen. Siehe Anhang II Abschnitt II Buchstabe A Nummer 2 Buchstabe b Nummer 1.

([97]) Nach den vorliegenden Informationen sind diese Faktoren als „angemessen im Sinne der gesellschaftlich anerkannten Konventionen“ zu betrachten. Siehe Anhang II Abschnitt II Buchstabe A Nummer 2 Buchstabe b Nummer 1.

([98]) Zu ähnlichen Erwägungen im Zusammenhang mit Zwangsermittlungen (Abhörmaßnahmen) siehe auch Oberster Gerichtshof, Urteil vom 16. Dezember 1999, 1997 (A) 636.

([99]) In diesem Zusammenhang haben die japanischen Behörden auf die PPC-Leitlinien (General Rule Edition) und Punkt 5/14 des von der PPC für die Anwendung des APPI erstellten Fragen-Antworten-Katalogs hingewiesen. Nach Ansicht der japanischen Behörden „sind die Unternehmer angesichts des zunehmenden Bewusstseins des Einzelnen in Bezug auf seine Rechte auf den Schutz der Privatsphäre und der damit verbundenen Arbeitsbelastung immer zurückhaltender bei der Beantwortung solcher Anfragen“. Siehe Anhang II Abschnitt II Buchstabe A Nummer 2, auch mit Bezug auf die Bekanntmachung der NPA aus dem Jahr 1999. Nach den vorliegenden Informationen gab es in der Tat Fälle, in denen sich die Unternehmer geweigert haben, zu kooperieren. So stellt LINE (die meistverwendete Messaging-App in Japan) in ihrem Transparenzbericht für das Jahr 2017 Folgendes fest: „Nach dem Eingang von Anfragen von Ermittlungsbehörden usw. … überprüfen wir die Angemessenheit nach dem Aspekt der Rechtmäßigkeit, des Verbraucherschutzes usw. Im Rahmen dieser Überprüfung lehnen wir den Antrag zu dem Zeitpunkt ab, wenn ein Rechtsmangel vorliegt. Ist der Umfang der Forderung für Ermittlungszwecke zu weit gefasst, bitten wir die Ermittlungsbehörde um eine entsprechende Erläuterung. Wenn die Erläuterung nicht stichhaltig ist, wird die Anfrage nicht von uns beantwortet.“ Im Internet abrufbar unter: https://linecorp.com/en/security/transparency/top

([100]) Als Strafe ist ein mit Zwangsarbeit verbundener Freiheitsentzug von drei Jahren bzw. eine Geldstrafe von bis zu zwei Millionen Yen für jede Person vorgesehen, die „im Telekommunikationsbereich tätig ist“.

([101]) „Gerechtfertigte Handlungen“ sind nach dem Strafgesetzbuch insbesondere diejenigen Handlungen eines Telekommunikationsdiensteanbieters, durch die er rechtskräftige Maßnahmen des Staates (Zwangsmaßnahmen) befolgt, z. B. wenn Ermittlungsbehörden Maßnahmen aufgrund eines Gerichtsbeschlusses treffen. Siehe Anhang II Abschnitt II Buchstabe A Nummer 2 Buchstabe b Nummer 2, mit Bezug auf die Leitlinien zum Schutz personenbezogener Informationen in der Telekommunikationsbranche.

Informationen“ und sieht in diesem Zusammenhang eine Reihe von Beschränkungen und Garantien vor (siehe Erwägungsgrund 118) ([102]). Darüber hinaus ergeben sich aus der Tatsache, dass ein Verwaltungsorgan personenbezogene Informationen „nur dann [speichern darf], wenn die Speicherung für die Erfüllung der durch Gesetze und Vorschriften vorgesehenen Aufgaben erforderlich ist“ (Artikel 3 Absatz 1 APPIHAO), — zumindest indirekt — Beschränkungen für die Ersterhebung.

3.2.2. *Unabhängige Aufsicht*

(131) In Japan fällt die Erhebung elektronischer Informationen im Bereich der Strafverfolgung in erster Linie ([103]) in die Zuständigkeit der Präfekturpolizei ([104]), die in dieser Hinsicht verschiedenen Aufsichtsebenen unterliegen.

(132) Erstens muss die Polizei in allen Fällen, in denen elektronische Informationen mit Zwangsmitteln erhoben werden (Durchsuchung und Beschlagnahme), vorab einen Gerichtsbeschluss erwirken (siehe Erwägungsgrund 121). Daher wird die Erhebung in diesen Fällen einer vorherigen richterlichen Prüfung unterzogen, die auf einem strengen Standard für den „hinreichenden Grund“ basiert.

(133) Auch wenn bei Anträgen auf freiwillige Offenlegung keine Ex-ante-Kontrolle durch einen Richter vorgesehen ist, können Unternehmer, an die solche Anfragen gerichtet sind, Letztere ablehnen, ohne negative Folgen befürchten zu müssen (und müssen die Auswirkungen einer Offenlegung auf den Schutz der Privatsphäre beachten). Darüber hinaus arbeiten die Polizeibeamten nach Artikel 192 Absatz 1 StPO stets mit dem zuständigen Staatsanwalt (und der Präfekturkommission für öffentliche Sicherheit) zusammen und koordinieren mit diesem ihre Maßnahmen ([105]). Der Staatsanwalt wiederum kann die erforderlichen allgemeinen Anweisungen zur Festlegung von Standards für eine faire Ermittlung erteilen und/oder spezifische Anordnungen in Bezug auf eine konkrete Ermittlung (Artikel 193 StPO) erlassen. Werden solche Anweisungen und/oder Anordnungen nicht befolgt, kann die Staatsanwaltschaft Disziplinarmaßnahmen einleiten (Artikel 194 StPO). Die Präfekturpolizei arbeitet somit unter der Aufsicht der Staatsanwaltschaft.

(134) Zweitens kann nach Artikel 62 der Verfassung jedes Haus des japanischen Parlaments Ermittlungen in Bezug auf die Regierung durchführen, auch im Hinblick auf die Rechtmäßigkeit der Informationserhebung durch die Polizei. Zu diesem Zweck kann sie die Vorladung und Vernehmung von Zeugen und/oder die Vorlage von Aufzeichnungen verlangen. Diese Ermittlungsbefugnisse sind im Parlamentsgesetz, insbesondere in Kapitel XII, näher geregelt. Insbesondere sieht Artikel 104 des Parlamentsgesetzes vor, dass das Kabinett, Behörden und andere Teile der Regierung „den Anträgen eines Hauses oder eines seiner Ausschüsse auf Vorlage von Berichten und Aufzeichnungen, die für die Prüfung von Ermittlungen erforderlich sind, nachkommen müssen“. Eine Verweigerung der Zusammenarbeit ist nur dann zulässig, wenn die Regierung einen nachvollziehbaren Grund angibt, der vom Parlament akzeptiert wird, oder wenn sie eine förmliche Erklärung abgibt, dass die Vorlage der Berichte oder Aufzeichnungen „den nationalen Interessen ernsthaft schaden würde“ ([106]). Darüber hinaus können Parlamentsmitglieder dem Kabinett schriftliche Anfragen stellen (Artikel 74, 75 des Parlamentsgesetzes), und in der Vergangenheit wurde in solchen „schriftlichen Anfragen“ auch die Handhabung personenbezogener Informationen durch die Verwaltung thematisiert ([107]). Die Rolle des Parlaments bei der Kontrolle der Exekutive wird durch Berichterstattungspflichten gestärkt, zum Beispiel nach Artikel 29 des Abhörgesetzes.

(135) Drittens unterliegt die Präfekturpolizei auch innerhalb der Exekutive einer unabhängigen Aufsicht. Dazu gehören insbesondere die Präfekturkommissionen für öffentliche Sicherheit, die auf Präfekturebene eingerichtet wurden, um die demokratische Verwaltung und die politische Neutralität der Polizei zu gewährleisten ([108]). Die Kommissionen setzen sich aus Mitgliedern zusammen, die vom Präfekturgouverneur mit Zustimmung der Präfekturversammlung ernannt werden (aus einem Kreis von Bürgern, die in den fünf vorhergehenden Jahren keine Polizeibeamten waren) und eine feste Amtszeit haben (Entlassung nur aus wichtigem Grund) ([109]). Nach den vorliegenden Informationen sind sie nicht weisungsgebunden und können daher als vollständig unabhängig betrachtet werden ([110]). Was die

([102]) Zu den Rechten der betroffenen Personen siehe Abschnitt 3.1.
([103]) Grundsätzlich kann ein Staatsanwalt — oder ein Staatsanwaltsgehilfe auf Anordnung eines Staatsanwalts —, wenn er es für notwendig hält, bei einer Straftat ermitteln (Artikel 191 Absatz 1 StPO).
([104]) Nach den vorliegenden Informationen führt die Nationale Polizeibehörde keine strafrechtlichen Ermittlungen in Einzelfällen durch. Siehe Anhang II Abschnitt II Buchstabe A Nummer 1 Buchstabe a.
([105]) Siehe auch Artikel 246 StPO, nach dem die Kriminalpolizei verpflichtet ist, die Fallakte an den Staatsanwalt weiterzuleiten, sobald sie die Ermittlungen zu einer Straftat durchgeführt hat („Grundsatz der Weiterleitung in allen Fällen“).
([106]) Alternativ kann das Parlament verlangen, dass das „Board of Oversight and Review of Specially Designated Secrets“ eine Untersuchung zur Verweigerung der Antwort durchführt. Siehe Artikel 104-II des Parlamentsgesetzes.
([107]) Siehe Anhang II Abschnitt II Buchstabe B Nummer 4.
([108]) Zudem ist nach Artikel 100 des Gesetzes über die örtliche Selbstverwaltung die lokale Versammlung befugt, die Tätigkeit der auf Präfekturebene eingerichteten Vollzugsbehörden, einschließlich der Präfekturpolizei, zu untersuchen.
([109]) Siehe die Artikel 39 bis 41 des Polizeigesetzes. Zur politischen Neutralität siehe auch Artikel 42 des Polizeigesetzes.
([110]) Siehe Anhang II Abschnitt II Buchstabe B Nummer 3 („System unabhängiger Räte“).

Aufgaben und Befugnisse der Präfekturkommissionen für öffentliche Sicherheit angeht, so sind sie nach Artikel 38 Absatz 3 in Verbindung mit Artikel 2 und Artikel 36 Absatz 2 des Polizeigesetzes für den „Schutz der Rechte und Freiheiten des Einzelnen" zuständig. Zu diesem Zweck sind sie befugt, alle Ermittlungstätigkeiten der Präfekturpolizei zu „beaufsichtigen" ([111]), auch die Erhebung personenbezogener Daten. Insbesondere können die Kommissionen „der Präfekturpolizei im Einzelnen oder in konkreten Einzelfällen, in denen das Fehlverhalten von Polizeibediensteten untersucht wird, erforderlichenfalls Anweisungen erteilen" ([112]). Wenn der Leiter der Präfekturpolizei ([113]) eine solche Anweisung erhält oder selbst auf ein mögliches Fehlverhalten (einschließlich Gesetzesverstößen und sonstigen Pflichtverletzungen) aufmerksam wird, hat er diesem Verdacht umgehend nachzugehen und das Untersuchungsergebnis der Präfekturkommission für öffentliche Sicherheit zu melden (Artikel 56 Absatz 3 des Polizeigesetzes). Wenn die Kommission dies als notwendig ansieht, kann sie auch eines ihrer Mitglieder benennen, das den Stand der Umsetzung überprüft. Das Verfahren wird fortgesetzt, bis die Präfekturkommission für öffentliche Sicherheit davon überzeugt ist, dass der Vorfall angemessen behandelt wurde.

(136) Im Hinblick auf die ordnungsgemäße Anwendung des APPIHAO verfügt der zuständige Minister oder Behördenleiter (z. B. der Generalkommissar der NPA) über Durchsetzungsbefugnisse, die der Aufsicht durch das Ministerium für innere Angelegenheiten und Kommunikation (*Ministry of Internal Affairs and Communications* — MIC) unterliegen. Nach Artikel 49 APPIHAO kann das MIC von den Leitern der Verwaltungsorgane (Ministern) „Berichte über den Stand der Durchsetzung dieses Gesetzes einholen". Zu dieser Aufsichtsfunktion tragen die 51 „Informationszentralen" des MIC (eine in jeder Präfektur in ganz Japan) bei, die jedes Jahr Tausende von Anfragen von Einzelpersonen bearbeiten ([114]) (wobei wiederum mögliche Gesetzesverstöße aufgedeckt werden können). Wenn das MIC dies für die Einhaltung des Gesetzes für notwendig hält, kann es vom betreffenden Verwaltungsorgan verlangen, Erläuterungen und Materialien vorzulegen sowie eine Stellungnahme zur Handhabung personenbezogener Informationen abzugeben (Artikel 50 und 51 APPIHAO).

3.2.3. *Individueller Rechtsschutz*

(137) Neben der amtlichen Aufsicht haben Einzelpersonen auch verschiedene Möglichkeiten, individuellen Rechtsschutz zu erhalten, sowohl durch unabhängige Behörden (wie die Präfekturkommissionen für öffentliche Sicherheit oder die PPC) als auch durch die japanischen Gerichte.

(138) Erstens sind Verwaltungsorgane in Bezug auf die von ihnen erhobenen personenbezogenen Informationen verpflichtet, „sich um eine ordnungsgemäße und zügige Bearbeitung von Beschwerden zu bemühen", wenn es um die spätere Verarbeitung dieser Informationen geht (Artikel 48 APPIHAO). Auch wenn Kapitel IV des APPIHAO über die Rechte des Einzelnen keine Anwendung auf personenbezogene Informationen findet, die in „Dokumenten über Gerichtsverfahren und beschlagnahmte Gegenstände" (Artikel 53-2 Absatz 2 StPO) enthalten sind — zu denen personenbezogene Informationen gehören, die im Rahmen von strafrechtlichen Ermittlungen erhoben wurden —, können Einzelpersonen eine Beschwerde einreichen, indem sie sich auf die allgemeinen Datenschutzgrundsätze wie beispielsweise die Verpflichtung berufen, personenbezogene Informationen nur dann zu speichern, „wenn die Speicherung zur Erfüllung von [Strafverfolgungsfunktionen] erforderlich ist" (Artikel 3 Absatz 1 APPIHAO).

(139) Darüber hinaus wird mit Artikel 79 des Polizeigesetzes Personen, die Bedenken in Bezug auf die „Ausübung von Pflichten" durch Polizeikräfte haben, das Recht eingeräumt, eine Beschwerde bei der (zuständigen) unabhängigen Präfekturkommission für öffentliche Sicherheit einzureichen. Die Kommission wird solche Beschwerden „gewissenhaft" und in Übereinstimmung mit Gesetzen und lokalen Verordnungen bearbeiten und den Beschwerdeführer schriftlich über die Ergebnisse informieren. Ausgehend von ihrer Befugnis, die Präfekturpolizei in Bezug auf „Fehlverhalten der Polizeikräfte" (Artikel 38 Absatz 3 und Artikel 43-2 Absatz 1 des Polizeigesetzes) zu beaufsichtigen und ihr „Anweisungen zu erteilen", kann sie die Präfekturpolizei auffordern, Fakten zu untersuchen, geeignete Maßnahmen auf der Grundlage der Ergebnisse dieser Untersuchung zu ergreifen und über die Ergebnisse zu berichten. Ist sie der Auffassung, dass die von der Polizei durchgeführte Untersuchung nicht zufriedenstellend war, kann die Kommission auch Anweisungen zur Bearbeitung der Beschwerde erteilen.

(140) Um die Bearbeitung von Beschwerden zu erleichtern, hat die NPA eine „Bekanntmachung" über die ordnungsgemäße Bearbeitung von Beschwerden über die Amtsausübung durch Polizeibeamte an die Polizei und die Präfekturkommissionen für öffentliche Sicherheit gerichtet. Darin legt die NPA Normen für die Auslegung und Umsetzung

([111]) Siehe Artikel 5 Absatz 3 und Artikel 38 Absatz 3 des Polizeigesetzes.

([112]) Siehe Artikel 38 Absatz 3 und Artikel 43-2 Absatz 1 des Polizeigesetzes. Wenn sie im Sinne des Artikels 43-2 Absatz 1 „eine Anweisung erteilt", kann die Präfekturkommission für öffentliche Sicherheit einen von der Kommission benannten Ausschuss mit der Überwachung ihrer Umsetzung beauftragen (Absatz 2). Außerdem kann die Kommission Disziplinarmaßnahmen oder die Entlassung des Leiters der Präfekturpolizei (Artikel 50 Absatz 2) sowie anderer Polizeibeamter (Artikel 55 Absatz 4 des Polizeigesetzes) empfehlen.

([113]) Gleiches gilt für den Superintendent General im Falle der Tokyo Metropolitan Police (siehe Artikel 48 Absatz 1 des Polizeigesetzes).

([114]) Nach den vorliegenden Informationen haben die „Informationszentralen" im Geschäftsjahr 2017 (April 2017 bis März 2018) insgesamt 5 186 Anfragen von Einzelpersonen bearbeitet.

des Artikels 79 des Polizeigesetzes fest. Unter anderem muss die Präfekturpolizei ein „System für die Bearbeitung von Beschwerden" einrichten und alle Beschwerden „umgehend" bearbeiten und der zuständigen Präfekturkommission für öffentliche Sicherheit melden. Beschwerden sind in der Bekanntmachung definiert als Anträge auf Korrektur „eines besonderen Nachteils, der auf ein rechtswidriges oder unangemessenes Verhalten zurückzuführen ist" ([115]), oder „der Unterlassung einer notwendigen Maßnahme durch einen Polizeibeamten in Erfüllung seiner Pflichten" ([116]) sowie als „Beanstandung einer unangemessenen Art der Amtsausübung durch einen Polizeibeamten". In diesen weit gefassten sachlichen Anwendungsbereich der Beschwerde fällt daher jede mutmaßlich rechtswidrige Erhebung von Daten, und der Beschwerdeführer muss nicht nachweisen, dass ihm aus den Maßnahmen des Polizeibeamten ein Schaden erwachsen ist. Wichtig ist, dass nach der Bekanntmachung (unter anderem) Ausländer Hilfe bei der Formulierung einer Beschwerde erhalten. Nach Eingang einer Beschwerde müssen die Präfekturkommissionen für öffentliche Sicherheit dafür sorgen, dass die Präfekturpolizei den Sachverhalt prüft, „entsprechend dem Ergebnis der Prüfung" Maßnahmen trifft und über die Ergebnisse Bericht erstattet. Hält die Kommission die Prüfung für unzureichend, so erteilt sie eine Anweisung zur Bearbeitung der Beschwerde, die die Präfekturpolizei befolgen muss. Auf der Grundlage der eingegangenen Berichte und der getroffenen Maßnahmen teilt die Kommission dem Beschwerdeführer unter anderem mit, welche Maßnahmen getroffen wurden, um der Beschwerde abzuhelfen. In ihrer Bekanntmachung weist die NPA mit Nachdruck darauf hin, dass Beschwerden „in ernsthafter Weise" bearbeitet werden sollten und dass das Ergebnis „innerhalb einer Zeitspanne" mitgeteilt werden sollte, „die unter Berücksichtigung der sozialen Normen und des gesunden Menschenverstands angemessen erscheint".

(141) Zweitens hat die japanische Regierung, da die Rechtsbehelfe naturgemäß im Ausland in einem fremden System und in einer Fremdsprache eingelegt werden müssen, von ihren Befugnissen Gebrauch gemacht, um ein spezifisches von der PPC verwaltetes und beaufsichtigtes Verfahren für die Bearbeitung und Erledigung von Beschwerden in diesem Bereich zu schaffen, damit Unionsbürgern, deren personenbezogene Daten an Unternehmer in Japan übermittelt und dann von den Behörden eingesehen werden, der Rechtsbehelf erleichtert wird. Dieses Verfahren stützt sich auf die Kooperationspflicht, die den japanischen Behörden im Rahmen des APPI auferlegt wurde, und auf die besondere Rolle der PPC bei internationalen Datenübermittlungen aus Drittländern nach Artikel 6 APPI und der „Grundlegenden Richtlinie" (die von der japanischen Regierung durch Kabinettsverordnung festgelegt wurde). Die Einzelheiten dieses Verfahrens sind in den offiziellen Erklärungen, Zusicherungen und Verpflichtungen der japanischen Regierung dargelegt, die diesem Beschluss als Anhang II beigefügt ist. Das Verfahren, für das keine Antragsbefugnis gilt, steht Einzelpersonen unabhängig davon offen, ob sie einer Straftat verdächtigt oder beschuldigt werden.

(142) Im Rahmen des Verfahrens kann eine Person, die den Verdacht hat, dass ihre aus der Europäischen Union übermittelten Daten von Behörden in Japan (einschließlich der für die Strafverfolgung zuständigen Behörden) unter Verstoß gegen die geltenden Vorschriften erhoben oder verwendet wurden, eine Beschwerde an die PPC richten (selbst oder über ihre Datenschutzbehörde im Sinne des Artikels 51 DSGVO). Die PPC ist verpflichtet, die Beschwerde zu bearbeiten und in einem ersten Schritt die zuständigen Behörden, einschließlich der zuständigen Aufsichtsbehörden, darüber zu informieren. Diese Behörden sind verpflichtet, mit der PPC zusammenzuarbeiten, „auch durch Bereitstellung der erforderlichen Informationen und der entsprechenden Materialien, damit die PPC prüfen kann, ob die Erhebung oder die spätere Verwendung personenbezogener Informationen im Einklang mit den geltenden Vorschriften erfolgt ist" ([117]). Diese Pflicht, die sich aus Artikel 80 APPI ergibt (der bestimmt, dass die japanischen Behörden mit der PPC zusammenarbeiten müssen), gilt ganz allgemein und damit auch für die Überprüfung von Ermittlungsmaßnahmen dieser Behörden, die sich zudem in schriftlichen Zusicherungen der zuständigen Ministerien und Behördenleiter zu einer solchen Zusammenarbeit verpflichtet haben (siehe Anhang II).

(143) Ergibt die Bewertung, dass ein Verstoß gegen die geltenden Vorschriften vorliegt, „umfasst die Zusammenarbeit der betroffenen Behörden mit der PPC die Verpflichtung, den Verstoß zu beheben", was im Falle der rechtswidrigen Erhebung personenbezogener Informationen auch die Löschung dieser Daten einschließt. Wichtig ist, dass diese Verpflichtung unter der Aufsicht der PPC erfüllt wird, die „vor Abschluss der Bewertung bestätigt, dass der Verstoß vollständig behoben wurde".

(144) Sobald die Bewertung abgeschlossen ist, unterrichtet die PPC die Person innerhalb eines angemessenen Zeitraums über das Ergebnis der Bewertung und gegebenenfalls über durchgeführte Korrekturmaßnahmen. Gleichzeitig informiert die PPC die Person auch über die Möglichkeit, von der zuständigen Behörde eine Bestätigung des Ergebnisses zu verlangen, und die Identität der Behörde, bei der ein solcher Antrag auf Bestätigung zu stellen ist. Die

([115]) Das Erfordernis eines „besonderen Nachteils" bedeutet lediglich, dass der Beschwerdeführer von dem Verhalten (oder der Untätigkeit) der Polizei individuell betroffen sein muss, nicht aber, dass er einen Schaden nachweisen muss.

([116]) Zu diesen Pflichten gehört auch die Einhaltung des Rechts, einschließlich der gesetzlichen Anforderungen an die Erhebung und Verwendung personenbezogener Daten. Siehe Artikel 2 Absatz 2 und Artikel 3 des Polizeigesetzes.

([117]) Bei der Durchführung ihrer Bewertung arbeitet die PPC mit dem MIC zusammen, das, wie in Erwägungsgrund 136 erläutert, die Vorlage von Erläuterungen und Materialien sowie die Abgabe von Stellungnahmen zur Handhabung personenbezogener Informationen durch das jeweilige Verwaltungsorgan verlangen kann (Artikel 50 und 51 APPIHAO).

Möglichkeit, eine solche Bestätigung einschließlich der Gründe für die Entscheidung der zuständigen Behörde zu erhalten, kann der betroffenen Person bei allen weiteren Schritten von Nutzen sein, etwa bei der Einlegung von Rechtsbehelfen. Die Herausgabe detaillierter Informationen über das Ergebnis der Bewertung kann Beschränkungen unterliegen, sofern berechtigte Gründe vorliegen, dass die Übermittlung dieser Informationen ein Risiko für laufende Ermittlungen darstellen könnte.

(145) Drittens kann eine Person, die mit einem richterlichen Beschlagnahmebeschluss (Gerichtsbeschluss) ([118]) bezüglich ihrer personenbezogenen Daten oder mit den Maßnahmen der Polizei oder Staatsanwaltschaft, die einen solchen Beschluss vollstrecken, nicht einverstanden ist, einen Antrag auf Aufhebung oder Änderung dieses Beschlusses oder dieser Maßnahmen stellen (Artikel 429 Absatz 1, Artikel 430 Absätze 1 und 2 StPO, Artikel 26 des Abhörgesetzes) ([119]). Wenn das überprüfende Gericht zu dem Ergebnis gelangt, dass entweder der Gerichtsbeschluss selbst oder seine Vollstreckung („Beschlagnahmeverfahren") rechtswidrig ist, gibt es dem Antrag statt und ordnet die Rückgabe der beschlagnahmten Gegenstände an ([120]).

(146) Viertens kann sich eine Person, die der Ansicht ist, dass die Erhebung ihrer personenbezogenen Informationen im Rahmen einer strafrechtlichen Ermittlung rechtswidrig war, im Rahmen ihres Strafverfahrens auf diese Rechtswidrigkeit berufen — als indirektere Form der gerichtlichen Kontrolle. Wenn das Gericht zustimmt, werden die Beweismittel in dem fraglichen Verfahren nicht zugelassen.

(147) Schließlich kann ein Gericht nach Artikel 1 Absatz 1 des Staatshaftungsgesetzes Schadensersatz gewähren, wenn ein Beamter, der die öffentliche Gewalt des Staates ausübt, in Erfüllung seiner Aufgaben in rechtswidriger und schuldhafter (vorsätzlicher oder fahrlässiger) Weise der betroffenen Person Schaden zugefügt hat. Nach Artikel 4 des Staatshaftungsgesetzes richtet sich die Haftung des Staates auf Schadensersatz nach den Bestimmungen des japanischen Bürgerlichen Gesetzbuches. In diesem Zusammenhang sieht Artikel 710 des Bürgerlichen Gesetzbuches vor, dass die Haftung auch immaterielle Schäden (z. B. in Form von „psychischer Belastung") umfasst, die nicht das Eigentum betreffen. Dazu gehören auch Fälle, in denen die Privatsphäre einer Person durch rechtswidrige Überwachung und/oder die Erhebung ihrer personenbezogenen Informationen (z. B. durch die rechtswidrige Vollstreckung eines Gerichtsbeschlusses) verletzt wurde ([121]).

(148) Neben finanziellem Schadensersatz können Einzelpersonen aufgrund ihrer Persönlichkeitsrechte nach Artikel 13 der japanischen Verfassung unter bestimmten Voraussetzungen auch Unterlassungsansprüche (z. B. die Löschung ihrer von Behörden erhobenen personenbezogenen Daten) geltend machen ([122]).

(149) In Bezug auf all diese Rechtsbehelfe sieht der von der japanischen Regierung geschaffene Streitschlichtungsprozess vor, dass sich eine Person, die mit dem Ergebnis des Verfahrens weiterhin unzufrieden ist, an die PPC wenden kann, „die die Person über die verschiedenen Möglichkeiten und genauen Verfahren zur Einlegung von Rechtsbehelfen nach japanischen Gesetzen und Vorschriften informiert". Darüber hinaus „steht [die PCC] der Person unterstützend zur Seite und berät sie beispielsweise bei der Einleitung weiterer Maßnahmen bei der zuständigen Verwaltungs- oder Justizbehörde".

(150) Dazu gehört auch die Inanspruchnahme der Verfahrensrechte nach der Strafprozessordnung. Beispielsweise „informiert die PPC, wenn die Untersuchung ergibt, dass eine Person in einem Strafverfahren als Verdächtiger gilt, die betroffene Person über diese Tatsache" ([123]) sowie über die Möglichkeit nach Artikel 259 StPO, die Strafverfolgungsbehörde um Benachrichtigung zu bitten, sobald diese beschließt, auf ein Strafverfahren zu verzichten. Ergibt die Untersuchung ferner, dass ein Verfahren im Zusammenhang mit den personenbezogenen Informationen der Person eingeleitet wurde und der Fall inzwischen abgeschlossen ist, informiert die PPC die Person darüber, dass die Fallakte nach Artikel 53 StPO (und Artikel 4 des Act on Final Criminal Case Records (Gesetz über das abschließende Strafregister)) eingesehen werden kann. Der Zugang zu dieser Akte ist wichtig, da sie der Person dabei hilft,

([118]) Dazu gehört auch ein Gerichtsbeschluss über Abhörmaßnahmen, für die das Abhörgesetz eine besondere Meldepflicht vorsieht (Artikel 23). Nach dieser Bestimmung muss die Ermittlungsbehörde die Personen, deren Kommunikation abgehört (und damit in das Abhörprotokoll aufgenommen) wurde, schriftlich über diese Tatsache informieren. Ein weiteres Beispiel ist Artikel 100 Absatz 3 StPO, wonach das Gericht, wenn es an oder von dem Angeklagten verschickte Postsendungen oder Telegramme beschlagnahmt hat, den Absender oder Empfänger benachrichtigen muss, es sei denn, es besteht die Gefahr, eine solche Benachrichtigung würde das Gerichtsverfahren behindern. Artikel 222 Absatz 1 StPO verweist auf diese Bestimmung für Durchsuchungen und Beschlagnahmen durch eine Ermittlungsbehörde.

([119]) Ein solcher Antrag bewirkt zwar nicht automatisch die Aussetzung der Vollstreckung des Beschlagnahmebeschlusses, doch kann das prüfende Gericht die Aussetzung anordnen, bis es in der Sache eine Entscheidung getroffen hat. Siehe Artikel 429 Absatz 2 und Artikel 432 in Verbindung mit Artikel 424 StPO.

([120]) Siehe Anhang II Abschnitt II Buchstabe C Nummer 1.

([121]) Siehe Anhang II Abschnitt II Buchstabe C Nummer 2.

([122]) Siehe z. B. Bezirksgericht Tokyo, Urteil vom 24. März 1988 (Nr. 2925); Bezirksgericht Osaka, Urteil vom 26. April 2007 (Nr. 2925). Nach Auffassung des Bezirksgerichts Osaka muss eine Reihe von Faktoren abgewogen werden, wie beispielsweise: i) Art und Inhalt der betreffenden personenbezogenen Informationen, ii) Art und Weise, wie sie erhoben wurden, iii) die Nachteile für die betroffene Person, falls die Informationen nicht gelöscht werden, und iv) das öffentliche Interesse, einschließlich der Nachteile für die Behörde, falls die Informationen gelöscht werden.

([123]) Auf jeden Fall gibt die Staatsanwaltschaft dem Angeklagten nach Einleitung des Strafverfahrens Gelegenheit, diese Beweismittel einzusehen (siehe die Artikel 298 bis 299 StPO). Zu den Opfern von Straftaten siehe die Artikel 316 bis 333 StPO.

die gegen sie durchgeführten Ermittlungen besser zu verstehen und somit gegebenenfalls eine gerichtliche Klage (z. B. eine Schadensersatzklage) vorzubereiten, falls sie der Ansicht ist, dass ihre Daten unrechtmäßig erhoben oder verwendet wurden.

### 3.3. **Zugriff und Verwendung durch japanische Behörden für Zwecke der nationalen Sicherheit**

(151) Nach Auskunft der japanischen Behörden gibt es in Japan kein Gesetz, auf dessen Grundlage Zwangsanfragen zur Einholung von Informationen oder „administrative Abhörmaßnahmen" außerhalb strafrechtlicher Ermittlungen zulässig wären. Aus Gründen der nationalen Sicherheit dürfen Informationen daher nur aus einer Informationsquelle, die für jedermann frei zugänglich ist, oder durch freiwillige Offenlegung bezogen werden. Unternehmer, die ein Ersuchen um freiwillige Zusammenarbeit (in Form der Offenlegung elektronischer Informationen) erhalten, sind rechtlich nicht verpflichtet, diese Informationen zur Verfügung zu stellen ([124]).

(152) Nach den vorliegenden Informationen sind zudem nur vier staatliche Stellen befugt, elektronische Informationen, die sich im Besitz japanischer Unternehmer befinden, aus Gründen der nationalen Sicherheit einzuholen, nämlich i) das Nachrichten- und Untersuchungsbüro des Kabinetts (*Cabinet Intelligence & Research Office* — CIRO), ii) das Verteidigungsministerium (*Ministry of Defence* — MOD), iii) die Polizei (sowohl die NPA ([125]) als auch die Präfekturpolizei) und iv) der Nachrichtendienst für öffentliche Sicherheit (*Public Security Intelligence Agency* — PSIA). Das CIRO erhebt jedoch niemals Informationen direkt bei Unternehmern, auch nicht durch das Abfangen von Kommunikation. Wenn es Informationen von anderen staatlichen Behörden erhält, um sie für das Kabinett zu analysieren, müssen diese anderen Behörden ihrerseits die Rechtsvorschriften einhalten, einschließlich der in diesem Beschluss analysierten Beschränkungen und Garantien. Seine Tätigkeit ist daher im Zusammenhang mit der Übermittlung von Daten nicht von Belang.

#### 3.3.1. *Rechtsgrundlage und anwendbare Beschränkungen/Garantien*

(153) Nach den vorliegenden Informationen erfasst das MOD (elektronische) Informationen auf der Grundlage des MOD-Errichtungsgesetzes (*MOD Establishment Act*). Nach Artikel 3 dieses Gesetzes hat das MOD die Aufgabe, die Streitkräfte zu verwalten und zu führen und „die damit verbundenen Angelegenheiten zu regeln, um den Frieden und die Unabhängigkeit des Landes sowie die nationale Sicherheit zu gewährleisten". Artikel 4 Absatz 4 sieht vor, dass das MOD für die „Verteidigung und den Schutz", für die von den Streitkräften zu ergreifenden Maßnahmen sowie für die Entsendung von Truppen zuständig ist, einschließlich der Erhebung der für die Erfüllung dieser Aufgaben erforderlichen Informationen. Sie ist nur im Rahmen der freiwilligen Kooperation befugt, (elektronische) Informationen bei Unternehmern zu erheben.

(154) Die Präfekturpolizei hingegen ist unter anderem für die „Aufrechterhaltung der öffentlichen Sicherheit und Ordnung" verantwortlich (Artikel 35 Absatz 2 in Verbindung mit Artikel 2 Absatz 1 Polizeigesetz). In diesem Zuständigkeitsbereich darf die Polizei Informationen erheben, jedoch nur auf freiwilliger Basis ohne rechtliche Wirkung. Zudem ist die Tätigkeit der Polizei „streng begrenzt" auf das, was für die Erfüllung ihrer Aufgaben erforderlich ist. Darüber hinaus muss sie „unparteiisch, neutral, unvoreingenommen und fair" handeln und darf ihre Befugnisse niemals „in einer Weise missbrauchen, die den in der japanischen Verfassung garantierten Rechten und Freiheiten des Einzelnen zuwiderläuft" (Artikel 2 Polizeigesetz).

(155) Der PSIA schließlich kann Untersuchungen nach dem Gesetz zur Verhütung subversiver Tätigkeiten (*Subversive Activities Prevention Act* — SAPA) und dem Gesetz über die Kontrolle von Organisationen, die wahllos Massenmorde verübt haben (*Act on the Control of Organisations Who Have Committed Acts of Indiscriminate Mass Murder* — ACO), durchführen, wenn diese Untersuchungen notwendig sind, um den Erlass von Kontrollmaßnahmen gegen bestimmte Organisationen vorzubereiten ([126]). Nach beiden Gesetzen kann die Kommission für die Prüfung der öffentlichen Sicherheit auf Antrag des Generaldirektors des PSIA bestimmte „Verfügungen" erlassen (Überwachung/Verbote im Falle des ACO ([127]), Auflösung/Verbote im Falle des SAPA ([128])), und in diesem Zusammenhang kann der PSIA Ermittlungen durchführen ([129]). Nach den vorliegenden Informationen werden diese Ermittlungen stets auf

([124]) Die Unternehmer können sich daher ohne die Gefahr von Sanktionen oder anderen negativen Folgen frei gegen eine Zusammenarbeit entscheiden. Siehe Anhang II Abschnitt III Buchstabe A Nummer 1.

([125]) Nach den vorliegenden Informationen besteht die Hauptaufgabe der NPA jedoch darin, die Ermittlungen der verschiedenen Präfekturpolizeien zu koordinieren und Informationen mit ausländischen Behörden auszutauschen. Auch in dieser Funktion unterliegt die NPA der Aufsicht durch die Nationale Kommission für öffentliche Sicherheit, die unter anderem für den Schutz der Rechte und Freiheiten des Einzelnen zuständig ist (Artikel 5 Absatz 1 des Polizeigesetzes).

([126]) Siehe Anhang II Abschnitt III Buchstabe A Nummer 1 Ziffer 3. Der jeweilige Anwendungsbereich dieser beiden Gesetze ist begrenzt, wobei sich das SAPA auf „terroristische subversive Aktivitäten" und das ACO auf den „wahllosen Massenmord" (d. h. eine „terroristisch subversive Aktivität" nach dem SAPA, „durch die eine große Anzahl von Personen wahllos ermordet wird") bezieht.

([127]) Siehe die Artikel 5 und 8 ACO. Eine Überwachungsanordnung geht zudem mit einer Berichterstattungspflicht für die von der Maßnahme betroffene Organisation einher. Zu den Verfahrensgarantien, insbesondere den Transparenzanforderungen und der vorherigen Genehmigung durch die Public Security Examination Commission, siehe die Artikel 12 und 13 sowie die Artikel 15 bis 27 ACO.

([128]) Siehe die Artikel 5 und 7 SAPA. Zu den Verfahrensgarantien, insbesondere den Transparenzanforderungen und der vorherigen Genehmigung durch die Public Security Examination Commission, siehe die Artikel 11 bis 25 SAPA.

([129]) Siehe Artikel 27 SAPA und die Artikel 29 und 30 ACO.

freiwilliger Basis durchgeführt, was bedeutet, dass der PSIA eine Person nicht zwingen darf, personenbezogene Informationen zur Verfügung zu stellen ([130]). Kontrollen und Untersuchungen dürfen nur in dem für die Erreichung des Kontrollzwecks erforderlichen Mindestumfang durchgeführt werden und keinesfalls dazu dienen, die durch die japanische Verfassung garantierten Rechte und Freiheiten „unverhältnismäßig" zu beschränken (Artikel 3 Absatz 1 SAPA/ACO). Zudem darf der PSIA nach Artikel 3 Absatz 2 SAPA/ACO solche Kontrollen oder die zur Vorbereitung solcher Kontrollen durchgeführten Untersuchungen unter keinen Umständen missbrauchen. Hat ein PSIA-Mitarbeiter seine Befugnisse nach dem jeweiligen Gesetz missbraucht, indem er eine Person zu etwas gezwungen hat, wozu sie nicht verpflichtet ist, oder indem er in die Ausübung der Rechte einer Person eingegriffen hat, so kann er nach Artikel 45 SAPA oder Artikel 42 ACO strafrechtlich verfolgt werden. Schließlich schreiben beide Gesetze ausdrücklich vor, dass ihre Bestimmungen, einschließlich der darin gewährten Befugnisse, „unter keinen Umständen Gegenstand einer erweiterten Auslegung sein dürfen" (Artikel 2 SAPA/ACO).

(156) In allen in diesem Abschnitt beschriebenen Fällen des staatlichen Zugriffs aus Gründen der nationalen Sicherheit gelten die vom japanischen Obersten Gerichtshof für freiwillige Ermittlungen festgelegten Beschränkungen, was bedeutet, dass die Erhebung von (elektronischen) Informationen den Grundsätzen der Erforderlichkeit und Angemessenheit entsprechen muss („angemessene Vorgehensweise") ([131]). Wie die japanischen Behörden ausdrücklich bestätigt haben, „werden Informationen nur erhoben und verarbeitet, soweit dies für die Erfüllung der besonderen Aufgaben der zuständigen Behörde sowie aufgrund besonderer Bedrohungen erforderlich ist". Damit ist „ausgeschlossen, dass aus Gründen der nationalen Sicherheit massenweise und anlassunabhängig personenbezogene Informationen erhoben oder auf sie zugegriffen wird" ([132]).

(157) Nach ihrer Erhebung fallen außerdem alle personenbezogenen Informationen, die von Behörden zum Zwecke der nationalen Sicherheit gespeichert wurden, in Bezug auf die spätere Speicherung, Verwendung und Offenlegung unter den Schutz des APPIHAO (siehe Erwägungsgrund 118).

3.3.2. *Unabhängige Aufsicht*

(158) Die Erhebung personenbezogener Informationen zum Zwecke der nationalen Sicherheit unterliegt mehreren Aufsichtsebenen durch die drei Staatsgewalten.

(159) Erstens kann das japanische Parlament über seine Fachausschüsse die Rechtmäßigkeit von Ermittlungen auf der Grundlage seiner parlamentarischen Kontrollbefugnisse prüfen (Artikel 62 der Verfassung, Artikel 104 des Parlamentsgesetzes; siehe Erwägungsgrund 134). Diese Aufsichtsfunktion wird durch besondere Pflichten zur Berichterstattung über die Tätigkeiten unterstützt, die auf der Grundlage einiger der oben genannten Rechtsgrundlagen ([133]) ausgeübt werden.

(160) Zweitens gibt es innerhalb der Exekutive mehrere Aufsichtsmechanismen.

(161) In Bezug auf das MOD wird die Aufsicht durch das Büro des Generalinspektors für die Einhaltung gesetzlicher Vorschriften (Inspector General's Office of Legal Compliance — IGO) ([134]) wahrgenommen, das auf der Grundlage von Artikel 29 des MOD-Errichtungsgesetzes als Dienststelle innerhalb des MOD unter der Aufsicht des Verteidigungsministers (dem es untersteht), jedoch unabhängig von den operativen Abteilungen des MOD eingerichtet wurde. Das IGO hat die Aufgabe, die Einhaltung der Gesetze und Vorschriften sowie die ordnungsgemäße Erfüllung der Aufgaben durch die MOD-Beamten sicherzustellen. Zu seinen Kompetenzen gehört die Befugnis zur Durchführung sogenannter Verteidigungskontrollen (Defence Inspections), sowohl in regelmäßigen Abständen („ordentliche Verteidigungskontrollen") als auch im Einzelfall („außerordentliche Verteidigungskontrollen"), die in der Vergangenheit auch den ordnungsgemäßen Umgang mit personenbezogenen Informationen umfasst haben ([135]). Im Rahmen dieser Kontrollen kann das IGO Standorte (Büros) betreten und die Vorlage von Dokumenten

([130]) Siehe Anhang II Abschnitt III Buchstabe A Nummer 1 Ziffer 3.

([131]) Siehe Anhang II Abschnitt III Buchstabe A Nummer 2 Buchstabe b. „Aus der Rechtsprechung des Obersten Gerichtshofs ergibt sich, dass ein an einen Unternehmer gerichtetes Ersuchen um freiwillige Zusammenarbeit für die Ermittlungen im Zusammenhang mit einer mutmaßlichen Straftat erforderlich und geeignet sein muss, den Zweck der Ermittlungen zu erreichen. Obwohl sich die Ermittlungen der Ermittlungsbehörden im Bereich der nationalen Sicherheit sowohl hinsichtlich ihrer Rechtsgrundlage als auch ihres Zwecks von den Ermittlungen der Ermittlungsbehörden im Bereich der Strafverfolgung unterscheiden, gelten die zentralen Grundsätze ‚Erforderlichkeit für die Ermittlungen' und ‚Angemessenheit der Vorgehensweise' in ähnlicher Weise auch im Bereich der nationalen Sicherheit und müssen unter angemessener Berücksichtigung der besonderen Umstände des Einzelfalls beachtet werden".

([132]) Siehe Anhang II Abschnitt III Buchstabe A Nummer 2 Buchstabe b.

([133]) Siehe z. B. Artikel 36 SAPA/Artikel 31 ACO (in Bezug auf den PSIA).

([134]) Der Leiter des IGO ist ein ehemaliger Staatsanwalt. Siehe Anhang II Abschnitt III Buchstabe B Nummer 3.

([135]) Siehe Anhang II Abschnitt III Buchstabe B Nummer 3. Im Rahmen der ordentlichen Verteidigungskontrolle 2016 im Hinblick auf „Bewusstsein/Bereitschaft zur Einhaltung der Gesetze" wurde nach dem vorliegenden Beispiel unter anderem der „Status des Schutzes personenbezogener Informationen" (Verwaltung, Speicherung, usw.) geprüft. In dem anschließenden Bericht wurden Fälle von unsachgemäßer Datenverwaltung festgestellt und Verbesserungen in dieser Hinsicht gefordert. Das MOD hat den Bericht über seine Website veröffentlicht.

oder Informationen verlangen, einschließlich einer Stellungnahme des stellvertretenden Verteidigungsministers. Die Kontrolle wird mit einem Bericht an den Verteidigungsminister abgeschlossen, in dem die Ergebnisse und Verbesserungsmaßnahmen dargelegt werden (deren Umsetzung durch weitere Kontrollen nochmals überprüft werden kann). Der Bericht wiederum bildet die Grundlage für Anweisungen des Verteidigungsministers, die zur Bewältigung der Situation erforderlichen Maßnahmen zu treffen; der Stellvertretende Vizeminister ist mit der Durchführung dieser Maßnahmen beauftragt und hat über die Folgemaßnahmen Bericht zu erstatten.

(162) Was die Präfekturpolizei betrifft, so wird die Aufsicht von den unabhängigen Präfekturkommissionen für öffentliche Sicherheit gewährleistet, wie in Erwägungsgrund 135 im Zusammenhang mit der Strafverfolgung erläutert wurde.

(163) Schließlich darf der PSIA, wie angegeben, nur insoweit Ermittlungen durchführen, als dies im Hinblick auf den Erlass einer Verbots-, Auflösungs- oder Überwachungsanordnung im Rahmen des SAPA/ACO erforderlich ist, und für diese Anordnungen wird die Ex-ante-Aufsicht durch die unabhängige ([136]) Prüfungskommission für öffentliche Sicherheit (Public Security Examination Commission) gewährleistet. Darüber hinaus werden ordentliche/regelmäßige Kontrollen (in deren Rahmen die Tätigkeiten des PSIA umfassend untersucht werden) ([137]) und außerordentliche interne Kontrollen ([138]) der Tätigkeiten einzelner Abteilungen/Büros usw. von speziell benannten Inspektoren durchgeführt, die damit einhergehen können, dass die Leiter der jeweiligen Abteilungen usw. Anweisungen zur Ergreifung von Korrektur- oder Verbesserungsmaßnahmen erhalten.

(164) Diese Aufsichtsmechanismen, die durch die Möglichkeit für Einzelpersonen, die Intervention der PPC als unabhängige Aufsichtsbehörde anzustoßen, weiter verstärkt werden (siehe Abschnitt 168 weiter unten), bieten einen angemessenen Schutz vor dem Risiko des Missbrauchs der Kompetenzen japanischer Behörden im Bereich der nationalen Sicherheit und vor jeder rechtswidrigen Erhebung von elektronischen Informationen.

3.3.3. *Individueller Rechtsschutz*

(165) Was den individuellen Rechtsschutz betrifft, so sind die Verwaltungsorgane in Bezug auf die von ihnen erhobenen und somit „gespeicherten" personenbezogenen Informationen verpflichtet, „sich um eine ordnungsgemäße und zügige Bearbeitung von Beschwerden zu bemühen", wenn es um eine solche Verarbeitung geht (Artikel 48 APPIHAO).

(166) Darüber hinaus haben Einzelpersonen (auch im Ausland lebende Ausländer) anders als bei strafrechtlichen Ermittlungen grundsätzlich ein Recht auf Offenlegung ([139]), Berichtigung (einschließlich Löschung) und Aussetzung der Verwendung/Weitergabe nach dem APPIHAO. Dessen ungeachtet kann der Leiter des Verwaltungsorgans die Offenlegung von Informationen verweigern, „wenn es berechtigte Gründe gibt, … die darauf hindeuten, dass die Offenlegung der nationalen Sicherheit schaden könnte" (Artikel 14 Ziffer iv APPIHAO), und zwar ohne angeben zu müssen, ob solche Informationen vorhanden sind (Artikel 17 APPIHAO). Zwar kann eine Person nach Artikel 36 Absatz 1 Ziffer i APPIHAO die Aussetzung der Verwendung oder die Löschung beantragen, falls das Verwaltungsorgan die Informationen rechtswidrig erhalten hat oder sie über das zur Erreichung des angegebenen Zwecks erforderliche Maß hinaus speichert/verwendet, die Behörde kann den Antrag jedoch ablehnen, wenn sie feststellt, dass die Aussetzung der Verwendung „die ordnungsgemäße Durchführung der Angelegenheiten im Zusammenhang mit dem Zweck der Verwendung der gespeicherten personenbezogenen Informationen aufgrund der Art der genannten Angelegenheiten behindern könnte" (Artikel 38 APPIHAO). Wenn es jedoch möglich ist, Teile, die einer Ausnahme unterliegen, problemlos zu trennen und abzugrenzen, müssen die Verwaltungsorgane zumindest eine teilweise Offenlegung gewähren (siehe z. B. Artikel 15 Absatz 1 APPIHAO) ([140]).

([136]) Nach dem Gesetz über die Errichtung der Kommission für die Prüfung der öffentlichen Sicherheit müssen der Vorsitzende und die Mitglieder der Kommission „ihre Befugnisse unabhängig ausüben" (Artikel 3). Sie werden vom Premierminister mit Zustimmung der beiden Häuser des Parlaments ernannt und können nur „aus wichtigem Grund" (z. B. Freiheitsentzug, Fehlverhalten, psychische oder physische Störungen, Eröffnung eines Insolvenzverfahrens) entlassen werden.

([137]) Verordnung über die ordentliche Kontrolle durch den Nachrichtendienst für öffentliche Sicherheit (Generaldirektor des PSIA, Anweisung Nr. 4, 1986).

([138]) Verordnung über die außerordentliche Kontrolle durch den Nachrichtendienst für öffentliche Sicherheit (Generaldirektor des PSIA, Anweisung Nr. 11, 2008). Außerordentliche Kontrollen werden durchgeführt, wenn der Generaldirektor des PSIA dies für notwendig erachtet.

([139]) Dies bezieht sich auf das Recht, eine Kopie der „gespeicherten personenbezogenen Informationen" zu erhalten.

([140]) Siehe auch die Möglichkeit der „Offenlegung nach Ermessen" selbst in einem Fall, in dem „Informationen, die der Geheimhaltung unterliegen", in den „gespeicherten personenbezogenen Informationen" enthalten sind, für die eine Offenlegung angestrebt wird (Artikel 16 APPIHAO).

(167) In jedem Fall muss das Verwaltungsorgan innerhalb einer bestimmten Frist (von 30 Tagen, die unter bestimmten Voraussetzungen um weitere 30 Tage verlängert werden kann) einen schriftlichen Beschluss fassen. Wenn der Antrag abgelehnt oder nur teilweise bewilligt wird oder wenn die Person das Verhalten des Verwaltungsorgans aus anderen Gründen als „rechtswidrig oder ungerecht" ansieht, kann die Person eine behördliche Überprüfung auf der Grundlage des Verwaltungsbeschwerdeprüfungsgesetzes beantragen ([141]). In einem solchen Fall muss der Leiter des Verwaltungsorgans, das über die Beschwerde entscheidet, die Kontrollstelle für die Offenlegung von Informationen und den Schutz personenbezogener Informationen (*Information Disclosure and Personal Information Protection Review Board*, Artikel 42 und 43 APPIHAO) konsultieren, ein unabhängiges Fachgremium, dessen Mitglieder vom Premierminister mit Zustimmung der beiden Häuser des Parlaments ernannt werden. Nach den vorliegenden Informationen kann die Kontrollstelle eine Untersuchung ([142]) durchführen und in diesem Zusammenhang das Verwaltungsorgan auffordern, die gespeicherten personenbezogenen Informationen, einschließlich der als Verschlusssache eingestuften Inhalte, sowie weitere Informationen und Dokumente vorzulegen. Der dem Beschwerdeführer sowie dem Verwaltungsorgan übermittelte und veröffentlichte Abschlussbericht ist zwar nicht rechtlich verbindlich, ihm wird aber in fast allen Fällen gefolgt ([143]).Darüber hinaus hat die Person die Möglichkeit, die Entscheidung über die Beschwerde auf der Grundlage des Verwaltungsrechtsstreitigkeitengesetzes vor Gericht anzufechten. Dies gibt den Weg frei für eine gerichtliche Kontrolle in Bezug auf die Anwendung der nationalen Sicherheitsausnahme(n), einschließlich der Frage, ob eine solche Ausnahme missbraucht wurde oder noch immer gerechtfertigt ist.

(168) Um die Ausübung der oben genannten Rechte nach dem APPIHAO zu erleichtern, hat das MIC 51 „Informationszentralen" eingerichtet, die umfassende Informationen über diese Rechte, die geltenden Antragsverfahren und mögliche Rechtsbehelfe bereitstellen ([144]). Die Verwaltungsorgane müssen „Informationen zur Verfügung stellen, die zur Identifizierung der gespeicherten personenbezogenen Informationen beitragen" ([145]), und „andere geeignete Maßnahmen unter dem Aspekt der Erleichterung für die Person treffen, die den Antrag zu stellen beabsichtigt" (Artikel 47 Absatz 1 APPIHAO).

(169) Wie im Falle von strafrechtlichen Ermittlungen können auch im Bereich der nationalen Sicherheit Einzelpersonen Rechtsbehelfe einlegen, indem sie sich direkt an die PPC wenden. Dadurch wird das spezifische Streitschlichtungsverfahren ausgelöst, das die japanische Regierung für EU-Bürger eingerichtet hat, deren personenbezogene Daten im Rahmen dieses Beschlusses übermittelt werden (siehe ausführliche Erläuterungen in den Erwägungsgründen 141 bis 144 und 149).

(170) Darüber hinaus können Einzelpersonen Rechtsschutz in Form einer Schadensersatzklage nach dem Staatshaftungsgesetz, das auch immaterielle Schäden erfasst, und unter bestimmten Voraussetzungen die Löschung der erhobenen Daten verlangen (siehe Erwägungsgrund 147).

### 4. SCHLUSSFOLGERUNG: ANGEMESSENES SCHUTZNIVEAU FÜR AUS DER EUROPÄISCHEN UNION AN UNTERNEHMER IN JAPAN ÜBERMITTELTE PERSONENBEZOGENE DATEN

(171) Die Kommission ist der Auffassung, dass das APPI, ergänzt durch die Ergänzenden Vorschriften in Anhang I, in Verbindung mit den offiziellen Erklärungen, Zusicherungen und Verpflichtungen in Anhang II ein Schutzniveau für aus der Europäischen Union übermittelte personenbezogene Daten gewährleistet, das der Sache nach demjenigen gleichwertig ist, das durch die Verordnung (EU) 2016/679 garantiert wird.

(172) Darüber hinaus ist die Kommission der Auffassung, dass die Aufsichtsmechanismen und Rechtsbehelfe im japanischen Recht es insgesamt ermöglichen, Verstöße durch empfangende PIHBO zu erkennen und in der Praxis zu ahnden und der betroffenen Person Rechtsbehelfe anzubieten, um Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten und schließlich die Berichtigung oder Löschung dieser Daten zu erwirken.

([141]) Verwaltungsbeschwerdeprüfungsgesetz (Gesetz Nr. 160 aus dem Jahr 2014), insbesondere Artikel 1 Absatz 1.

([142]) Siehe Artikel 9 des Gesetzes über die Errichtung der Kontrollstelle für die Offenlegung von Informationen und den Schutz personenbezogener Informationen (Gesetz Nr. 60 aus dem Jahr 2003).

([143]) Nach den vorliegenden Informationen ist das Verwaltungsorgan dem Bericht in den 13 Jahren seit 2005 (dem Jahr, in dem das APPIHAO in Kraft trat) nur in zwei von mehr als 2000 Fällen nicht gefolgt, obwohl die Kontrollstelle den Verwaltungsentscheidungen in einer Reihe von Fällen widersprochen hat. Zudem muss das Verwaltungsorgan, wenn es eine von den Feststellungen des Berichts abweichende Entscheidung trifft, klar die Gründe dafür angeben. Siehe Anhang II Abschnitt III Buchstabe C, mit Bezug auf Artikel 50 Absatz 1 Ziffer iv des Verwaltungsbeschwerdeprüfungsgesetzes.

([144]) Die Informationszentralen — eine in jeder Präfektur — geben den Bürgern Erläuterungen zu personenbezogenen Informationen, die von Behörden erhoben werden (z. B. in bestehenden Datenbanken), und zu den geltenden Datenschutzvorschriften (APPIHO), einschließlich der Art und Weise, wie die Rechte auf Offenlegung, Berichtigung oder Aussetzung der Verwendung ausgeübt werden können. Gleichzeitig fungieren die Informationszentralen als Kontaktstelle für Anfragen/Beschwerden von Bürgern. Siehe Anhang II Abschnitt II Buchstabe C Nummer 4 Buchstabe a.

([145]) Siehe auch die Artikel 10 und 11 APPIHAO über das „Register der Dateien mit personenbezogenen Informationen", die jedoch weit gefasste Ausnahmen für „Dateien mit personenbezogenen Informationen" enthalten, die für strafrechtliche Ermittlungen ausgearbeitet oder beschafft wurden oder deren Inhalt Sicherheitsbelange oder andere wichtige Interessen des Staates betrifft (siehe Artikel 10 Absatz 2 Ziffern i und ii APPIHAO).

(173) Schließlich ist die Kommission auf der Grundlage der verfügbaren Informationen über die japanische Rechtsordnung, einschließlich der in Anhang II enthaltenen Erklärungen, Zusicherungen und Verpflichtungen der japanischen Regierung, der Auffassung, dass jeder Eingriff in die Grundrechte der Personen, deren personenbezogene Daten aus der Europäischen Union an Japan übermittelt werden, durch japanische Behörden aus Gründen des öffentlichen Interesses, insbesondere aus Gründen der Strafverfolgung und der nationalen Sicherheit, auf das zur Erreichung des betreffenden berechtigten Ziels unbedingt erforderliche Maß beschränkt ist und dass ein wirksamer Rechtsschutz vor solchen Eingriffen besteht.

(174) Daher ist die Kommission in Anbetracht der Feststellungen dieses Beschlusses der Auffassung, dass Japan ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der Europäischen Union an PIHBO in Japan, die dem APPI unterliegen, übermittelt werden, es sei denn, der Empfänger gehört zu einer der in Artikel 76 Absatz 1 APPI genannten Kategorien und der Verarbeitungszweck entspricht ganz oder teilweise einem der in dieser Bestimmung vorgesehenen Zwecke.

(175) Auf dieser Grundlage kommt die Kommission zu dem Schluss, dass der Angemessenheitsstandard nach Artikel 45 der Verordnung (EU) 2016/679, wie er unter Berücksichtigung der Charta der Grundrechte der Europäischen Union insbesondere im Schrems-Urteil ([146]) ausgelegt wurde, erfüllt ist.

## 5. MAßNAHMEN DER DATENSCHUTZBEHÖRDEN UND UNTERRICHTUNG DER KOMMISSION

(176)ß Nach der Rechtsprechung des Gerichtshofs ([147]) 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 Japan 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.

(177) Daher sollte die Kommission die Situation in Bezug auf den Rechtsrahmen und die tatsächliche Praxis bei der Verarbeitung personenbezogener Daten, wie in diesem Beschluss bewertet, fortlaufend überwachen, einschließlich der Einhaltung der in Anhang II enthaltenen Erklärungen, Zusicherungen und Verpflichtungen durch die japanischen Behörden. Um diesen Prozess zu erleichtern, wird von den japanischen Behörden erwartet, dass sie die Kommission über wesentliche Entwicklungen im Zusammenhang mit diesem Beschluss informieren, und zwar sowohl in Bezug auf die Verarbeitung personenbezogener Daten durch Unternehmer als auch auf die Beschränkungen und Schutzmaßnahmen, die für den Zugriff der Behörden auf personenbezogene Daten gelten. Dies sollte auch für Beschlüsse der PPC nach Artikel 24 APPI gelten, mit denen das Schutzniveau eines Drittlands als dem in Japan garantierten Schutzniveau gleichwertig anerkannt wird.

(178) Damit die Kommission ihre Kontrollfunktion wirksam ausüben kann, sollten die Mitgliedstaaten die Kommission über alle relevanten Maßnahmen der nationalen Datenschutzbehörden (data protection authorities; im Folgenden „DPA") informieren, insbesondere über Anfragen oder Beschwerden von betroffenen EU-Bürgern in Bezug auf die Übermittlung personenbezogener Daten aus der Europäischen Union an Unternehmer in Japan. Ferner sollte die Kommission über jegliche Hinweise darauf informiert werden, dass die Maßnahmen der japanischen 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.

(179) 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. 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. Gleichzeitig muss das nationale Recht, wie vom Gerichtshof im Schrems-Urteil ([148]) erläutert und in Artikel 58 Absatz 5 der Verordnung anerkannt wurde, wenn eine DPA, auch auf eine Beschwerde hin, die Vereinbarkeit eines Angemessenheitsbeschlusses der Kommission mit den Grundrechten des Einzelnen auf Privatsphäre und Datenschutz infrage stellt, Rechtsbehelfe vorsehen, die es ihr ermöglichen, diese Rügen vor einem nationalen Gericht geltend zu machen, das im Zweifelsfall das Verfahren aussetzen und ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss ([149]).

([146]) Siehe oben Fußnote 3.
([147]) Schrems, Rn. 76.
([148]) Schrems, Rn. 65.
([149]) 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."

## 6. REGELMÄßIGE ÜBERPRÜFUNG DER ANGEMESSENHEITSFESTSTELLUNG

(180) In Anwendung des Artikels 45 Absatz 3 der Verordnung (EU) 2016/679 ([150]) und angesichts der Tatsache, dass sich das von der japanischen Rechtsordnung gewährte Schutzniveau ändern könnte, sollte die Kommission nach der Annahme dieses Beschlusses regelmäßig prüfen, ob die Feststellungen über die Angemessenheit des von Japan gewährleisteten Schutzniveaus noch sachlich und rechtlich gerechtfertigt sind.

(181) Zu diesem Zweck sollte dieser Beschluss innerhalb von zwei 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 DSGVO eingesetzten Ausschuss je nach Ergebnis, ob der Zweijahreszyklus beibehalten werden sollte. In jedem Fall sollten die anschließenden Überprüfungen mindestens alle vier Jahre stattfinden ([151]). Die Überprüfung sollte sich auf alle Aspekte der Funktionsweise dieses Beschlusses erstrecken, insbesondere auf die Anwendung der Ergänzenden Vorschriften (unter besonderer Berücksichtigung des Schutzes im Falle von Weiterübermittlungen), die Anwendung der Vorschriften über die Einwilligung, auch im Falle des Widerrufs, die Wirksamkeit der Ausübung der Rechte des Einzelnen sowie die Beschränkungen und Garantien in Bezug auf den staatlichen Zugriff, einschließlich des in Anhang II dieses Beschlusses dargelegten Rechtsbehelfsmechanismus. Gegenstand der Überprüfung sollte ferner die Wirksamkeit der Aufsicht und Durchsetzung in Bezug auf die Vorschriften sein, die für PIHBO sowie im Bereich der Strafverfolgung und der nationalen Sicherheit gelten.

(182) Zur Durchführung der Überprüfung sollte die Kommission mit der PPC zusammenkommen, gegebenenfalls unter Mitwirkung anderer japanischer 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 gemeinsamen Überprüfung sollte die Kommission die PPC auffordern, umfassende Informationen über alle Aspekte, die für die Feststellung der Angemessenheit von Belang sind, vorzulegen, auch über die Beschränkungen und Garantien in Bezug auf den staatlichen Zugriff ([152]). Die Kommission sollte auch Erläuterungen zu allen für diesen Beschluss maßgeblichen, ihr vorliegenden Informationen einholen, einschließlich öffentlicher Berichte von japanischen Behörden oder anderen Beteiligten in Japan, der EDPB, einzelnen DPA, zivilgesellschaftlichen Gruppen, Medienberichten oder jeder anderen verfügbaren Informationsquelle.

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

## 7. AUSSETZUNG DES ANGEMESSENHEITSBESCHLUSSES

(184) Kommt die Kommission auf der Grundlage der regelmäßigen und unangekündigten Kontrollen oder anderer verfügbarer Informationen zu dem Schluss, dass das Schutzniveau der japanischen Rechtsordnung nicht mehr als im Wesentlichen gleichwertig mit demjenigen in der Europäischen Union angesehen werden kann, sollte sie die zuständigen japanischen Behörden darüber informieren und verlangen, dass innerhalb eines bestimmten, angemessenen Zeitrahmens geeignete Maßnahmen ergriffen werden. Dazu gehören auch die Vorschriften, die sowohl für Unternehmer gelten als auch für japanische Behörden, die für die Strafverfolgung oder die nationale Sicherheit zuständig sind. Ein entsprechendes Verfahren würde zum Beispiel eingeleitet, wenn Weiterübermittlungen — auch auf der Grundlage von Beschlüssen der PPC nach Artikel 24 APPI, mit denen das Schutzniveau eines Drittlands als dem in Japan garantierten Schutzniveau gleichwertig anerkannt wird — nicht mehr mit Garantien vorgenommen werden, die die Kontinuität des Schutzes im Sinne des Artikels 44 DSGVO gewährleisten.

(185) Wenn die zuständigen japanischen Behörden am Ende des festgelegten Zeitraums nicht glaubhaft gemacht haben, dass dieser Beschluss weiterhin auf einem angemessenen Schutzniveau beruht, sollte die Kommission in Anwendung von Artikel 45 Absatz 5 der Verordnung (EU) 2016/679 das Verfahren einleiten, das zur teilweisen oder vollständigen Aussetzung oder Aufhebung dieses Beschlusses führt. Alternativ sollte die Kommission das Verfahren zur Änderung dieses Beschlusses einleiten, indem sie insbesondere Datenübermittlungen zusätzlichen Bedingungen unterwirft oder den Anwendungsbereich der Angemessenheitsfeststellung auf Datenübermittlungen beschränkt, für die die Kontinuität des Schutzes im Sinne des Artikels 44 DSGVO gewährleistet ist.

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

([151]) 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.

([152]) Siehe auch Anhang II Abschnitt IV: „Im Rahmen der regelmäßigen Überprüfung des Angemessenheitsbeschlusses werden die PPC und die Europäische Kommission Informationen über die Verarbeitung von Daten unter den Bedingungen der Angemessenheitsfeststellung austauschen, einschließlich derjenigen, die in dieser Erklärung dargelegt sind."

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

(187) Die Kommission sollte ferner die Einleitung des Verfahrens zur Änderung, Aussetzung oder Aufhebung dieses Beschlusses in Betracht ziehen, wenn die zuständigen japanischen Behörden im Rahmen der gemeinsamen Überprüfung oder anderweitig nicht die Informationen oder Erläuterungen liefern, die für die Bewertung des Schutzniveaus für personenbezogene Daten, die aus der Europäischen Union an Japan 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.

(188) In Fällen hinreichend begründeter Dringlichkeit, zum Beispiel, wenn eine schwerwiegende Verletzung von Rechten betroffener Personen droht, sollte die Kommission erwägen, nach Artikel 93 Absatz 3 der Verordnung (EU) 2016/679 in Verbindung mit Artikel 8 der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([153]) einen Beschluss zur Aussetzung oder Aufhebung dieses Beschlusses zu erlassen, der unmittelbar gelten sollte.

## 8. **SCHLUSSBEMERKUNGEN**

(189) Der Europäische Datenschutzausschuss hat seine Stellungnahme ([154]) veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

(190) Das Europäische Parlament hat eine Entschließung zu einer Strategie für den digitalen Handel verabschiedet, in der die Kommission aufgefordert wird, der Annahme von Angemessenheitsbeschlüssen mit wichtigen Handelspartnern unter den in der Verordnung (EU) 2016/679 festgelegten Bedingungen als grundlegenden Mechanismus bei der Absicherung der Übertragung personenbezogener Daten aus der Europäischen Union Vorrang einzuräumen und sie zu beschleunigen ([155]).Das Europäische Parlament hat auch eine Entschließung zu der Angemessenheit des von Japan gewährten Schutzes personenbezogener Daten ([156]) verabschiedet.

(191) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 93 Absatz 1 DSGVO eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

*Artikel 1*

(1) Für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 bietet Japan ein angemessenes Schutzniveau für personenbezogene Daten, die aus der Europäischen Union an personenbezogene Informationen handhabende Unternehmer in Japan übermittelt werden, die dem Gesetz zum Schutz personenbezogener Informationen, ergänzt durch die Ergänzenden Vorschriften in Anhang I, in Verbindung mit den offiziellen Erklärungen, Zusicherungen und Verpflichtungen in Anhang II, unterliegen.

([153]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

([154]) Stellungnahme 28/2018 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus in Japan, verabschiedet am 5. Dezember 2018.

([155]) Europäisches Parlament, Entschließung vom 12. Dezember 2017 „Auf dem Weg zu einer Strategie für den digitalen Handel" (2017/2065(INI)). Siehe insbesondere Nummer 8 („… weist darauf hin, dass personenbezogene Daten an Drittländer übermittelt werden können, ohne auf allgemeine Bestimmungen in Handelsabkommen zurückzugreifen, wenn die … in Kapitel V der Verordnung (EU) 2016/679 verankerten Anforderungen sowohl derzeit als auch künftig erfüllt sind; stellt fest, dass Angemessenheitsbeschlüsse (auch Teilbeschlüsse und bereichsbezogene Beschlüsse) ein grundlegender Mechanismus bei der Absicherung der Übertragung personenbezogener Daten von der EU in ein Drittland sind; weist darauf hin, dass die EU nur mit vier ihrer 20 größten Handelspartner Angemessenheitsbeschlüsse angenommen hat …") und Nummer 9 („fordert die Kommission auf, der Annahme von Angemessenheitsbeschlüssen Vorrang einzuräumen und sie zu beschleunigen, sofern Drittländer durch ihr einzelstaatliches Recht oder ihre internationalen Verpflichtungen ein Maß an Schutz sicherstellen, das mit demjenigen, das in der EU gewährt wird, ‚im Wesentlichen gleichwertig' ist …").

([156]) Entschließung des Europäischen Parlaments vom 13. Dezember 2018 „Angemessenheit des von Japan gewährten Schutzes personenbezogener Daten" (2018/2979(RSP)).

(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 jeweils aufgeführten Zwecke entsprechen:

a) Rundfunkanstalten, Zeitungsverlage, Kommunikationsagenturen und andere Presseorganisationen (einschließlich Personen, die im Rahmen ihrer Geschäftstätigkeit Presseaktivitäten ausüben), soweit sie personenbezogene Daten für Pressezwecke verarbeiten,

b) Personen, die professionell schreiben, soweit dies personenbezogene Daten umfasst,

c) Hochschulen und andere Organisationen oder Gruppen, die sich mit wissenschaftlichen Studien befassen, und Personen, die einer solchen Organisation oder Gruppe angehören, soweit sie personenbezogene Daten für die Zwecke wissenschaftlicher Studien verarbeiten,

d) religiöse Einrichtungen, soweit sie personenbezogene Daten für die Zwecke religiöser Aktivitäten (einschließlich aller damit verbundenen Aktivitäten) verarbeiten, und

e) politische Einrichtungen, soweit sie personenbezogene Daten für die Zwecke ihrer politischen Aktivitäten (einschließlich aller damit verbundenen Aktivitäten) verarbeiten.

*Artikel 2*

Üben die zuständigen Behörden in den Mitgliedstaaten ihre Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 zum Schutz von Einzelpersonen bei der Verarbeitung ihrer personenbezogenen Daten aus und führt dies zur Aussetzung oder zum endgültigen Verbot der Übermittlung von Daten an einen bestimmten Unternehmer in Japan im Sinne des Artikels 1, so unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission.

*Artikel 3*

(1) Die Kommission überwacht fortlaufend die Anwendung des Rechtsrahmens, auf den sich dieser Beschluss stützt, einschließlich der Bedingungen, unter denen Weiterübermittlungen vorgenommen werden, um zu prüfen, ob Japan weiter ein angemessenes Schutzniveau im Sinne des Artikels 1 bietet.

(2) Die Mitgliedstaaten und die Kommission unterrichten einander über Fälle, in denen die Kommission für den Schutz personenbezogener Informationen oder eine andere zuständige japanische 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 japanischer 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) Innerhalb von zwei 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 japanischen Behörden durchgeführten gemeinsamen Überprüfung erhalten hat.

(5) Liegen der Kommission Hinweise darauf vor, dass ein angemessenes Schutzniveau nicht länger gewährleistet ist, so unterrichtet die Kommission die zuständigen japanischen Behörden. Erforderlichenfalls kann sie beschließen, diesen Beschluss auszusetzen, zu ändern oder aufzuheben oder seinen Anwendungsbereich einzuschränken, insbesondere wenn Hinweise darauf vorliegen, dass

a) Unternehmer in Japan, die nach diesem Beschluss personenbezogene Daten aus der Europäischen Union erhalten haben, die in den Ergänzenden Vorschriften in Anhang I festgelegten zusätzlichen Garantien nicht beachten oder Aufsicht und Durchsetzung diesbezüglich unzureichend sind;

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

Die Kommission kann Entwürfe solcher Maßnahmen auch vorlegen, wenn sie aufgrund mangelnder Kooperation der japanischen Regierung nicht feststellen kann, ob die Feststellung in Artikel 1 Absatz 1 berührt ist.

*Artikel 4*

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 23. Januar 2019

*Für die Kommission*
Věra JOUROVÁ
*Mitglied der Kommission*

*ANHANG 1*

**ERGÄNZENDE VORSCHRIFTEN NACH DEM GESETZ ÜBER DEN SCHUTZ PERSONENBEZOGENER INFORMATIONEN FÜR DIE HANDHABUNG VON AUF DER GRUNDLAGE EINES ANGEMESSENHEITSBESCHLUSSES AUS DER EU ÜBERMITTELTEN PERSONENBEZOGENEN DATEN**

Inhaltsverzeichnis



[Begriffe]

| | |
|---|---|
| „Angemessenheitsbeschluss“ | Beschluss der Europäischen Kommission, wonach in einem Drittland oder einem Gebiet in diesem Drittland usw. ein angemessenes Schutzniveau für personenbezogene Daten nach Artikel 45 der DSGVO gewährleistet ist |
| „DSGVO“ | Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) |
| „EU“ | Europäische Union, einschließlich ihrer Mitgliedstaaten und unter Berücksichtigung des EWR-Abkommens Island, Liechtenstein und Norwegen |
| „Gesetz“ | Gesetz über den Schutz personenbezogener Informationen (Gesetz Nr. 57, 2003) |
| „Kabinettsverordnung“ | Kabinettsverordnung zur Durchsetzung des Gesetzes über den Schutz personenbezogener Informationen (Kabinettsverordnung Nr. 507, 2003) |
| „Leitlinien zu den allgemeinen Vorschriften“ | Leitlinien zum Gesetz über den Schutz personenbezogener Informationen (Band „Allgemeine Vorschriften“) (Mitteilung der Kommission für den Schutz personenbezogener Informationen Nr. 65, 2015) |
| „Vorschriften“ | Durchsetzungsvorschriften zum Gesetz über den Schutz personenbezogener Informationen (Vorschriften der Kommission für den Schutz personenbezogener Informationen Nr. 3, 2016) |

Um eine wechselseitige und reibungslose Übermittlung personenbezogener Daten zwischen Japan und der EU zu ermöglichen, hat die Kommission für den Schutz personenbezogener Informationen die EU als anderes Land benannt, das über ein System zum Schutz personenbezogener Informationen verfügt, dessen Standards mit denen des japanischen als gleichwertig angesehen werden, was den Schutz der Rechte und Interessen einer Person auf der Grundlage von Artikel 24 des Gesetzes angeht; die Europäische Kommission hat gleichzeitig beschlossen, dass Japan ein angemessenes Schutzniveau für personenbezogene Daten gemäß Artikel 45 der DSGVO gewährleistet.

Daher ist eine wechselseitige und reibungslose Übermittlung personenbezogener Daten zwischen Japan und der EU möglich, bei der für ein hohes Maß an Schutz der Rechte und Interessen einzelner Personen gesorgt ist. Um für dieses hohe Maß an Schutz personenbezogener Informationen, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt werden, zu sorgen, und angesichts der Tatsache, dass es zwar große Übereinstimmungen zwischen den beiden System gibt, jedoch einige wichtige Unterschiede bestehen, hat die Kommission für den Schutz personenbezogener Informationen diese ergänzenden Vorschriften auf der Grundlage der Bestimmungen des Gesetzes über die Umsetzung usw. der Zusammenarbeit mit den Regierungen in anderen Ländern erlassen; auf diese Weise soll auch für den angemessenen Umgang mit personenbezogenen Informationen, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt wurden, durch einen personenbezogene Informationen handhabenden Unternehmer sowie die ordnungsgemäße und wirksame Umsetzung der Verpflichtungen nach diesen Vorschriften gesorgt werden ([1]).

([1]) Artikel 4, Artikel 6, Artikel 8, Artikel 24, Artikel 60 und Artikel 78 des Gesetzes und Artikel 11 der Vorschriften.

Insbesondere ist in Artikel 6 des Gesetzes die Befugnis vorgesehen, die notwendigen rechtlichen und sonstigen Maßnahmen zu treffen, um einen erhöhten Schutz personenbezogener Informationen zu gewährleisten und durch strengere Vorschriften, die die Vorschriften gemäß dem Gesetz und der Kabinettsverordnung ergänzen bzw. über diese hinausgehen, ein international entsprechendes/gleichwertiges System bezüglich personenbezogener Informationen zu schaffen. Die Kommission für den Schutz personenbezogener Informationen ist als die für die allgemeine Verwaltung des Gesetzes zuständige Behörde daher befugt, gemäß Artikel 6 des Gesetzes strengere Regelungen zu erlassen, indem sie die derzeitigen Ergänzenden Vorschriften verfasst, mit denen für einen erhöhten Schutz der Rechte und Interessen von Personen bezüglich des Umgangs mit personenbezogenen Daten gesorgt wird, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt werden, auch hinsichtlich der Definition personenbezogener Informationen, die einer besonderen Sorgfalt bedürfen, gemäß Artikel 2 Absatz 3 des Gesetzes und gespeicherter personenbezogener Informationen gemäß Artikel 2 Absatz 7 des Gesetzes (einschließlich der entsprechenden Speicherdauer).

Basierend hierauf sind die Ergänzenden Vorschriften für einen personenbezogene Informationen handhabenden Unternehmer, der auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelte personenbezogene Daten erhält, bindend; somit ist er verpflichtet, diese einzuhalten. Als rechtlich verbindliche Vorschriften können die Rechte und Verpflichtungen von der Kommission für den Schutz personenbezogener Informationen in gleicher Weise wie die Bestimmungen des Gesetzes durchgesetzt werden, die sie durch strengere und/oder ausführlichere Bestimmungen der Vorschriften ergänzt. Bei einer Verletzung der Rechte und Verpflichtungen nach den Ergänzenden Vorschriften können Einzelpersonen zudem in gleicher Weise Gerichte anrufen, wie dies für die Bestimmungen des Gesetzes gilt, die durch strengere und/oder ausführlichere Vorschriften ergänzt werden.

Kommt ein personenbezogene Informationen handhabender Unternehmer einer oder mehreren Verpflichtungen nach den Ergänzenden Vorschriften nicht nach, so ist die Kommission für den Schutz personenbezogener Informationen befugt, Maßnahmen nach Artikel 42 des Gesetzes zu erlassen. Was allgemeine personenbezogene Informationen angeht, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt werden, so gilt das Versäumnis eines personenbezogene Informationen handhabenden Unternehmers, einer Empfehlung nach Artikel 42 Absatz 1 des Gesetzes nachzukommen, ohne dass hierfür ein berechtigter Grund ([2]) besteht, immer als schwerwiegende, unmittelbare Verletzung der Rechte und Interessen einer Person im Sinne des Artikels 42 Absatz 2 des Gesetzes.

(1) Personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen (Artikel 2 Absatz 3 des Gesetzes)

Artikel 2 Absatz 3 des Gesetzes

(3) Im Rahmen dieses Gesetzes gelten als „personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen" personenbezogene Informationen, die die Rasse, den Glauben, den sozialen Status, die Krankengeschichte, die Vorstrafen des Betroffenen, die Tatsache, dass er durch eine Straftat einen Schaden erlitten hat, oder andere Beschreibungen usw. umfassen und deren Handhabung gemäß einer Kabinettsverordnung einer besonderen Sorgfalt bedarf, damit keine unfaire Diskriminierung, kein Schaden und keine sonstigen Nachteile zulasten des Betroffenen verursacht werden.

Artikel 2 der Kabinettsverordnung

Als entsprechende Beschreibungen usw. gemäß einer Kabinettsverordnung nach Artikel 2 Absatz 3 des Gesetzes gelten Beschreibungen usw., die einem oder mehreren der nachfolgend aufgeführten Punkte entsprechen (ausgenommen solcher, die unter die Krankenakte oder das Vorstrafenregister des Betroffenen fallen):

i) das Vorliegen einer körperlichen Behinderung, einer Intelligenzminderung oder einer psychischen Behinderung (einschließlich von Entwicklungsstörungen) oder anderer physischer oder geistiger funktioneller Beeinträchtigungen gemäß den Vorschriften der Kommission für den Schutz personenbezogener Daten;

ii) die Ergebnisse einer medizinischen Kontrolle oder sonstigen Untersuchung (im Folgenden „medizinische Kontrolle usw.") zur Vorbeugung und Früherkennung einer Krankheit, die ein Arzt oder eine andere mit medizinischen Aufgaben betraute Person (im Folgenden „Arzt usw.") an einem Betroffenen vornimmt;

iii) die Tatsache, dass ein Arzt usw. dem Betroffenen auf der Grundlage der Ergebnisse der medizinischen Kontrolle usw. oder aufgrund einer Krankheit, Verletzung oder sonstiger psychischer oder physischer Veränderungen Empfehlungen für die Verbesserung des psychischen oder physischen Zustands ausgesprochen hat oder ihm medizinische Versorgung hat zukommen lassen oder eine Verschreibung erteilt hat;

iv) die Tatsache, dass eine Festnahme, Durchsuchung, Beschlagnahme, Inhaftierung, Einleitung einer strafrechtlichen Untersuchung oder andere Verfahren im Zusammenhang mit einem Strafverfahren zulasten eines Betroffenen als Beschuldigtem oder Angeklagtem durchgeführt wurden;

([2]) Als berechtigter Grund gelten ein außergewöhnliches Ereignis außerhalb der Kontrolle des personenbezogene Informationen handhabenden Unternehmers, das vernünftigerweise nicht vorhergesehen werden kann (z. B. Naturkatastrophen), oder Fälle, in denen die Notwendigkeit, im Zusammenhang mit einer Empfehlung, die die Kommission für den Schutz personenbezogener Informationen nach Artikel 42 Absatz 1 des Gesetzes ausgesprochen hat, Maßnahmen zu ergreifen, nicht mehr besteht, weil der personenbezogene Informationen handhabende Unternehmer alternative Maßnahmen ergriffen hat, mit denen die Verletzung vollständig behoben wurde.

v) die Tatsache, dass eine Untersuchung, Beobachtungs- und Schutzmaßnahmen, eine Anhörung oder ein Beschluss, schützende Maßnahmen oder sonstige Verfahren im Zusammenhang mit einem Jugendschutzfall zulasten des Betroffenen als jugendlichem Straftäter oder einschlägig Verdächtigem gemäß Artikel 3 Absatz 1 des Jugendgesetzes durchgeführt wurden.

Artikel 5 der Vorschriften

Als physische und psychische funktionelle Beeinträchtigungen gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen gemäß Artikel 2 Ziffer i der Verordnung gelten die nachstehend aufgeführten:

i) körperliche Behinderungen gemäß der beigefügten Tabelle des Gesetzes über die Fürsorge für Menschen mit körperlichen Behinderungen (Gesetz Nr. 283 von 1949)

ii) Intelligenzminderungen gemäß dem Gesetz über die Fürsorge für Menschen mit Intelligenzminderung (Gesetz Nr. 37 von 1960)

iii) psychische Behinderungen gemäß dem Gesetz über psychische Gesundheit und Fürsorge für Menschen mit psychischen Behinderungen (Gesetz Nr. 123 von 1950) (einschließlich Entwicklungsstörungen nach Artikel 2 Absatz 1 des Gesetzes über die Unterstützung von Personen mit Entwicklungsstörungen und mit Ausnahme von Intelligenzminderungen nach dem Gesetz über die Fürsorge für Menschen mit Intelligenzminderung)

iv) eine unheilbare Krankheit oder eine sonstige Krankheit, deren Schwere gemäß Kabinettsverordnung nach Artikel 4 Absatz 1 des Gesetzes über umfassende Unterstützung des täglichen und sozialen Lebens von Menschen mit Behinderungen (Gesetz Nr. 123 von 2005) jenen gleichwertig ist, die vom Minister für Gesundheit, Arbeit und Soziales in genanntem Absatz festgelegt wurden.

Enthalten personenbezogene Daten, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt wurden, Daten betreffend das Sexualleben oder die sexuelle Orientierung einer Person oder die Zugehörigkeit zu einer Gewerkschaft, was im Rahmen der DSGVO als besondere Kategorien personenbezogener Daten definiert ist, so müssen personenbezogene Informationen handhabende Unternehmer diese personenbezogenen Daten in gleicher Weise behandeln wie besonderer Sorgfalt bedürfende personenbezogene Informationen im Sinne von Artikel 2 Absatz 3 des Gesetzes.

(2) Gespeicherte personenbezogene Daten (Artikel 2 Absatz 7 des Gesetzes)

Artikel 2 Absatz 7 des Gesetzes

(7) Der Begriff „gespeicherte personenbezogene Daten“ bezeichnet im Rahmen dieses Gesetzes personenbezogene Daten, die ein personenbezogene Informationen handhabender Unternehmer offenlegen oder korrigieren, deren Inhalte er ergänzen oder löschen, deren Nutzung er einstellen, die er löschen oder deren Weitergabe an Dritte er einstellen darf, und bei denen es sich weder um solche Daten handelt, bei denen gemäß einer Kabinettsverordnung die Wahrscheinlichkeit besteht, dass sie der Öffentlichkeit oder anderen Interessen schaden, wenn ihr Vorhandensein oder Fehlen bekannt wird, oder die innerhalb einer per Kabinettsverordnung festgelegten Frist von höchstens einem Jahr zu löschen sind.

Artikel 4 der Kabinettsverordnung

Bei den per Kabinettsverordnung nach Artikel 2 Absatz 7 festgelegten Daten handelt es sich um personenbezogene Daten,

i) bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens dem Leben, der körperlichen Unversehrtheit oder dem Vermögen eines Betroffenen oder eines Dritten schaden würde;

ii) bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens eine rechtswidrige oder ungerechte Handlung fördern oder veranlassen würde;

iii) bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens die nationale Sicherheit beeinträchtigen, ein Vertrauensverhältnis zu einem anderen Land oder einer internationalen Organisation zerstören oder bei Verhandlungen mit einem anderen Land oder einer internationalen Organisation Nachteile mit sich bringen würde;

iv) bei denen die Möglichkeit besteht, dass das Bekanntwerden ihres Vorhandenseins oder Fehlens die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung behindern würde, zum Beispiel die Verhütung, Bekämpfung oder Untersuchung einer Straftat.

Artikel 5 der Kabinettsverordnung

Der Zeitraum, der per Kabinettsverordnung nach Artikel 2 Absatz 7 des Gesetzes festgelegt wird, beträgt sechs Monate.

Auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelte personenbezogene Daten müssen als gespeicherte personenbezogene Daten im Sinne von Artikel 2 Absatz 7 des Gesetzes gehandhabt werden, und zwar unabhängig davon, innerhalb welcher Frist sie zu löschen sind.

Fallen personenbezogene Daten, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt wurden, unter personenbezogene Daten, bei denen gemäß einer Kabinettsverordnung die „Wahrscheinlichkeit besteht, dass sie der Öffentlichkeit oder anderen Interessen schaden, wenn ihr Vorhandensein oder Fehlen bekannt wird", so brauchen solche Daten nicht als gespeicherte personenbezogene Daten gehandhabt zu werden (siehe Artikel 4 der Kabinettsverordnung, Leitlinien mit allgemeinen Vorschriften, „2–7. Gespeicherte personenbezogene Daten").

(3) Festlegung eines Verwendungszwecks, Beschränkungen aufgrund eines Verwendungszwecks (Artikel 15 Absatz 1, Artikel 16, Absatz 1 und Artikel 26 Absätze 1 und 3 des Gesetzes)

Artikel 15 Absatz 1 des Gesetzes

(1) Ein personenbezogene Informationen handhabender Unternehmer muss bei der Handhabung personenbezogener Informationen den Zweck ihrer Verwendung (im Folgenden „Verwendungszwecks") so genau wie möglich angeben.

Artikel 16 Absatz 1 des Gesetzes

1) Ein personenbezogene Informationen handhabender Unternehmer darf personenbezogene Informationen nicht ohne vorherige Zustimmung des Betroffenen über das Maß hinaus handhaben, das notwendig ist, um einen gemäß den Bestimmungen des vorstehenden Artikels festgelegten Verwendungszweck zu erreichen.

Artikel 26 Absätze 1 und 3 des Gesetzes

1) Ein personenbezogene Informationen handhabender Unternehmer muss, wenn er personenbezogene Daten von Dritten erhält, gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen Folgendes angeben; (entfällt)

   i) (entfällt)

   ii) die Umstände, unter denen diese personenbezogenen Daten von dem Dritten erworben wurden;

3) Nachdem er die Angaben nach Absatz 1 gemacht hat, muss der personenbezogene Informationen handhabende Unternehmer gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen Aufzeichnungen über das Datum, an dem er die personenbezogener Daten erhalten hat, Angaben hierzu sowie andere Angaben gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen aufbewahren.

Handhabt ein personenbezogene Informationen handhabender Unternehmer personenbezogene Informationen über das für die Erreichung eines Verwendungszwecks gemäß Artikel 15 Absatz 1 des Gesetzes erforderliche Maß hinaus, muss er vorab die Zustimmung des Betroffenen einholen (Artikel 16 Absatz 1 des Gesetzes). Erhält ein personenbezogene Informationen handhabender Unternehmer personenbezogene Daten von einem Dritten, so muss er gemäß den Vorschriften Angaben etwa über die Umstände machen, unter denen der betreffende Dritte in den Besitz der Daten gelangt ist, und diese Angaben aufzeichnen (Artikel 26 Absätze 1 und 3 des Gesetzes).

Erhält ein personenbezogene Informationen handhabender Unternehmer auf der Grundlage eines Angemessenheitsbeschlusses personenbezogene Daten aus der EU, so müssen Angaben zu den Umständen, unter denen die betreffenden Daten erworben wurden, gemäß Artikel 26 Absätze 1 und 3 gemacht und aufgezeichnet werden, einschließlich des Verwendungszwecks, zu dem sie aus der EU übermittelt wurden.

Analog gilt, falls ein personenbezogene Informationen handhabender Unternehmer von einem anderen personenbezogene Informationen handhabenden Unternehmer personenbezogene Daten erhält, die zuvor auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt wurden, dass Angaben zu den Umständen, unter denen die betreffenden Daten erworben wurden, gemäß Artikel 26 Absätze 1 und 3 gemacht und aufgezeichnet werden müssen, einschließlich des Verwendungszwecks, zu dem sie übermittelt wurden.

In vorstehend genanntem Fall ist der personenbezogene Informationen handhabende Unternehmer verpflichtet, den Zweck anzugeben, für den die betreffenden Daten im Rahmen des Verwendungszwecks genutzt werden, zu dem sie, wie nach Artikel 26 Absätze 1 und 3 angegeben und aufgezeichnet, ursprünglich oder anschließend übermittelt wurden, sowie die Daten im Rahmen dieses genannten Zwecks zu nutzen (gemäß Artikel 15 Absatz 1 und Artikel 16 Absatz 1 des Gesetzes).

4) Beschränkung der Übermittlung an einen Dritten in einem anderen Land (Artikel 24 des Gesetzes, Artikel 11 Absatz 2 der Vorschriften)

Artikel 24 des Gesetzes

Mit Ausnahme der in den einzelnen Ziffern des ersten Absatzes des vorstehenden Artikels genannten Fälle muss ein personenbezogene Informationen handhabender Unternehmer vorab die Zustimmung des Betroffenen zur Übermittlung der betreffenden Daten an einen Dritten in einem anderen Land einholen, wenn er personenbezogene Daten an einen Dritten (ausgenommen eine Person, die über ein System gemäß den Standards verfügt, die nach den Vorschriften der Kommission für den Schutz personenbezogener Informationen erforderlich sind, um kontinuierlich einer gleichwertigen Tätigkeit nachzugehen wie ein personenbezogene Informationen handhabender Unternehmer bezüglich der Handhabung von personenbezogenen Daten; in diesem Sinne nachstehend in diesem Artikel verwendet) in einem anderen Land (d. h. einem Land oder einer Region außerhalb des Hoheitsgebiets Japans; in diesem Sinne nachstehend in diesem Artikel verwendet; ausgenommen jene Länder, die gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen als Länder anerkannt sind, welche über ein System für den Schutz personenbezogener Informationen verfügen, dessen Standards bezüglich des Schutzes der Rechte und Interessen von Einzelpersonen mit denen Japans gleichwertig sind; in diesem Sinne nachstehend in diesem Artikel verwendet) übermittelt. In diesem Fall finden die Bestimmungen des vorstehenden Artikels keine Anwendung.

Artikel 11 Absatz 2 der Vorschriften

Standards nach den Vorschriften der Kommission für den Schutz personenbezogener Informationen gemäß Artikel 24 des Gesetzes müssen unter einen der folgenden Punkte fallen:

i) ein personenbezogene Informationen handhabender Unternehmer und eine Person, die personenbezogene Daten erhält, haben bezüglich der Handhabung von personenbezogenen Daten durch die Person, die diese erhält, die Umsetzung von Maßnahmen im Sinne der Bestimmungen nach Kapitel IV Abschnitt 1 des Gesetzes in angemessener und vernünftiger Weise sichergestellt;

ii) eine Person, die personenbezogene Daten erhält, wurde auf der Grundlage eines internationalen Rahmens für die Handhabung von personenbezogenen Informationen entsprechend anerkannt.

Übermittelt ein personenbezogene Informationen handhabender Unternehmer einem Dritten in einem anderen Land personenbezogene Daten, die er auf der Grundlage eines Angemessenheitsbeschlusses aus der EU erhalten hat, so muss er gemäß Artikel 24 des Gesetzes vorab die Zustimmung des Betroffenen zur Übermittlung der betreffenden Daten an einen Dritten in einem anderen Land einholen, nachdem dem Betroffenen die Informationen über die eine Übermittlung erforderlich machenden Umstände mitgeteilt wurden, die er für seine Entscheidung über die Zustimmung braucht; hiervon ausgenommen sind die folgenden Fälle i) bis iii).

(i) Der Dritte ist in einem Land niedergelassen, das nach den Vorschriften als ein Land gilt, in dem ein System zum Schutz personenbezogener Informationen besteht, dessen Standards beim Schutz der Rechte und Interessen von Einzelpersonen denen in Japan als gleichwertig anerkannt sind.

(ii) Der personenbezogene Informationen handhabende Unternehmer und der Dritte, der die personenbezogenen Daten erhält, haben bezüglich der Handhabung personenbezogener Daten durch den Dritten zusammen Maßnahmen ergriffen, die für ein dem Gesetz in Verbindung mit den vorliegenden Vorschriften gleichwertiges Schutzniveau sorgen und die in angemessener und vernünftiger Weise umgesetzt wurden (d. h. durch einen Vertrag, sonstige verbindliche Vereinbarungen oder verbindliche Vereinbarungen innerhalb einer Unternehmensgruppe).

(iii) In Fällen, die unter einen der Punkte in Artikel 23 Absatz 1 des Gesetzes fallen.

5) Anonym verarbeitete Informationen (Artikel 2 Absatz 9 und Artikel 36 Absätze 1 und 2 des Gesetzes)

Artikel 2 Absatz 9 des Gesetzes

9) Der Begriff „anonym verarbeitete Informationen“ bezeichnet in diesem Gesetz Informationen im Zusammenhang mit einer Person, die das mögliche Ergebnis einer Verarbeitung personenbezogener Informationen sind, welche weder die Identifizierung einer bestimmten Person durch Maßnahmen gemäß den nachstehenden Ziffern im Einklang mit der Unterteilung der personenbezogenen Informationen gemäß den einzelnen Ziffern noch die Wiederherstellung personenbezogener Informationen ermöglicht.

i) personenbezogene Informationen, die unter Absatz 1 Ziffer i fallen;

Teilweises Löschen der Beschreibungen usw., die in den betreffenden personenbezogenen Informationen enthalten sind (auch durch Ersetzen des fraglichen Teils der Beschreibungen usw. durch andere Beschreibungen usw., indem eine Methode ohne Regelmäßigkeit verwendet wird, die eine Wiederherstellung des fraglichen Teils der Beschreibungen usw. ermöglichen würde).

ii) personenbezogene Informationen, die unter Absatz 1 Ziffer ii fallen;

Löschen aller Codes zur Personenidentifizierung, die in den betreffenden personenbezogenen Informationen enthalten sind (auch durch Ersetzen der betreffenden Codes zur Personenidentifizierung durch andere Beschreibungen usw., indem eine Methode ohne Regelmäßigkeit verwendet wird, die eine Wiederherstellung der fraglichen Codes zur Personenidentifizierung ermöglichen würde).

Artikel 36 Absatz 1 des Gesetzes

1) Ein personenbezogene Informationen handhabender Unternehmer muss bei der Erstellung anonym verarbeiteter Informationen (beschränkt auf jene, die anonym verarbeitete Datenbanken für Informationen usw. bilden, im Folgenden in diesem Sinne verwendet) personenbezogene Informationen im Einklang mit den Standards verarbeiten, die gemäß den Vorschriften der Kommission über den Schutz personenbezogener Informationen dafür erforderlich sind, eine Identifizierung einer bestimmten Person oder die Wiederherstellung der ursprünglich verwendeten personenbezogenen Informationen unmöglich zu machen.

Artikel 19 der Vorschriften

Die Standards gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen nach Artikel 36 Absatz 1 des Gesetzes lauten folgendermaßen:

i) Vollständiges oder teilweises Löschen der Beschreibungen usw. in personenbezogenen Informationen, durch die eine bestimmte Person identifiziert werden kann (einschließlich durch ein Ersetzen dieser Beschreibungen usw. durch andere Beschreibungen usw., indem eine Methode ohne Regelmäßigkeit verwendet wird, die eine vollständige oder teilweise Wiederherstellung des fraglichen Teils der Beschreibungen usw. ermöglichen würde).

ii) Löschen aller Codes zur Personenidentifizierung, die in den personenbezogenen Informationen enthalten sind (einschließlich durch ein Ersetzen solcher Codes durch andere Beschreibungen usw., indem eine Methode ohne Regelmäßigkeit verwendet wird, die eine Wiederherstellung der Codes zur Personenidentifizierung ermöglichen würde).

iii) Löschen jener Codes (beschränkt auf die Codes, die Mehrfachinformationen miteinander verknüpfen, welche tatsächlich von einem personenbezogene Informationen handhabenden Unternehmer gehandhabt werden), durch die persönliche Informationen und Informationen, die durch an den personenbezogenen Informationen vorgenommenen Handlungen gewonnen wurden, verknüpft wurden (auch durch das Ersetzen der betreffenden Codes durch diese anderen Codes, durch die keine Verknüpfung der betreffenden personenbezogenen Informationen mit den Informationen möglich ist, die durch an diesen Informationen vorgenommene Handlungen gewonnen wurden, wobei eine Methode ohne Regelmäßigkeit verwendet wird, die eine Wiederherstellung dieser Codes ermöglichen könnte).

iv) Löschen aller idiosynkratischen Beschreibungen usw. (auch durch ein Ersetzen solcher Beschreibungen usw. durch andere Beschreibungen usw., indem eine Methode ohne Regelmäßigkeiten verwendet wird, die eine Wiederherstellung der idiosynkratischen Beschreibungen ermöglichen würde).

v) Neben Maßnahmen gemäß den vorstehenden Ziffern Ergreifung angemessener Maßnahmen auf der Grundlage der Ergebnisse der Prüfung der Merkmale usw. von Datenbanken für personenbezogene Informationen usw., wie etwa Unterschiede, die zwischen Beschreibungen usw., die in personenbezogenen Informationen enthalten sind, und Beschreibungen usw., die in anderen personenbezogenen Informationen enthalten sind, bestehen, welche die Datenbank mit personenbezogenen Informationen usw. bilden, die die betreffenden personenbezogenen Informationen enthalten.

Artikel 36 Absatz 2 des Gesetzes

(2) Ein personenbezogene Informationen handhabender Unternehmer muss nach der Erstellung anonym verarbeiteter Informationen im Einklang mit den Standards gemäß den Vorschriften der Kommission über den Schutz personenbezogener Informationen, — wie etwa derjenigen, die notwendig sind, um die unerlaubte Veröffentlichung von Informationen im Zusammenhang mit den Beschreibungen usw. und den Codes zur Personenidentifizierung, die aus zur Erstellung der anonym verarbeiteten Informationen genutzten personenbezogenen Informationen gelöscht wurden, sowie von Informationen über die Verarbeitungsmethode, die nach den Bestimmungen des vorstehenden Absatzes angewandt wurde, zu verhindern —, Maßnahmen zur Sicherheitskontrolle solcher Informationen ergreifen.

Artikel 20 der Vorschriften

Die Standards gemäß den Vorschriften der Kommission für den Schutz personenbezogener Informationen nach Artikel 36 Absatz 2 des Gesetzes lauten folgendermaßen:

i) Eindeutige Festlegung der Befugnis und der Verantwortlichkeiten einer Person, die Informationen im Zusammenhang mit diesen Beschreibungen usw. sowie die Codes zur Personenidentifizierung handhabt, welche aus den personenbezogenen Informationen gelöscht wurden, die zur Erstellung der anonymisierten Informationen genutzt wurden, und die jene Informationen handhabt, die mit der gemäß den Bestimmungen von Artikel 36 Absatz 1 angewandten Verarbeitungsmethode im Zusammenhang stehen (beschränkt auf solche Informationen, durch die personenbezogene Informationen durch die Nutzung der entsprechenden Informationen wiederhergestellt werden können (im Folgenden in diesem Artikel „mit der Verarbeitungsmethode usw. zusammenhängende Informationen");

ii) Festlegung von Vorschriften und Verfahren für die Handhabung von mit der Verarbeitungsmethode usw. zusammenhängenden Informationen, angemessene Handhabung von mit der Verarbeitungsmethode usw. zusammenhängenden Informationen im Einklang mit den Vorschriften und Verfahren sowie Bewertung der Handhabung und — auf der Grundlage dieser Bewertungsergebnisse — Ergreifen erforderlicher Verbesserungsmaßnahmen;

iii) Ergreifen notwendiger und geeigneter Maßnahmen, um zu verhindern, dass unbefugte Personen mit der Verarbeitungsmethode usw. zusammenhängende Informationen handhaben.

Personenbezogene Informationen, die auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelt wurden, gelten nur dann als anonym verarbeitete Informationen im Sinne von Artikel 2 Absatz 9 des Gesetzes, wenn der personenbezogene Informationen handhabende Unternehmer Maßnahmen ergreift, die ein Rückgängigmachen der Anonymisierung der betreffenden Personen für jedermann unmöglich macht, auch durch das Löschen von mit der Verarbeitungsmethode usw. zusammenhängenden Informationen (d. h. Informationen im Zusammenhang mit den Beschreibungen usw. sowie den Codes zur Personenidentifizierung, die aus den personenbezogenen Informationen gelöscht wurden, die zur Erstellung der anonym verarbeiteten Informationen genutzt wurden, sowie Informationen, die mit der gemäß den Bestimmungen von Artikel 36 Absatz 1 angewandten Verarbeitungsmethode im Zusammenhang stehen (beschränkt auf solche Informationen, durch die personenbezogene Informationen durch die Nutzung der entsprechenden Informationen wiederhergestellt werden können)).

*ANHANG 2*

Frau Věra Jourová, Kommissarin für Justiz, Verbraucher und Gleichstellung der Europäischen Kommission

Sehr geehrte Frau Kommissarin,

die konstruktiven Gespräche zwischen Japan und der Europäischen Kommission über den Aufbau eines Rahmens für die gegenseitige Übermittlung personenbezogener Daten zwischen Japan und der EU begrüße ich sehr.

Auf Ersuchen der Europäischen Kommission, gerichtet an die Regierung Japans, übermittle ich in der Anlage ein Dokument mit einer Übersicht über den Rechtsrahmen für den Zugang der Regierung Japans zu Informationen.

Dieses Dokument betrifft zahlreiche Ministerien und Behörden der japanischen Regierung, sodass die jeweiligen Fachministerien und -behörden (das Kabinettssekretariat, die staatliche Polizeibehörde, die Kommission für den Schutz personenbezogener Daten, das Innen- und Kommunikationsministerium, das Justizministerium, der Nachrichtendienst für öffentliche Sicherheit, das Verteidigungsministerium) im Rahmen ihrer jeweiligen Ressorts für die betreffenden Passagen dieses Dokuments inhaltlich zuständig sind. Nachstehend finden Sie die zuständigen Ministerien und Behörden sowie die entsprechenden Unterschriften.

Die Kommission für den Schutz personenbezogener Daten nimmt alle Anfragen 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.

Hochachtungsvoll

Yoko Kamikawa

Ministerin für Justiz

Verfasser dieses Dokuments sind das Ministerium für Justiz sowie die nachstehend aufgeführten Ministerien und Behörden.

Koichi Hamano

Berater, Kabinettssekretariat

Schunichi Kuryu

Generalkommissar der staatlichen Polizeibehörde

Mari Sonoda

Generalsekretärin, Kommission für den Schutz personenbezogener Daten

Mitsuru Yasuda

Stellvertretender Minister, Ministerium für Inneres und Kommunikation

Seimei Nakagawa

Nachrichtendienst für öffentliche Sicherheit

Kenichi Takahashi

Administrativer stellvertretender Minister für Verteidigung

14. September 2018

**Die Erhebung und Nutzung personenbezogener Informationen durch die japanischen Behörden für die Zwecke der Strafverfolgung und der nationalen Sicherheit**

Das folgende Dokument bietet einen Überblick über den rechtlichen Rahmen für die Erhebung und Nutzung personenbezogener (elektronischer) Informationen durch die japanischen Behörden für die Zwecke der Strafverfolgung und der nationalen Sicherheit (im Folgenden „staatlicher Zugriff"), insbesondere in Bezug auf die verfügbaren Rechtsgrundlagen, die geltenden Auflagen (Beschränkungen) und Garantien, einschließlich der unabhängigen Aufsicht und der möglichen individuellen Rechtsbehelfe. Adressatin dieser Darstellung ist die Europäische Kommission; sie erhält damit die Zusicherung, dass der staatliche Zugriff auf personenbezogene Informationen, die von der EU nach Japan übermittelt werden, auf das notwendige und angemessene Maß beschränkt bleibt, dass der Zugriff einer unabhängigen Aufsicht unterliegt und dass die von einer etwaigen Verletzung ihres Grundrechts auf Privatsphäre und Datenschutz betroffenen Personen Rechtsbehelfe einlegen können. Mit dieser Darstellung wird zugleich ein neuer Rechtsbehelfsmechanismus eingeführt, der von der Kommission für den Schutz personenbezogener Daten (Personal Information Protection Commission - PPC) verwaltet wird und der Bearbeitung der Beschwerden von EU-Bürgerinnen und -Bürgern betreffend den staatlichen Zugriff auf ihre aus der EU nach Japan übermittelten personenbezogenen Daten dient.

## I. **Allgemeine Rechtsgrundsätze für den staatlichen Zugriff**

Als eine Form der Ausübung öffentlicher Gewalt muss der staatliche Zugriff in voller Übereinstimmung mit dem Gesetz erfolgen (Legalitätsprinzip). In Japan sind personenbezogene Daten sowohl im privaten als auch im öffentlichen Sektor durch einen mehrfach gestaffelten Mechanismus geschützt.

### A. Verfassungsrechtlicher Rahmen und Vorbehalt des Rechtsprinzips

Das Recht auf Privatsphäre ist in Artikel 13 der Verfassung verankert und in der ständigen Rechtsprechung als verfassungsmäßiges Recht anerkannt. Der Oberste Gerichtshof hat hierzu entschieden, dass natürliche Personen nicht wünschen, dass andere ohne guten Grund ihre personenbezogenen Daten kennen, und dass diese Erwartung geschützt werden soll ([1]). Ein weitergehender Schutz ist in Artikel 21 Absatz 2 der Verfassung verankert, der die Achtung des Kommunikationsgeheimnisses gewährleistet, und in Artikel 35 der Verfassung, der das Recht garantiert, keiner Durchsuchung und Beschlagnahme ohne Gerichtsbeschluss unterzogen zu werden, was bedeutet, dass die Erhebung personenbezogener Daten, einschließlich des Zugriffs darauf, mit Zwangsmitteln stets auf der Grundlage einer gerichtlichen Anordnung erfolgen muss. Ein solcher Gerichtsbeschluss darf nur zur Untersuchung einer bereits begangenen Straftat ausgestellt werden. Daher ist eine Erhebung von Informationen durch Zwangsmittel für die Zwecke (nicht einer strafrechtlichen Ermittlung, sondern) der nationalen Sicherheit nach dem Rechtsrahmen Japans nicht gestattet.

Darüber hinaus muss im Einklang mit dem Vorbehalt des Rechtsprinzips die Zwangserhebung von Informationen gesondert gesetzlich genehmigt werden. Im Falle einer nicht durch Zwangsmittel erfolgenden/freiwilligen Erhebung werden die Informationen aus einer Quelle gewonnen, die frei zugänglich ist, oder sie werden aufgrund eines Antrags auf freiwillige Offenlegung erhalten, d. h. eines Antrags, der gegen die natürliche oder juristische Person, die Inhaberin der Informationen ist, nicht durchgesetzt werden kann. Dies ist jedoch nur insoweit zulässig, als die Behörde für die Durchführung der Untersuchung zuständig ist, da jede Behörde nur im Rahmen ihrer gesetzlich definierten administrativen Zuständigkeit tätig werden darf (unabhängig davon, ob ihre Tätigkeiten die Rechte und Freiheiten des Einzelnen berühren oder nicht). Dieser Grundsatz gilt auch für die Fähigkeit einer Behörde zur Erhebung personenbezogener Daten.

### B. Besondere Vorschriften für den Schutz personenbezogener Daten

Das Gesetz über den Schutz personenbezogener Informationen (Act on Protection of Personal Information - APPI) und das Gesetz über den Schutz personenbezogener Informationen bei Verwaltungsorganen (Act on the Protection of Personal Information Held by Administrative Organs — APPIHAO), die auf den verfassungsrechtlichen Bestimmungen beruhen und diese präzisieren, garantieren das Recht auf personenbezogene Daten im privaten und im öffentlichen Sektor.

Nach Artikel 7 APPI muss die PPC die „Grundlegende Richtlinie für den Schutz personenbezogener Daten" (im Folgenden „Grundlegende Richtlinie") formulieren. Diese „Grundlegende Richtlinie" wird mit Beschluss des japanischen Kabinetts als zentralem Organ der japanischen Regierung (Premierminister und Staatsminister) erlassen und gibt die Richtung für den Schutz personenbezogener Daten in Japan vor. Auf diese Weise fungiert die PPC als unabhängige Aufsichtsbehörde und dient als „Kommandozentrale" des japanischen Datenschutzsystems.

Immer dann, wenn Verwaltungsorgane personenbezogene Daten erheben, und unabhängig davon, ob sie dies mit Zwangsmitteln tun oder nicht, müssen sie grundsätzlich ([2]) die Auflagen des APPIHAO erfüllen. Das APPIHAO ist ein allgemeines Gesetz, das für die Verarbeitung von „gespeicherten personenbezogenen Informationen" ([3]) durch „Verwaltungsorgane" (gemäß der Definition in Artikel 2 Absatz 1 APPIHAO) gilt. Somit ist es auch auf die Datenverarbeitung in den Bereichen Strafverfolgung und nationale Sicherheit anwendbar. Mit Ausnahme der Präfekturpolizei handelt es sich bei allen Behörden, die zur Durchführung eines staatlichen Zugriffs befugt sind, um staatliche Behörden, die unter die

([1]) Oberster Gerichtshof, Urteil vom 12. September 2003 (2002 (Ju) Nr. 1656).

([2]) Für Ausnahmen in Bezug auf Kapitel 4 APPIHAO siehe S. 16 unten.

([3]) „Gespeicherte personenbezogene Informationen" nach Artikel 2 Absatz 5 APPIHAO bezeichnen personenbezogene Informationen, die ein Bediensteter eines Verwaltungsorgans im Zuge der Erfüllung seiner Aufgaben erstellt oder erlangt hat und die diesem Organ für die organisatorische Verwendung durch seine Bediensteten vorliegen.

Definition „Verwaltungsorgan“ fallen. Der Umgang der Präfekturpolizei mit personenbezogenen Informationen ist in den Präfekturverordnungen ([4]) geregelt, in denen dem APPIHAO gleichwertige Rechte und Pflichten in Bezug auf die Grundsätze für den Schutz personenbezogener Informationen festgelegt sind.

II. **Staatlicher Zugriff zu Strafverfolgungszwecken**

A) Rechtsgrundlagen und Einschränkungen

1) Erhebung personenbezogener Informationen mit Zwangsmitteln

*a) Rechtsgrundlagen*

Nach Artikel 35 der Verfassung darf gegen das Recht aller Personen auf Schutz ihrer Häuser, Papiere und Güter vor Zugriff, Durchsuchung und Beschlagnahme nicht verstoßen werden, es sei denn, es wurde wegen eines „hinreichenden Grundes“ ein Gerichtsbeschluss erwirkt, in dem insbesondere der zu durchsuchende Ort und die zu beschlagnahmenden Gegenstände beschrieben sind. Somit darf die Erhebung elektronischer Informationen mit Zwangsmitteln durch Behörden im Rahmen einer strafrechtlichen Ermittlung nur auf der Grundlage eines Gerichtsbeschlusses erfolgen. Dies gilt sowohl für die Sammlung elektronischer Aufzeichnungen, die (persönliche) Informationen enthalten, als auch für die Echtzeit-Überwachung von Kommunikation (das sogenannte Abhören). Die einzige Ausnahme von dieser Regel (die jedoch im Zusammenhang mit der elektronischen Übermittlung personenbezogener Daten aus dem Ausland nicht von Belang ist) stellt Artikel 220 Absatz 1 der Strafprozessordnung ([5]) dar, wonach ein Staatsanwalt, ein Staatsanwaltsgehilfe oder ein Beamter der Kriminalpolizei bei der Festnahme eines Verdächtigen oder eines „offenkundigen Straftäters“ erforderlichenfalls eine Durchsuchung und Beschlagnahme „vor Ort bei der Festnahme“ vornehmen kann.

Nach Artikel 197 Absatz 1 StPO sind Zwangsmaßnahmen zwecks Untersuchung „nur dann anzuwenden, wenn in der StPO besondere Bestimmungen vorgesehen sind“. Was die Erhebung elektronischer Informationen mit Zwangsmitteln betrifft, so handelt es sich bei den einschlägigen Rechtsgrundlagen in diesem Zusammenhang sowohl um Artikel 218 Absatz 1 StPO (wonach ein Staatsanwalt, ein Staatsanwaltsgehilfe oder ein Beamter der Kriminalpolizei, sofern dies für die Untersuchung einer Straftat erforderlich ist, eine Durchsuchung, Beschlagnahme oder Inaugenscheinnahme aufgrund eines von einem Richter erlassenen Gerichtsbeschlusses durchführen kann) als auch um Artikel 222-2 StPO (wonach Zwangsmaßnahmen zur Überwachung der elektronischen Kommunikation ohne Zustimmung beider Parteien auf der Grundlage anderer Gesetze durchgeführt werden). Die letztgenannte Bestimmung nimmt Bezug auf das „Gesetz über die Abhörung zur Strafverfolgung“ (Wiretapping Act; im Folgenden „Abhörgesetz“); darin ist in Artikel 3 Absatz 1 geregelt, unter welchen Bedingungen die Kommunikation im Zusammenhang mit bestimmten schweren Straftaten auf der Grundlage eines gerichtlichen Abhörbeschlusses abgehört werden dürfen ([6]).

In polizeilicher Hinsicht liegt die Ermittlungsbefugnis stets bei der Präfekturpolizei, während die staatliche Polizeibehörde (National Police Agency - NPA) keinerlei strafrechtliche Ermittlungen auf der Grundlage der Strafprozessordnung durchführt.

*b) Einschränkungen*

Die Erhebung elektronischer Informationen mit Zwangsmitteln wird durch die Verfassung und die gesetzlichen Ermächtigungsgrundlagen gemäß ihrer Auslegung in der ständigen Rechtsprechung eingeschränkt, worin insbesondere die Kriterien festgelegt sind, die bei der Ausstellung eines Gerichtsbeschlusses von den Gerichten anzuwenden sind. Zudem enthält das APPIHAO eine Reihe von Beschränkungen sowohl für die Erhebung von Informationen als auch für den Umgang damit (und lokale Verordnungen schreiben im Wesentlichen dieselben Kriterien für die Präfekturpolizei vor).

(1) Einschränkungen aufgrund der Verfassung und der gesetzlichen Ermächtigungsgrundlagen

Nach Artikel 197 Absatz 1 StPO sind Zwangsvorschriften „nur dann anzuwenden, wenn in der StPO besondere Bestimmungen vorgesehen sind“. In Artikel 218 Absatz 1 StPO ist dann festgelegt, dass die Beschlagnahme usw. auf der Grundlage einer richterlichen Anordnung nur vorgenommen werden darf, „wenn dies für die Untersuchung einer Straftat erforderlich ist“. Obwohl die Kriterien für die Beurteilung der Erforderlichkeit in Gesetzesvorschriften nicht näher

([4]) Jede Präfektur hat eine eigene Präfekturverordnung für den Schutz personenbezogener Informationen durch die Präfekturpolizei. Diese Präfekturverordnungen liegen nicht in englischer Übersetzung vor.

([5]) Nach Artikel 220 Absatz 1 StPO können ein Staatsanwalt, ein Staatsanwaltsgehilfe oder ein Beamter der Kriminalpolizei bei der Festnahme eines Verdächtigen erforderlichenfalls folgende Maßnahmen ergreifen: a) Betreten der Wohnung einer anderen Person usw., um nach dem Verdächtigen zu suchen; b) Durchsuchung, Beschlagnahme oder Inaugenscheinnahme vor Ort bei der Festnahme.

([6]) Im Einzelnen sieht diese Bestimmung vor, dass „der Staatsanwalt oder die Kriminalpolizei in den Fällen, die unter einen der folgenden Punkte fallen, und sofern ausreichender Verdacht besteht, dass Kommunikation zur Begehung, Vorbereitung, Verabredung von Folgetaten wie Unterdrückung von Beweismitteln usw., Anweisungen und anderer Kommunikationsaustausch zum Verbrechen stattfinden wird, wie in jedem der genannten Punkte ausgeführt, (im Folgenden im zweiten und dritten Punkt als ‚eine Reihe von Straftaten‘ bezeichnet) und dass Kommunikation über mit dieser Straftat zusammenhängende Angelegenheiten (im Folgenden in diesem Absatz als ‚die Straftat betreffende Kommunikation‘ bezeichnet) stattfinden wird, sowie in den Fällen, in denen es äußerst schwierig ist, auf andere Art den Straftäter zu identifizieren oder die Umstände/Einzelheiten der Begehung aufzuklären, die Kommunikation betreffend diese Straftat auf der Grundlage eines gerichtlichen Abhörbeschlusses abhören dürfen; dies gilt für ein Kommunikationsmittel, das durch Telefonnummer und andere Nummern/Codes zur Identifizierung von Herkunft oder Bestimmung des Telefons bestimmt ist und das von dem Verdächtigen aufgrund eines Vertrags mit einem Telekommunikationsanbieter verwendet wird, usw. (außer jene, bei denen kein Verdacht vorliegt, dass sie für ‚die Straftat betreffende Kommunikation‘ verwendet werden); bei jenen, bei denen ein begründeter Verdacht besteht, dass sie für ‚die Straftat betreffende Kommunikation‘ verwendet werden, darf das Abhören der ‚die Straftat betreffenden Kommunikation‘ mithilfe dieses Kommunikationsmittels vorgenommen werden.“

bestimmt sind, hat der Oberste Gerichtshof ([7]) entschieden, dass der Richter bei der Beurteilung der Erforderlichkeit von Bestimmungen eine Gesamtbewertung vornehmen sollte, wobei insbesondere Folgendes zu berücksichtigen ist:

a) Schwere der Straftat und wie sie begangen wurde;

b) Wert und Bedeutung des beschlagnahmten Materials als Beweismittel;

c) Wahrscheinlichkeit des Verbergens oder der Vernichtung der beschlagnahmten Materialien;

d) Umfang der durch eine Beschlagnahme verursachten Nachteile;

e) andere damit zusammenhängende Bedingungen.

Einschränkungen ergeben sich auch aus dem in Artikel 35 der Verfassung verlangten Nachweis einer „hinreichenden Ursache". Nach dem Grundsatz der „hinreichenden Ursache" können Gerichtsbeschlüsse unter folgenden Voraussetzungen ausgestellt werden: [1] Es besteht die Notwendigkeit strafrechtlicher Ermittlungen (vgl. das oben genannte Urteil des Obersten Gerichtshofs vom 18. März 1969 (1968 (Shi) Nr. 100)). [2] Es besteht eine Situation, in der man davon ausgeht, dass der Verdächtige (der Angeklagte) eine Straftat begangen hat (Artikel 156 Absatz 1 StPO) ([8]). [3] Der Gerichtsbeschluss zur Durchsuchung von Körper, Gegenständen, Wohnsitz oder einer anderen Immobilie einer anderen Person als dem Angeklagten sollte nur dann ausgestellt werden, wenn vernünftigerweise davon ausgegangen werden kann, dass die zu beschlagnahmenden Gegenstände vorhanden sind (Artikel 102 Absatz 2 StPO). Ist ein Richter der Auffassung, dass die von den Ermittlungsbehörden vorgelegten Beweise keine ausreichende Begründung für den Verdacht auf eine Straftat darstellen, wird er den Antrag auf Ausstellung eines Gerichtsbeschlusses abweisen. In diesem Zusammenhang ist darauf hinzuweisen, dass im Rahmen des Gesetzes über die Bekämpfung der organisierten Kriminalität und die Überwachung illegal erworbener Vermögenswerte (Act on Punishment of Organized Crimes and Control of Crime Proceeds) „vorbereitende Handlungen zur Begehung" einer geplanten Straftat (z. B. die Vorbereitung von Geldern für die Begehung einer terroristischen Straftat) selbst eine Straftat darstellen und somit Gegenstand einer Untersuchung mit Zwangsmitteln auf der Grundlage eines Gerichtsbeschlusses sein können.

Betrifft der Gerichtsbeschluss schließlich die Durchsuchung von Körper, Gegenständen, Wohnsitz oder einer anderen Immobilie einer anderen Person als dem Verdächtigen oder Angeklagten, darf er nur dann ausgestellt werden, wenn vernünftigerweise davon ausgegangen werden kann, dass die zu beschlagnahmenden Gegenstände vorhanden sind (Artikel 102 Absatz 2 und Artikel 222 Absatz 1 StPO).

Was konkret die Überwachung der Kommunikation zum Zwecke strafrechtlicher Ermittlungen auf der Grundlage des Abhörgesetzes betrifft, so darf sie nur durchgeführt werden, wenn die strengen Anforderungen nach dessen Artikel 3 Absatz 1 erfüllt sind. Demnach ist für die Überwachung stets ein vorab ergangener Gerichtsbeschluss erforderlich, der nur in begrenzten Fällen ([9]) ausgestellt werden darf.

2) Einschränkungen aufgrund des APPIHAO

Für die Erhebung ([10]) und Weiterverarbeitung (vor allem auch die Speicherung, Verwaltung und Verwendung) personenbezogener Informationen durch Verwaltungsorgane sind im APPIHAO insbesondere folgende Einschränkungen festgelegt:

a) Nach Artikel 3 Absatz 1 APPIHAO dürfen Verwaltungsorgane personenbezogene Informationen nur speichern, wenn dies für die Erfüllung der Aufgaben erforderlich ist, für die sie nach Maßgabe der Gesetze und sonstigen Vorschriften zuständig sind. Bei der Speicherung sind sie auch verpflichtet, (soweit möglich) den Verwendungszweck der personenbezogenen Informationen anzugeben. Nach Artikel 3 Absätze 2 und 3 APPIHAO dürfen die Verwaltungsorgane keine personenbezogenen Informationen speichern, die den für den genannten Verwendungszweck erforderlichen Umfang übersteigen, und dürfen den Verwendungszweck nicht so verändern, dass er das übersteigt, was vernünftigerweise als für den ursprünglichen Zweck angemessen und zweckdienlich angesehen werden kann.

b) Nach Artikel 5 APPIHAO muss der Leiter eines Verwaltungsorgans dafür sorgen, dass die gespeicherten personenbezogenen Informationen richtig und aktuell sind, soweit dies für die Erfüllung des Verwendungszwecks erforderlich ist.

c) Nach Artikel 6 Absatz 1 APPIHAO muss der Leiter eines Verwaltungsorgans die erforderlichen Maßnahmen treffen, um die unerlaubte Veröffentlichung, den Verlust oder die Beschädigung zu verhindern und den ordnungsgemäßen Umgang mit den gespeicherten personenbezogenen Informationen zu gewährleisten.

d) Nach Artikel 7 APPIHAO darf kein Bediensteter (auch kein ehemaliger) die gesammelten personenbezogenen Informationen einer anderen Person ohne hinreichende Begründung weitergeben oder diese Informationen zu einem ungerechtfertigten Zweck verwenden.

([7]) Urteil vom 18. März 1969 (1968 (Shi) Nr. 100).
([8]) Siehe Artikel 156 Absatz 1 der Strafprozessordnung: „Bei Einreichung des Antrags nach Absatz 1 des vorausgehenden Artikels stellt der Antragsteller Materialien zur Verfügung, auf deren Grundlage der Verdächtige oder Angeklagte als Straftäter anzusehen ist."
([9]) Siehe Fußnote 6.
([10]) Artikel 3 Absätze 1 und 2 APPIHAO beschränken den Umfang der Speicherung und damit auch der Erhebung personenbezogener Informationen.

e) Darüber hinaus ist in Artikel 8 Absatz 1 APPIHAO festgelegt, dass der Leiter eines Verwaltungsorgans — sofern in den Gesetzen und sonstigen Vorschriften nichts anderes bestimmt ist — die gespeicherten personenbezogenen Informationen für einen anderen als den festgelegten Verwendungszweck weder nutzen noch einer anderen Person überlassen darf. Nach Artikel 8 Absatz 2 gelten zwar unter bestimmten Umständen Ausnahmen von dieser Regel, allerdings nur, wenn eine solche außergewöhnliche Offenlegung nicht zu einer „ungerechtfertigten" Beeinträchtigung der Rechte und Interessen des Datensubjekts oder eines Dritten führen kann.

f) Nach Artikel 9 APPIHAO muss der Leiter eines Verwaltungsorgans erforderlichenfalls den Verwendungszweck oder die Methode der Verwendung einschränken oder sonstige erforderliche Einschränkungen verhängen, falls die gespeicherten personenbezogenen Informationen einer anderen Person überlassen werden; vom Empfänger kann auch verlangt werden, erforderliche Maßnahmen gegen die unerlaubte Veröffentlichung der Informationen und zum ordnungsgemäßen Umgang damit zu ergreifen.

g) Nach Artikel 48 APPIHAO muss der Leiter eines Verwaltungsorgans dafür Sorge tragen, dass etwaige Beschwerden über den Umgang mit personenbezogenen Informationen ordnungsgemäß und zügig bearbeitet werden.

2) Erhebung personenbezogener Informationen durch Ersuchen um freiwillige Mitarbeit (freiwillige Ermittlungen)

*a) Rechtsgrundlage*

Neben dem Einsatz von Zwangsmitteln werden personenbezogene Informationen entweder aus einer Quelle gewonnen, die frei zugänglich ist oder auf freiwilliger Offenlegung beruht, auch durch Unternehmen, die solche Informationen besitzen.

Nach Artikel 197 Absatz 2 StPO sind Staatsanwaltschaft und Kriminalpolizei befugt, sich „schriftlicher Anfragen in Ermittlungsangelegenheiten" (sogenannter „Anfrageformulare") zu bedienen. Nach der Strafprozessordnung sind die Personen, die Gegenstand der Anfrage sind, aufgefordert, den Ermittlungsbehörden Auskunft zu geben. Es gibt jedoch keine Möglichkeit, eine Auskunft zu erzwingen, wenn die öffentlichen Stellen oder die öffentlichen und/oder privaten Organisationen, die die Anfragen erhalten haben, dies verweigern. Kommen sie der Anfrage nicht nach, können weder strafrechtliche noch andere Sanktionen verhängt werden. Halten die Ermittlungsbehörden die verlangten Auskünfte für unverzichtbar, müssen sie die Informationen durch Durchsuchung und Beschlagnahme auf der Grundlage eines Gerichtsbeschlusses beschaffen.

Da die Sensibilisierung der Bürger für den Schutz ihrer Privatsphäre zunimmt und der mit solchen Anfragen verbundene Aufwand wächst, werden die Unternehmen bei der Beantwortung solcher Anfragen immer zurückhaltender ([11]). Bei der Entscheidung, ob sie kooperieren, berücksichtigen die Unternehmen insbesondere die Art der verlangten Informationen, ihre Beziehung zu der Person, um deren Informationen es geht, etwaige Reputationsrisiken, Risiken für Rechtsstreitigkeiten usw.

*b) Einschränkungen*

Wie die Erhebung elektronischer Informationen mit Zwangsmitteln wird auch die freiwillige Ermittlung durch die Verfassung, gemäß ihrer Auslegung in der ständigen Rechtsprechung, und die gesetzlichen Ermächtigungsgrundlagen eingeschränkt. Darüber hinaus ist es den Unternehmen rechtlich nicht gestattet, Informationen in bestimmten Situationen offenzulegen. Zudem enthält das APPIHAO eine Reihe von Einschränkungen sowohl für die Erhebung von Informationen als auch für den Umgang damit (und lokale Verordnungen schreiben im Wesentlichen dieselben Kriterien für die Präfekturpolizei vor).

1) Einschränkungen aufgrund der Verfassung und der gesetzlichen Ermächtigungsgrundlagen

Indem er den Zweck von Artikel 13 der Verfassung würdigte, hat der Oberste Gerichtshof in zwei Urteilen vom 24. Dezember 1969 (1965 (A) Nr. 1187) und vom 15. April 2008 (2007 (A) Nr. 839) von den Ermittlungsbehörden durchgeführte freiwillige Ermittlungen eingeschränkt. Diese Urteile betrafen zwar Fälle, in denen personenbezogene Informationen (in Form von Bildern) durch Foto- oder Filmaufnahmen gesammelt wurden, dennoch sind die Ergebnisse auch für freiwillige (nicht mit Zwangsmitteln erfolgende) Ermittlungen relevant, die die Privatsphäre des Einzelnen im Allgemeinen beeinträchtigen. Sie gelten daher für die Erhebung personenbezogener Informationen im Wege der freiwilligen Ermittlung und müssen befolgt werden, wobei den besonderen Umständen des jeweiligen Falls Rechnung zu tragen ist.

Diesen Urteilen zufolge hängt die Rechtmäßigkeit einer freiwilligen Ermittlung von der Erfüllung dieser dreier Kriterien ab:

— „Verdacht auf eine Straftat" (d. h. es ist zu prüfen, ob eine Straftat begangen wurde);

— „Notwendigkeit der Ermittlung" (d. h. es ist zu prüfen, ob sich die Anfrage auf das für die Zwecke der Ermittlung erforderliche Maß beschränkt); und

([11]) Siehe Mitteilung der staatlichen Polizeibehörde vom 7. Dezember 1999 (S. 9), in der der gleiche Punkt genannt wird.

— „Eignung der Methoden“ (d. h. es ist zu prüfen, ob freiwillige Ermittlungen „geeignet“ oder angemessen sind, um den Zweck der Untersuchung zu erfüllen) ([12]).

Im Allgemeinen wird anhand dieser drei Kriterien die Rechtmäßigkeit der freiwilligen Ermittlung unter dem Gesichtspunkt beurteilt, ob sie gemessen an den sozialen Konventionen als angemessen angesehen werden kann.

Die vorgeschriebene „Notwendigkeit“ der Ermittlung ergibt sich auch unmittelbar aus Artikel 197 StPO und wurde in den Anweisungen der staatlichen Polizeibehörde (NPA) an die Präfekturpolizei für die Verwendung der „Anfrageformulare“ bestätigt. Die NPA-Mitteilung vom 7. Dezember 1999 enthält eine Reihe von verfahrensbezogenen Einschränkungen, darunter die Maßgabe, „Anfrageformulare“ nur dann zu verwenden, wenn dies für die Ermittlungszwecke erforderlich ist. Darüber hinaus ist Artikel 197 Absatz 1 StPO auf strafrechtliche Ermittlungen beschränkt und darf somit nur angewandt werden, wenn ein konkreter Verdacht besteht, dass bereits eine Straftat begangen wurde. Umgekehrt greift diese Rechtsgrundlage nicht für die Erhebung und Verwendung von personenbezogenen Informationen, wenn noch kein Gesetzesverstoß vorliegt.

2) Einschränkungen betreffend bestimmte Unternehmen

In bestimmten Bereichen gelten zusätzliche Einschränkungen, die auf den in anderen Gesetzen enthaltenen Schutzbestimmungen beruhen.

Erstens sind die Ermittlungsbehörden und die Telekommunikationsdiensteanbieter, die im Besitz personenbezogener Informationen sind, verpflichtet, das nach Artikel 21 Absatz 2 der Verfassung ([13]) garantierte Kommunikationsgeheimnis zu wahren. Telekommunikationsdiensteanbieter sind dazu auch nach Artikel 4 des Telekommunikationsgesetzes ([14]) verpflichtet. Gemäß den „Leitlinien für den Schutz personenbezogener Informationen bei der Telekommunikation“, die vom Ministerium für Inneres und Kommunikation (Ministry of Internal Affairs and Communications — MIC) auf der Grundlage der Verfassung und des Telekommunikationsgesetzes erlassen wurden, dürfen Telekommunikationsdiensteanbieter in Fällen, in denen das Kommunikationsgeheimnis bedroht ist, keine personenbezogenen Informationen, die das Kommunikationsgeheimnis verletzen, an Dritte weitergeben, es sei denn, sie haben die Einwilligung des Betroffenen eingeholt oder sie können einen der „Rechtfertigungsgründe“ für die Nichteinhaltung des Strafgesetzbuches geltend machen. Als Rechtfertigungsgründe gelten „gerechtfertigte Handlungen“ (Artikel 35 Strafgesetzbuch), „Notwehr“ (Artikel 36 Strafgesetzbuch) und „Abwehr einer unmittelbaren Gefahr“ (Artikel 37 Strafgesetzbuch). „Gerechtfertigte Handlungen“ nach dem Strafgesetzbuch sind nur die Handlungen, durch die ein Telekommunikationsdiensteanbieter den Zwangsmitteln des Staates nachkommt, was eine freiwillige Ermittlung ausschließt. Wenn daher die Ermittlungsbehörden auf der Grundlage eines „Anfrageformulares“ persönliche Informationen verlangen (Artikel 197 Absatz 2 StPO), ist es einem Telekommunikationsdiensteanbieter untersagt, die Daten offenzulegen.

Zweitens sind die Unternehmer verpflichtet, Ersuchen um freiwillige Kooperation abzulehnen, wenn ihnen die Offenlegung personenbezogener Informationen gesetzlich untersagt ist. Dies gilt beispielsweise auch dann, wenn der Unternehmer, etwa nach Artikel 134 StGB ([15]), verpflichtet ist, die Vertraulichkeit der Informationen zu wahren.

3) Einschränkungen aufgrund des APPIHAO

Für die Erhebung und Weiterverarbeitung personenbezogener Informationen durch Verwaltungsorgane sind im APPIHAO, wie in Abschnitt II Buchstabe A Nummer 1 Buchstabe b Ziffer 2 ausgeführt, Einschränkungen festgelegt. Gleichwertige Einschränkungen ergeben sich aus den für die Präfekturpolizei geltenden Präfekturverordnungen.

B) Aufsicht

1) Gerichtliche Aufsicht

Die Erhebung personenbezogener Informationen mit Zwangsmitteln muss auf einem Gerichtsbeschluss ([16]) beruhen und unterliegt somit der vorherigen richterlichen Überprüfung. Ist die Ermittlung rechtswidrig, kann ein Richter die entsprechenden Beweismittel in dem anschließenden Strafverfahren ausschließen. Ein Angeklagter kann in seinem Strafverfahren diesen Ausschluss beantragen, wenn er geltend macht, dass die Ermittlung rechtswidrig war.

([12]) Die Schwere der Straftat und die Dringlichkeit sind maßgebliche Faktoren, um die „Eignung der Methoden“ zu beurteilen.

([13]) In Artikel 21 Absatz 2 der Verfassung heißt es: „Es wird keine Zensur aufrechterhalten, und die Geheimhaltung der Kommunikationsmittel wird nicht verletzt.“

([14]) Artikel 4 des Telekommunikationsgesetzes lautet: „1) Das Kommunikationsgeheimnis der von einem Telekommunikationsdiensteanbieter erbrachten Kommunikationsleistungen darf nicht verletzt werden. 2) Jede Person, die einer geschäftlichen Tätigkeit im Bereich der Telekommunikation nachgeht, darf keine in Ausübung ihrer Tätigkeit erlangten Geheimnisse im Zusammenhang mit von einem Telekommunikationsdiensteanbieter erbrachten Kommunikationsleistungen offenlegen. Dies gilt selbst nach Beendigung dieser Tätigkeit.“

([15]) Nach Artikel 134 StGB gilt: „1) Legt ein Arzt, Apotheker, Arzneimittelhändler, eine Hebamme, ein Anwalt, Verteidiger, Notar oder jede andere Person, die zuvor einen solchen Beruf ausgeübt hat, ohne triftigen Grund die vertraulichen Informationen einer anderen Person offen, die ihm/ihr in der Ausübung dieses Berufs bekannt geworden sind, ist ein mit Zwangsarbeit verbundener Freiheitsentzug von bis zu 6 Monaten oder eine Geldstrafe von bis zu 100 000 Yen zu verhängen. 2) Dies gilt ebenfalls, wenn eine Person, die derzeit einer religiösen Tätigkeit nachgeht oder früher nachging, ohne triftigen Grund die vertraulichen Informationen einer anderen Person offenlegt, die ihr bei der Ausübung dieser religiösen Tätigkeit bekannt geworden sind.“

([16]) Zu der Ausnahme von dieser Vorschrift siehe Fußnote 5.

2) Aufsicht gemäß APPIHAO

In Japan liegt die Aufsichts- und Durchsetzungsbefugnis gemäß dem APPIHAO beim Minister bzw. bei jedem Ministeriums- oder Behördenleiter, während der Minister für Inneres und Kommunikation die Durchsetzung des APPIHAO durch alle anderen Ministerien untersuchen kann.

Hält der Minister für Inneres und Kommunikation — beispielsweise aufgrund der Untersuchung des Stands der Durchsetzung des APPIHAO ([17]), der Bearbeitung der Beschwerden oder der Anfragen an eine der Informationszentralen — dies für die Zwecke des APPIHO für erforderlich, kann er nach Artikel 50 APPIHAO den Leiter eines Verwaltungsorgans auffordern, Belege und Erläuterungen zum Umgang des betreffenden Verwaltungsorgans mit personenbezogenen Informationen vorzulegen. Der Minister kann dem Leiter des Verwaltungsorgans Stellungnahmen über die Verarbeitung von personenbezogenen Informationen im betroffenen Verwaltungsorgan übermitteln, wenn er dies für die Zwecke dieses Gesetzes für erforderlich hält. Darüber hinaus kann der Minister beispielsweise über die ihm nach den Artikeln 50 und 51 zur Verfügung stehenden Schritte eine Überprüfung der Maßnahmen beantragen, wenn Verdacht auf einen Verstoß gegen das Gesetz oder eine unsachgemäße Durchführung des Gesetzes besteht. Dies trägt dazu bei, die einheitliche Anwendung und Einhaltung des APPIHAO sicherzustellen.

3) Aufsicht der Kommissionen für öffentliche Sicherheit über die Polizei

Hinsichtlich der Polizeiverwaltung wird die staatliche Polizeibehörde durch die Nationale Kommission für die öffentliche Sicherheit beaufsichtigt, während die Präfekturpolizei der Aufsicht einer der Präfekturkommissionen für öffentliche Sicherheit unterliegt, die in jeder Präfektur vorhanden sind. Jede dieser Aufsichtsstellen gewährleistet die demokratische Führung und die politische Neutralität der Polizeiverwaltung.

Die Nationale Kommission für öffentliche Sicherheit ist für jene Angelegenheiten zuständig, die nach dem Polizeigesetz und anderen Gesetzen in ihre Kompetenz fallen. Dazu gehört die Ernennung des Generalkommissars der NPA und der örtlichen leitenden Polizeibeamten sowie die Erstellung umfassender Vorgaben, die grundlegende Leitlinien oder Maßnahmen für die Verwaltung der NPA enthalten.

Die Präfekturkommissionen für öffentliche Sicherheit setzen sich aus Vertretern der Einwohner der jeweiligen Präfektur gemäß Polizeigesetz zusammen und leiten die Präfekturpolizei als System unabhängiger Räte. Die Mitglieder werden nach Artikel 39 Polizeigesetz vom Gouverneur der Präfektur mit Zustimmung der Präfekturversammlung ernannt. Ihre Amtszeit beträgt drei Jahre und sie können nur aus bestimmten gesetzlich definierten Gründen (z. B. Unfähigkeit zur Erfüllung ihrer Aufgaben, Pflichtverletzungen, Dienstvergehen usw.) gegen ihren Willen des Amts enthoben werden, was ihre Unabhängigkeit gewährleistet (siehe Artikel 40 und 41 Polizeigesetz). Um ihre politische Neutralität zu gewährleisten, ist es Mitgliedern der Kommission nach Artikel 42 Polizeigesetz zudem verboten, gleichzeitig als Mitglied eines Gesetzgebungsorgans zu fungieren, leitendes Mitglied einer politischen Partei oder eines anderen politischen Gremiums zu werden oder sich aktiv an politischen Bewegungen zu beteiligen. Jede Kommission fällt zwar unter die Zuständigkeit des jeweiligen Präfektur-Gouverneurs, was diesem jedoch keinerlei Befugnis verleiht, ihr Anweisungen zur Wahrnehmung ihrer Aufgaben zu erteilen.

Nach Artikel 38 Absatz 3 in Verbindung mit Artikel 2 und Artikel 36 Absatz 2 Polizeigesetz sind die Präfekturkommissionen für öffentliche Sicherheit für den „Schutz der Rechte und Freiheiten des Einzelnen" zuständig. Zu diesem Zweck erstatten ihnen die Polizeichefs der Präfekturpolizei — auch in regelmäßigen, drei oder vier Mal monatlich stattfindenden Sitzungen — Bericht über die unter ihre Zuständigkeit fallenden Tätigkeiten. Die Kommissionen erlassen Leitlinien zu diesen Fragen, indem sie umfassende Vorgaben festlegen.

Zur Aufsichtsfunktion der Präfekturkommissionen für öffentliche Sicherheit gehört auch, dass sie der Präfekturpolizei in konkreten Einzelfällen Anweisungen erteilen können, wenn sie dies im Zusammenhang mit einer Inspektion der Arbeit der Präfekturpolizei oder bei Fehlverhalten ihres Personals für erforderlich halten. Außerdem können die Kommissionen, wenn sie dies für erforderlich halten, ein Mitglied der Kommission damit beauftragen, den Stand der Umsetzung der Anweisung (Artikel 43-2 Polizeigesetz) zu überprüfen.

([17]) Um Transparenz zu gewährleisten und die Aufsicht durch das MIC zu erleichtern, ist der Leiter eines Verwaltungsorgans nach Artikel 11 APPIHAO verpflichtet, jede nach Artikel 10 Absatz 1 APPIHAO vorgeschriebene Information zu erfassen, wie z. B. den Namen des Verwaltungsorgans, von dem die Datei gespeichert wird, der Verwendungszweck der Datei, die Methode der Erhebung der personenbezogenen Informationen usw. (das sogenannte „Register der Dateien mit personenbezogenen Informationen"). Von der Pflicht zur Meldung an das MIC und zur Aufnahme in das öffentliche Register sind jedoch personenbezogene Informationen ausgenommen, die unter Artikel 10 Absatz 2 APPIHAO fallen, etwa jene, die im Rahmen einer strafrechtlichen Ermittlung erstellt oder erlangt wurden oder die nationale Sicherheit berührende Angelegenheiten betreffen. Nach Artikel 7 des Gesetzes über die Verwaltung von öffentlichen Registern und Archiven ist der Leiter eines Verwaltungsorgans jedoch stets verpflichtet, die Einstufung, den Titel, die Speicherdauer, den Speicherort usw. von Verwaltungsdokumenten aufzuzeichnen („Dateiverwaltungsregister für Verwaltungsdokumente"). Die Indexdaten für beide Register werden im Internet veröffentlicht und ermöglichen es den Bürgern, zu überprüfen, welche Art von personenbezogenen Informationen die Datei enthält und welches Verwaltungsorgan die Informationen speichert.

4) Aufsicht durch das Parlament

Das japanische Parlament kann Untersuchungen der Tätigkeit von Behörden durchführen und zu diesem Zweck die Vorlage von Unterlagen und die Aussage von Zeugen verlangen (Artikel 62 der Verfassung). In diesem Zusammenhang kann der zuständige Parlamentsausschuss prüfen, ob die von der Polizei ergriffenen Maßnahmen zur Erhebung von Informationen angemessen sind.

Diese Befugnisse sind im Parlamentsgesetz genauer präzisiert. Nach Artikel 104 Parlamentsgesetz kann das Parlament das Kabinett und die öffentlichen Behörden auffordern, Berichte und Aufzeichnungen vorzulegen, die für die Durchführung der Untersuchung erforderlich sind. Darüber hinaus können die Parlamentsmitglieder „schriftliche Anfragen" gemäß Artikel 74 Parlamentsgesetz einreichen. Diese Anfragen sind vom Vorsitzenden der Parlamentskammer zu genehmigen und müssen vom Kabinett grundsätzlich innerhalb von sieben Tagen schriftlich beantwortet werden (ist die Beantwortung innerhalb dieser Frist nicht möglich, ist dies zu begründen und eine neue Frist zu setzen, vgl. Artikel 75 Parlamentsgesetz). In der Vergangenheit bezogen sich schriftliche Anfragen des Parlaments auch auf den Umgang der Verwaltung mit personenbezogenen Informationen ([18]).

C. Individueller Rechtsschutz

Gemäß Artikel 32 der japanischen Verfassung darf niemandem der Rechtsweg verwehrt werden. Darüber hinaus garantiert Artikel 17 der Verfassung jeder Person das Recht, den Staat oder eine öffentliche Stelle auf (gesetzlich geregelten) Schadenersatz zu verklagen, wenn sie durch die rechtswidrige Handlung eines Beamten Schaden erlitten hat.

1) Gerichtlicher Rechtsschutz gegen die Erhebung von Informationen mit Zwangsmitteln auf der Grundlage eines Gerichtsbeschlusses (Artikel 430 StPO)

Gemäß Artikel 430 Absatz 2 StPO kann eine Person, die mit den auf einem Gerichtsbeschluss beruhenden Maßnahmen eines Polizeibeamten zur Beschlagnahme von Gegenständen (auch solcher, die personenbezogene Informationen enthalten) nicht einverstanden ist, beim zuständigen Gericht einen Antrag (eine sogenannte „Quasi-Beschwerde") einreichen, um diese Maßnahmen „aufheben oder ändern" zu lassen.

Um eine solche Beschwerde einzureichen, muss die Person den Abschluss des Falls nicht abwarten. Stellt das Gericht fest, dass die Beschlagnahme nicht erforderlich war oder dass die Beschlagnahme aus anderen Gründen als rechtswidrig zu gelten hat, kann es die Aufhebung oder Änderung dieser Maßnahmen anordnen.

2) Rechtsschutz im Rahmen der Zivilprozessordnung und des Staatshaftungsgesetzes

Personen, die der Auffassung sind, dass ihr Recht auf Privatsphäre nach Artikel 13 der Verfassung verletzt wurde, können eine Zivilklage erheben und verlangen, dass die bei einer strafrechtlichen Ermittlung erhobenen personenbezogenen Informationen gelöscht werden.

Außerdem kann eine Person nach dem Staatshaftungsgesetz in Verbindung mit den einschlägigen Artikeln des Zivilgesetzbuchs eine Schadenersatzklage erheben, wenn sie der Auffassung ist, dass ihr Recht auf Schutz der Privatsphäre verletzt wurde und sie durch die Erhebung ihrer personenbezogenen Informationen oder die Überwachung geschädigt wurde ([19]). Da der „Schaden", für den auf Schadenersatz geklagt wird, nicht auf Sachschäden beschränkt ist (Artikel 710 Zivilgesetzbuch), kann dies auch „seelische Belastungen" umfassen. Die Höhe der Entschädigung für solche immateriellen Schäden wird vom Richter auf der Grundlage einer „unbeeinflussten Bewertung unter Berücksichtigung verschiedener Faktoren im Einzelfall" ([20]) festgesetzt.

Artikel 1 Absatz 1 Staatshaftungsgesetz verleiht einen Anspruch auf Schadenersatz, wenn i) ein Beamter, der die öffentliche Gewalt des Staates (oder einer öffentlichen Einrichtung) ausübt, ii) in Erfüllung seiner Aufgaben in iii) vorsätzlicher oder fahrlässiger und iv) rechtswidriger Weise v) einer anderen Person Schaden zugefügt hat.

Die Person muss gemäß der Zivilprozessordnung Klage erheben. Nach den geltenden Vorschriften kann er das Gericht anrufen, in dessen Zuständigkeit der Ort liegt, an dem die unerlaubte Handlung begangen wurde.

([18]) Siehe z. B. die schriftliche Anfrage Nr. 92 des Rätehauses vom 27. März 2009 über den Umgang mit Informationen, die bei strafrechtlichen Ermittlungen erhoben wurden, einschließlich der Verletzung von Datenschutzverpflichtungen durch Polizei- und Justizbehörden.

([19]) Ein Beispiel für eine solche Klage wäre der Fall der illegalen „Listen der Agentur für Verteidigung" (Bezirksgericht Niigata, Urteil vom 11. Mai 2006 (2002(Wa) Nr. 514)). In diesem Fall wurde von einem Beamten der Verteidigungsagentur eine Liste der Personen, die bei der Verteidigungsagentur die Offenlegung von Verwaltungsdokumenten beantragt hatten, erstellt, gepflegt und verteilt. Diese Liste enthielt Angaben zu personenbezogenen Informationen des Klägers. Der Kläger machte eine Verletzung seiner Privatsphäre, seines Rechts auf Einsicht usw. geltend und forderte vom Beklagten Schadenersatz nach Artikel 1 Absatz 1 Staatshaftungsgesetz. Das Gericht gab dieser Klage teilweise statt und sprach dem Kläger einen teilweisen Schadenersatz zu.

([20]) Oberster Gerichtshof, Urteil vom 5. April 1910 (1910 (O) Nr. 71).

3) Individueller Rechtsschutz gegen rechtswidrige oder unzulässige Ermittlungen der Polizei: Beschwerde an die Präfekturkommission für öffentliche Sicherheit (Artikel 79 Polizeigesetz)

Gemäß Artikel 79 des Polizeigesetzes ([21]) (in einer Anweisung des Leiters der NPA an die Präfekturpolizei und die Präfekturkommissionen für öffentliche Sicherheit ([22]) weiter ausgeführt) können Einzelpersonen bei der zuständigen Präfekturkommission für öffentliche Sicherheit eine schriftliche Beschwerde ([23]) gegen rechtswidriges oder unzulässiges Verhalten eines Polizisten bei der Ausübung seiner Aufgaben einreichen; dies schließt Aufgaben in Bezug auf die Erhebung und Nutzung personenbezogener Informationen ein. Die Kommission bearbeitet solche Beschwerden gewissenhaft und in Übereinstimmung mit den Gesetzen und lokalen Verordnungen und informiert den Beschwerdeführer schriftlich über die Ergebnisse ihrer Untersuchungen.

Ausgehend von ihrer Aufsichtsbefugnis gemäß Artikel 38 Absatz 3 des Polizeigesetzes erteilt die Präfekturkommission für öffentliche Sicherheit der Präfekturpolizei eine Anweisung, den Sachverhalt zu untersuchen, die erforderlichen Maßnahmen entsprechend dem Ergebnis der Untersuchung umzusetzen und der Kommission über die Ergebnisse Bericht zu erstatten. Wenn sie dies für notwendig hält, kann die Kommission auch eine Anweisung zur Bearbeitung der Beschwerde erteilen, beispielsweise wenn sie der Auffassung ist, dass die Untersuchung der Polizei unzureichend ist. Diese Umsetzung wird in der Mitteilung der NPA an die Leiter der Präfekturpolizei beschrieben.

Die Unterrichtung des Beschwerdeführers über das Ergebnis der Ermittlungen erfolgt auch vor dem Hintergrund der polizeilichen Berichte über die Untersuchung und der auf Ersuchen der Kommission ergriffenen Maßnahmen.

4) Individueller Rechtsschutz gemäß dem APPIHAO und der Strafprozessordnung

*a) APPIHAO*

Gemäß Artikel 48 APPIHAO bemühen sich Verwaltungsorgane, alle Beschwerden über den Umgang mit personenbezogenen Informationen ordnungsgemäß und zügig zu bearbeiten. Als Möglichkeit der Bereitstellung konsolidierter Informationen für Einzelpersonen (z. B. über die Rechte auf Offenlegung, Berichtigung und Aussetzung der Nutzung im Rahmen des APPIHAO) und als Kontaktstelle für Anfragen hat das MIC in jeder Präfektur auf der Grundlage von Artikel 47 Absatz 2 APPIHAO Informationszentralen zur Offenlegung von Informationen und zum Schutz personenbezogener Informationen eingerichtet. Anfragen nicht in Japan ansässiger Personen sind ebenfalls möglich. Im Haushaltsjahr 2017 (April 2017 bis März 2018) beispielsweise beantworteten die Informationszentralen in insgesamt 5186 Fällen Anfragen.

Artikel 12 und 27 APPIHAO gewähren Einzelpersonen das Recht auf Offenlegung und Berichtigung gespeicherter personenbezogener Informationen. Darüber hinaus können Einzelpersonen gemäß Artikel 36 APPIHAO die Aussetzung der Nutzung oder die Löschung ihrer gespeicherten personenbezogenen Informationen beantragen, wenn das Verwaltungsorgan die gespeicherten personenbezogenen Informationen nicht rechtmäßig erhalten hat oder diese Informationen unter Verstoß gegen das Gesetz speichert oder nutzt.

Was jedoch personenbezogene Informationen betrifft, die für strafrechtliche Ermittlungen erhoben (entweder aufgrund eines Gerichtsbeschlusses oder mittels eines „Anfrageformulars") und gespeichert werden ([24]), so fallen diese Informationen in der Regel in die Kategorie der „personenbezogenen Informationen, die in Dokumenten über Gerichtsverfahren und beschlagnahmte Gegenstände enthalten sind". Derartige personenbezogene Informationen sind daher gemäß Artikel 53-2 der Strafprozessordnung vom Anwendungsbereich der Rechte des Einzelnen in Kapitel 4 APPIHAO ausgenommen ([25]). Die Verarbeitung solcher personenbezogenen Informationen und die Rechte des Einzelnen auf Zugang und Berichtigung unterliegen stattdessen besonderen Vorschriften nach der Strafprozessordnung und dem Gesetz über das abschließende

([21]) Artikel 79 des Polizeigesetzes (Auszug):
1. Wer Anlass zur Beschwerde gegen die Wahrnehmung der Aufgaben durch das Personal der Präfekturpolizei hat, kann nach dem in der Verordnung über die Nationale Kommission für die öffentliche Sicherheit festgelegten Verfahren bei der Präfekturkommission für öffentliche Sicherheit eine schriftliche Beschwerde einlegen.
2. Die Präfekturkommission für öffentliche Sicherheit, bei der eine Beschwerde gemäß vorstehendem Absatz eingegangen ist, bearbeitet diese gewissenhaft und in Übereinstimmung mit den Gesetzen und lokalen Verordnungen und informiert den Beschwerdeführer schriftlich über die Ergebnisse, außer in folgenden Fällen:
   1) Die Beschwerde wurde offensichtlich eingelegt, um die rechtmäßige Wahrnehmung der Aufgaben der Präfekturpolizei zu behindern;
   2) der derzeitige Wohnsitz des Beschwerdeführers ist unbekannt;
   3) es ist deutlich, dass die Beschwerde gemeinsam mit anderen Beschwerdeführern eingelegt wurde, und andere Beschwerdeführer wurden bereits über das Ergebnis der gemeinsamen Beschwerde informiert.

([22]) NPA, Mitteilung über die ordnungsgemäße Bearbeitung von Beschwerden über die Wahrnehmung der Aufgaben durch Polizeibedienstete vom 13. April 2001, mit Anlage 1 „Standards zur Auslegung und Anwendung des Artikels 79 des Polizeigesetzes".

([23]) Nach der Mitteilung der NPA (siehe vorherige Fußnote) erhalten Personen, die bei der Abfassung einer Beschwerde Schwierigkeiten haben, Unterstützung. Dies gilt ausdrücklich auch für Ausländer.

([24]) Andererseits kann es Dokumente geben, die nicht als „Dokumente über Gerichtsverfahren" eingestuft werden, da sie selbst nicht durch einen Gerichtsbeschluss oder eine schriftliche Anfrage in Ermittlungsangelegenheiten erlangt wurden, aber auf der Grundlage solcher Dokumente erstellt wurden. Dies wäre der Fall, wenn private Informationen nicht unter Artikel 45 Absatz 1 APPIHAO fallen, sodass diese Informationen nicht von der Anwendung des Kapitels 4 APPIHAO ausgeschlossen wären.

([25]) Artikel 53-2 Absatz 2 der Strafprozessordnung schreibt vor, dass Kapitel IV APPIHAO nicht auf personenbezogene Informationen anzuwenden ist, die in Dokumenten über Gerichtsverfahren und beschlagnahmte Gegenstände enthalten sind.

Strafregister (siehe unten) ([26]). Dieser Ausschluss ist durch verschiedene Faktoren gerechtfertigt, wie etwa den Schutz der Privatsphäre der betroffenen Personen, das Untersuchungsgeheimnis und die ordnungsgemäße Durchführung des Strafverfahrens. Die Bestimmungen des Kapitels 2 APPIHAO, die die Grundsätze für den Umgang mit solchen Informationen regeln, bleiben allerdings anwendbar.

*b) Strafprozessordnung*

Nach der Strafprozessordnung hängen die Möglichkeiten des Zugangs zu personenbezogenen Informationen, die zum Zwecke strafrechtlicher Ermittlungen erhoben werden, sowohl vom Stadium des Verfahrens als auch von der Rolle des Einzelnen in den Ermittlungen (Verdächtiger, Angeklagter, Opfer usw.) ab.

In Abweichung von der Regel nach Artikel 47 der Strafprozessordnung, der zufolge Dokumente über Gerichtsverfahren nicht vor Beginn des Verfahrens öffentlich gemacht werden dürfen (da dies die Ehre und/oder die Privatsphäre der Betroffenen verletzen und die Ermittlungen und das Verfahren behindern könnte), ist die Einsichtnahme in solche Informationen durch das Opfer einer Straftat grundsätzlich zulässig, soweit dies unter Berücksichtigung des Zwecks der Bestimmung des Artikels 47 der Strafprozessordnung für angemessen erachtet wird ([27]).

Was Verdächtige betrifft, so erfahren sie in der Regel bei der Befragung durch die Kriminalpolizei oder die Staatsanwaltschaft, dass sie Gegenstand strafrechtlicher Ermittlungen sind. Beschließt die Staatsanwaltschaft anschließend, keine Strafverfolgung einzuleiten, so informiert sie den Verdächtigen auf dessen Antrag unverzüglich hierüber (Artikel 259 der Strafprozessordnung).

Darüber hinaus gibt die Staatsanwaltschaft nach der Einleitung der Strafverfolgung dem Angeklagten oder seinem Rechtsbeistand Gelegenheit zur Einsichtnahme in die Beweismittel, bevor sie diese dem Gericht zur Prüfung vorlegt (Artikel 299 der Strafprozessordnung). Dies ermöglicht es dem Angeklagten, seine im Rahmen strafrechtlicher Ermittlungen erhobenen personenbezogenen Informationen zu prüfen.

Schließlich wird der Schutz personenbezogener Informationen, die im Rahmen strafrechtlicher Ermittlungen erhoben werden — sei es von einem Verdächtigen, einem Angeklagten oder jeder anderen Person (z. B. einem Opfer einer Straftat) — durch die Vertraulichkeitsverpflichtung (Artikel 100 des Gesetzes über den nationalen öffentlichen Dienst) und die Androhung von Sanktionen bei einer Offenlegung vertraulicher Informationen im Rahmen der Wahrnehmung öffentlicher Aufgaben (Artikel 109 Ziffer xii des Gesetzes über den öffentlichen Dienst) gewährleistet.

5) Individueller Rechtsschutz gegen rechtswidrige oder unzulässige Ermittlungen der Behörden: Beschwerde bei der PPC

Gemäß Artikel 6 APPI ergreift die Regierung in Zusammenarbeit mit den Regierungen von Drittländern durch die Förderung der Zusammenarbeit mit internationalen Organisationen und anderweitig im internationalen Rahmen die notwendigen Maßnahmen, um ein international konformes System für personenbezogene Informationen zu errichten. Auf der Grundlage dieser Bestimmung wird der PPC als der allgemein für die Verwaltung des APPI zuständigen Behörde durch die Grundlegende Richtlinie zum Schutz personenbezogener Informationen (per Kabinettsbeschluss angenommen) die Befugnis übertragen, die notwendigen Maßnahmen zu treffen, um die Unterschiede zwischen den Systemen und Abläufen in Japan und in dem betreffenden anderen Land zu überbrücken, damit eine angemessene Handhabung der aus diesem Land erhaltenen personenbezogenen Informationen gewährleistet werden kann.

Darüber hinaus ist die PPC, wie in Artikel 61 Buchstaben i und ii APPI vorgesehen, mit der Ausarbeitung und Förderung einer grundlegenden Politik sowie mit der Mediation bei Beschwerden gegen Unternehmer betraut. Schließlich müssen die Verwaltungsorgane eng miteinander kommunizieren und zusammenarbeiten (Artikel 80 APPI).

Auf der Grundlage dieser Bestimmungen behandelt die PPC Beschwerden von Einzelpersonen wie folgt:

a) Eine Person, die den Verdacht hat, dass ihre aus der EU übermittelten Daten von öffentlichen Behörden in Japan (einschließlich der Behörden, die für die in Kapitel II und Kapitel III der vorliegenden „Erklärung" genannten Tätigkeiten zuständig sind) unter Verstoß gegen die geltenden Vorschriften (einschließlich derer, die dieser „Erklärung" unterliegen) erhoben oder verwendet wurden, kann eine Beschwerde bei der PPC (direkt oder über ihre Datenschutzbehörde) einlegen.

b) Die PPC befasst sich mit der Beschwerde, auch indem sie von ihren Befugnissen gemäß Artikel 6, Artikel 61 Ziffer ii und Artikel 80 APPI Gebrauch macht, und informiert die zuständigen öffentlichen Behörden, einschließlich der einschlägigen Aufsichtsgremien, über die Beschwerde.

([26]) Im Rahmen der Strafprozessordnung und des Gesetzes über das abschließende Strafregister unterliegen der Zugang zu beschlagnahmten Gegenständen sowie der Zugang zu und die Berichtigung von Dokumenten und personenbezogenen Informationen in Bezug auf Strafverfahren einem einzigartigen und eigenen System von Regeln, die auf den Schutz der Privatsphäre der Betroffenen und des Untersuchungsgeheimnisses, die ordnungsgemäße Durchführung des Strafverfahrens usw. abzielen.

([27]) Konkret ist die Einsichtnahme in Informationen im Zusammenhang mit objektiven Beweismitteln im Hinblick auf die ausbleibende Strafverfolgung in den Fällen, die die Beteiligung des Opfers gemäß Artikel 316-33 ff. der Strafprozessordnung erfordern, für Opfer von Straftaten grundsätzlich zulässig, um einen befriedigenderen Schutz der Opfer von Straftaten zu erreichen.

Diese Behörden sind gemäß Artikel 80 APPI verpflichtet, mit der PPC zusammenzuarbeiten, auch durch Bereitstellung der erforderlichen Informationen und des entsprechenden Materials, damit die PPC bewerten kann, ob die Erhebung oder die spätere Verwendung personenbezogener Informationen in Übereinstimmung mit den geltenden Vorschriften stattgefunden hat. Bei ihrer Bewertung arbeitet die PPC mit dem MIC zusammen.

c) Ergibt die Bewertung, dass ein Verstoß gegen die geltenden Vorschriften vorliegt, umfasst die Zusammenarbeit der betroffenen Behörden mit der PPC die Verpflichtung, den Verstoß zu beheben.

Im Falle einer unrechtmäßigen Erfassung personenbezogener Informationen gemäß den geltenden Vorschriften schließt dies die Löschung der erhobenen personenbezogenen Informationen ein.

Bei einem Verstoß gegen die geltenden Vorschriften bestätigt die PPC vor Abschluss der Bewertung auch, dass der Verstoß vollständig behoben wurde.

d) Sobald die Bewertung abgeschlossen ist, unterrichtet die PPC die Person innerhalb eines angemessenen Zeitraums über das Ergebnis der Bewertung und gegebenenfalls über durchgeführte Korrekturmaßnahmen. Bei dieser Unterrichtung informiert die PPC die Person auch über die Möglichkeit, von der zuständigen Behörde eine Bestätigung des Ergebnisses zu verlangen, und darüber, bei welcher Behörde ein solcher Antrag auf Bestätigung zu stellen ist.

Die Herausgabe detaillierter Informationen über das Ergebnis der Bewertung kann Beschränkungen unterliegen, sofern berechtigte Gründe vorliegen, dass die Übermittlung dieser Informationen ein Risiko für laufende Ermittlungen darstellen könnte.

Wenn die Beschwerde die Erhebung oder Nutzung personenbezogener Daten im Bereich der Strafverfolgung betrifft und die Untersuchung ergibt, dass ein Verfahren im Zusammenhang mit den personenbezogenen Informationen der Person eingeleitet wurde und der Fall inzwischen abgeschlossen ist, informiert die PPC die Person darüber, dass die Fallakte nach Artikel 53 der Strafprozessordnung und Artikel 4 des Gesetzes über das abschließende Strafregister eingesehen werden kann.

Wenn die Untersuchung ergibt, dass eine Person in einem Strafverfahren als Verdächtiger gilt, informiert die PPC die betroffene Person hierüber sowie über die Möglichkeit, einen Antrag nach Artikel 259 der Strafprozessordnung zu stellen.

e) Wenn eine Person mit dem Ergebnis des Verfahrens weiterhin unzufrieden ist, kann sie sich an die PPC wenden, die die Person über die verschiedenen Möglichkeiten und genauen Verfahren zur Einlegung von Rechtsbehelfen nach japanischen Gesetzen und Vorschriften informiert. Die PCC steht der Person unterstützend zur Seite und berät sie beispielsweise bei der Einleitung weiterer Maßnahmen bei der zuständigen Verwaltungs- oder Justizbehörde.

III. **Staatlicher Zugriff für Zwecke der nationalen Sicherheit**

A. Rechtsgrundlagen und Beschränkungen für die Erhebung personenbezogener Informationen

1) Rechtsgrundlagen für die Erhebung von Informationen durch das betreffende Ministerium/die betreffende Behörde

Wie bereits erwähnt, muss die Erhebung personenbezogener Informationen für Zwecke der nationalen Sicherheit durch Verwaltungsorgane im Rahmen ihrer Verwaltungsgerichtsbarkeit erfolgen.

In Japan gibt es kein Gesetz, das die Erhebung von Informationen mittels Zwangsmaßnahmen rein zum Zwecke der nationalen Sicherheit ermöglicht. Gemäß Artikel 35 der Verfassung ist es nur auf der Grundlage eines von einem Gericht zur Aufklärung einer Straftat ausgestellten Gerichtsbeschlusses möglich, personenbezogene Informationen zu erheben. Ein solcher Gerichtsbeschluss kann daher nur zum Zwecke strafrechtlicher Ermittlungen ausgestellt werden. Dies bedeutet, dass in der japanischen Rechtsordnung die Erhebung/der Zugang zu Informationen für Zwecke der nationalen Sicherheit mittels Zwangsmaßnahmen nicht zulässig ist. Stattdessen können die betreffenden Ministerien oder Behörden im Bereich der nationalen Sicherheit nur Informationen aus Quellen erhalten, auf die frei zugegriffen werden kann, oder Informationen von Unternehmern oder Einzelpersonen durch freiwillige Offenlegung erhalten. Unternehmer, die ein Ersuchen um freiwillige Zusammenarbeit erhalten, sind rechtlich nicht verpflichtet, diese Informationen zur Verfügung zu stellen, sodass sie keine negativen Folgen zu befürchten haben, wenn sie die Zusammenarbeit ablehnen.

Eine Reihe von Ministerialabteilungen und Behörden verfügen über Zuständigkeiten im Bereich der nationalen Sicherheit.

1) Kabinettssekretariat

Das Kabinettssekretariat nimmt die Erhebung von und die Suche nach Informationen zu wichtigen Maßnahmen des Kabinetts vor ([28]), wie in Artikel 12-2 des Kabinettsgesetzes festgelegt ([29]). Das Kabinettssekretariat ist jedoch nicht befugt, personenbezogene Daten direkt von Unternehmern zu erheben. Es erhebt, integriert, analysiert und bewertet Informationen aus öffentlich zugänglichen Quellen, von anderen Behörden usw.

2) NPA/Präfekturpolizei

In jeder Präfektur ist die Präfekturpolizei dazu befugt, in ihrem Zuständigkeitsbereich nach Artikel 2 des Polizeigesetzes Informationen zu erheben. Es kann vorkommen, dass die NPA in ihrem Zuständigkeitsbereich nach dem Polizeigesetz direkt Informationen erhebt. Dies betrifft insbesondere die Tätigkeiten des Sicherheitsdienstes der NPA und ihrer Abteilung für Auswärtige Angelegenheiten und Nachrichtendienst. Gemäß Artikel 24 des Polizeigesetzes ist der Sicherheitsdienst für Angelegenheiten zuständig, die die Sicherheitspolizei ([30]) betreffen, und die Abteilung für Auswärtige Angelegenheiten und Nachrichtendienst für Fragen betreffend Ausländer sowie japanische Staatsangehörige, deren Tätigkeitsschwerpunkte im Ausland liegen.

3) Nachrichtendienst für öffentliche Sicherheit (Public Security Intelligence Agency — PSIA)

Für die Anwendung des Gesetzes zur Verhütung subversiver Tätigkeiten (Subversive Activities Prevention Act — SAPA) und des Gesetzes über die Kontrolle von Organisationen, die wahllos Massenmorde verübt haben (Act on the Control of Organizations Who Have Committed Acts of Indiscriminate Mass Murder — ACO) ist hauptsächlich der Nachrichtendienst für öffentliche Sicherheit (PSIA) zuständig. Hierbei handelt es sich um eine dem Justizministerium unterstellte Behörde.

Das SAPA und das ACO sehen vor, dass im Rahmen der Verfassung unter strengen Auflagen administrative Anordnungen (d. h. Maßnahmen zur Einschränkung der Tätigkeiten solcher Organisationen, zu ihrer Auflösung usw.) gegen Organisationen beschlossen werden können, die bestimmte schwerwiegende Handlungen („terroristische subversive Tätigkeiten" oder „wahllose Massenmorde") begehen, die gegen die „öffentliche Sicherheit" oder das „grundlegende Gesellschaftssystem" gerichtet sind. „Terroristische subversive Tätigkeiten" fallen in den Anwendungsbereich des SAPA (siehe Artikel 4 zu Tätigkeiten wie Aufständen, Anstiftung zu Aggression von außen, Mord mit politischer Absicht usw.), während das ACO gegen „wahllose Massenmorde" gerichtet ist (siehe Artikel 4 ACO). Das SAPA oder das ACO können nur gegen genau bestimmte Organisationen, die eine konkrete interne oder externe Bedrohung für die öffentliche Sicherheit darstellen, angewandt werden.

Zu diesem Zweck sehen das SAPA und das ACO eine rechtliche Ermittlungsbefugnis vor. Die grundlegenden Ermittlungsbefugnisse der PSIA-Bediensteten sind in Artikel 27 SAPA und Artikel 29 ACO festgelegt. Ermittlungen des PSIA nach diesen Bestimmungen werden in dem Maße durchgeführt, wie dies im Hinblick auf die oben angeführten Anordnungen zur Kontrolle bestimmter Organisationen erforderlich ist (beispielsweise waren bisher radikale linke Gruppen, die Sekte *Aum Shinrikyo* und bestimmte, eng mit Nordkorea verbundene inländische Gruppen Gegenstand von Ermittlungen). Diese Ermittlungen können jedoch nicht auf Zwangsmaßnahmen beruhen, sodass eine Organisation im Besitz personenbezogener Informationen nicht gezwungen werden kann, diese Informationen zur Verfügung zu stellen.

Die Erhebung und Nutzung der Informationen, die dem PSIA gegenüber auf freiwilliger Basis offengelegt werden, unterliegt den einschlägigen gesetzlichen Garantien und Beschränkungen, unter anderem der Geheimhaltung der Kommunikation, die durch die Verfassung garantiert wird, und den Vorschriften des APPIHAO für den Umgang mit personenbezogenen Informationen.

4) Verteidigungsministerium (Ministry of Defence — MOD)

Was die Erhebung von Informationen durch das Verteidigungsministerium (MOD) betrifft, so erhebt es Informationen auf der Grundlage der Artikel 3 und 4 des Gesetzes über die Errichtung des MOD, soweit dies für die Wahrnehmung der Angelegenheiten innerhalb seiner administrativen Zuständigkeit erforderlich ist; dies umfasst Verteidigung und Schutz, Maßnahmen der Selbstverteidigungsstreitkräfte sowie die Entsendung der Selbstverteidigungsstreitkräfte des Heeres, der Marine und der Luftwaffe. Das Verteidigungsministerium kann Informationen zu diesen Zwecken nur im Wege der freiwilligen Zusammenarbeit und aus frei zugänglichen Quellen erheben. Es erhebt keine Informationen über die breite Öffentlichkeit.

2) Beschränkungen und Garantien

*a) Gesetzliche Beschränkungen*

1) Allgemeine Beschränkungen auf der Grundlage des APPIHAO

Beim APPIHAO handelt es sich um ein allgemeines Gesetz, das für die Erhebung personenbezogener Daten und den Umgang damit durch Verwaltungsorgane in all ihren Tätigkeitsbereichen gilt. Daher gelten die in Abschnitt II.A.1 Buchstabe b Ziffer 2 beschriebenen Beschränkungen und Garantien auch für die Speicherung und Verwendung personenbezogener Informationen und ähnliche Zwecke im Bereich der nationalen Sicherheit.

([28]) Dies wird vom Nachrichtendienst- und Forschungsbüro des Kabinetts auf der Grundlage des Artikels 4 der Verordnung zum Aufbau des Kabinettssekretariat vorgenommen.

([29]) Dies umfasst „die Erhebung von und die Suche nach nachrichtendienstlichen Informationen zu wichtigen Maßnahmen des Kabinetts".

([30]) Die Sicherheitspolizei ist für die Bekämpfung der Kriminalität im Zusammenhang mit der öffentlichen Sicherheit und dem nationalen Interesse zuständig. Dazu gehören die Bekämpfung der Kriminalität und die Sammlung von Informationen hinsichtlich rechtswidriger Handlungen in Bezug auf links- und rechtsextreme Gruppen sowie schädliche, gegen Japan gerichtete Aktivitäten.

2) Besondere für die Polizei geltende Beschränkungen (sowohl für die NPA als auch für die Präfekturpolizei)

Wie im Abschnitt über die Erhebung von Informationen zu Strafverfolgungszwecken angegeben, kann die Polizei nur Informationen erheben, die in ihren Zuständigkeitsbereich fallen, und dies gemäß Artikel 2 Absatz 2 des Polizeigesetzes nur in einem auf die Erfüllung ihrer Aufgaben „streng begrenzten" Umfang und auf „unparteiliche, neutrale, unvoreingenommene und faire" Art und Weise. Darüber hinaus darf sie ihre Befugnisse „niemals in einer Weise missbrauchen, die den in der japanischen Verfassung garantierten Rechten und Freiheiten des Einzelnen zuwiderläuft".

3) Besondere für den PSIA geltende Beschränkungen

Sowohl nach Artikel 3 SAPA als auch nach Artikel 3 ACO dürfen Ermittlungen im Rahmen dieser Gesetze nicht über das Maß hinausgehen, das nötig ist, um den angestrebten Zweck zu erreichen, und nicht in einer Weise durchgeführt werden, die die grundlegenden Menschenrechte ungebührlich einschränkt. Darüber hinaus stellt nach Artikel 45 SAPA und Artikel 42 ACO ein Missbrauch der Befugnisse durch einen Bediensteten des PSIA eine Straftat dar, die mit höheren strafrechtlichen Sanktionen belegt werden kann als ein Amtsmissbrauch in anderen Bereichen des öffentlichen Sektors „im Allgemeinen".

4) Besondere für das MOD geltende Beschränkungen

Was die Erhebung und Organisation von Informationen durch das MOD betrifft, so sind gemäß Artikel 4 des Gesetzes über die Errichtung des MOD die Tätigkeiten des Ministeriums zur Erhebung von Informationen beschränkt auf das zur Erfüllung seiner Pflichten „erforderliche" Maß im Hinblick auf 1) Verteidigung und Schutz, 2) Maßnahmen der Selbstverteidigungsstreitkräfte sowie 3) die Organisation, die Personalstärke, den Aufbau, die Ausstattung und die Entsendung der Selbstverteidigungsstreitkräfte des Heeres, der Marine und der Luftwaffe.

*b) Sonstige Beschränkungen*

Wie bereits in Abschnitt II.A.2) Buchstabe b Ziffer 1 betreffend strafrechtliche Ermittlungen erläutert, ergibt sich aus der Rechtsprechung des Obersten Gerichtshofs, dass ein Antrag auf freiwillige Mitarbeit, der an einen Unternehmer gerichtet wird, für die Ermittlungen zu einer mutmaßlichen Straftat notwendig sein und für die Zwecke der Ermittlungen angemessen sein muss.

Obwohl sich die Ermittlungen der Ermittlungsbehörden im Bereich der nationalen Sicherheit sowohl in Bezug auf ihre Rechtsgrundlage als auch auf ihren Zweck von den Ermittlungen der Ermittlungsbehörden im Bereich der Strafverfolgung unterscheiden, gelten die zentralen Grundsätze „Notwendigkeit der Ermittlungen" und „Angemessenheit der Vorgehensweise" in ähnlicher Weise auch im Bereich der nationalen Sicherheit und müssen unter angemessener Berücksichtigung der besonderen Umstände des jeweiligen Falles eingehalten werden.

Die hier angeführten Beschränkungen stellen insgesamt sicher, dass Informationen nur erhoben und verarbeitet werden, soweit dies für die Erfüllung der besonderen Aufgaben der zuständigen Behörde sowie aufgrund besonderer Bedrohungen erforderlich ist. Damit ist ausgeschlossen, dass aus Gründen der nationalen Sicherheit massenweise und anlassunabhängig personenbezogene Informationen erhoben werden oder auf sie zugegriffen wird.

B. Aufsicht

1) Aufsicht auf der Grundlage des APPIHAO

Wie in Abschnitt II.B.2 erläutert, ist der Minister oder der Leiter jedes Ministeriums oder jeder Behörde mit der Befugnis ausgestattet, die Einhaltung des APPIHAO im betreffenden Ministerium bzw. der betreffenden Behörde zu überwachen und durchzusetzen. Darüber hinaus kann der Minister für Inneres und Kommunikation den Stand der Durchsetzung des Gesetzes prüfen, jeden Minister auffordern, auf der Grundlage der Artikel 49 und 50 des Gesetzes Material und Erklärungen vorzulegen, und auf der Grundlage des Artikels 51 des Gesetzes an jeden Minister eine Stellungnahme richten. Er kann beispielsweise durch die in den Artikeln 50 und 51 des Gesetzes genannten Handlungen um eine Änderung der Maßnahmen ersuchen.

2) Ausübung der Aufsicht über die Polizei durch die Kommissionen für öffentliche Sicherheit

Wie im Abschnitt „II. Staatlicher Zugriff für Strafverfolgungszwecke" erläutert, üben die unabhängigen Präfekturkommissionen für öffentliche Sicherheit die Aufsicht über die Tätigkeit der Präfekturpolizei aus.

Bei der Nationalen Polizeibehörde (National Police Agency — NPA) übt die Nationale Kommission für die öffentliche Sicherheit die Aufsichtsfunktion aus. Nach Artikel 5 des Polizeigesetzes ist diese Kommission für den „Schutz der Rechte und Freiheiten des Einzelnen" zuständig. Zu diesem Zweck legt sie insbesondere umfassende Maßnahmen fest, die Vorschriften für die Verwaltung der in den einzelnen Punkten des Artikels 5 Absatz 4 des Polizeigesetzes vorgesehenen Angelegenheiten und sonstige grundlegende Anweisungen oder Maßnahmen enthalten, auf denen die Durchführung der genannten Tätigkeiten beruhen sollte. Die Nationale Kommission für die öffentliche Sicherheit (National Public Safety Commission — NPSC) ist in gleichem Maße unabhängig wie die Präfekturkommissionen für öffentliche Sicherheit (Prefectural Public Safety Commissions — PPSC).

3) Ausübung der Aufsicht des MOD durch das Büro des Generalinspektors für die Einhaltung gesetzlicher Vorschriften

Das Büro des Generalinspektors für die Einhaltung gesetzlicher Vorschriften (Inspector General's Office of Legal Compliance — IGO) ist ein unabhängiges Büro im Verteidigungsministerium (MOD), das gemäß Artikel 29 des Gesetzes über die Errichtung des MOD unter direkter Aufsicht des Verteidigungsministers steht. Das IGO kann Kontrollen der Einhaltung von Gesetzen und sonstigen Vorschriften durch Bedienstete des MOD durchführen. Diese Kontrollen werden als „Verteidigungskontrollen" bezeichnet.

Das IGO führt aus der Sicht eines unabhängigen Büros Kontrollen durch, um die rechtliche Einhaltung im gesamten Ministerium einschließlich der Selbstverteidigungsstreitkräfte (Self-Defense Forces — SDF) zu gewährleisten. Es nimmt seine Aufgaben unabhängig von den operativen Abteilungen des MOD wahr. Nach einer Kontrolle erstattet das IGO unverzüglich und unmittelbar dem Verteidigungsminister über seine Ergebnisse Bericht und führt die erforderlichen Maßnahmen zur Abhilfe an. Der Verteidigungsminister kann auf der Grundlage des Berichts des IGO Anordnungen erlassen, um die erforderlichen Abhilfemaßnahmen zu ergreifen. Der stellvertretende Minister ist für die Umsetzung dieser Maßnahmen verantwortlich und muss dem Verteidigungsminister über den Stand der Umsetzung Bericht erstatten.

Im Rahmen einer freiwilligen Transparenzmaßnahme werden die Ergebnisse der Verteidigungskontrollen jetzt auf der Website des MOD veröffentlicht (obwohl dies gesetzlich nicht vorgeschrieben ist).

Es gibt drei Kategorien von Verteidigungskontrollen:

(i) Regelmäßige Verteidigungskontrollen, die periodisch durchgeführt werden ([31]);

(ii) Verteidigungskontrollen, die durchgeführt werden, um zu überprüfen, ob Abhilfemaßnahmen wirksam umgesetzt wurden;

(iii) besondere Verteidigungskontrollen, die zu bestimmten Aspekten im Auftrag des Verteidigungsministers durchgeführt werden.

Im Rahmen solcher Kontrollen kann der Generalinspekteur von der betreffenden Dienststelle Berichte anfordern, die Vorlage von Dokumenten anfordern, Kontrollen vor Ort durchführen, Erklärungen des stellvertretenden Ministers anfordern usw. In Anbetracht der Art der Kontrollaufgaben des IGO wird dieses Büro von hochrangigen Rechtsexperten geleitet (ehemalige Oberstaatsanwälte).

4) Ausübung der Aufsicht des PSIA

Der PSIA führt sowohl regelmäßige als auch besondere Kontrollen der Tätigkeiten seiner einzelnen Büros und Dienststellen auf allen Ebenen (Public Security Intelligence Bureau, Public Security Intelligence Offices und Sub Offices usw.) durch. Zum Zwecke der regelmäßigen Kontrollen wird/werden ein stellvertretender Generaldirektor und/oder ein Direktor als Inspektor(en) benannt. Diese Kontrollen betreffen auch die Verwaltung personenbezogener Informationen.

5) Ausübung der Aufsicht durch das Parlament

Was die Erhebung von Informationen zu strafrechtlichen Zwecken betrifft, so kann das Parlament über seinen zuständigen Ausschuss die Rechtmäßigkeit der Erhebung von Informationen im Bereich der nationalen Sicherheit untersuchen. Die Untersuchungsbefugnisse des Parlaments stützen sich auf Artikel 62 der Verfassung und die Artikel 74 und 104 des Parlamentsgesetzes.

C. Individueller Rechtsschutz

Individueller Rechtsschutz können auf dem gleichen Wege wie im Bereich der Strafverfolgung in Anspruch genommen werden. Dies umfasst auch den neuen Rechtsbehelfsmechanismus für die Bearbeitung und Lösung von Beschwerden von Einzelpersonen aus der EU, der von der PPC verwaltet und beaufsichtigt wird. In diesem Zusammenhang wird auf die entsprechenden Passagen in Abschnitt II.C verwiesen.

Darüber hinaus gibt es besondere Wege des individuellen Rechtsschutzes, die im Bereich der nationalen Sicherheit zur Verfügung stehen.

Personenbezogene Informationen, die von einem Verwaltungsorgan aus Gründen der nationalen Sicherheit erhoben werden, unterliegen den Bestimmungen des Kapitels 4 APPIHAO. Dies umfasst das Recht auf Offenlegung (Artikel 12), das Recht auf Berichtigung (einschließlich Hinzufügung oder Streichung) (Artikel 27) der gespeicherten personenbezogenen Informationen des Einzelnen sowie das Recht, die Aussetzung der Nutzung der personenbezogenen Daten zu

([31]) Als Beispiel für eine Kontrolle im Zusammenhang mit den in dieser Erklärung behandelten Aspekten ist die Regelmäßige Verteidigungskontrolle von 2016 im Hinblick auf die „Sensibilisierung und Vorbereitung für die Einhaltung der Vorschriften" zu nennen, da der Schutz personenbezogener Informationen einer der Schwerpunkte dieser Kontrolle war. Im Einzelnen betraf die Kontrolle unter anderem die Verwaltung und die Speicherung personenbezogener Informationen. In seinem Bericht stellte das IGO mehrere unangemessene Aspekte bei der Verwaltung personenbezogener Informationen fest, die verbessert werden sollten, wie z. B. das Versäumnis, die Daten mittels eines Kennworts zu schützen. Der Bericht kann auf der Website des MOD abgerufen werden.

fordern, falls das Verwaltungsorgan die betreffenden Informationen unrechtmäßig erlangt hat (Artikel 36). Allerdings unterliegt die Ausübung dieser Rechte im nationalen Sicherheitsraum bestimmten Beschränkungen: Anträgen auf Offenlegung, Berichtigung oder Aussetzung wird nicht stattgegeben, wenn sie „Informationen, bei denen der Leiter eines Verwaltungsorgans hinreichende Gründe für die Feststellung hat, dass eine Offenlegung die nationale Sicherheit beeinträchtigen oder die Beziehungen des gegenseitigen Vertrauens zu einem anderen Land oder einer internationalen Organisation schädigen würde oder bei Verhandlungen mit einem anderen Land oder einer internationalen Organisation nachteilig wäre“ (Artikel 14 Ziffer iv), betreffen. Es fällt also nicht jede Erhebung von Informationen auf freiwilliger Basis im Zusammenhang mit der nationalen Sicherheit unter diese Ausnahme, da dies stets eine konkrete Abschätzung der mit ihrer Offenlegung verbundenen Risiken erfordert.

Außerdem kann eine Einzelperson, wenn ihr Antrag mit der Begründung abgelehnt wird, dass die betreffenden Informationen als nicht offenlegbar im Sinne des Artikels 14 Ziffer iv angesehen werden, eine Verwaltungsbeschwerde zur Überprüfung einer solchen Entscheidung einlegen, indem sie beispielsweise geltend macht, dass die Voraussetzungen des Artikels 14 Ziffer iv im vorliegenden Fall nicht erfüllt sind. In diesem Fall konsultiert der Leiter des betreffenden Verwaltungsorgans vor seiner Entscheidung die Kontrollstelle für die Offenlegung von Informationen und den Schutz personenbezogener Informationen. Diese Stelle überprüft die Beschwerde aus unabhängiger Sicht. Es handelt sich hierbei um ein unabhängiges Fachgremium, dessen Mitglieder vom japanischen Premierminister mit Zustimmung der beiden Häuser des Parlaments ernannt werden und über ausgezeichnetes Fachwissen verfügen ([32]). Die Kontrollstelle verfügt über starke Untersuchungsbefugnisse, darunter die Möglichkeit, Dokumente und die Offenlegung der in Frage stehenden personenbezogenen Informationen anzufordern, Beratungen unter Ausschluss der Öffentlichkeit durchzuführen und das Vaughn-Index-Verfahren anzuwenden ([33]). Anschließend erstellt sie einen schriftlichen Bericht, der der betroffenen Einzelperson übermittelt wird ([34]). Die in dem Bericht getroffenen Feststellungen werden veröffentlicht. Obwohl der Bericht formal nicht rechtsverbindlich ist, werden fast alle Berichte von dem betreffenden Verwaltungsorgan befolgt ([35]).

Schließlich kann der Betroffene gemäß Artikel 3 Absatz 3 des Verwaltungsrechtsstreitigkeitengesetzes Klage erheben, um den Widerruf der Entscheidung des Verwaltungsorgans, die personenbezogenen Informationen nicht offenzulegen, zu erwirken.

### IV. **Regelmäßige Überprüfung**

Im Rahmen der regelmäßigen Überprüfung des Angemessenheitsbeschlusses werden die PPC und die Europäische Kommission Informationen über die Verarbeitung von Daten unter den Bedingungen der Angemessenheitsfeststellung austauschen, einschließlich derjenigen, die in dieser Erklärung dargelegt sind.

---

([32]) Siehe Artikel 4 des Gesetzes über die Kontrollstelle für die Offenlegung von Informationen und den Schutz personenbezogener Informationen.

([33]) Siehe Artikel 9 des Gesetzes über die Kontrollstelle für die Offenlegung von Informationen und den Schutz personenbezogener Informationen.

([34]) Siehe Artikel 16 des Gesetzes über die Kontrollstelle für die Offenlegung von Informationen und den Schutz personenbezogener Informationen.

([35]) In den letzten drei Jahren gab es keinen Präzedenzfall, bei dem das betreffende Verwaltungsorgan eine Entscheidung getroffen hätte, die von den Schlussfolgerungen der Kontrollstelle abwich. Auch davor gab es äußerst wenige solcher Fälle: nur zwei von insgesamt 2 000 Fällen seit 2005 (als das APPIHAO in Kraft getreten ist). Trifft das Verwaltungsorgan eine Entscheidung oder einen Beschluss, die bzw. der von den Schlussfolgerungen der Kontrollstelle abweicht, so gibt es gemäß Artikel 50 Absatz 1 Nummer 4 des Verwaltungsbeschwerdeprüfungsgesetzes in Verbindung mit der Ersetzung des Artikels 42 Absatz 2 APPIHAO klare Gründe hierfür an.