

II

(Ikke-lovgivningsmæssige retsakter)

AFGØRELSE

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2019/419

af 23. januar 2019

i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 vedrørende Japans tilstrækkelige beskyttelse af personoplysninger i henhold til loven om beskyttelse af personlige oplysninger*(meddelt under nummer K(2019) 304)***(EØS-relevant tekst)**

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) ⁽¹⁾, særlig artikel 45, stk. 3,

efter høring af Den Europæiske Tilsynsførende for Databeskyttelse:

1. INDLEDNING

- (1) I forordning (EU) 2016/679 fastsættes reglerne for overførsel af personoplysninger fra en dataansvarlig eller databehandler i Den Europæiske Union til tredjelande og internationale organisationer, i det omfang overførslen falder inden for forordningens anvendelsesområde. Reglerne om internationale overførsler af personoplysninger er fastsat i kapitel V i forordningen, nærmere bestemt dennes artikel 44-50. Strømmen af personoplysninger til og fra lande uden for Unionen er nødvendig af hensyn til udbygningen af det internationale samarbejde og den internationale handel, og reglerne sikrer, at beskyttelsesniveauet for personoplysninger i EU ikke undergraves.
- (2) I henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 kan Kommissionen ved hjælp af en gennemførelsesretsakt fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau. I henhold til denne betingelse kan personoplysninger overføres til tredjelandet, området, sektoren eller den internationale organisation uden yderligere godkendelse, jf. artikel 45, stk. 1, og betragtning 103 i forordningen.
- (3) Som omhandlet i artikel 45, stk. 2, i forordning (EU) 2016/679 skal vedtagelsen en afgørelse om tilstrækkeligheden af beskyttelsesniveauet finde sted på grundlag af en omfattende analyse af det pågældende tredjelandets retsorden, både hvad angår de regler, der finder anvendelse på dataimportøren, og de begrænsninger og garantier, der gælder med hensyn til offentlige myndigheders adgang til personoplysninger. I vurderingen skal det fastslås, om det pågældende tredjeland sikrer et beskyttelsesniveau, som »i det væsentlige svarer« til det, der sikres i Den Europæiske Union (betragtning 104 i forordning (EU) 2016/679). Som Den Europæiske Unions Domstol har præciseret, kræves der ikke et identisk beskyttelsesniveau ⁽²⁾. Det betyder navnlig, at de midler, som tredjelandet anvender, kan være forskellige fra de midler, som gennemføres inden for Den Europæiske Union, så længe de i praksis viser sig at være effektive med henblik på at sikre et tilstrækkeligt beskyttelsesniveau ⁽³⁾. Standarden for

⁽¹⁾ EUT L 119 af 4.5.2016, s. 1. (»databeskyttelsesforordningen«).

⁽²⁾ Sag C-362/14, Maximilian Schrems mod Data Protection Commissioner (»Schrems«), EU:C:2015:650, præmis 73.

⁽³⁾ Schrems, præmis 74.

tilstrækkelighed er derfor ikke, at EU-reglerne duplikeres punkt for punkt. Testen består snarere i, om det pågældende udenlandske system som helhed sikrer det krævede beskyttelsesniveau gennem kerneindholdet i retten til privatlivets fred og den effektive gennemførelse, overvågning og håndhævelse heraf ⁽⁴⁾.

- (4) Kommissionen har foretaget en grundig analyse af den japanske lovgivning og praksis. På grundlag af overvejelserne i betragtning 6-175 konkluderer Kommissionen, at Japan sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres til organisationer, som falder inden for anvendelsesområdet af loven om beskyttelse af personlige oplysninger ⁽⁵⁾ og af de yderligere betingelser omhandlet i denne afgørelse. Disse betingelser fastlægges i de supplerende regler (bilag I), som er vedtaget af Japans kommission for beskyttelse af personlige oplysninger (PPC) ⁽⁶⁾, og i den japanske regerings officielle redegørelser, forsikringer og tilsagn til Europa-Kommissionen (bilag II).
- (5) Det fastsættes ved denne afgørelse, at overførsler fra en dataansvarlig eller databehandler i Det Europæiske Økonomiske Samarbejdsområde (EØS) ⁽⁷⁾ til sådanne organisationer i Japan kan finde sted, uden at der behøves yderligere tilladelse. Denne afgørelse berører ikke den direkte anvendelse af forordning (EU) 2016/679 på sådanne organisationer, hvis betingelserne i forordningens artikel 3 er opfyldt.

2. REGLERNE FOR ERHVERVSDRIVENDES BEHANDLING AF OPLYSNINGER

2.1. De japanske lovrammer for databeskyttelse

- (6) Den retlige ordning for beskyttelse af privatlivets fred og databeskyttelse i Japan har sine rødder i landets forfatning, som er fra 1946.
- (7) I forfatningens artikel 13 bestemmes følgende:

»Alle mennesker respekteres som individer. Deres ret til liv, frihed og stræben efter lykke skal, i det omfang dette ikke griber ind i den offentlige velfærd, være det vigtigste hensyn i lovgivningen og i myndighedernes øvrige anliggender.«

- (8) På grundlag af denne bestemmelse har den japanske højesteret præciseret den enkeltes rettigheder med hensyn til beskyttelse af personlige oplysninger. I en afgørelse fra 1969 anerkendte den retten til privatlivets fred og databeskyttelse som en forfatningssikret ret ⁽⁸⁾. Retten fastslog navnlig, at »enhver har friheden til at beskytte sine personlige oplysninger mod videregivelse til tredjemand eller offentliggørelse uden gyldig grund«. Derudover fastslog den japanske højesteret i en afgørelse af 6. marts 2008 (»Juki-Net«) ⁽⁹⁾, at »borgernes frihed i privatlivet skal beskyttes mod udøvelse af offentlig myndighed, og at dette indebærer, at den enkeltes frihed i privatlivet også omfatter, at enhver har friheden til at beskytte sine personlige oplysninger mod videregivelse til tredjemand eller offentliggørelse uden gyldig grund.« ⁽¹⁰⁾

- (9) Den 30. maj 2003 trådte en række love om databeskyttelse i kraft i Japan:

— Loven om beskyttelse af personlige oplysninger (APPI)

— Loven om beskyttelse af personlige oplysninger i administrative organer (APPIHAO)

— Loven om beskyttelse af personlige oplysninger i inkorporerede administrative agenturer (APPI-IAA).

⁽⁴⁾ Se meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, COM(2017) 7 af 10.1.2017, punkt 3.1., s. 6.

⁽⁵⁾ Lov om beskyttelse af personlige oplysninger (lov nr. 57 af 2003).

⁽⁶⁾ Flere oplysninger om PPC kan findes via følgende link: <https://www.ppc.go.jp/en/> (herunder kontaktoplysninger for forespørgsler og klager: <https://www.ppc.go.jp/en/contactus/access/>).

⁽⁷⁾ Denne afgørelse er EØS-relevant. I henhold til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS-aftalen) udvides Den Europæiske Unions indre marked til at omfatte de tre EØS-stater Island, Liechtenstein og Norge. Det Blandede EØS-Udvalgs afgørelse om indarbejdelse af forordning (EU) 2016/679 i bilag XI til EØS-aftalen blev vedtaget af Det Blandede EØS-udvalg den 6. juli 2018 og trådte i kraft den 20. juli 2018. Forordningen er således omfattet af nævnte aftale.

⁽⁸⁾ Højesteret, det samlede kollegiums dom af 24. december 1969, Keishu bind 23, nr. 12, s. 1625.

⁽⁹⁾ Højesteret, dom af 6. marts 2008, Minshu bind 62, nr. 3, s. 665.

⁽¹⁰⁾ Højesteret, dom af 6. marts 2008, Minshu bind 62, nr. 3, s. 665.

- (10) De to sidstnævnte retsakter (ændret i 2016) indeholder bestemmelser om beskyttelse af personlige oplysninger i offentlige enheder. Databeskyttelse omfattet af disse to retsakter er ikke genstanden for konstateringen af et tilstrækkeligt beskyttelsesniveau i denne afgørelse, idet denne er begrænset til den beskyttelse af personlige oplysninger, som foretages af »erhvervsdrivende, der håndterer personlige oplysninger« (PIHBO'er), i den i APPI anvendte betydning.
- (11) Der er foretaget ændringer af APPI de seneste år. Kundgørelsen af den ændrede APPI fandt sted den 9. september 2015, og den trådte i kraft den 30. maj 2017. Med ændringen indførtes en række nye garantier, og den indebar også en styrkelse af de eksisterende garantier, således at det japanske databeskyttelsessystem blev bragt tættere på det europæiske. Ændringen omfattede bl.a. en række individuelle rettigheder og oprettelsen af en uafhængig tilsynsmyndighed (PPC) med ansvar for tilsyn med og håndhævelse af APPI.
- (12) Behandlingen af personlige oplysninger, der falder inden for denne afgørelses anvendelsesområde, er ud over at være omfattet af APPI også omfattet af gennemførelsesregler udstedt på grundlag deraf. Dette omfatter en ændring af kabinetsbekendtgørelsen om gennemførelse af loven om beskyttelse af personlige oplysninger af 5. oktober 2016 og såkaldte håndhævelsesregler til loven om beskyttelse af personlige oplysninger vedtaget af PPC ⁽¹¹⁾. Begge regelsæt er retligt bindende og kan håndhæves, og de trådte i kraft på samme tidspunkt som den ændrede APPI.
- (13) Endvidere fastlagde det japanske regeringskabinet (bestående af premierministeren og ministre i hans regering) den 28. oktober 2016 en »grundlæggende politik« for på »udtømmende og integreret vis at fremme foranstaltninger vedrørende beskyttelse af personlige oplysninger«. I henhold til artikel 7 i APPI fastlægges den »grundlæggende politik« ved en kabinetsafgørelse, og den omfatter politiske retningslinjer for håndhævelsen af APPI, som er rettet til både de centrale og lokale myndigheder.
- (14) Den japanske regering vedtog for nylig ændringer af den »grundlæggende politik« ved en kabinetsafgørelse af 12. juni 2018. Med henblik på at lette internationale dataoverførsler får PPC som den kompetente myndighed i forbindelse med forvaltningen og gennemførelsen af APPI ved kabinetsafgørelsen delegeret »beføjelser til at træffe de nødvendige foranstaltninger til at slå bro over forskellene mellem systemerne og aktiviteterne mellem Japan og det pågældende tredjeland i henhold til lovens artikel 6 med henblik på at sikre passende håndtering af personlige oplysninger fra et sådant land«. Det fastsættes ved kabinetsafgørelsen, at dette omfatter beføjelser til at indføre øget beskyttelse, ved at PPC vedtager strengere regler, som supplerer og er mere vidtgående end dem i APPI og kabinetsbekendtgørelsen. I henhold til afgørelsen skal disse strengere regler være bindende og kunne håndhæves over for japanske erhvervsdrivende.
- (15) På grundlag af artikel 6 i APPI og nævnte kabinetsafgørelse vedtog PPC den 15. juni 2018 »supplerende regler i henhold til lov om beskyttelse af personlige oplysninger vedrørende håndteringen af personoplysninger, der overføres fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet« (de »supplerende regler«) med henblik på at øge beskyttelsen af personlige oplysninger, der overføres fra Den Europæiske Union til Japan på grundlag af nærværende afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Disse supplerende regler er retligt bindende for japanske erhvervsdrivende og kan håndhæves af både PPC og domstolene på samme måde som de bestemmelser i APPI, som de supplerer med strengere og/eller mere udførlige regler ⁽¹²⁾. Eftersom japanske erhvervsdrivende, som modtager og/eller viderebehandler personoplysninger fra Den Europæiske Union, vil være retligt forpligtet til at overholde de supplerende regler, vil de skulle sikre, at de kan identificere sådanne personoplysninger gennem hele deres »livscyklus« (f.eks. via tekniske »tagging«) eller organisatoriske midler (opbevaring i en dedikeret database) ⁽¹³⁾. I de følgende afsnit analyseres indholdet af hver enkelt supplerende regel som en del af vurderingen af de artikler i APPI, som den supplerer.
- (16) Modsat før ændringen i 2015, hvor det hørte under forskellige japanske ministerier i specifikke sektorer, bemyndiger APPI nu PPC til at vedtage »retningslinjer« »for at sikre en korrekt og effektiv gennemførelse af de foranstaltninger, som en erhvervsdrivende skal træffe« i henhold til databeskyttelsesreglerne. PPC giver via sine retningslinjer en autoritativ fortolkning af disse regler, navnlig af APPI. Ifølge de oplysninger, der er modtaget fra PPC, udgør disse retningslinjer en integreret del af den retlige ramme, og de skal sammenholdes med teksten til APPI,

⁽¹¹⁾ Findes på: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

⁽¹²⁾ Jf. de supplerende regler (indledningsafsnit).

⁽¹³⁾ Det generelle krav om, at fortegnelser (kun) må opbevares i en bestemt periode ændrer ikke herved. Selvom oplysningernes oprindelse er blandt de oplysninger, som den erhvervende PIHBO ifølge artikel 26, stk. 1, i APPI skal bekræfte, vedrører kravet i henhold til artikel 26, stk. 4, i APPI sammenholdt med artikel 18 i PPC's regler kun en særlig form for fortegnelse (jf. artikel 16 i PPC's regler) og forhindrer ikke en PIHBO i at sikre identificering af dataene i længere perioder. Dette er blevet bekræftet af PPC, som har anført at »[o]plysningerne om oprindelsen af EU-dataene skal opbevares af PIHBO'en, så længe det er nødvendigt med henblik på at overholde de supplerende regler.«

kabinetsbekendtgørelsen, PPC's regler og en række »spørgsmål og svar«⁽¹⁴⁾ udarbejdet af PPC. De er derfor »bindende for erhvervsdrivende«. Hvis retningslinjerne fastslår, at en erhvervsdrivende »skal« eller »ikke må« handle på en bestemt måde, vil PPC konkludere, at manglende overholdelse af de pågældende bestemmelser udgør en overtrædelse af loven⁽¹⁵⁾.

2.2. Materielt og personligt anvendelsesområde

- (17) Anvendelsesområdet for APPI bestemmes af de fastlagte begreber personlige oplysninger, personoplysninger og erhvervsdrivende, der håndterer personlige oplysninger. Samtidig er der i APPI nogle væsentlige undtagelser fra dennes anvendelsesområde, især for anonymt behandlede personoplysninger og for særlige typer af behandling foretaget af visse operatører. I APPI anvendes udtrykket »behandling« ikke, men derimod det tilsvarende »håndtering«, som ifølge de oplysninger, som er modtaget fra PPC, omfatter »enhver handling, der foretages med hensyn til personoplysninger«, herunder erhvervelse, input, akkumulering, organisering, opbevaring redigering/behandling, fornyelse, sletning, output, anvendelse og meddelelse af personlige oplysninger.

2.2.1. Definition af personlige oplysninger

- (18) Først og fremmest skelnes der i forbindelse med APPI's materielle anvendelsesområde mellem personlige oplysninger og personoplysninger, og det er kun visse bestemmelser i loven, der finder anvendelse på førstnævnte kategori. I henhold til artikel 2, stk. 1, i APPI omfatter begrebet »personlige oplysninger« alle oplysninger vedrørende en levende fysisk person, som gør det muligt at identificere pågældende. I definitionen sondres der mellem to kategorier af personlige oplysninger: i) individuelle identifikationskoder og ii) andre personlige oplysninger, hvorved en bestemt person kan identificeres. Sidstnævnte kategori omfatter også oplysninger, som ikke i sig selv muliggør identificering, men som let lader sig sammenstille med andre oplysninger og derved gør det muligt at identificere en bestemt person. Ifølge PPC's retningslinjer⁽¹⁶⁾ skal det afgøres fra sag til sag, om oplysninger let lader sig sammenstille, hvorved der tages hensyn til den erhvervsdrivendes faktiske situation (»forhold«). Dette antages, hvis en sådan sammenstilling er (eller ville kunne) udføres af en gennemsnitlig (»normal«) virksomhed med de for den til rådighed stående midler. Det er f.eks. ikke let at sammenstille oplysninger, hvis en virksomhed skal gøre sig usædvanlige anstrengelser eller begå ulovlige handlinger for at indhente de oplysninger, som skal sammenstilles, fra en eller flere erhvervsdrivende.

2.2.2. Definition af personoplysninger

- (19) Kun visse typer personlige oplysninger er omfattet af begrebet »personoplysninger« i APPI. »Personoplysninger« er defineret som »personlige oplysninger, der udgør en database over personlige oplysninger«, dvs. en »kollektiv mængde af oplysninger«, som omfatter personlige oplysninger, der er »systematisk organiseret, således at der kan søges efter bestemte personlige oplysninger ved hjælp af en computer«⁽¹⁷⁾, eller personlige oplysninger, som »i henhold til en kabinetsbekendtgørelse betragtes som værende systematisk organiserede, således at der let kan søges efter bestemte personlige oplysninger«, men »undtaget dem, der i henhold til en kabinetsbekendtgørelse giver meget begrænset mulighed for at skade en persons rettigheder og interesser i betragtning af anvendelsesmetoden«⁽¹⁸⁾.
- (20) Denne undtagelse er yderligere specificeret i kabinetsbekendtgørelsens artikel 3, stk. 1, hvorefter de tre følgende kumulative betingelser skal være opfyldt: i) den kollektive mængde af oplysninger skal være blevet »tilvejebragt med henblik på at blive solgt til en lang række uspecificerede personer, og tilvejebringelsen må ikke være blevet gennemført i strid med en lov eller en på grundlag deraf udstedt bekendtgørelse«, ii) den skal kunne »erhverves til enhver tid af et stort antal uspecificerede personer«, og iii) de deri indeholdte personoplysninger skal »leveres til

⁽¹⁴⁾ PPC, spørgsmål og svar, af 16. februar 2017 (ændret den 30. maj 2017), tilgængelig via følgende link: <https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf>. I PPC's »spørgsmål og svar« diskuteres en række emner fra retningslinjerne via praktiske eksempler, f.eks. hvad der udgør følsomme personoplysninger, fortolkningen af individuelt samtykke, tredjemandsoverførsler i forbindelse med cloudcomputing eller registreringsforpligtelsen i forbindelse med grænseoverskridende overførsler. Disse »spørgsmål og svar« er kun tilgængelige på japansk.

⁽¹⁵⁾ På foranledning af et specifikt spørgsmål har PPC meddelt Det Europæiske Databeskyttelsesråd, at »de japanske domstole baserer fortolkningen på retningslinjerne, når de anvender APPI/PPC's regler i individuelle sager, der indbringes for dem, og de har således direkte henvist til ordlyden af PPC's retningslinjer i deres domme. Derfor er PPC's retningslinjer også set i dette perspektiv bindende for erhvervsdrivende. PPC har ikke kendskab til, at domstolene nogensinde har fraveget retningslinjerne«. I den forbindelse har PPC henvist Kommissionen til en dom på databeskyttelsesområdet, hvor retten udtrykkeligt lagde retningslinjer til grund for sin afgørelse (jf. byretten i Osaka, afgørelse af 19. maj 2006, Hanrei Jiho, bind 1948, s. 122, hvor retten fandt, at en erhvervsdrivende var forpligtet til at træffe en sikkerhedskontrolforanstaltning på grundlag af sådanne retningslinjer).

⁽¹⁶⁾ PPC's retningslinjer (om generelle regler), s. 6.

⁽¹⁷⁾ Dette omfatter ethvert elektronisk register. PPC's retningslinjer (om generelle regler, s. 17) indeholder specifikke eksempler herpå, f.eks. en liste over e-mailadresser, som er gemt i e-mailsoftwaren.

⁽¹⁸⁾ Artikel 2, stk. 4 og 6, i APPI.

deres oprindelige formål uden at tilføje andre oplysninger vedrørende en levende fysisk person». Ifølge de redegørelser, der er modtaget fra PPC, er denne begrænsede undtagelse blevet indført for at fritage telefonbøger eller andre lignende registre.

- (21) Sondringen mellem »personlige oplysninger« og »personoplysninger« er relevant for oplysninger indsamlet i Japan, fordi sådanne oplysninger ikke altid udgør en del af en »database over personlige oplysninger« (f.eks. et enkelt sæt oplysninger, der indsamles og behandles manuelt), således at de bestemmelser i APPI, der kun vedrører personoplysninger, ikke finder anvendelse⁽¹⁹⁾.
- (22) Derimod ville denne sondring ikke være relevant i forbindelse med personoplysninger, der importeres fra Den Europæiske Union til Japan på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Eftersom sådanne oplysninger overføres elektronisk (da dette er den sædvanlige måde at udveksle oplysninger på i den digitale tidsalder, især over store afstande som mellem EU og Japan) og dermed bliver en del af dataimportørens elektroniske registreringssystem, vil sådanne EU-oplysninger falde ind under kategorien »personoplysninger« i henhold til APPI. I de ekstraordinære tilfælde, hvor personoplysninger på anden måde overføres fra EU (f.eks. i papirform), vil de stadig være omfattet af APPI, hvis de bliver en del af en »kollektiv mængde af oplysninger«, der er systematisk organiseret, således at der let kan søges efter specifikke oplysninger (artikel 2, stk. 4, nr. ii), i APPI). Ifølge kabinetsbekendtgørelsens artikel 3, stk. 2, vil dette være tilfældet, når oplysningerne er ordnet »efter en bestemt regel«, og databasen indeholder værktøjer som f.eks. en indholdsfortegnelse eller et indeks med henblik på at lette søgningen. Det svarer til definitionen på et »register« som omhandlet i databeskyttelsesforordningens artikel 2, stk. 1.

2.2.3. Definition af opbevarede personoplysninger

- (23) Visse bestemmelser i APPI, navnlig artikel 27-30 vedrørende individuelle rettigheder, finder kun anvendelse på en specifik kategori af personoplysninger, nemlig »opbevarede personoplysninger«. Disse er defineret i artikel 2, stk. 7, i APPI som andre personoplysninger end dem, som enten i) »i henhold til en kabinetsbekendtgørelse er potentielt til skade for offentlige eller andre interesser, hvis deres tilstedeværelse eller fravær bliver kendt«, eller »hvis sletning skal finde sted inden for en ved en kabinetsbekendtgørelse fastlagt periode på højst et år«.
- (24) Den første af disse to kategorier beskrives i artikel 4 i kabinetsbekendtgørelsen og omfatter fire forskellige undtagelser⁽²⁰⁾. Disse undtagelser forfølger mål, der svarer til målene i artikel 23, stk. 1, i forordning (EU) 2016/679, navnlig beskyttelse af den registrerede (en »berørt« i APPI's terminologi) og andres frihedsrettigheder, statens sikkerhed, den offentlige sikkerhed, retshåndhævelse på det strafferetlige område eller andre vigtige målsætninger i forbindelse med generelle samfundsinteresser. Desuden følger det af ordlyden af kabinetsbekendtgørelsens artikel 4, stk. 1, nr. i)-iv), at anvendelsen af dem altid forudsætter en specifik risiko i forbindelse med en af de beskyttede væsentlige interesser⁽²¹⁾.
- (25) Den anden kategori er nærmere beskrevet i artikel 5 i kabinetsbekendtgørelsen. Sammenholdt med artikel 2, stk. 7, i APPI indeholder bestemmelsen en undtagelse af personoplysninger, »hvis sletning skal finde sted« inden for en periode på seks måneder, fra anvendelsesområdet for begrebet »opbevarede personoplysninger«. PPC har forklaret, at denne undtagelse har til formål at tilskynde virksomhederne til at opbevare og behandle oplysninger i kortest mulig tid. Dette ville imidlertid betyde, at registrerede fra EU ikke vil kunne nyde godt af vigtige rettigheder alene på grund af varigheden af den periode, som en given virksomhed opbevarer deres oplysninger i.
- (26) For at afhjælpe denne situation er det ved supplerende regel nr. 2) fastlagt, at personoplysninger, som overføres fra Den Europæiske Union, »håndteres som opbevarede personoplysninger i den i artikel 2, stk. 7, i APPI anvendte betydning, uanset om sletningen skal finde sted efter en fastlagt periode«. Opbevaringsperioden vil derfor ikke have nogen indvirkning på de rettigheder, som registrerede fra EU har.

⁽¹⁹⁾ F.eks. artikel 23 i APPI om betingelserne for udveksling af personoplysninger med tredjemand.

⁽²⁰⁾ Dvs. personoplysninger i) »hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, potentielt vil være til skade for en berørt eller tredjemands liv, legeme eller formue« ii) »hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, potentielt vil opmuntre eller foranledige til en ulovlig eller uretmæssig handling« iii) »hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, muligvis vil undergrave den nationale sikkerhed, ødelægge et tillidsforhold til et andet land eller en international organisation, eller have ugunstig virkning i forhandlinger med et andet land eller en international organisation« og iv) »hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, muligvis vil være til hinder for opretholdelsen af den offentlige sikkerhed og orden, f.eks. forebyggelsen, bekæmpelsen og efterforskningen af kriminalitet«.

⁽²¹⁾ Hvis disse betingelser er til stede, kræves der ingen underretning af den pågældende person. Dette er i overensstemmelse med databeskyttelsesforordningens artikel 23, stk. 2, litra h), hvori det fastlægges, at registrerede ikke behøver at blive underrettet om begrænsningen, hvis dette »kan skade formålet med begrænsningen«.

2.2.4. Definition af anonymt behandlede personlige oplysninger

- (27) De krav, der finder anvendelse på anonymt behandlede personlige oplysninger, jf. definitionen i artikel 2, stk. 9, i APPI, er fastlagt i lovens kapitel 4, afsnit 2 (»Forpligtelser for en virksomhed i forbindelse med anonymt behandlede personlige oplysninger«). Omvendt er sådanne oplysninger ikke omfattet af bestemmelserne i kapitel IV, afsnit 1, i APPI, som indeholder lovens bestemmelser om databeskyttelsesgarantier og -rettigheder i forbindelse med behandlingen af personoplysninger. Selv om »anonymt behandlede personlige oplysninger« således ikke er omfattet af de »normale« databeskyttelsesregler (fastlagt i kapitel IV, afsnit 1, og artikel 42 i APPI), falder de inden for anvendelsesområdet for APPI, særlig artikel 36-39.
- (28) I henhold til artikel 2, stk. 9, i APPI er »anonymt behandlede personlige oplysninger« oplysninger om en person, som er fremkommet ved »behandlingen af personlige oplysninger« via foranstaltninger, der er foreskrevet i APPI (artikel 36, stk. 1) og nærmere fastlagt i PPC's regler (artikel 19), således at det er blevet umuligt at identificere en bestemt person eller genskabe de personlige oplysninger.
- (29) Det følger af disse bestemmelser, hvilket også er blevet bekræftet af PPC, at den proces, hvor personlige oplysninger gøres »anonyme«, ikke behøver at være teknisk irreversibel. I henhold til artikel 36, stk. 2, i APPI, er erhvervsdrivende, der håndterer »anonymt behandlede personlige oplysninger« kun forpligtet til at forhindre fornyet identifikation ved at træffe foranstaltninger til sikringen af »beskrivelser mv. og af individuelle identifikationskoder slettet fra personlige oplysninger, som er blevet anvendt til at generere de anonymt behandlede oplysninger, samt oplysninger vedrørende en anvendt behandlingsmetode«.
- (30) Eftersom »anonymt behandlede personlige oplysninger«, jf. definitionen i APPI, omfatter data, som muliggør fornyet identifikation af den enkelte, vil dette kunne betyde, at personoplysninger overført fra Den Europæiske Union kan miste en del af den eksisterende beskyttelse via en proces, der i henhold til forordning (EU) 2016/679 ville blive betragtet som en form for »pseudonomisering« snarere end »anonymisering« (således at oplysningernes karakter af personoplysninger ikke ændres).
- (31) Med henblik på denne situation er der i de supplerende regler fastlagt yderligere krav, som kun gælder personoplysninger overført fra Den Europæiske Union i henhold til denne afgørelse. I henhold til regel nr. 5) i de supplerende regler skal sådanne personlige oplysninger kun betragtes som anonymt behandlede personlige oplysninger i henhold til APPI, »hvis den erhvervsdrivende, der håndterer personlige oplysninger, træffer foranstaltninger, som gør fornyet identifikation af den enkelte umulig for alle, herunder ved at slette oplysninger vedrørende behandlingsmetoden m.v.« Det sidstnævnte bliver i de supplerende regler nærmere specificeret som oplysninger vedrørende beskrivelser m.v. og individuelle identifikationskoder, der er blevet slettet fra personlige oplysninger, som er blevet anvendt til at generere »anonymt behandlede personlige oplysninger«, samt oplysninger vedrørende en behandlingsmetode, som er blevet anvendt i forbindelse med sletning af disse beskrivelser og individuelle identifikationskoder. Med andre ord kræver de supplerende regler, at den erhvervsdrivende, der genererer »anonymt behandlede personlige oplysninger«, ødelægger den »nøgle«, der gør det muligt at identificere oplysningerne igen. Dette betyder, at personoplysninger fra Den Europæiske Union kun vil være omfattet af bestemmelserne i APPI om »anonymt behandlede personlige oplysninger« i tilfælde, hvor de ligeledes ville blive betragtet som anonyme oplysninger i henhold til forordning (EU) 2016/679 ⁽²²⁾.

2.2.5. Definition af erhvervsdrivende, der håndterer personlige oplysninger (PIHBO)

- (32) For så vidt angår den omfattede personkreds finder APPI kun anvendelse på erhvervsdrivende, der håndterer personlige oplysninger (PIHBO'er). En PIHBO defineres i artikel 2, stk. 5, i APPI som »en person, der stiller en database over personlige oplysninger til rådighed med henblik på anvendelse i virksomhed« med undtagelse af regerings- og forvaltningsorganerne på både centralt og lokalt plan.
- (33) Ifølge PPC's retningslinjer betyder »virksomhed« enhver form for »adfærd, der har til formål udøve et gentaget og vedvarende socialt anerkendt forehavende med et bestemt formål, uanset om dette er med gevinst for øje eller ej«. Organisationer, der ikke er juridiske personer (f.eks. de facto-sammenslutninger), eller fysiske personer betragtes som en PIHBO, hvis de har rådighed over (anvender) en database over personlige oplysninger o.lign. i deres virksomhed ⁽²³⁾. Derfor skal begrebet »virksomhed« i APPI forstås meget bredt, idet det både omfatter aktiviteter med og uden gevinst for øje, som kan udføres af alle typer af organisationer og af enkeltpersoner. Desuden omfatter »anvendelse i virksomhed« også personlige oplysninger, som ikke anvendes i den erhvervsdrivendes (eksterne) kommercielle relationer, men derimod internt, f.eks. i behandlingen af medarbejdernes oplysninger.

⁽²²⁾ Jf. betragtning 26 i forordning (EU) 2016/679.

⁽²³⁾ PPC's retningslinjer (om generelle regler), s. 18.

- (34) Der skelnes ikke mellem individers nationalitet, bopæl eller opholdssted i forhold til den beskyttelse, som er fastlagt i APPI. Det samme gælder enkeltpersoners muligheder for at klage til PPC eller at indbringe sager for domstolene.

2.2.6. Begreberne dataansvarlig og databehandler

- (35) I APPI skelnes der ikke mellem de forpligtelser, som pålægges dataansvarlige og databehandlere. Fraværet af denne sondring påvirker beskyttelsesniveauet, eftersom alle PIHBO'er er underlagt alle bestemmelser i loven. En PIHBO, der overlader håndteringen af personoplysninger til en befuldmægtiget (svarende til en databehandler i databeskyttelsesforordningen), er fortsat underlagt forpligtelserne i APPI og de supplerende regler med hensyn til de oplysninger, som den har overdraget. Samtidig er PIHBO'er i henhold til artikel 22 i APPI forpligtet til at foretage »det nødvendige tilsyn« med den befuldmægtigede. PPC har derudover bekræftet, at den befuldmægtigede også er bundet af forpligtelserne i APPI og de supplerende regler.

2.2.7. Sektorbestemte undtagelser

- (36) Ved artikel 76 i APPI undtages visse typer af databehandling fra anvendelsen af lovens kapitel IV, som indeholder de centrale bestemmelser om databeskyttelse (grundlæggende principper, erhvervsdrivendes forpligtelser, individuelle rettigheder, PPC's overvågning). De typer behandling, der er omfattet af de sektorbestemte undtagelser i artikel 76, er også undtaget fra PPC's håndhævelsesbeføjelser, jf. artikel 43, stk. 2, i APPI⁽²⁴⁾.
- (37) De relevante kategorier for de sektorspecifikke undtagelser i artikel 76 i APPI fastlægges via et dobbelt kriterium, som bygger på den type af PIHBO, som foretager behandlingen af de personlige oplysninger, og formålet med behandlingen. Undtagelsen gælder nærmere bestemt for: i) radio- og tv-spredningsorganer, avisudgivere, kommunikationsbureauer og andre presseorganer (herunder personer, som udøver presseaktiviteter som erhverv) i det omfang, de behandler personlige oplysninger til presseformål, ii) personer, der er professionelle skribenter, i det omfang dette involverer personlige oplysninger, iii) universiteter og alle organisationer eller grupper, hvis formål er akademiske undersøgelser, eller enhver person, der tilhører en sådan organisation, i det omfang de behandler personlige oplysninger med henblik på akademiske undersøgelser, iv) religiøse organer, i det omfang de behandler personlige oplysninger med henblik på religiøse aktiviteter (herunder alle tilknyttede aktiviteter), og v) politiske organer, i det omfang de behandler personlige oplysninger med henblik på deres politiske aktiviteter (herunder alle tilknyttede aktiviteter). Andre typer PIHBO'ers behandling af personlige oplysninger med henblik på et af de i artikel 76 anførte formål og ovennævnte PIHBO'ers behandling af personlige oplysninger med henblik på andre formål, f.eks. i personaleforhold, er fortsat omfattet af bestemmelserne i kapitel IV.
- (38) For at sikre et tilstrækkeligt beskyttelsesniveau for personoplysninger overført fra Den Europæiske Union til erhvervsdrivende i Japan er det kun behandlingen af personlige oplysninger inden for anvendelsesområdet af kapitel IV i APPI – dvs. behandling foretaget af en PIHBO i situationer, som ikke falder inden for en af de sektorbestemte undtagelser – som bør være omfattet af denne afgørelse. Afgørelsens anvendelsesområde bør derfor tilpasses APPI's. Ifølge de oplysninger, der er modtaget fra PPC, vil det blive betragtet som en international overførsel, når en PIHBO omfattet af denne afgørelse foretager en efterfølgende ændring af anvendelsesformålet (i det omfang dette er tilladt), således at en af de sektorspecifikke undtagelser i artikel 76 i APPI finder anvendelse (eftersom behandlingen af de personlige oplysninger i sådanne tilfælde ikke længere vil være omfattet af kapitel IV i APPI og dermed vil falde uden for dennes anvendelsesområde). Det samme gælder i tilfælde af, at en PIHBO videregiver personlige oplysninger til en enhed, der er omfattet af artikel 76 i APPI, til brug for et af de behandlingsformål, der er angivet i bestemmelsen. For så vidt angår personoplysninger, der overføres fra Den Europæiske Union, ville dette derfor udgøre en videreoverførsel, som vil være underlagt de relevante garantier (navnlig garantierne i artikel 24 i APPI og supplerende regel nr. 4). Hvis PIHBO'en støtter sig til den registreredes samtykke⁽²⁵⁾, vil denne skulle meddele pågældende alle de nødvendige oplysninger, herunder at de personlige oplysninger ikke længere vil være beskyttet af APPI.

⁽²⁴⁾ I udøvelsen af sine beføjelser med hensyn til at foretage undersøgelser og håndhæve reglerne over for de øvrige operatører må PPC aldrig begrænse deres ytringsfrihed, deres akademiske frihed, religionsfrihed og frihed til at udøve politiske aktiviteter (artikel 43, stk. 1, i APPI).

⁽²⁵⁾ PPC har forklaret, at samtykke i PPC's retningslinjer fortolkes som »en tilkendegivelse fra en berørt om accept af, at pågældendes personlige oplysninger må håndteres ved hjælp af en metode, som er angivet af den erhvervsdrivende, der håndterer personlige oplysninger«. I PPC's retningslinjer (om generelle regler, s. 24) er der anført, samtykkeformer, som betragtes som »almindelig forretningspraksis i Japan«, f.eks. mundtligt samtykke, returnering af formularer eller andre dokumenter, samtykke via e-mail, afkrydsning af et felt på en webside, klik på en hjemmeside, brug af en samtykkeknop, tryk på en berøringsskærm osv. Alle disse metoder udgør en udtrykkelig form for samtykke.

2.3. Garantier, rettigheder og forpligtelser

2.3.1. Formålsbegrænsning

- (39) Personoplysninger skal behandles til et specifikt formål og efterfølgende udelukkende anvendes, såfremt anvendelsen ikke er uforenelig med behandlingsformålet. Dette databeskyttelsesprincip er garanteret i artikel 15 og 16 i APPI.
- (40) APPI bygger på det princip, at en erhvervsdrivende skal angive anvendelsens formål »så præcist som muligt« (artikel 15, stk. 1) og derefter er bundet af dette formål i behandlingen af oplysningerne.
- (41) I den forbindelse fastsættes det i artikel 15, stk. 2, i APPI, at PIHBO'en ikke må ændre det oprindelige formål »ud over, hvad der med rimelighed må betragtes som relevant for anvendelsesformålet forud for ændringen«, hvilket i PPC's retningslinjer fortolkes som svarende til, hvad der objektivt kan forventes af den registrerede på grundlag af »normale sociale konventioner« ⁽²⁶⁾.
- (42) I henhold til artikel 16, stk. 1, i APPI må PIHBO'er derudover ikke behandle personlige oplysninger ud over, »hvad der er nødvendigt for at opnå et anvendelsesformål«, jf. artikel 15, uden på forhånd at indhente den registreredes samtykke, medmindre en af undtagelserne i artikel 16, stk. 3, finder anvendelse ⁽²⁷⁾.
- (43) Hvis der er tale om personlige oplysninger, der erhverves fra en anden erhvervsdrivende, er PIHBO'en i princippet fri til at bestemme et nyt anvendelsesformål ⁽²⁸⁾. For at sikre, at en sådan modtager, når der er tale om en overførsel fra Den Europæiske Union, er bundet af det formål, som dataene blev overført til, kræves det i henhold til supplerende regel nr. 3) i tilfælde, »hvor en [PIHBO] modtager personoplysninger fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet«, eller en sådan erhvervsdrivende »fra en anden [PIHBO] modtager personoplysninger, der tidligere er blevet overført fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet« (videregivelse), at modtageren skal »specificere formålet med at anvende de nævnte personoplysninger inden for rammerne af det anvendelsesformål, som oplysningerne enten oprindeligt eller sidenhen blev modtaget til«. Med andre ord sikrer reglen, at det i henhold til forordning (EU) 2016/679 angivne formål i en overførselskontekst fortsætter med at være bestemmende for behandlingen, og at en ændring af dette formål på et hvilket som helst trin af den behandling, der finder sted i Japan, vil kræve samtykke fra den registrerede i EU. For at indhente dette samtykke er PIHBO'en forpligtet til at kontakte den registrerede, men er dette ikke muligt, er konsekvensen blot, at det oprindelige formål skal fastholdes.

2.3.2. Behandlingens lovlighed og rimelighed

- (44) Den yderligere beskyttelse, der er omhandlet i betragtning 43, er så meget desto mere relevant, eftersom det er gennem princippet om formålsbegrænsning, at det japanske system ligeledes sikrer, at personoplysninger behandles lovligt og rimeligt.
- (45) I henhold til APPI skal en PIHBO i forbindelse med sin indsamling af personlige oplysninger udførligt specificere formålet med at anvende de personlige oplysninger ⁽²⁹⁾ og med det samme oplyse den registrerede om (eller offentliggøre) dette anvendelsesformål ⁽³⁰⁾. I artikel 17 i APPI er det desuden fastlagt, at en PIHBO ikke må skaffe sig personlige oplysninger ved bedrag eller andre upassende metoder. For så vidt angår visse kategorier af oplysninger, f.eks. følsomme personlige oplysninger, forudsætter erhvervelsen deraf den registreredes samtykke (artikel 17, stk. 2, i APPI).

⁽²⁶⁾ PPC's »spørgsmål og svar« indeholder en række eksempler til illustration heraf. Blandt eksemplerne på situationer, hvor ændringen er inden for, hvad der med rimelighed må betragtes som relevant, er navnlig anvendelsen af personlige oplysninger, som er erhvervet fra købere af varer eller tjenesteydelser i forbindelse med en kommerciel transaktion, med det formål at informere disse købere om andre relevante varer eller tjenesteydelser (f.eks. operatøren af et fitnesscenter, der registrerer medlemmernes e-mailadresser for at informere dem om kurser og programmer). PPC's »spørgsmål og svar« indeholder samtidig et eksempel på en situation, hvor ændringen af anvendelsesformålet ikke er tilladt, nemlig hvis en virksomhed sender oplysninger om virksomhedens varer og tjenesteydelser til e-mailadresser, som den har indsamlet for at kunne advare om svindel eller tyveri af et medlemskort.

⁽²⁷⁾ Disse undtagelser kan følge af andre love og forskrifter eller vedrøre situationer, hvor håndteringen af personlige oplysninger er nødvendig i) med henblik på beskyttelse af menneskers »liv, legeme eller ejendom«, ii) for at »styrke den offentlige hygiejne eller fremme børns sundhed« eller iii) for »at samarbejde med statslige organer eller deres repræsentanter« i udførelsen af deres lovbestemte opgaver. Desuden gælder kategori i) og ii) kun, hvis det er vanskeligt at opnå den registreredes samtykke, og kategori iii) gælder kun, hvis indhentningen af den registreredes samtykke vil kunne gribe forstyrrende ind i udførelsen af disse opgaver.

⁽²⁸⁾ I henhold til artikel 23, stk. 1, i APPI er den enkeltes samtykke derudover i princippet nødvendigt, hvis oplysningerne skal videregives til tredjemand. Derigennem kan den enkelte udøve en vis kontrol med en anden erhvervsdrivendes brug af pågældendes oplysninger.

⁽²⁹⁾ I henhold til artikel 15, stk. 1, i APPI, skal en sådan angivelse være så »udførlig som muligt«.

⁽³⁰⁾ Artikel 18, stk. 1, i APPI.

- (46) Som beskrevet i betragtning 41 og 42 må PIHBO'en endvidere ikke behandle de personlige oplysninger med andre formål for øje, med mindre den registrerede giver sit samtykke til denne behandling, eller en af undtagelserne i artikel 16, stk. 3, i APPI finder anvendelse.
- (47) Endelig begrænser artikel 23, stk. 1, i APPI videregivelsen af personlige oplysninger til tredjemand ⁽³¹⁾ til specifikke tilfælde, medmindre der som en generel hovedregel er indhentet forudgående samtykke ⁽³²⁾. Ved artikel 23, stk. 2-4, i APPI fastsættes undtagelser til kravet om indhentning af samtykke. Disse undtagelser finder imidlertid kun anvendelse med hensyn til ikkefølsomme oplysninger og kræver, at den erhvervsdrivende på forhånd oplyser de berørte personer om hensigten om at videregive deres personlige oplysninger til tredjemand og muligheden for at gøre indsigelse mod enhver yderligere videregivelse ⁽³³⁾.
- (48) For så vidt angår overførsler fra Den Europæiske Union vil personoplysninger nødvendigvis først være blevet indsamlet og behandlet i Unionen i overensstemmelse med reglerne i forordning (EU) 2016/679. Dette vil altid omfatte på den ene side indsamling og behandling, herunder til overførsel fra Den Europæiske Union til Japan, på grundlag af forordningens artikel 6, stk. 1, og på den anden side indsamling til et udtrykkeligt angivet og legitimt formål samt forbud mod yderligere behandling, herunder via overførsel, såfremt denne er uforenelig med sådanne formål, jf. forordningens artikel 5, stk. 1, litra b), og artikel 6, stk. 4.
- (49) I henhold til supplerende regel nr. 3) vil den PIHBO, der modtager oplysningerne efter overførslen, skulle »bekræfte« de(t) specifikke formål, der ligger til grund for overførslen (dvs. det i henhold til forordning (EU) 2016/679 angivne formål) og foretage videre behandling af disse oplysninger i overensstemmelse med et sådant eller sådanne formål ⁽³⁴⁾. Det er således ikke blot den, som først erhverver sådanne personoplysninger i Japan, der er bundet af det eller de i henhold til forordningen angivne formål, men også enhver fremtidig modtager af disse oplysninger (herunder en befuldmægtiget).
- (50) I tilfælde af at PIHBO'en ønsker at ændre det formål, der tidligere er blevet angivet i henhold til forordning (EU) 2016/679, vil denne derudover i henhold til artikel 16, stk. 1, i APPI i princippet skulle indhente den registreredes samtykke. Uden dette samtykke vil enhver behandling af oplysninger, som går ud over, hvad der er nødvendigt for at opnå dette anvendelsesformål, udgøre en overtrædelse af artikel 16, stk. 1, som vil kunne håndhæves af PPC og ved domstolene.
- (51) Eftersom en overførsel i henhold til forordning (EU) 2016/679 kræver et gyldigt retsgrundlag og et specifikt formål, som afspejles i det anvendelsesformål, der »bekræftes« i henhold til APPI, betyder dette, at kombinationen af de relevante bestemmelser i APPI og supplerende regel nr. 3) sikrer den fortsatte lovlighed af behandlingen af oplysninger fra EU i Japan.

2.3.3. Oplysningernes rigtighed og minimering

- (52) Oplysninger bør være korrekte og om nødvendigt ajourførte. Oplysningerne bør også være tilstrækkelige, relevante og ikke for omfattende i forhold til behandlingsformålet.
- (53) Disse principper sikres i japansk lovgivning ved artikel 16, stk. 1, i APPI, som forbyder håndteringen af personlige oplysninger ud over, »hvad der er nødvendigt for at opnå et anvendelsesformål«. Ifølge PPC udelukker dette ikke blot anvendelsen af oplysninger, som ikke er tilstrækkelige, og for omfattende anvendelse af oplysninger (ud over, hvad der er nødvendigt for at opnå anvendelsesformålet), men også et forbud mod håndtering af oplysninger, som ikke er relevante for at opnå anvendelsesformålet.

⁽³¹⁾ Befuldmægtigede ikke er omfattet af begrebet »tredjemand« med henblik på anvendelsen af artikel 23 (jf. stk. 5), men denne undtagelse gælder kun, for så vidt som befuldmægtigede håndterer personoplysninger inden for rammerne af overdragelsen (»i det omfang, det er nødvendigt for at opnå anvendelsesformålet«), dvs. handler som en databehandler.

⁽³²⁾ De øvrige (ekstraordinære) grunde er: i) videregivelsen af personlige oplysninger »på grundlag af love og forskrifter«, ii) tilfælde, »hvor der er behov for at beskytte menneskers liv, legeme eller formue, og når det er vanskeligt at indhente en berørts samtykke«, iii) tilfælde, »hvor der er behov for at styrke den offentlige hygiejne eller fremme børns sundhed, og når det er vanskeligt at indhente en berørts samtykke«, og iv) tilfælde, »hvor der er behov for samarbejde med hensyn til et statsligt organ eller en lokalforvaltning, eller en af disse bemyndiget person, der varetager anliggender i henhold til love og forskrifter, og når indhentningen af en berørts samtykke potentielt vil kunne virke indgribende på varetagelsen af disse anliggender«.

⁽³³⁾ I den forbindelse skal navnlig kategorierne af oplysninger, der vil blive delt med tredjemand, og overførselsmetoden oplyses. Derudover skal PIHBO'en oplyse den registrerede om muligheden for at gøre indsigelse, og hvordan man rent praktisk gør dette.

⁽³⁴⁾ Ifølge artikel 26, stk. 1, nr. ii), skal en PIHBO ved modtagelsen af personoplysninger fra tredjemand »bekræfte« (verificere) »de omstændigheder, hvorunder tredjemanden har erhvervet de pågældende personoplysninger«. Selv om det ikke udtrykkeligt er angivet i artikel 26, at PIHBO'en derefter skal følge dette formål, fremgår dette krav eksplicit af supplerende regel nr. 3).

- (54) For så vidt angår forpligtelsen til at sikre, at data er korrekte og ajourførte, indeholder artikel 19 i APPI et krav om, at PIHBO'en skal »stræbe efter at sikre, at personoplysninger er korrekte og ajourførte i det omfang, det er nødvendigt for at opnå anvendelsesformålet«. Denne bestemmelse skal læses sammen med artikel 16, stk. 1, i APPI: ifølge de forklaringer, som PPC har givet, vil behandlingen af personlige oplysninger ikke blive anset for at opnå anvendelsesformålet, når en PIHBO ikke overholder de beskrevne standarder med hensyn til rigtighed, og følgelig vil håndteringen blive betragtet som ulovlig i henhold til artikel 16, stk. 1.

2.3.4. Opbevaringsbegrænsning

- (55) Oplysninger bør i princippet ikke opbevares i et længere tidsrum end det, der er nødvendigt til de formål, hvortil personoplysningerne behandles.
- (56) Ifølge artikel 19 i APPI skal PIHBO'er »stræbe [...] efter at slette personoplysningerne, så snart denne anvendelse ikke længere er nødvendig«. Denne bestemmelse skal sammenholdes med artikel 16, stk. 1, i APPI, som forbyder håndteringen af personlige oplysninger ud over, »hvad der er nødvendigt for at opnå et anvendelsesformål«. Når anvendelsesformålet er opnået, kan behandlingen af de personlige oplysninger ikke betragtes som nødvendig mere, og den kan derfor ikke fortsætte (medmindre PIHBO'en får den registreredes samtykke dertil).

2.3.5. Datasikkerhed

- (57) Personoplysninger bør behandles således, at de er sikre, herunder via beskyttelse mod uautoriseret og ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse. Med henblik herpå bør de erhvervsdrivende træffe passende tekniske eller organisatoriske foranstaltninger for at beskytte personoplysninger mod potentielle trusler. Disse foranstaltninger bør vurderes under hensyntagen til det aktuelle tekniske niveau og de relaterede omkostninger.
- (58) Dette princip er gennemført i japansk lov ved artikel 20 i APPI, hvori det fastlægges, at en PIHBO »skal træffe nødvendige og passende foranstaltninger med henblik på sikkerhedskontrollen for personoplysninger, herunder at forebygge læk, tab eller beskadigelse af de personoplysninger, som den håndterer«. I PPC's retningslinjer forklares de foranstaltninger, der skal træffes, herunder metoderne til indførelse af grundlæggende politikker, databehandlingsregler og forskellige »kontrollforanstaltninger« (vedrørende organisationssikkerhed samt menneskelig, fysisk og teknologisk sikkerhed) ⁽³⁵⁾. Derudover indeholder PPC's retningslinjerne og et dedikeret cirkulære (tillæg 8 om »Indholdet af de sikkerhedsforanstaltninger, der skal træffes«), som PPC har offentliggjort, yderligere oplysninger om foranstaltninger i forbindelse med sikkerhedshændelser, f.eks. læk af personlige oplysninger, inden for rammerne af de sikkerhedsforanstaltninger, PIHBO'er skal træffe ⁽³⁶⁾.
- (59) Når personlige oplysninger håndteres af medarbejdere eller underleverandører, skal der derudover sikres »nødvendigt og passende tilsyn«, jf. artikel 20 og 21 i APPI, med henblik på sikkerhedskontrol. Endelig kan forsætlig lækage eller tyveri af personlige oplysninger i henhold til artikel 83 i APPI straffes med op til et års fængsel.

2.3.6. Gennemsigthed

- (60) Registrerede bør underrettes om de vigtigste dele af behandlingen af deres personoplysninger.
- (61) I henhold til artikel 18, stk. 1, skal PIHBO'en gøre oplysninger om anvendelsesformålet for de erhvervede personlige oplysninger tilgængelige for den registrerede, undtagen i »tilfælde, hvor et anvendelsesformål på forhånd er blevet meddelt offentligheden«. Samme forpligtelse gælder i tilfælde af en tilladt ændring af formålet (artikel 18, stk. 3). Derved sikres det også, at den registrerede bliver underrettet om, at pågældendes oplysninger er blevet indsamlet. Selv om det ikke er et generelt krav i APPI, at PIHBO'en skal underrette den registrerede om de forventede modtagere af de personlige oplysninger i forbindelse med indsamlingen, er disse oplysninger en nødvendig betingelse for enhver videregivelse af oplysninger til tredjemand (modtager) på grundlag af artikel 23, stk. 2, dvs. hvor videregivelsen finder sted uden den registreredes forudgående samtykke.

⁽³⁵⁾ PPC's retningslinjer (om generelle regler), s. 41 og s. 86-98.

⁽³⁶⁾ Ifølge afsnit 3-3-2 i PPC's retningslinjer skal PIHBO'en i tilfælde af sådanne lækager, skader eller tab foretage de nødvendige undersøgelser og navnlig vurdere omfanget af krænkelsen af den enkeltes rettigheder og interesser samt arten og mængden af de berørte personlige oplysninger.

- (62) For så vidt angår »opbevarede personoplysninger« fastlægges det i artikel 27 i APPI, at PIHBO'en skal oplyse den registrerede om sin identitet (kontaktoplysninger), anvendelsesformålet og procedurerne for besvarelsen af en anmodning vedrørende den registreredes individuelle rettigheder i henhold til artikel 28, 29 og 30 i APPI.
- (63) Da personoplysninger overført fra Den Europæiske Union i henhold til de supplerende regler vil blive anset for »opbevarede personoplysninger« uanset deres opbevaringsperiode (medmindre undtagelser finder anvendelse), vil de altid være omfattet af gennemsigtighedskravene i begge førnævnte bestemmelser.
- (64) Både kravene i artikel 18 og forpligtelsen til at oplyse om anvendelsesformålet i artikel 27 i APPI er underlagt de samme undtagelser, som hovedsagelig er baseret på hensyn til almenvellet og beskyttelsen af den registreredes, tredjemands og den dataansvarliges rettigheder og interesser⁽³⁷⁾. Ifølge fortolkningen i PPC's retningslinjer gælder disse undtagelser i meget specifikke situationer, f.eks. når oplysninger om anvendelsesformålet ville kunne risikere at underminere legitime foranstaltninger truffet af den erhvervsdrivende til beskyttelse af bestemte interesser (f.eks. bekæmpelse af svig, industrispionage, sabotage).

2.3.7. Særlige kategorier af oplysninger

- (65) Der bør være særlige garantier, når »særlige kategorier« af oplysninger behandles.
- (66) »Følsomme personlige oplysninger« defineres i artikel 2, stk. 3, i APPI. Denne bestemmelse henviser til »personlige oplysninger såsom den berørtes race, tro, sociale status, sygdomshistorie, straffeattest, hvorvidt pågældende har lidt skader i forbindelse med en forbrydelse eller andre beskrivelser mv., som i henhold til en kabinetsbekendtgørelse er de beskrivelser, som kræver særlig håndtering, således at de ikke forårsager uretfærdig forskelsbehandling, fordomme eller andre ulemper for den berørte.« Disse kategorier svarer langt hen ad vejen til listen over følsomme oplysninger i artikel 9 og 10 i forordning (EU) 2016/679. Navnlig »sygdomshistorie« svarer til sundhedsoplysninger, mens »straffeattest, og hvorvidt pågældende har lidt skader i forbindelse med en forbrydelse« materielt svarer til de i artikel 10 i forordning (EU) 2016/679 omhandlede kategorier. De i artikel 2, stk. 3, i APPI omhandlede kategorier er genstand for yderligere fortolkning i kabinetsbekendtgørelsen og i PPC's retningslinjer. I henhold til afsnit 2.3., punkt 8, i PPC's retningslinjer fortolkes underkategorierne af »sygdomshistorie«, som beskrives i artikel 2, nr. ii) og iii), i kabinetsbekendtgørelsen, således, at de også omfatter genetiske og biometriske data. Selv om listen ikke udtrykkeligt indeholder udtrykkene »etnisk oprindelse« eller »politisk overbevisning«, indeholder den imidlertid henvisninger til »race« og »tro«. Som forklaret i afsnit 2.3., punkt 1 og 2, i PPC's retningslinjer omfatter henvisningen til »race« »etniske forbindelser eller forbindelser til en bestemt del af verden«, mens »tro« forstås som både religiøse og politiske overbevisninger.
- (67) Som det fremgår af bestemmelsens ordlyd, er dette ikke en lukket liste, eftersom der kan tilføjes yderligere kategorier af oplysninger, såfremt deres behandling medfører en risiko for »uretfærdig forskelsbehandling, fordomme eller andre ulemper for den berørte«.
- (68) Mens begrebet »følsomme« oplysninger i sagens natur er en social konstruktion, der bygger på kulturelle og juridiske traditioner, moralske overvejelser, politiske valg osv. i et givent samfund, har Kommissionen i lyset af vigtigheden af at sikre tilstrækkelige garantier for følsomme oplysninger i forbindelse med overførsler til erhvervsdrivende i Japan tilsikret sig, at den særlige beskyttelse, som »følsomme personlige oplysninger« er underlagt i Japan, bliver udvidet til alle kategorier af »følsomme oplysninger« i forordning (EU) 2016/679. Med henblik herpå fastlægges det i supplerende regel nr. 1), at PIHBO'er skal behandle oplysninger overført fra Den Europæiske Union vedrørende en persons sexliv, seksuelle orientering eller fagforeningsmedlemskab »på samme måde som følsomme personlige oplysninger i den i artikel 2, stk. 3, [i APPI] anvendte betydning«.

⁽³⁷⁾ Der er tale om i) tilfælde, hvor underretningen af den registrerede om anvendelsesformålet eller offentliggørelsen deraf potentielt vil »være til skade for en berørt eller tredjemands liv, legeme eller formue« eller »PIHBO'ens [...] rettigheder eller legitime interesser«, ii) tilfælde, hvor »der er behov for at samarbejde i relation til et statsligt organ eller en lokalforvaltning« i forbindelse med udførelsen af deres lovbestemte opgaver, og hvor sådanne oplysninger vil kunne virke indgribende på disse »anliggender«, og iii) tilfælde, hvor anvendelsesformålet er klart i lyset af den situation, hvor oplysningerne er blevet indhentet.

- (69) Hvad angår yderligere materielle garantier for følsomme personlige oplysninger har PIHBO'er i henhold til artikel 17, stk. 2, i APPI ikke ret til at erhverve denne type oplysninger uden forudgående samtykke fra den berørte person, og hertil gælder kun få undtagelser ⁽³⁸⁾. Derudover er denne kategori af personlige oplysninger udelukket fra en eventuel videregivelse til tredjemand på grundlag af den i artikel 23, stk. 2, i APPI fastlagte procedure (tilladelse til overførsel af oplysninger til tredjemand uden den berørte persons forudgående samtykke).

2.3.8. Ansvarlighed

- (70) I henhold til princippet om ansvarlighed skal enheder, der behandler oplysninger, træffe passende organisatoriske foranstaltninger med henblik på effektiv overholdelse af deres databeskyttelsesforpligtelser, og de skal være i stand til at dokumentere denne overholdelse, navnlig over for den kompetente tilsynsmyndighed.
- (71) Som nævnt i fodnote 34 (betragtning 49) skal PIHBO'er i henhold til artikel 26, stk. 1, i APPI bekræfte identiteten på den tredjemand, som videregiver personoplysninger til dem, og de »omstændigheder«, hvorunder tredjemanden har erhvervet disse oplysninger (er der tale om personoplysninger omfattet af denne afgørelse, skal disse omstændigheder i henhold til APPI og supplerende regel nr. 3) omfatte, at oplysningerne stammer fra Den Europæiske Union, samt formålet med den oprindelige dataoverførsel). Denne foranstaltning har bl.a. til formål at sikre lovligheden af databehandlingen i hele kæden af PIHBO'er, der håndterer personoplysningerne. I henhold til artikel 26, stk. 3, i APPI skal PIHBO'er desuden registrere modtagelsesdatoen og de (obligatoriske) oplysninger, som den har modtaget fra tredjemanden, jf. stk. 1, samt navnet på den pågældende person (den registrerede), de behandlede oplysningskategorier og, i det omfang det er relevant, at den registrerede har givet sit samtykke til udveksling af sine personoplysninger. Som angivet i artikel 18 i PPC's regler skal disse fortegnelser opbevares i en periode på mindst et til tre år afhængigt af omstændighederne. I forbindelse med udførelsen af sine opgaver kan PPC kræve forelæggelse af sådanne fortegnelser ⁽³⁹⁾.
- (72) PIHBO'er skal hurtigt og på en passende måde håndtere klager fra berørte enkeltpersoner vedrørende behandlingen af deres personlige oplysninger. For at lette behandlingen af klager skal de oprette et system, som kan sikre opfyldelsen af dette formål, hvilket indebærer, at de skal indføre passende procedurer i deres organisation (f.eks. tildeling af ansvar eller oprettelse af et kontaktpunkt).
- (73) Endelig oprettes der med APPI en ramme for brancheorganisationernes deltagelse med henblik på at sikre et højt niveau af overholdelse af reglerne (jf. kapitel IV, afsnit 4). Sådanne organisationer, der er akkrediteret med hensyn til beskyttelse af personlige oplysninger ⁽⁴⁰⁾, har til opgave at fremme beskyttelsen af personlige oplysninger ved at støtte virksomheder via deres sagkundskab, men de bidrager også til gennemførelsen af garantier, navnlig ved at håndtere individuelle klager og hjælpe med at løse dermed forbundne konflikter. Med henblik herpå kan de anmode deltagende PIHBO'er om at træffe visse foranstaltninger, såfremt det er nødvendigt ⁽⁴¹⁾. Derudover skal PIHBO'er i tilfælde af brud på datasikkerheden i princippet underrette PPC og den registrerede (eller offentligheden) og iværksætte de nødvendige tiltag, herunder foranstaltninger til at minimere enhver skade og til at forebygge gentagelsen af lignende hændelser ⁽⁴²⁾. Selv om der er tale om frivillige ordninger, havde PPC den 10. august 2017 registreret 44 organisationer, hvoraf JIPDEC (Japan Information Processing and Development Center) som den

⁽³⁸⁾ Der er følgende undtagelser: i) »på grundlag af love og forskrifter«, ii) »tilfælde, hvor der er behov for at beskytte menneskers liv, legeme eller formue, og når det er vanskeligt at indhente en berørts samtykke«, iii) »tilfælde, hvor der er behov for at styrke den offentlige hygiejne eller fremme børns sundhed, og når det er vanskeligt at indhente en berørts samtykke«, og iv) tilfælde, »hvor der er behov for samarbejde med hensyn til et statsligt organ eller en lokalforvaltning, eller en af disse bemyndiget person, der varetager anliggender i henhold til love og forskrifter, og når indhentningen af den berørtes samtykke potentielt vil kunne virke indgribende på varetagelsen af disse anliggender«, og v) tilfælde, hvor de nævnte følsomme personlige oplysninger videregives til offentligheden af en registreret, et statsligt organ, en lokal myndighed, en person, der falder ind under en af kategorierne i artikel 76, stk. 1, eller andre personer, jf. PPC's regler. En yderligere kategori vedrører »andre tilfælde, som i henhold til en kabinetsbekendtgørelse svarer til de tilfælde, som er beskrevet i ovenstående numre«, hvilket i henhold til den nuværende kabinetsbekendtgørelse navnlig omfatter en persons iøjnefaldende træk (f.eks. en synlig lidelse eller sygdom), såfremt de følsomme oplysninger (uforvarende) er blevet erhvervet ved visuel observation eller ved at filme eller fotografere den registrerede, f.eks. via overvågningskameraer.

⁽³⁹⁾ I henhold til artikel 40, stk. 1, i APPI, kan PPC i det omfang, det er nødvendigt med henblik på at gennemføre de relevante bestemmelser i APPI, kræve, at en PIHBO forelægger de dertil fornødne oplysninger eller materialer vedrørende håndteringen af personlige oplysninger.

⁽⁴⁰⁾ APPI indeholder bl.a. bestemmelser om regler for akkreditering af disse organisationer; se artikel 47-50 i APPI.

⁽⁴¹⁾ Artikel 52 i APPI.

⁽⁴²⁾ PPC meddelelse nr. 1/2017 »Vedrørende de foranstaltninger, der skal træffes i de tilfælde, hvor brud på sikkerheden for personoplysninger eller en anden hændelse har fundet sted«.

største alene omfatter 15 436 deltagende erhvervsdrivende⁽⁴³⁾. De akkrediterede ordninger omfatter brancheorganisationer som f.eks. sammenslutningen af japanske børsrådgivere, den japanske sammenslutning for køreskolelærere og sammenslutningen af ægteskabsrådgivere⁽⁴⁴⁾.

- (74) Organisationer, som er akkrediteret med hensyn til beskyttelse af personlige oplysninger, skal forelægge årlige rapporter om deres aktiviteter. Ifølge oversigten over gennemførelsesstatus for APPI for regnskabsåret 2015, som PPC har offentliggjort, modtog de organisationer, der er akkrediteret med hensyn til beskyttelse af personlige oplysninger, i alt 442 klager, de krævede 123 redegørelser fra erhvervsdrivende inden for deres jurisdiktion, anmodede om dokumenter fra disse erhvervsdrivende i 41 tilfælde og gav 181 instruktioner og 2 anbefalinger⁽⁴⁵⁾.

2.3.9. Begrænsninger for videreoverførsel

- (75) Beskyttelsesniveauet for personoplysninger, der overføres fra Den Europæiske Union til erhvervsdrivende i Japan, må ikke kunne undermineres ved videreoverførsel af sådanne oplysninger til modtagere i tredjelande uden for Japan. Sådanne »videreoverførsler«, der set fra den japanske erhvervsdrivendes synspunkt udgør internationale overførsler fra Japan, bør kun tillades, såfremt den efterfølgende modtager uden for Japan selv er underlagt regler, der sikrer et beskyttelsesniveau svarende til det, der garanteres i den japanske retsorden.
- (76) Den første beskyttelse er fastlagt i artikel 24 i APPI, som generelt forbyder overførslen af personoplysninger til tredjemand uden for Japans område uden forudgående samtykke fra den berørte person. Supplerende regel nr. 4) sikrer, at et sådant samtykke ved dataoverførsler fra Den Europæiske Union skal være velinformeret, idet reglen kræver, at den berørte person skal have »oplysninger om omstændighederne i forbindelse med overførslen, således at det er muligt for denne at træffe sin samtykkebeslutning«. Den registrerede skal på dette grundlag oplyses om, at oplysningerne vil blive overført til udlandet (uden for anvendelsesområdet for APPI) og om det konkrete bestemmelsesland. Dette vil gøre det muligt for pågældende at vurdere risikoen for privatlivets fred i forbindelse med overførslen. Som det kan udledes af artikel 23 i APPI (jf. betragtning 47), skal de oplysninger, som meddeles den berørte, omfatte de obligatoriske elementer i henhold til dennes stk. 2, dvs. kategorierne af personoplysninger, som videregives til tredjemand, og videregivelsesmetoden.
- (77) I artikel 24 i APPI sammenholdt med artikel 11-2 i PPC's regler fastlægges en række undtagelser til denne samtykkebaserede regel. I henhold til artikel 24 finder de samme undtagelser, som i artikel 23, stk. 1, i APPI desuden også anvendelse på internationale dataoverførsler⁽⁴⁶⁾.
- (78) For at sikre kontinuitet i beskyttelsen af personoplysninger, der overføres fra EU til Japan i henhold til denne afgørelse, øges beskyttelsesniveauet for videreoverførsel af sådanne oplysninger fra en PIHBO til en modtager i et tredjeland ved supplerende regel nr. 4). Dette sker ved at begrænse og fastlægge det grundlag for internationale overførsler, der kan anvendes af PIHBO'en som et alternativ til samtykke. Mere specifikt, og uden at dette berører de undtagelser, der er fastlagt i artikel 23, stk. 1, i APPI, må personoplysninger overført i henhold til denne afgørelse kun (videre)overføres uden samtykke i to tilfælde: i) såfremt oplysningerne sendes til et tredjeland, som PPC i henhold til artikel 24 i APPI har anerkendt, har et beskyttelsesniveau svarende til det japanske⁽⁴⁷⁾, eller ii) såfremt PIHBO'en og den modtagende tredjemand sammen har gennemført foranstaltninger, der sikrer et beskyttelsesniveau svarende til APPI, sammenholdt med de supplerende regler, ved hjælp af en kontrakt, andre former for bindende aftaler eller bindende foranstaltninger inden for en koncern. Den anden kategori svarer til de instrumenter, som anvendes i henhold til forordning (EU) 2016/679 for at sikre tilstrækkelige garantier (navnlig kontraktbestemmelser og bindende virksomhedsregler). Som bekræftet af PPC er overdragelsen til tredjemand derudover selv i disse tilfælde fortsat underlagt de almindelige regler for enhver videregivelse af personoplysninger til tredjemand i henhold til APPI (dvs. kravet om at indhente samtykke i henhold til artikel 23, stk. 1, i APPI eller alternativt oplysningskravet med en mulighed for at trække sig i henhold til artikel 23, stk. 2, i APPI). Hvis den

⁽⁴³⁾ Ifølge tal offentliggjort på JIPDEC's PrivacyMark-websted, dateret den 2. oktober 2017.

⁽⁴⁴⁾ PPC's liste over organisationer, der er akkrediteret med hensyn til beskyttelse af personlige oplysninger, som findes på internettet under: <https://www.ppc.go.jp/personal/nintei/list/> eller https://www.ppc.go.jp/files/pdf/nintei_list.pdf

⁽⁴⁵⁾ PPC's oversigt over gennemførelsesstatus for APPI for regnskabsåret 2015 (oktober 2016) findes på webadressen (kun på japansk): https://www.ppc.go.jp/files/pdf/personal_sekougaigyuu_27ppc.pdf

⁽⁴⁶⁾ Se fodnote 32.

⁽⁴⁷⁾ I henhold til artikel 11 i PPC's regler kræver dette ikke blot materielle standarder svarende til APPI under en uafhængig håndhævelsesmyndigheds tilsyn, men også at gennemførelsen af de relevante regler sikres i tredjelandet.

registrerede ikke kan kontaktes med en anmodning om samtykke eller for at meddele de krævede forhåndsoplysninger i henhold til artikel 23, stk. 2, i APPI, må overførslen ikke finde sted.

- (79) Når der ses bort fra de tilfælde, hvor PPC har konkluderet, at det pågældende tredjeland sikrer et beskyttelsesniveau svarende til det, der garanteres af APPI⁽⁴⁸⁾, udelukker kravene i supplerende regel nr. 4) således anvendelsen af overførselsinstrumenter, når disse ikke opretter en bindende aftale mellem den japanske dataeksportør og dataimportøren i tredjelandet, og de ikke garanterer det krævede beskyttelsesniveau. Dette vil være tilfældet for f.eks. APEC Cross Border Privacy Rules (CBPR) System, som Japan deltager i⁽⁴⁹⁾, eftersom beskyttelsen i dette system ikke følger af en bindende aftale mellem eksportøren og importøren i forbindelse med deres bilaterale forhold og klart er på et lavere niveau end den beskyttelse, der garanteres ved en kombination af APPI og de supplerende regler⁽⁵⁰⁾.
- (80) Endelig følger en yderligere garanti i tilfælde af (videre)overførsel af artikel 20 og 22 i APPI. Når en operatør fra et tredjeland (en dataimportør) handler på vegne af PIHBO'en (dataeksportøren), som er en (under-)databehandler, har sidstnævnte i henhold til disse bestemmelser pligt til at sikre tilsynet med førstnævnte for så vidt angår sikkerheden i databehandlingen.

2.3.10. Individuelle rettigheder

- (81) Ligesom EU's databeskyttelseslovgivning tillægger APPI enkeltpersoner en række rettigheder, som kan håndhæves. Dette omfatter retten til indsigt (»at få oplyst«), berigtigelse og sletning samt retten til at gøre indsigelse (»indstilling af anvendelsen«).
- (82) For det første har en registreret i henhold til artikel 28, stk. 1 og 2, ret til at anmode en PIHBO om at »oplyse om opbevarede personoplysninger, som kan identificere pågældende«, og efter at have modtaget en sådan anmodning skal PIHBO'en »oplyse opbevarede personoplysninger« til den registrerede. Artikel 29 (ret til korrektion) og 30 (retten til indstilling af anvendelsen) har samme opbygning som artikel 28.
- (83) Ifølge kabinetsbekendtgørelsens artikel 9 skal meddelelser vedrørende personlige oplysninger som omhandlet i artikel 28, stk. 2, i APPI gives skriftligt, medmindre PIHBO'en og den registrerede har aftalt andet.
- (84) Disse rettigheder er underlagt tre typer restriktioner vedrørende den enkeltes egne eller tredjemands rettigheder og interesser⁽⁵¹⁾, alvorlige indgreb i PIHBO'ens forretningsaktiviteter⁽⁵²⁾ og sager, hvor indsigten ville være i strid med andre love og forskrifter⁽⁵³⁾. De situationer, hvori disse restriktioner vil kunne gælde, svarer til nogle af de undtagelser, der finder anvendelse i henhold til artikel 23, stk. 1, i forordning (EU) 2016/679, som tillader begrænsninger af den enkeltes rettigheder i forbindelse med »beskyttelse af den registrerede eller andres rettigheder

⁽⁴⁸⁾ Indtil nu har PPC endnu ikke vedtaget en afgørelse i henhold til artikel 24 i APPI om anerkendelse af, at et tredjeland har et beskyttelsesniveau svarende til det japanske. Den eneste afgørelse, som PPC på nuværende tidspunkt overvejer at vedtage, vedrører EØS. Med hensyn til eventuelle andre fremtidige afgørelser vil Kommissionen nøje overvåge situationen og om nødvendigt træffe de nødvendige foranstaltninger til at afhjælpe eventuelle negative virkninger for kontinuiteten i beskyttelsen (jf. betragtning 176, 177 og 184 og artikel 3, stk. 1).

⁽⁴⁹⁾ Dog er kun to japanske selskaber certificerede under APEC CBPR System (se https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Uden for Japan er de eneste andre erhvervsdrivende, der er certificeret efter dette system, et begrænset antal amerikanske virksomheder (23) (se <https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list>).

⁽⁵⁰⁾ For eksempel ingen definition af og specifikke bestemmelser for beskyttelse af følsomme oplysninger og ingen forpligtelse til begrænset opbevaring. Se også artikel 29-gruppens udtalelse 02/2014 om et referencedokument vedrørende krav til bindende virksomhedsregler fremsendt til de nationale databeskyttelsesmyndigheder i EU og grænseoverskridende regler for privatlivets fred fremsendt til APEC CBPR-ansvarlighedsbefuldmægtigede, 6. marts 2014.

⁽⁵¹⁾ Ifølge PPC vil kun sådanne interesser kunne begrunde en begrænsning, som »det lovgivningsmæssigt er værd at beskytte«. Denne vurdering skal foretages fra sag til sag »under hensyntagen til indgrebet i den grundlæggende ret til privatlivets fred, herunder databeskyttelse, i overensstemmelse med anerkendelsen deraf i forfatningen og retspraksis«. Beskyttede interesser kan f.eks. omfatte handels- eller forretningshemmeligheder.

⁽⁵²⁾ Konceptet at gribe alvorligt ind i den korrekte gennemførelse af den erhvervsdrivendes forretninger illustreres i PPC's retningslinjer gennem forskellige eksempler, f.eks. gentagne og identiske komplekse anmodninger fra den samme person, hvor disse anmodninger indebærer en betydelig byrde for en erhvervsdrivende, som vil kunne påvirke dennes evne til at besvare andre anmodninger negativt (PPC's retningslinjer (om generelle regler, s. 62)). PPC har mere overordnet bekræftet, at denne kategori er begrænset til undtagelses-tilfælde, der går ud over den blotte ulempe. En PIHBO kan navnlig ikke afslå at give indsigt, blot fordi der anmodes om en stor mængde oplysninger.

⁽⁵³⁾ PPC har bekræftet, at sådanne love skal respektere den forfatningssikrede ret til privatlivets fred og således »afspejle en nødvendig og rimelig begrænsning«.

og frihedsrettigheder» eller »andre vigtige målsætninger i forbindelse med beskyttelse af [...] generelle samfundsinteresser«. Selv om det må synes at være en bred kategori af tilfælde, hvor indsigt vil kunne være i strid med »andre love og forskrifter«, så skal love og forskrifter, hvori der fastlægges begrænsninger i denne henseende, respektere den forfatningssikrede ret til privatlivets fred, og de må kun pålægge begrænsninger, såfremt udøvelsen af denne rettighed ikke »griber ind i den offentlige velfærd«⁽⁵⁴⁾. Dette kræver en afvejning af de foreliggende interesser.

- (85) Hvis de ønskede oplysninger ikke findes, eller den berørte PIHBO beslutter ikke at give adgang til de opbevarede oplysninger, skal den straks underrette den pågældende, jf. artikel 28, stk. 3, i APPI.
- (86) For det andet har en registreret i henhold til artikel 29, stk. 1, i APPI ret til at anmode om berigtigelse af, tilføjelser til eller sletning af sine opbevarede personoplysninger, hvis oplysningerne ikke er korrekte. Ved modtagelsen af en sådan anmodning skal PIHBO'en »foretage de nødvendige undersøgelser« og på grundlag af resultaterne heraf »foretage en berigtigelse osv. af indholdet af de opbevarede oplysninger«.
- (87) For det tredje har en registreret i henhold til artikel 30, stk. 1 og 2, i APPI, ret til at anmode en PIHBO om at indstille anvendelsen af personlige oplysninger eller om at slette sådanne oplysninger, hvis de håndteres i strid med artikel 16 (vedrørende formålsbegrænsning) eller er erhvervet i strid med artikel 17 i APPI (vedrørende erhvervelse ved bedrag eller andre upassende metoder, eller hvor der ikke er givet samtykke i forbindelse med de følsomme oplysninger). I henhold til artikel 30, stk. 3 og 4, i APPI gælder ligeledes, at den enkelte har ret til at anmode PIHBO'en om at indstille videregivelsen af oplysningerne til tredjemand, såfremt dette vil være i strid med artikel 23, stk. 1, eller artikel 24 i APPI (vedrørende videregivelse til tredjemand, herunder internationale overførsler).
- (88) Såfremt der er grundlag for anmodningen, skal PIHBO'en uden tøven indstille anvendelsen af oplysningerne eller videregivelsen til tredjemand, i det omfang det er nødvendigt for at afhjælpe overtrædelsen, eller, hvis tilfældet er omfattet af en undtagelse (navnlig hvis indstillingen af anvendelsen vil medføre særlig høje omkostninger)⁽⁵⁵⁾, træffe de nødvendige alternative foranstaltninger til beskyttelse af den berørte persons rettigheder og interesser.
- (89) Til forskel fra EU-retten indeholder APPI og relevante regler under almindeligt lovniveau ikke bestemmelser, som specifikt vedrører muligheden for at modsætte sig behandling med henblik på direkte markedsføring. En sådan behandling vil dog i henhold til denne afgørelse finde sted i forbindelse med overførsel af personoplysninger, der tidligere er blevet indsamlet i Den Europæiske Union. I medfør af artikel 21, stk. 2, i forordning (EU) 2016/679 skal den registrerede altid have muligheden for at gøre indsigelse mod en overførsel af data til behandling med henblik på direkte markedsføring. Som forklaret i betragtning 43 er en PIHBO i øvrigt i henhold til supplerende regel nr. 3) forpligtet til at behandle de oplysninger, der modtages i henhold til afgørelsen, til det samme formål, hvortil oplysningerne er blevet overført fra Den Europæiske Union, medmindre den registrerede giver sit samtykke til en ændring af anvendelsen. Hvis overførslen således er foretaget til et andet formål end direkte markedsføring, vil en PIHBO i Japan være afskåret fra at behandle oplysningerne med henblik på direkte markedsføring uden samtykke fra den registrerede i EU.
- (90) I alle de i artikel 28 og 29 i APPI omhandlede tilfælde skal PIHBO'en straks meddele den enkelte resultatet af pågældendes anmodning og desuden begrunde ethvert (delvist) afslag på grundlag af de lovmæssige undtagelser, som er fastlagt i artikel 27-30 (artikel 31 i APPI).

⁽⁵⁴⁾ Forfatningens artikel 13 er af højesteret blevet fortolket som en fastlæggelse af retten til privatlivets fred (se ovenfor i betragtning 7 og 8). Selv om denne rettighed kan være begrænset i tilfælde, hvor den »griber ind i den offentlige velfærd«, har højesteret i sin dom af 6. marts 2008 (jf. betragtning 8) præciseret, at enhver begrænsning (der i dette tilfælde tillod en offentlig myndigheds indsamling og behandling af personoplysninger) skal afvejes i forhold til retten til privatlivets fred, under hensyntagen til faktorer såsom de pågældende oplysningers art, de med behandlingen af disse oplysninger forbundne risici for enkeltpersoner, de gældende garantier og de fordele, som opnås i offentlighedens interesse som følge af behandlingen. Dette er meget lig den afvejning, der i EU-retten kræves på grundlag af principperne om nødvendighed og proportionalitet for at give tilladelse til begrænsning af databeskyttelsesrettigheder og garantier.

⁽⁵⁵⁾ For yderligere redegørelser for disse undtagelser, se Professor Katsuya Ugas bemærkninger til artiklerne i den reviderede lov om beskyttelse af personlige oplysninger (Article by Article Commentary of the revised Act on the Protection of Personal Information, 2015, s. 217). F.eks. er et eksempel på en anmodning, der forårsager »meget store omkostninger« et tilfælde, hvor kun nogle navne på en lang liste (f.eks. i et telefonbog) behandles i strid med princippet om formålsbegrænsning, og registret allerede er til salg, således at en tilbagekaldelse af disse eksemplarer og deres erstatning med nye vil være meget bekostelig. I det samme eksempel vil det, såfremt der allerede er blevet solgt eksemplarer til mange mennesker, og det er umuligt at indsamle dem alle, også være »vanskeligt at gennemføre en indstilling af anvendelsen«. I disse scenarier bør de »nødvendige alternative foranstaltninger« f.eks. omfatte offentliggørelse eller distribution af en ændringsmeddelelse. En sådan foranstaltning udelukker ikke andre (retlige) prøvelsesforanstaltninger, uanset om det vedrører krænkelse af privatlivets fred, skade på omdømme (ærekrænkelse) som følge af offentliggørelsen eller krænkelse af andre interesser.

- (91) Hvad angår betingelserne for at fremsætte en anmodning, så kan PIHBO'en i henhold til artikel 32 i APPI (sammenholdt med kabinetsbekendtgørelsen) fastsætte rimelige procedurer herfor, herunder angående de oplysninger, som er nødvendige for at identificere de opbevarede personoplysninger. I henhold til stk. 4 i denne artikel, må PIHBO'er imidlertid ikke pålægge »den berørte uforholdsmæssige byrder«. I visse tilfælde kan PIHBO'er også opkræve gebyrer, såfremt beløbet forbliver »inden for rammerne af, hvad der er rimeligt i betragtning af de faktiske omkostninger« (artikel 33 i APPI).
- (92) Endelig kan den enkelte gøre indsigelse mod videregivelsen sine personlige oplysninger til tredjemand, jf. artikel 23, stk. 2, i APPI, eller afvise at give sit samtykke, jf. artikel 23, stk. 1 (og derved forhindre videregivelse, hvis dette ikke kan ske på et andet retsgrundlag). Tilsvarende kan den enkelte standse behandlingen af oplysninger til et andet formål ved at afvise at give samtykke i henhold til artikel 16, stk. 1, i APPI.
- (93) Til forskel fra EU-retten indeholder APPI og relevante regler under almindeligt lovniveau ikke generelle bestemmelser, som vedrører beslutninger, der påvirker den registrerede, og som udelukkende bygger på automatisk behandling af personoplysninger. Spørgsmålet er imidlertid behandlet i visse sektorspecifikke regler, der finder anvendelse i Japan, og som er særligt relevante for denne form for behandling. Dette omfatter sektorer, hvor virksomhederne med overvejende sandsynlighed vil benytte sig af automatisk behandling af personoplysninger til at træffe beslutninger, der påvirker enkeltpersoner (f.eks. i den finansielle sektor). F.eks. indeholder de samlede retningslinjer for tilsynet med store banker, som blev revideret i juni 2017, krav om, at den berørte person får en specifik begrundelse for afvisningen af en anmodning om at indgå en låneaftale. Disse regler giver således beskyttelse i de formodentlig meget få tilfælde, hvor de automatiske beslutninger træffes af den »importerende« japanske erhvervsdrivende selv (i stedet for af den »eksporterende« dataansvarlige fra EU).
- (94) I forbindelse med personoplysninger, der er blevet indsamlet i Den Europæiske Union, vil enhver beslutning baseret på automatisk behandling under alle omstændigheder typisk blive taget af den dataansvarlige i Unionen (som har en direkte relation til den berørte registrerede), og den vil således være omfattet af forordning (EU) 2016/679 ⁽⁵⁶⁾. Dette omfatter overførselsscenarier, hvor behandlingen foretages af en udenlandsk (f.eks. japansk) erhvervsdrivende, der handler som mandatar (databehandler) på vegne af den dataansvarlige fra EU (eller som en underdatabehandler, der handler på vegne af en databehandler fra EU, som har modtaget oplysningerne fra den indsamlede dataansvarlige fra EU), og som på dette grundlag således træffer beslutningen. Fraværet af specifikke regler om automatiske beslutninger i APPI vil derfor sandsynligvis ikke have indvirkning på beskyttelsesniveauet for personoplysninger overført i henhold til denne afgørelse.

2.4. Tilsyn og håndhævelse

2.4.1. Uafhængigt tilsyn

- (95) For at sikre, at et tilstrækkeligt databeskyttelsesniveau også garanteres i praksis, bør der være oprettet en uafhængig tilsynsmyndighed med beføjelser til at overvåge og sikre, at databeskyttelsesreglerne overholdes. Denne myndighed bør være fuldstændig uafhængig og upartisk i udførelsen af sine opgaver og udøvelsen af sine beføjelser.
- (96) PPC er den japanske myndighed med ansvaret for tilsyn med og håndhævelse af APPI. Myndigheden består af en formand og otte kommissærer, der udnævnes af premierministeren med samtykke fra begge kamre i parlamentet. Embedsperioden for formanden og de enkelte kommissærer er fem år med mulighed for genudnævnelse (artikel 64 i APPI). Kommissærerne kan kun afskediges med gyldig grund i et begrænset antal særlige tilfælde ⁽⁵⁷⁾ og må ikke være aktivt engagerede i politiske aktiviteter. I henhold til APPI skal fuldtidskommissærer desuden afholde sig fra enhver anden lønnet beskæftigelse eller erhvervsvirksomhed. Alle kommissærer er også omfattet af interne regler, som forhindrer dem i at deltage i forhandlinger i tilfælde af en mulig interessekonflikt. PPC bistås af et sekretariat under en generalsekretærs ledelse, og dette sekretariat er blevet oprettet med henblik på at udføre de opgaver, som PPC er blevet tillagt (artikel 70 i APPI). Både kommissæren og alle ansatte i sekretariatet er underlagt strenge regler om tavshedspligt (artikel 72 og 82 i APPI).

⁽⁵⁶⁾ I de ekstraordinære tilfælde, hvor den japanske erhvervsdrivende har en direkte relation til den registrerede i EU, vil det omvendt typisk være en konsekvens af, at den erhvervsdrivende har rettet sin indsats mod den pågældende person i Den Europæiske Union ved at tilbyde denne varer eller tjenesteydelser eller ved at overvåge dennes adfærd. I dette scenarie vil den japanske erhvervsdrivende selv være omfattet af reglerne i forordning (EU) 2016/679 (artikel 3, stk. 2) og således skulle overholde EU's databeskyttelseslovgivning.

⁽⁵⁷⁾ Ifølge artikel 65 i APPI er afskedigelse af en kommissær mod dennes vilje kun mulig af en af følgende grunde: i) indledning af konkursbehandling, ii) dom for overtrædelse af APPI eller loven om anvendelse af numre, iii) en fængselsdom uden arbejde eller en endnu hårdere dom eller iv) manglende evne til at udføre opgaver på grund af fysisk eller psykisk sygdom eller embedsmisbrug.

- (97) PPC's beføjelser, som udøves i fuld uafhængighed⁽⁵⁸⁾, er hovedsagelig fastlagt i artikel 40, 41 og 42 i APPI. I henhold til artikel 40 kan PPC anmode PIHBO'er om at rapportere eller fremsende dokumenter om behandlingsaktiviteter, og PPC kan ligeledes foretage inspektioner, både på stedet og af fortegnelser eller andre dokumenter. I det omfang det er nødvendigt for at håndhæve APPI, kan PPC også sørge for vejledning og rådgivning til PIHBO'er vedrørende håndteringen af personlige oplysninger. PPC har allerede gjort brug af denne beføjelse i henhold til artikel 41 i APPI i form af vejledning til Facebook efter afsløringerne vedrørende Facebook og Cambridge Analytica.
- (98) Det væsentligste er, at PPC har beføjelser til – på foranledning af en klage eller på eget initiativ – at fremsætte henstillinger eller udstede påbud med henblik på at håndhæve APPI og andre bindende regler (herunder de supplerende regler) i individuelle sager. Disse beføjelser er fastlagt i artikel 42 i APPI. Mens bestemmelsens stk. 1 og 2 foreskriver en todelt procedure, hvor PPC (kun) kan udstede et påbud efter en forudgående henstilling, giver stk. 3 mulighed for direkte udstedelse af et påbud i hastende tilfælde.
- (99) Der henvises ikke til alle bestemmelser i kapitel IV, afsnit 1, i APPI i artikel 42, stk. 1 – hvorved anvendelsesområdet for artikel 42, stk. 2, også fastlægges – men dette skyldes, at visse af disse bestemmelser ikke vedrører PIHBO'ens forpligtelser⁽⁵⁹⁾, og at alle væsentlige former for beskyttelse allerede ydes via andre bestemmelser, som indgår i listen. Men selv om artikel 15 (hvori det kræves, at PIHBO'en fastlægger anvendelsesformålet og udelukkende behandler de relevante personlige oplysninger inden for disse rammer) f.eks. ikke er nævnt, kan manglende overholdelse af dette krav give anledning til en henstilling som følge af overtrædelse af artikel 16, stk. 1 (forbuddet mod, at PIHBO'en behandler personlige oplysninger ud over, hvad der er nødvendigt for at opnå anvendelsesformålet, medmindre der indhentes samtykke hos den registrerede)⁽⁶⁰⁾. En anden bestemmelse, der ikke er anført i artikel 42, stk. 1, er artikel 19 i APPI om oplysningers korrekthed og opbevaring. Manglende overholdelse af denne bestemmelse kan håndhæves enten som en overtrædelse af artikel 16, stk. 1, eller baseres på en overtrædelse af artikel 29, stk. 2, hvis den pågældende person anmoder om rettelse eller sletning af ukorrekte eller unødvendige oplysninger, og PIHBO'en nægter at efterkomme anmodningen. For så vidt angår den registreredes rettigheder i henhold til artikel 28, stk. 1, artikel 29, stk. 1, og artikel 30, stk. 1, sikres PPC's tilsyn ved at give det håndhævelsesbeføjelser med hensyn til PIHBO'ens dertil svarende forpligtelser, der er fastsat i de nævnte artikler.
- (100) I henhold til artikel 42, stk. 1, i APPI kan PPC, hvis det anerkender, at der et »behov for beskyttelse af en persons rettigheder og interesser i tilfælde, hvor en [PIHBO] har overtrådt« specifikke bestemmelser i APPI, fremsætte en henstilling om at »standse overtrædelsen eller træffe andre fornødne foranstaltninger med henblik på at afhjælpe overtrædelsen«. En sådan henstilling er ikke bindende, men baner vejen for et bindende pålæg i henhold til artikel 42, stk. 2, i APPI. Hvis henstillingen ikke bliver fulgt, og det sker »uden legitime grunde«, og PPC »indser, at der er overhængende fare for en alvorlig overtrædelse af en persons rettigheder og interesser«, kan PPC pålægge PIHBO'en at træffe foranstaltninger i overensstemmelse med henstillingen.
- (101) Med de supplerende regler præciseres og styrkes PPC's håndhævelsesbeføjelser yderligere. Såfremt der er tale om af oplysninger importeret fra Den Europæiske Union, vil PPC således altid betragte en PIHBO's undladelse af at handle i overensstemmelse med en henstilling, der er fremsat i henhold til artikel 42, stk. 1, i APPI, hvor dette sker uden dette sker uden legitime grunde, som en alvorlig overtrædelse, der indebærer en overhængende fare for den enkeltes rettigheder og interesser, jf. artikel 42, stk. 2, og derfor også betragte det som en overtrædelse, der kræver, at der udstedes et bindende pålæg. Som »legitime grunde« til ikke at efterkomme en henstilling vil PPC desuden kun acceptere en »begivenhed af ekstraordinær karakter [der forhindrer efterkommelsen] uden for [PIHBO'ens] kontrol, som ikke med rimelighed har kunnet forudses (f.eks. naturkatastrofer)«, eller tilfælde, hvor behovet for at træffe foranstaltninger med hensyn til en henstilling »ikke længere er til stede, fordi [PIHBO'en] har truffet alternative foranstaltninger, der fuldt ud afhjælper overtrædelsen«.

⁽⁵⁸⁾ Jf. artikel 62 i APPI.

⁽⁵⁹⁾ F.eks. vedrører visse bestemmelser PIHBO-aktiviteter, som er valgfrie (artikel 32 og 33 i APPI) eller indsatsforpligtelser, som i sagens natur ikke kan håndhæves (artikel 31 og 35, artikel 36, stk. 6, og artikel 39, i APPI). Visse bestemmelser er ikke rettet til PIHBO'er, men til andre aktører. Dette er f.eks. tilfældet med hensyn til artikel 23, stk. 4, artikel 26, stk. 2, og artikel 34 i APPI (håndhævelsen af artikel 26, stk. 2, i APPI sikres imidlertid gennem muligheden for strafferetlige sanktioner i henhold til artikel 88, nr. i), i APPI.

⁽⁶⁰⁾ Som forklaret ovenfor i betragtning 48 vil »anvendelsesformålet« i en overførselskontekst blive angivet af EU-dataeksportøren, som i denne forbindelse er bundet af den i artikel 5, stk. 1, litra b), i forordning (EU) 2016/679 fastlagte forpligtelse. Denne forpligtelse håndhæves af den kompetente databeskyttelsesmyndighed i Den Europæiske Union.

- (102) Manglende overholdelse af et pålæg fra PPC betragtes som en strafbar handling i henhold til artikel 84 i APPI, og findes PIHBO'en skyldig, kan denne idømmes fængsel med arbejde i op til seks måneder eller en bøde på op til 300 000 yen. I henhold til artikel 85, nr. i), i APPI er manglende samarbejde med PPC eller obstruktion af dets undersøgelser desuden strafbart med en bøde på op til 300 000 yen. Disse strafferetlige sanktioner finder anvendelse i tillæg til dem, der kan pålægges for væsentlige overtrædelser af APPI (se betragtning 108).

2.4.2. Prøvelse

- (103) Med henblik på at sikre tilstrækkelig beskyttelse og navnlig håndhævelse af individuelle rettigheder bør den registrerede have effektive muligheder for administrativ og retslig prøvelse, herunder skadeserstatning.
- (104) Før eller i stedet for indgivelsen klage til en myndighed eller anlæggelsen af en sag ved domstolene kan en person vælge at klage over behandlingen af vedkommendes personoplysninger til den dataansvarlige selv. I henhold til artikel 35 i APPI skal PIHBO'er bestræbe sig på at behandle sådanne klager »hensigtsmæssigt og hurtigt« og indføre et internt klagebehandlingssystem med henblik på at nå dette mål. I henhold til artikel 61, nr. ii), i APPI har PPC til opgave at sørge for »den nødvendige mægling med hensyn til en indgivet klage og tilbud om samarbejde til en erhvervsdrivende, som håndterer klagen«, hvilket i begge tilfælde omfatter klager indgivet af udlændinge. Den japanske lovgiver har i den forbindelse overladt det til de statslige myndigheder at træffe de »nødvendige foranstaltninger« til at muliggøre og lette PIHBO'ers løsning af klagesager (artikel 9), mens lokalforvaltningerne skal bestræbe sig på at sikre mægling i sådanne sager (artikel 13). I den forbindelse kan enkeltpersoner indgive klage hos et af mere end 1 700 forbrugercentre, som er oprettet af lokalforvaltningerne på grundlag af forbrugersikkerhedsloven ⁽⁶¹⁾, og de har desuden mulighed for at indgive en klage til det nationale center for forbrugerforhold i Japan. Sådanne klager kan også indgives med hensyn til en overtrædelse af APPI. I henhold til artikel 19 i den almindelige lov om forbrugerbeskyttelse ⁽⁶²⁾ skal lokale myndigheder bestræbe sig på at mægle med hensyn til klager og give parterne adgang til den nødvendige sagkundskab. Disse tvistbilæggelsesordninger synes at være ret effektive med en løsningsprocent på 91,2 % i mere end 75 000 klagesager i 2015.
- (105) Overtrædelser af bestemmelserne i APPI for en PIHBO kan give anledning til civile søgsmål og straffesager og strafferetlige sanktioner. Dette kan for det første være, hvis en person anser sine rettigheder for overtrådt i henhold til artikel 28, 29 og 30 i APPI, idet denne person kan bede retten om at meddele et påbud, hvorved PIHBO'en pålægges at efterkomme pågældendes anmodning i henhold til disse bestemmelser, dvs. at oplyse om opbevarede personoplysninger (artikel 28), berigtige opbevarede personoplysninger, der ikke er korrekte (artikel 29), eller indstille ulovlig behandling eller videregivelse til tredjemand (artikel 30). Et sådant søgsmål kan anlægges uafhængigt af artikel 709 i den borgerlige lovbog ⁽⁶³⁾ eller anden erstatningsretlig hjemmel ⁽⁶⁴⁾. Det betyder navnlig, at den enkelte ikke behøver at føre bevis for nogen skade.
- (106) Der kan for det andet være tilfælde, hvor en påstået overtrædelse ikke vedrører individuelle rettigheder i medfør af artikel 28, 29 og 30, men derimod generelle databeskyttelsesprincipper eller PIHBO'ens generelle forpligtelser, idet den berørte person kan anlægge et civil søgsmål mod den erhvervsdrivende på grundlag af bestemmelserne om erstatning i Japans borgerlige lovbog, navnlig dennes artikel 709. Mens et sagsanlæg i henhold til artikel 709 ud over skyld (forsæt eller uagtsomhed) kræver påvisning af skade, kan en sådan skade ifølge artikel 710 i den borgerlige lovbog både være af materiel og immateriel karakter. Der er ikke fastlagt nogen begrænsning med hensyn til erstatningens størrelse.
- (107) Hvad angår de til rådighed stående retsmidler omhandler artikel 709 i den borgerlige lovbog økonomisk erstatning. I japansk retspraksis er denne bestemmelse imidlertid også blevet fortolket således, at den giver mulighed for et påbud ⁽⁶⁵⁾. Hvis en registreret således anlægges en sag i henhold til artikel 709 i den borgerlige lovbog med påstand om, at den tiltalte har skadet pågældendes rettigheder eller interesser ved en overtrædelse af en bestemmelse i APPI, kan dette søgsmål ud over et krav om erstatning også omfatte en anmodning om nedlæggelse af forbud, navnlig med det formål at standse den ulovlige behandling.

⁽⁶¹⁾ Lov nr. 50 af 5. juni 2009.

⁽⁶²⁾ Lov nr. 60 af 22. august 2012.

⁽⁶³⁾ Artikel 709 i den borgerlige lovbog udgør hovedgrundlaget for civile erstatningssager. Bestemmelsen lyder: »en person, som forsætligt eller ved uagtsomhed har krænket andres rettigheder eller retligt beskyttede interesser, har pligt til at godtgøre enhver deraf følgende skade«.

⁽⁶⁴⁾ Dom fra landsretten i Tokyo af 20. maj 2015 (ikke offentliggjort); Byretten i Tokyo, dom af 8. september 2014, Westlaw Japan 2014WLJPCA09088002. Se også artikel 34, stk. 1 og 3, i APPI.

⁽⁶⁵⁾ Jf. højesterets dom af 24. september 2002 (*Hanrei Times* bind 1106, s. 72).

- (108) For det tredje har en registreret ud over civilretlige (dvs. erstatningsretlige) retsmidler mulighed for at indgive en anmeldelse hos anklagemyndigheden eller politiet vedrørende overtrædelser af APPI, som vil kunne føre til strafferetlige sanktioner. Kapitel VII i APPI indeholder en række strafferetlige bestemmelser. Den vigtigste (artikel 84) vedrører en PIHBO's manglende overholdelse af påbud fra PPC, jf. artikel 42, stk. 2 og 3. Hvis en erhvervsdrivende undlader at efterkomme et påbud meddelt af PPC, vil formanden for PPC (og enhver anden embedsmand) ⁽⁶⁶⁾ kunne videregive sagen til anklagemyndigheden eller politiet og på den måde bevirke, at der indledes en straffesag. Straffen for ikke at overholde et påbud fra PPC er fængsel med arbejde i op til seks måneder eller en bøde på op til 300 000 yen. Blandt de øvrige bestemmelser i APPI om sanktioner i tilfælde af overtrædelser til skade for registreredes rettigheder og interesser kan nævnes artikel 83 (om »hemmelig videregivelse eller anvendelse« af en database over personlige oplysninger »med det formål at opnå [...] ulovlige fortjenester«) og artikel 88, nr. i) (vedrørende tredjemands undladelse af at underrette en PIHBO korrekt, når sidstnævnte modtager personoplysninger i overensstemmelse med artikel 26, stk. 1, i APPI, navnlig vedrørende oplysningerne om tredjemandens egen forudgående erhvervelse af sådanne oplysninger). De strafferetlige sanktioner for denne type overtrædelser af APPI er henholdsvis fængsel med arbejde i op til et år eller en bøde på op til 500 000 yen (artikel 83) og en administrativ bøde på op til 100 000 yen (artikel 88, nr. i)). Truslen om strafferetlige sanktioner vil sandsynligvis allerede have en betydelig afskrækkende virkning på den virksomhedsledelse, der står for styringen af PIHBO's behandlingsaktiviteter, og på de personer, der håndterer oplysningerne, men artikel 87 præciserer derudover, at når en repræsentant, en ansat eller en anden type medarbejder i en virksomhed har begået en overtrædelse i henhold til artikel 83-85 i APPI, da »straffes aktøren, og den pågældende virksomhed pålægges den i de respektive artikler fastsatte bøde«. I dette tilfælde er det både den ansatte og virksomheden, som kan pålægges sanktioner op til det fulde maksimumsbeløb.
- (109) Endelig kan enkeltpersoner få prøvet sager vedrørende PPC's handlinger eller undladelser. Japansk lovgivning giver i den forbindelse adskillige muligheder for administrative klager og domstolsprøvelse.
- (110) Hvis en person ikke er tilfreds med en handling foretaget af PPC, kan pågældende indgive en administrativ klage i henhold til loven om administrativ rekurs ⁽⁶⁷⁾. I tilfælde hvor en person mener, at PPC burde have handlet, men undlod dette, kan pågældende omvendt i henhold til nævnte lovs artikel 36-3 anmode PPC om at træffe en disposition eller yde administrativ vejledning, hvis pågældende mener, at »en disposition eller administrativ vejledning, som er nødvendig for at afhjælpe overtrædelser, ikke er blevet truffet eller givet«.
- (111) For så vidt angår retslig prøvelse kan en person, der ikke er tilfreds med en administrativ disposition truffet af PPC, i henhold til loven om forvaltningsretssager anlægge en påbudssag (mandamus) ⁽⁶⁸⁾, hvori retten anmodes om at pålægge PPC at træffe yderligere foranstaltninger ⁽⁶⁹⁾. I visse tilfælde kan retten også meddele et foreløbigt påbud for at forhindre uoprettelig skade ⁽⁷⁰⁾. Endvidere kan den enkelte i henhold til samme lov anmode om tilbagekaldelse af en PPC-afgørelse ⁽⁷¹⁾.
- (112) Endelig kan en person også anlægge en sag om erstatning fra staten mod PPC i henhold til artikel 1, stk. 1, i lov om statsligt erstatningsansvar, dersom pågældende har lidt skade som følge af, at et påbud udstedt af PPC til en erhvervsdrivende var ulovligt, eller at PPC ikke har udøvet sine beføjelser.

3. JAPANSKE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG BRUG AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION

- (113) Kommissionen har også vurderet begrænsningerne og garantierne, herunder tilsynet og de enkelte prøvelsesmekanismer i japansk ret, når japanske myndigheder i offentlighedens interesse indsamler og efterfølgende anvender personoplysninger, der er blevet overført til erhvervsdrivende i Japan, navnlig med henblik på retshåndhævelse på det strafferetlige område og national sikkerhed (»myndighedsadgang«). I den forbindelse har Kommissionen modtaget officielle redegørelser, forsikringer og tilsagn fra Japan undertegnet på højeste ministerielle og forvaltningsmæssige niveau, og disse findes i bilag II til denne afgørelse.

⁽⁶⁶⁾ Artikel 239, stk. 2, i straffelovbogen.

⁽⁶⁷⁾ Lov nr. 160 af 2014.

⁽⁶⁸⁾ Artikel 37-2 i loven om forvaltningsretssager.

⁽⁶⁹⁾ Ifølge artikel 3, stk. 6, i loven om forvaltningsretssager er mandamus-søgsmål sager anlagt med henblik på at opnå et retsligt påbud til et forvaltningsorgan om at træffe en oprindeligt undladt administrativ disposition, som den burde have truffet.

⁽⁷⁰⁾ Artikel 37-5 i loven om forvaltningsretssager.

⁽⁷¹⁾ Kapitel II, afsnit 1, i loven om forvaltningsretssager.

3.1. Den overordnede retlige ramme

- (114) Som en udøvelse af offentlig myndighed skal myndighedsadgang i Japan finde sted i fuld overensstemmelse med loven (legalitetsprincippet). Den japanske forfatning indeholder i den forbindelse bestemmelser, der begrænser og sætter rammer for offentlige myndigheders indsamling af oplysninger. Som allerede nævnt i forbindelse med erhvervsdrivendes behandling af oplysninger har den japanske højesteret på grundlag af forfatningens artikel 13, som bl.a. beskytter retten til frihed, anerkendt retten til privatliv og databeskyttelse⁽⁷²⁾. Et vigtigt aspekt af denne ret er friheden til ikke at få sine personlige oplysninger videregivet til tredjemand uden tilladelse⁽⁷³⁾. Dette indebærer retten til effektiv beskyttelse af personoplysninger mod misbrug og (især) ulovlig adgang. Forfatningens artikel 35 sikrer yderligere beskyttelse for alle med hensyn til boligens, dokumenters og genstandes ukrænkelighed, således at de offentlige myndigheder skal indhente en retskendelse afsagt på et »tilstrækkeligt grundlag«⁽⁷⁴⁾ i alle tilfælde af »ransagninger og beslaglæggelser«. Højesteret præciserede i sin dom af 15. marts 2017 (i GPS-sagen), at dette krav om en retskendelse finder anvendelse, hver gang myndighederne forstyrrer (»trænger ind i«) privatsfæren på en måde, der går imod den pågældende persons vilje, således at der er tale om en efterforskning, som indebærer »tvangsindgreb«. Retten kan kun afsige en sådan kendelse på grundlag af konkret mistanke om en forbrydelse, dvs. når der forelægges konkrete beviser, på hvis grundlag den af person, der er genstand for efterforskningen, kan anses for at have begået en strafbar handling⁽⁷⁵⁾. Følgelig har de japanske myndigheder ikke hjemmel til at indsamle personoplysninger ved tvangsindgreb i situationer, hvor ingen overtrædelse af loven endnu har fundet sted⁽⁷⁶⁾, f.eks. for at forhindre en forbrydelse eller en sikkerhedstrussel (som det er tilfældet ved undersøgelser begrundet af nationale sikkerhedshensyn).
- (115) I henhold til legalitetsprincippet skal enhver indsamling af oplysninger, som udgør et tvangsindgreb i forbindelse med en efterforskning, have særlig lovhjemmel (hvilket f.eks. afspejles i artikel 197, stk. 1, i strafferetsplejelovbogen, som vedrører tvangsindgreb i forbindelse med indsamling af oplysninger i forbindelse med strafferetlig efterforskning). Dette krav gælder også for adgangen til elektroniske oplysninger.
- (116) Artikel 21, stk. 2, i forfatningen garanterer meddelelseshemmeligheden for alle kommunikationsmidler, og begrænsninger heraf tillades kun i offentlighedens interesse. Med Artikel 4 i loven om telekommunikation, hvorefter krænkelse af meddelelseshemmeligheden i forbindelse med teleselskabers forvaltning af meddelelser er forbudt, gennemføres dette krav om fortrolighed i den almindelige lovgivning. Dette er blevet fortolket som et forbud mod videregivelsen af meddelelsesoplysninger, undtagen når der foreligger brugersamtykke eller hjemmel dertil i en af de udtrykkelige undtagelser for strafferetligt ansvar i henhold til straffelovbogen⁽⁷⁷⁾.
- (117) Forfatningen garanterer også retten til domstolsprøvelse (artikel 32) og retten til at sagsøge staten med henblik på erstatning i tilfælde, hvor en person har lidt skade på grund af en ulovlig handling foretaget af en embedsmand (artikel 17).
- (118) Med hensyn til retten til databeskyttelse fastlægges der i kapitel III, afsnit 1, 2 og 3, i APPI generelle principper, som omfatter alle sektorer, herunder den offentlige sektor. Det bestemmes således ved artikel 3 i APPI, at alle personlige oplysninger skal håndteres i overensstemmelse med princippet om respekt for den enkeltes personlighed. Når personlige oplysninger er blevet indsamlet (»indhentet«) af offentlige myndigheder⁽⁷⁸⁾, herunder som en del af elektroniske fortegnelser, er deres behandling underlagt loven om beskyttelse af personlige oplysninger i

⁽⁷²⁾ Se f.eks. Højesterets dom af 12. september 2003, sag nr. 1656 (2002 (Ju)). Retten fastslog navnlig, at »alle enkeltpersoner har friheden til at beskytte deres personlige oplysninger mod videregivelse til tredjemand eller offentliggørelse uden gyldig grund«.

⁽⁷³⁾ Højesterets dom af 6. marts 2008 (Juki-net).

⁽⁷⁴⁾ Der er kun tale om et »tilstrækkeligt grundlag«, når den pågældende person (mistænkte, anklagede) anses for at have begået en strafbar handling, og ransagning og beslaglæggelse er nødvendig med henblik på den strafferetlige efterforskning. Se Højesterets dom af 18. marts 1969, sag nr. 100 (1968 (Ju)).

⁽⁷⁵⁾ Jf. artikel 156, stk. 1, i strafferetsplejereglerne.

⁽⁷⁶⁾ Det bør dog bemærkes, at med loven om straf for organiseret kriminalitet og forvaltning af udbytte fra strafbare handlinger af 15. juni 2017 er forberedelsen af terrorhandling og visse andre former for organiseret kriminalitet blevet strafbare. Efterforskningen må kun indledes i tilfælde af en konkret, bevisbaseret mistanke om, at alle tre nødvendige betingelser for at kunne fastslå denne strafbare handling er til stede (en organiseret kriminel gruppes indblanding, »planlægningshandlingen« og »forberedelseshandlingen til gennemførelse« af forbrydelsen). Se også artikel 38-40 i lov om forebyggelse af undergravende virksomhed (lov nr. 240 af 21. juli 1952).

⁽⁷⁷⁾ Jf. artikel 15, stk. 8, i retningslinjerne om beskyttelse af personlige oplysninger i telekommunikationssektoren.

⁽⁷⁸⁾ Administrative organer som defineret i artikel 2, stk. 1, i APPIHAO. Ifølge de oplysninger, der er modtaget fra den japanske regering, er alle offentlige myndigheder, undtagen præfekturpolitiet, omfattet af definitionen »administrative organer«. Samtidig arbejder præfekturpolitiet inden for de retlige rammer, der er fastlagt i præfekturernes bekendtgørelser om beskyttelse af personlige oplysninger (se artikel 11 i APPI og den grundlæggende politik), hvori der er fastlagt bestemmelser om beskyttelse af personlige oplysninger svarende til dem APPIHAO. Jf. bilag II, afsnit I.B. PPC har oplyst, at disse bekendtgørelser i henhold til den »grundlæggende politik« skal gennemføres på grundlag af APPIHAO, og ministeriet for interne anliggender og kommunikation udarbejder cirkulærer for at give de lokale myndigheder de nødvendige retningslinjer i denne henseende. PPC understreger, at »[i]nden for disse grænser fastlægges bekendtgørelserne om beskyttelse af personlige oplysninger i hvert præfektur [...] på grundlag af den grundlæggende politik og indholdet af cirkulærerne«.

administrative organer »APPIHAO«⁽⁷⁹⁾. Dette omfatter i princippet⁽⁸⁰⁾ også behandlingen af personoplysninger med henblik på retshåndhævelse på det strafferetlige område eller af hensyn til den nationale sikkerhed. I APPIHAO fastlægges det bl.a., at offentlige myndigheder: i) kun må opbevare personlige oplysninger i det omfang, det er nødvendigt for at udføre deres opgaver, ii) ikke må anvende sådanne oplysninger til et »urimeligt« formål eller videregive dem til tredjemand uden begrundelse, iii) skal angive formålet og ikke må ændre dette formål ud over, hvad der med rimelighed kan betragtes som relevant i forhold til det oprindelige formål (formålsbegrænsning), iv) i princippet ikke må anvende de opbevarede personlige oplysninger eller videregive dem til tredjemand med henblik på andre formål og, hvis de finder det nødvendigt, skal pålægge tredjemand restriktioner vedrørende anvendelsesformål eller -metode, v) skal bestræbe sig på at sikre oplysningernes rigtighed (datakvalitet), vi) skal træffe de nødvendige foranstaltninger med henblik på korrekt forvaltning af oplysningerne og for at forebygge lækage, tab eller skade (datasikkerhed) og vii) skal bestræbe sig på en reel og hurtig behandling af eventuelle klager over behandlingen af oplysningerne⁽⁸¹⁾.

3.2. De japanske myndigheders adgang til og brug af personoplysninger med henblik på retshåndhævelse på det strafferetlige område

- (119) Japansk ret indeholder en række klare begrænsninger for adgangen til og brugen af personoplysninger med henblik på retshåndhævelse på det strafferetlige område samt tilsyns- og prøvelsesmekanismer, der giver tilstrækkelige garantier for, at disse oplysninger beskyttes effektivt mod risikoen for ulovlig adgang og risikoen for misbrug.

3.2.1. Retsgrundlag og gældende begrænsninger/garantier

- (120) Inden for de i Japan gældende retlige rammer er indsamlingen af elektroniske oplysninger med henblik på retshåndhævelse på det strafferetlige område tilladt på grundlag af en retskendelse (indsamling ved tvangsindgreb) eller en anmodning om frivillig udlevering.

3.2.1.1. Efterforskning ved tvangsindgreb på grundlag af en retskendelse

- (121) Som anført i betragtning 115 skal enhver indsamling af oplysninger, som udgør et tvangsindgreb i forbindelse med en efterforskning, have særlig lovhjemmel, og den må kun foretages på grundlag af en retskendelse »afsagt på et tilstrækkeligt grundlag« (forfatningens artikel 35). For så vidt angår efterforskning af strafbare handlinger afspejles dette krav i bestemmelserne i strafferetsplejelovbogen. I henhold til strafferetsplejelovbogens artikel 197, stk. 1, må tvangsindgreb »ikke anvendes, medmindre særlige bestemmelser herom er fastsat i denne lovbog«. For så vidt angår indsamlingen af elektronisk information er det eneste relevante⁽⁸²⁾ retsgrundlag i denne henseende strafferetsplejelovbogens artikel 218 (ransagning og beslaglæggelse) og strafferetsplejelovbogens artikel 222-2, hvorefter tvangsindgreb med henblik på at opfange elektronisk kommunikation uden samtykke fra nogen af parterne skal gennemføres på grundlag af anden lovgivning, dvs. loven om aflytning i forbindelse med strafferetlig efterforskning (»aflytningsloven«). I begge tilfælde kræves en retskendelse.
- (122) Nærmere bestemt kan anklagemyndigheden eller politiet, hvis det er nødvendigt for efterforskningen af et strafbart forhold, i henhold til strafferetsplejelovbogens artikel 218, stk. 1, foretage ransagning eller beslaglæggelse (herunder pålægge udlevering af fortegnelser) på grundlag af en forud herfor afsagt retskendelse⁽⁸³⁾. En sådan kendelse skal bl.a. indeholde en angivelse af navnet på den mistænkte eller sigtede, den mistanke om et strafbart forhold, der ligger til grund⁽⁸⁴⁾, de elektromagnetiske fortegnelser, som skal beslaglægges, og »stedet og genstandene«, som skal undersøges (strafferetsplejelovbogens artikel 219, stk. 1).

⁽⁷⁹⁾ Personlige oplysninger, der indhentes af embedsmænd i et administrativt organ i forbindelse med udøvelsen af deres hverv, og som opbevares af det nævnte administrative organ til organisatorisk brug, er omfattet af definitionen »opbevarede personlige oplysninger« i den i artikel 2, stk. 3, i APPIHAO anvendte betydning, så længe de »registreres i administrative dokumenter«. Dette omfatter elektroniske oplysninger, der indsamles og derefter viderebehandles af sådanne organer, eftersom definitionen af »administrative dokumenter« i artikel 2, stk. 2, i lov om adgang til oplysninger i administrative organer (lov nr. 42 af 1999) omfatter elektromagnetiske fortegnelser.

⁽⁸⁰⁾ I henhold til artikel 53-2 i strafferetsplejelovbogen finder kapitel IV i APPIHAO ikke anvendelse på »dokumenter vedrørende retssager«, som ifølge de modtagne oplysninger omfatter elektroniske oplysninger indhentet på grundlag af en retskendelse eller anmodning om frivilligt samarbejde som led i en strafferetlig efterforskning. Det samme gælder med hensyn til oplysninger indsamlet på området national sikkerhed, hvor enkeltpersoner ikke vil kunne påberåbe sig deres rettigheder i henhold til APPIHAO, hvis chefen for den offentlige myndighed har »rimelig grund« til at antage, at denne indsigt »sandsynligvis vil være til skade for den nationale sikkerhed« (jf. artikel 14, nr. iv)). De offentlige myndigheder har imidlertid pligt til at give mindst delvis indsigt i oplysningerne, når dette er muligt (artikel 15).

⁽⁸¹⁾ Se de specifikke henvisninger til APPIHAO i bilag II, II.A. punkt 1), litra b), nr. 2).

⁽⁸²⁾ Selv om strafferetsplejelovbogens artikel 220 giver mulighed for ransagning og beslaglæggelse »på stedet« uden en retskendelse, i tilfælde hvor anklagemyndigheden eller politiet anholder en mistænkt/en åbenlys lovovertræder, er dette ikke relevant i en overførselskontekst og dermed heller ikke i forhold til denne afgørelse.

⁽⁸³⁾ I henhold til strafferetsplejelovbogens artikel 222, stk. 1, sammenholdt med artikel 110, skal retskendelser om ransagning/beslaglæggelse af fortegnelser forelægges den person, som berøres af foranstaltningen.

⁽⁸⁴⁾ Se også strafferetsplejelovbogens artikel 189, stk. 2, ifølge hvilken politiembedsmænd skal foretage efterforskning for så vidt angår lovovertræderen, »når pågældende finder, at der har fundet en lovovertrædelse sted«. På samme måde opstiller artikel 155, stk. 1, i strafferetsplejereglerne krav om, at en skriftlig anmodning om en kendelse bl.a. skal indeholde en angivelse af »mistanken om et strafbart forhold« og et »resumé af forbrydelsens faktiske omstændigheder«.

- (123) Hvad angår indgreb i meddelelseshemmeligheden i form af aflytning og lignende, tillader aflytningslovens artikel 3 kun foranstaltninger under meget strenge betingelser. De offentlige myndigheder skal på forhånd indhente en retskendelse, som kun må afsiges med henblik på efterforskning af alvorlige forbrydelser (anført i lovens bilag) ⁽⁸⁵⁾, og når det er »ekstremt vanskeligt at identificere forbryderen eller få skabt klarhed med hensyn til forbrydelsens situationer/detaljer på anden måde« ⁽⁸⁶⁾. I henhold til aflytningslovens artikel 5 afsiges kendelsen for en begrænset periode og dommeren kan pålægge yderligere betingelser. Aflytningsloven indeholder desuden yderligere garantier, f.eks. kravet om tilstedeværelse af vidner (artikel 12 og 20), forbuddet mod at aflytte visse privilegerede gruppers kommunikation (f.eks. læger og advokater) (artikel 15), forpligtelsen til at indstille aflytningen, hvis der ikke længere er grundlag for den, også inden for kendelsens gyldighedsperiode (artikel 18), eller det generelle krav om, at den berørte person skal underrettes og have adgang til fortegnelserne inden for tredive dage efter at aflytningen er blevet indstillet (artikel 23 og 24).
- (124) For alle tvangsindgreb på grundlag af en retskendelse må der kun foretages en undersøgelse »for så vidt som det er nødvendigt for at opnå dennes formål« – dvs. at målene med efterforskningen ikke kan nås på anden måde – jf. strafferetsplejelovbogens artikel 197, stk. 1. Selv om kriterierne for at afgøre, hvorvidt dette er nødvendigt, ikke er præciseret yderligere i den almindelige lovgivning, har den japanske højesteret ved dom fastslået, at den ret, som afsiger en kendelse, skal foretage en overordnet vurdering under hensyntagen til navnlig i) alvoren af lovovertrædelsen, og hvordan den blev begået, ii) værdien og betydningen af de materialer, som skal beslaglægges som bevismateriale, iii) sandsynligheden (risikoen) for, at dokumentationen kan blive skjult eller ødelagt, og iv) i hvilket omfang beslaglæggelse kan skade den pågældende person ⁽⁸⁷⁾.

3.2.1.2. Anmodning om frivillig udlevering på grundlag af et »undersøgelsesskema«

- (125) Inden for rammerne af deres beføjelser kan de offentlige myndigheder også indsamle elektroniske oplysninger baseret på anmodninger om frivillig udlevering. Dette vedrører en ikke-lovpligtig form for samarbejde, hvor efterkommelse af anmodningen ikke kan håndhæves ⁽⁸⁸⁾, hvilket betyder, at de offentlige myndigheder ikke skal indhente en retskendelse i den forbindelse.
- (126) I det omfang en sådan anmodning er rettet til en erhvervsdrivende og vedrører personlige oplysninger, skal den erhvervsdrivende overholde kravene i APPI. I henhold til artikel 23, stk. 1, i APPI må erhvervsdrivende kun i visse tilfælde videregive personlige oplysninger til tredjemand uden den berørte persons samtykke, herunder når videregivelsen er foretaget »på grundlag af love og forskrifter« ⁽⁸⁹⁾. For så vidt angår retshåndhævelsen på det strafferetlige område er retsgrundlaget for en sådan forespørgsel strafferetsplejelovbogens artikel 197, stk. 2, hvorefter »private organisationer kan anmodes om at rapportere om omstændigheder, hvis oplysning er nødvendig i forbindelse med efterforskningen«. Eftersom et sådant »undersøgelsesskema« kun må anvendes i forbindelse med en strafferetlig efterforskning, forudsætter det en konkret mistanke om en allerede begået forbrydelse ⁽⁹⁰⁾. Da en sådan efterforskning desuden normalt foretages af præfekturpolitiet, finder de i politilovens artikel 2, stk. 2 ⁽⁹¹⁾, fastlagte begrænsninger anvendelse. Ifølge denne bestemmelse er politiets aktiviteter »udelukkende begrænset« til at udføre dets opgaver og pligter (dvs. forebyggelse, forhindring og efterforskning af forbrydelser). I udførelsen af sine opgaver skal politiet desuden handle på en upartisk, fordomsfri og retfærdig måde, og det må aldrig misbruge sine beføjelser »på en sådan måde, at det griber ind i en persons forfatningssikrede rettigheder og friheder« (der som anført omfatter retten til privatlivets fred og databeskyttelse) ⁽⁹²⁾.
- (127) Særligt med hensyn til strafferetsplejelovbogens artikel 197, stk. 2, har det nationale politiagentur – der er den føderale myndighed med ansvar for bl.a. alle spørgsmål vedrørende kriminalpolitiet – udstedt instrukser til

⁽⁸⁵⁾ Bilaget omfatter 9 typer af forbrydelser, f.eks. forbrydelser med tilknytning til narkotika og våben, menneskehandel og organiseret drab. Det skal bemærkes, at den nyligt indførte strafbarhed for »forberedelsen af terrorhandling og anden organiseret kriminalitet« (se fodnote 76) ikke indgår i denne restriktive liste.

⁽⁸⁶⁾ I henhold til aflytningslovens artikel 23 skal den person, hvis meddelelser er blevet opfanget (og derfor er blevet registreret i fortegnelserne over denne aflytning), af efterforskningsmyndigheden have skriftlig meddelelse herom.

⁽⁸⁷⁾ Jf. bilag II, afsnit II.A, punkt 1), litra b), nr. 1).

⁽⁸⁸⁾ Ifølge de modtagne oplysninger er der ingen lovbestemte negative konsekvenser (herunder sanktioner) for de erhvervsdrivende, som ikke samarbejder. Jf. bilag II, afsnit II.A, punkt 2), litra a).

⁽⁸⁹⁾ Ifølge PPC's retningslinjer (om generelle regler) danner artikel 23, stk. 1, nr. i), grundlag for videregivelsen af personlige oplysninger i medfør af en retskendelse (strafferetsplejelovbogens artikel 218) og et »undersøgelsesskema« (strafferetsplejelovbogens artikel 197, stk. 2).

⁽⁹⁰⁾ Det betyder, at »undersøgelsesskemaet« kun må bruges til at indsamle oplysninger i individuelle sager og ikke til omfattende indsamling af personoplysninger. Jf. bilag II, afsnit II.A, punkt 2), litra b), nr. 1).

⁽⁹¹⁾ Samt forskrifter fra præfekturkommissionen for den offentlige sikkerhed, jf. strafferetsplejelovbogens artikel 189, stk. 1.

⁽⁹²⁾ Jf. også politilovens artikel 3, hvoraf det fremgår, at det i det embedsløfte, som alle politibetjente skal aflægge, hedder, at de »skal være tro mod forpligtelsen til at forsvare og håndhæve Japans forfatning og love og udføre deres pligter på en upartisk, rimelig, retfærdig og fordomsfri måde«.

præfekturpolitiet⁽⁹³⁾ om den »korrekte anvendelse af skriftlige undersøgelser i efterforskningsøjemed«. Ifølge denne meddelelse skal anmodninger foretages ved hjælp af en på forhånd fastlagt formular (»formular nr. 49«, eller det såkaldte »undersøgelsesskema«)⁽⁹⁴⁾ og omhandle fortegnelser »vedrørende en specifik efterforskning«, og de oplysninger, som efterspørges, skal være »nødvendige for [den] efterforskning«. I hver enkelt tilfælde skal chefen for efterforskningen »fuldt ud undersøge nødvendigheden, indholdet osv. af enkeltundersøgelse(n)« og indhente en intern godkendelse fra en højtstående embedsmand.

- (128) Den japanske højesteret har desuden i to domme fra 1969 og 2008⁽⁹⁵⁾ fastlagt begrænsninger i forbindelse med foranstaltninger, som ikke er tvangsindgreb, men som griber ind i retten til privatlivets fred⁽⁹⁶⁾. Højesteret fandt navnlig, at sådanne foranstaltninger skal være »rimelige« og holde sig inden for »generelt tilladelige grænser«, dvs. at de skal være nødvendige med henblik på efterforskningen af en mistænkt (tilvejebringelse af bevismateriale) og udføres ved hjælp af »passende metoder med henblik på at nå efterforskningens mål«⁽⁹⁷⁾. Dommene viser, at dette omfatter en proportionalitetstest, hvor der tages hensyn til alle sagens omstændigheder (f.eks. omfanget af indgrebet i retten til privatlivets fred, herunder forventningen om privatlivsbeskyttelse, forbrydelsens grovhed, sandsynligheden for at kunne fremskaffe relevant bevismateriale, mulige alternative efterforskningsmidler osv.)⁽⁹⁸⁾.
- (129) Ud over disse begrænsninger for udøvelsen af offentlig myndighed forventes det også af de erhvervsdrivende, at de kontrollerer (»bekræfter«) nødvendigheden af og »rationaliteten« i videregivelsen til en tredjemand⁽⁹⁹⁾. Dette omfatter spørgsmålet om, hvorvidt de i henhold til lov er forhindret i at samarbejde. Sådanne modstridende retlige forpligtelser kan især være en følge af fortrolighedsforpligtelser som i f.eks. straffelovbogens artikel 134 (vedrørende forholdet mellem en læge, advokat, præst osv. og dennes klient). Derudover gælder, at »enhver person, der er aktiv inden for telekommunikation, så længe denne bestrider et sådant hverv, skal bevare andres hemmeligheder, hvortil der er opnået kendskab gennem teleselskabets håndtering af meddelelser« (teleselskabslovens artikel 4, stk. 2). Denne forpligtelse understøttes af den sanktion, der følger af teleselskabslovens artikel 179, hvorefter enhver person, der har overtrådt meddelelshemmeligheden for meddelelser, der håndteres af et teleselskab, har begået en strafbar handling, som straffes med fængsel med arbejde i op til to år eller en bøde på op til 1 mio. yen⁽¹⁰⁰⁾. Selv om dette krav ikke er absolut og navnlig giver mulighed for krænkelse af meddelelshemmeligheden, hvis der er tale om »berettigede handlinger«, jf. straffelovbogens artikel 35, finder sådanne undtagelser ikke anvendelse for svar på uforpligtende anmodninger fra offentlige myndigheder om videregivelse af elektroniske oplysninger, jf. strafferetsplejelovbogens artikel 197, stk. 2⁽¹⁰¹⁾.

3.2.1.3. Yderligere anvendelse af de indsamlede oplysninger

- (130) Når personlige oplysninger er blevet indsamlet af japanske myndigheder, vil de være omfattet af APPIHAO. Denne lov regulerer håndteringen (behandlingen) af »opbevarede personlige oplysninger«, og fastlægger således en række

⁽⁹³⁾ I henhold til politilovens artikel 30, stk. 1, og artikel 31, stk. 2, skal generaldirektøren for det regionale politikontor (lokalafdelinger af det nationale politiagentur) »give anvisninger til og føre tilsyn med« præfekturpolitiet.

⁽⁹⁴⁾ I undersøgelsesskemaet skal der også angives kontaktoplysninger for den »håndteringsansvarlige« (»navnet på sektionen [stilling], den håndteringsansvarliges navn, telefonnummer på kontoret, lokalnummer osv.«).

⁽⁹⁵⁾ Højesterets dom af 24. december 1969 (1965(A) 1187); dom af 15. april 2008 (2007(A) 839).

⁽⁹⁶⁾ Selv om disse domme ikke vedrørte indsamling af elektroniske oplysninger, har den japanske regering præciseret, at anvendelsen af de kriterier, som er opstillet af højesteret, gælder enhver indgriben fra de offentlige myndigheds side i retten til privatlivets fred, herunder alle »frivillige undersøgelser«, og dermed er bindende for de japanske myndigheder i forbindelse med anmodninger om frivillig udlevering af oplysninger. Jf. bilag II, afsnit II.A, punkt 2), litra b), nr. 1).

⁽⁹⁷⁾ Ifølge de modtagne oplysninger skal disse faktorer betragtes som »rimelige i forhold til socialt accepterede konventioner«. Jf. bilag II, afsnit II.A, punkt 2), litra b), nr. 1).

⁽⁹⁸⁾ For lignende overvejelser i forbindelse med efterforskning ved tvangsindgreb (aflytning), se også højesterets dom af 16. december 1999, 1997 (A) 636.

⁽⁹⁹⁾ De japanske myndigheder har i den forbindelse henvist til PPC's retningslinjer (om generelle regler) og punkt 5/14 i den »spørgsmål og svar«, der er udarbejdet af PPC med henblik på anvendelsen af APPI. De japanske myndigheder har således påpeget, at »på baggrund af den voksende bevidsthed om den enkeltes rettigheder med hensyn til privatliv og den arbejdsbyrde, som sådanne anmodninger indebærer, er mange erhvervsdrivende mere og mere forsigtige med at imødekomme sådanne anmodninger«. Se bilag II, afsnit II.A, punkt 2), også med henvisning til det nationale politiagents meddelelse fra 1999. Ifølge de modtagne oplysninger har der faktisk været tilfælde, hvor erhvervsdrivende har nægtet at samarbejde. I 2017 udtalte LINE (den mest populære beskedapplikation i Japan) således følgende i sin rapport om gennemsigtighed: »Når vi modtager anmodninger fra efterforskningsmyndigheder mv., foretager vi [...] en vurdering heraf med hensyn til lovlighed, brugerbeskyttelse osv. I denne vurdering vil vi afvise anmodningen på det givne tidspunkt, hvis der er retlige mangler. Hvis omfanget er for bredt i forhold til efterforskningens formål, beder vi myndigheden om en begrundelse. Hvis begrundelsen ikke er tilstrækkelig, efterkommer vi ikke anmodningen«. Findes på internetadressen: <https://linecorp.com/en/security/transparency/top>

⁽¹⁰⁰⁾ Sanktionerne er 3 års fængsel med arbejde eller en bøde på højst 2 mio. yen for enhver person, der »er aktiv i telekommunikationssektoren«.

⁽¹⁰¹⁾ »Berettigede handlinger« i henhold til straffelovbogen er navnlig de handlinger, som et teleselskab foretager for at efterleve retskraftige statslige foranstaltninger (tvangsindgreb), f.eks. når efterforskningsmyndigheder træffer foranstaltninger på grundlag af en retskendelse. Se bilag II, afsnit II.A, punkt 2), litra b) nr. 2), med henvisning til retningslinjerne om beskyttelse af personlige oplysninger i telesektoren.

begrænsninger og garantier (jf. betragtning 118) ⁽¹⁰²⁾. Det forhold, at et administrativt organ kun må opbevare personlige oplysninger, »når opbevaringen er nødvendig for at varetage de opgaver, som hører under dets kompetence i henhold til love og forskrifter« (artikel 3, stk. 1, i APPIHAO), medfører desuden begrænsninger – i hvert fald indirekte – for den første indsamling.

3.2.2. Uafhængigt tilsyn

- (131) I Japan hører indsamlingen af elektroniske oplysninger på det strafferetlige område først og fremmest ⁽¹⁰³⁾ under præfekturpolitiets ansvarsområde ⁽¹⁰⁴⁾, og det er i den forbindelse underlagt forskellige former for tilsyn.
- (132) Politiet skal for det første altid indhente en forudgående retskendelse (jf. betragtning 121), når elektronisk kommunikation indsamles ved tvangsindgreb (ransagning og beslaglæggelse). Derfor vil indsamlingen i sådanne tilfælde blive genstand for en forudgående retslig kontrol på grundlag af streng betingelse om et »tilstrækkeligt grundlag«.
- (133) Selv om der ikke foretages nogen forudgående retslig kontrol i tilfælde af anmodninger om frivillig udlevering, kan erhvervsdrivende, der modtager sådanne anmodninger, undlade at imødekomme dem uden risiko for negative konsekvenser (og de vil skulle tage hensyn til enhver udleverings konsekvenser for privatlivets fred). I henhold til strafferetsplejelovbogens artikel 192, stk. 1, skal politiet altid samarbejde og koordinere dets aktiviteter med anklagemyndigheden (og præfekturkommissionen for den offentlige sikkerhed) ⁽¹⁰⁵⁾. Anklagemyndigheden kan således give de nødvendige generelle instrukser med fastlæggelse af standarder for en fair efterforskning og/eller give specifikke anvisninger i en konkret efterforskning (strafferetsplejelovbogens artikel 193). Hvis de pågældende instrukser og/eller anvisninger ikke følges, kan anklagemyndigheden anlægge en disciplinærsag (strafferetsplejelovbogens artikel 194). Præfekturpolitiet arbejder således under anklagemyndighedens tilsyn.
- (134) For det andet kan hvert af det japanske parlaments kamre i henhold til forfatningens artikel 62 foretage undersøgelser i relation til myndighederne, hvilket omfatter lovligheden af politiets indsamling af oplysninger. Med henblik herpå kan de forlange indkaldelse og afhøring af vidner og/eller fremlæggelse af fortegnelser. Disse undersøgelsesbeføjelser beskrives nærmere i parlamentsloven, særlig kapitel XII. Navnlig fastlægges det i parlamentslovens artikel 104, at kabinettet, offentlige myndigheder og den øvrige forvaltning »skal imødekomme anmodninger fremsat af et af kamrene eller dets udvalg med hensyn til fremlæggelse af de rapporter og fortegnelser, som er nødvendige i undersøgelsesøjemed«. Afslag på en sådan anmodning tillades kun, hvis disse myndigheder angiver en gyldig grund, som parlamentet finder acceptabel, eller ved udstedelse af en formel erklæring om, at fremlæggelse af rapporterne eller fortegnelserne vil være »til alvorlig skade for nationale interesser« ⁽¹⁰⁶⁾. Derudover kan parlamentsmedlemmer stille skriftlige spørgsmål til kabinettet (parlamentslovens artikel 74 og 75), og der har tidligere været eksempler på, at sådanne »skriftlige forespørgsler« også har omhandlet administrationens håndtering af personlige oplysninger ⁽¹⁰⁷⁾. Parlamentets rolle i tilsynet med den udøvende magt understøttes af rapporteringsforpligtelser, f.eks. i henhold til aflytningslovens artikel 29.
- (135) For så vidt angår den udøvende magt er der for det tredje også et uafhængigt tilsyn med præfekturpolitiet. Dette omfatter navnlig præfekturkommissionerne for den offentlige sikkerhed, der er oprettet på præfekturniveau for at sikre politiets demokratiske forvaltning og politiske neutralitet ⁽¹⁰⁸⁾. Disse kommissioner sammensættes af medlemmer udpeget af præfekturguvenøren med præfekturforsamlingens samtykke (forsamlingen vælges blandt borgere, som ikke har været embedsmænd i politiet de fem foregående år) og har en sikker mandatperiode (navnlig skal afskedigelse være velbegrundet) ⁽¹⁰⁹⁾. Ifølge de oplysninger, der er modtaget, er de ikke underlagt instrukser og kan dermed anses for at være fuldstændig uafhængige ⁽¹¹⁰⁾. For så vidt angår præfekturkommissionerne for den

⁽¹⁰²⁾ Se afsnit 3.1. for så vidt angår de berørte personers rettigheder.

⁽¹⁰³⁾ I princippet kan anklagemyndigheden, hvis denne skønner det nødvendigt, foretage efterforskning af en lovovertrædelse (strafferetsplejelovbogens artikel 191, stk. 1).

⁽¹⁰⁴⁾ Ifølge de modtagne oplysninger foretager det nationale politiagentur ikke individuelle strafferetlige efterforskninger. Jf. bilag II, afsnit II.A, punkt 1), litra a).

⁽¹⁰⁵⁾ Jf. også strafferetsplejelovbogens artikel 246, hvorefter politiet er forpligtet til at sende sagsakterne til anklagemyndigheden, når der er foretaget en efterforskning af en lovovertrædelse (»princippet om fremsendelse af alle sager«).

⁽¹⁰⁶⁾ Alternativt kan parlamentet anmode om, at nævnet for tilsyn med og vurdering af særligt udpegede hemmeligheder foretager en undersøgelse af dette afslag på at svare. Se parlamentslovens artikel 104-II.

⁽¹⁰⁷⁾ Jf. bilag II, afsnit II.B, punkt 4).

⁽¹⁰⁸⁾ Derudover har lokalforsamlingen ifølge bestemmelserne i artikel 100 i loven om lokalt selvstyre beføjelse til at undersøge aktiviteter udført af retshåndhavende myndigheder på præfekturniveau, herunder præfekturpolitiet.

⁽¹⁰⁹⁾ Jf. politilovens artikel 39-41. Jf. ligeledes politilovens artikel 42 vedrørende politisk neutralitet.

⁽¹¹⁰⁾ Jf. bilag II, afsnit II.B, punkt 3) (»uafhængigt rådssystem«).

offentlige sikkerheds opgaver og beføjelser har de i henhold til politilovens artikel 38, stk. 3, sammenholdt med dennes artikel 2 og artikel 36, stk. 2, ansvaret for at sørge for »beskyttelsen af den enkeltes rettigheder og frihed«. De har derfor beføjelse til at »føre tilsyn med«⁽¹¹¹⁾ alle præfekturpolitiets efterforskningsmæssige aktiviteter, herunder indsamlingen af personoplysninger. Kommissionerne kan navnlig »give instrukser til præfekturpolitiet i detaljeret form eller i en konkret sag om undersøgelse af politimedarbejders tjenestelige forseelser, såfremt det er nødvendigt«⁽¹¹²⁾. Når chefen for præfekturpolitiet⁽¹¹³⁾ modtager en sådan instruks, eller selv bliver opmærksom på et muligt tilfælde af ureglementeret adfærd (herunder lovovertrædelser eller andre forsømmelser af pligter) fra personalets side, skal pågældende straks undersøge sagen og sende resultaterne af undersøgelserne til præfekturkommissionen for den offentlige sikkerhed (politilovens artikel 56, stk. 3). Hvis præfekturkommissionen finder det nødvendigt, kan den også udpege et af sine medlemmer til at vurdere status med hensyn til gennemførelsen. Processen fortsætter, indtil præfekturkommissionen for den offentlige sikkerhed anser hændelsen for at være håndteret tilfredsstillende.

- (136) Med hensyn til den korrekte anvendelse af APPIHAO har den kompetente minister eller myndighedschef (f.eks. generalkommissæren for det nationale politiagentur) desuden håndhævelsesbeføjelser, dog under tilsyn af ministeriet for interne anliggender og kommunikation. Ifølge til artikel 49 i APPIHAO kan ministeriet »indsamle rapporter om status for håndhævelsen af denne lov« fra lederne af forvaltningsmæssige organer (ministre). Ministeriets 51 informationscentre (der er et i hvert præfektur i hele Japan) bidrager med input til denne tilsynsfunktion; centrene behandler hvert år tusindvis af forespørgsler fra enkeltpersoner⁽¹¹⁴⁾ (der potentielt vil kunne føre til afdækning af lovovertrædelser). Såfremt ministeriet finder det nødvendigt for at sikre overholdelse af loven, kan det anmode om redegørelser og materialer og afgive udtalelser vedrørende det berørte administrative organs håndtering af personlige oplysninger (artikel 50 og 51 i APPIHAO).

3.2.3. Individuel klage- eller prøvelsesadgang

- (137) Foruden det tilsyn, der foretages ex officio, har enkeltpersoner også flere individuelle klage- eller prøvelsesmuligheder, både over for uafhængige myndigheder (såsom præfekturkommissionen for den offentlige sikkerhed eller PPC) og ved de japanske domstole.
- (138) For så vidt angår personlige oplysninger indsamlet af administrative organer gælder for det første, at disse organer er forpligtede til at »bestræbe sig på hurtigt at behandle alle klager« vedrørende deres efterfølgende behandling af oplysningerne (artikel 48 i APPIHAO). Kapitel IV i APPIHAO om individuelle rettigheder finder ikke anvendelse for så vidt angår personlige oplysninger registreret i »dokumenter vedrørende retssager og beslaglagte genstande« (strafferetsplejelovbogens artikel 53-2, stk. 2) – hvilket omfatter personlige oplysninger indsamlet som en del af strafferetlige efterforskninger – men enkeltpersoner kan påberåbe sig generelle databeskyttelsesprincipper som f.eks. forpligtelsen til kun at opbevare personlige oplysninger, »når opbevaringen er nødvendig for at varetage [retshåndhævelsesfunktioner]« (artikel 3, stk. 1, APPIHAO).
- (139) Politilovens artikel 79 garanterer desuden enkeltpersoner, som er utilfredse med politipersonales »varetagelse af pligter«, retten til at indgive en klage hos den (kompetente) uafhængige præfekturkommission for den offentlige sikkerhed. Kommissionen behandler »loyalt« sådanne klager i overensstemmelse med lovgivningen og lokale anordninger, og den skal skriftligt meddele klageren resultatet. Kommissionen kan på grundlag af sin beføjelse til at føre tilsyn og give »instrukser« med hensyn til »tjenestelige forseelser« (politilovens artikel 38, stk. 3, og artikel 43-2, stk. 1) anmode præfekturpolitiet om at foretage en undersøgelse, træffe passende foranstaltninger på grundlag af resultaterne af denne undersøgelse og give meddelelse om resultaterne. Hvis kommissionen mener, at politiets undersøgelse har været utilstrækkelig, kan den også give instrukser om håndteringen af klagen.
- (140) Med henblik på at lette klagebehandlingen har det nationale politiagentur udstedt et cirkulære til politiet og præfekturkommissionerne for den offentlige sikkerhed om korrekt håndtering af klager vedrørende politiembedsmænds varetagelse af deres pligter. I dette dokument fastlægger det nationale politiagentur standarder for

⁽¹¹¹⁾ Jf. politilovens artikel 5, stk. 3, og artikel 38, stk. 3.

⁽¹¹²⁾ Jf. politilovens artikel 38, stk. 3, og artikel 43-2, stk. 1. Hvis præfekturkommissionen for den offentlige sikkerhed giver en instruks i overensstemmelse med artikel 43-2, stk. 1, kan den pålægge et af kommissionen udpeget udvalg at overvåge gennemførelsen af instruksen (stk. 2). Kommissionen kan også henstille til disciplinære foranstaltninger eller afskedigelse af chefen for præfekturpolitiet (artikel 50, stk. 2) og andre politiembedsmænd (artikel 55, stk. 4).

⁽¹¹³⁾ Det samme gælder for generalinspektøren for Tokyos politi (jf. politilovens artikel 48, stk. 1).

⁽¹¹⁴⁾ Ifølge de modtagne oplysninger for regnskabsåret 2017 (april 2017 til marts 2018) håndterede informationscentre samlet 5 186 forespørgsler fra enkeltpersoner.

fortolkningen og gennemførelsen af politilovens artikel 79. Deri kræves bl.a., at præfekturpolitiet opretter et »system til behandling af klager«, og at klagebehandlingen og rapporteringen om alle klager til præfekturkommissionen for den offentlige sikkerhed foretages »straks«. I cirkulæret defineres klager som krav om korrektion »med hensyn til enhver specifik ulempe, der er blevet påført som følge af en ulovlig eller uhensigtsmæssig adfærd«⁽¹¹⁵⁾ eller »en politiembedsmands undladelse af at træffe de nødvendige foranstaltninger ved udøvelsen af sine pligter«⁽¹¹⁶⁾ samt enhver »klage over en politiembedsmands utilstrækkelige udøvelse af sine pligter«. Det materielle anvendelsesområde for en klage er således bredt defineret, idet det omfatter alle klager om ulovlig indsamling af oplysninger, og klageren skal ikke kunne påvise nogen skade som følge af en politiembedsmands handlinger. Cirkulæret foreskriver navnlig, at udlændinge (blandt andre) skal have bistand ved udarbejdelsen af en klage. Ved klager skal præfekturkommissionerne for den offentlige sikkerhed sikre, at præfekturpolitiet foretager undersøgelser, iværksætter foranstaltninger »i overensstemmelse med resultaterne af undersøgelsen« og rapporterer om resultaterne. Hvis kommissionen anser undersøgelsen for at være utilstrækkelig, skal den give instrukser om håndteringen af klagen, som præfekturpolitiet pålægges at følge. På baggrund af de rapporter, der er modtaget, og de foranstaltninger, der er truffet, meddeler kommissionen bl.a. den berørte person de foranstaltninger, som er truffet med hensyn til klagen. I det nationale politiagenturs cirkulære understreges det, at klager skal behandles »på en reel måde«, og at resultatet af behandlingen skal meddeles »inden for den tid [...] som må anses for passende i lyset af sociale normer og almindelig fornuft«.

- (141) Eftersom klager og søgsmål for det andet vil skulle behandles i et fremmed system og på et fremmed sprog, har den japanske regering med henblik på at lette adgangen hertil for EU-borgere, hvis personoplysninger overføres til erhvervsdrivende i Japan, og som offentlige myndigheder derefter får adgang til, anvendt sine beføjelser til at oprette en særlig mekanisme, der administreres og overvåges af PPC, med henblik på håndtering af og løsninger i klager på dette område. Denne mekanisme bygger på den samarbejdsforpligtelse, som japanske myndigheder pålægges i henhold til APPI, og PPC's særlige rolle med hensyn til internationale dataoverførsler fra tredjelande i medfør af artikel 6 i APPI og den grundlæggende politik (som ved kabinetsbekendtgørelse er fastlagt af den japanske regering). Nærmere oplysninger om denne mekanisme findes i de officielle redegørelser, forsikringer og tilsagn fra den japanske regering, som er knyttet til denne afgørelse som bilag II. Mekanismen er ikke underlagt nogen stående krav og er åben for enhver, uafhængigt af om pågældende er mistænkt eller tiltalt for en strafbar handling.
- (142) Med denne mekanisme kan en person, som har mistanke om, at pågældendes oplysninger, der er blevet overført fra EU, i strid med gældende regler er blevet indsamlet eller anvendt af offentlige myndigheder i Japan (herunder de myndigheder, som har ansvaret for retshåndhævelsen på det strafferetlige område), indgive en klage til PPC (som enkeltperson eller via pågældendes databeskyttelsesmyndighed, jf. artikel 51 i databeskyttelsesforordningen). PPC vil være forpligtet til at behandle klagen og skal som et første skridt underrette de ansvarlige myndigheder, herunder de relevante tilsynsmyndigheder. Disse myndigheder har pligt til at samarbejde med PPC »herunder ved at fremsende de nødvendige oplysninger og relevant materiale, således at PPC kan vurdere, om indsamlingen eller den efterfølgende anvendelse af personlige oplysninger har fundet sted i overensstemmelse med gældende regler«⁽¹¹⁷⁾. Denne forpligtelse, som er afledt af artikel 80 i APPI (hvorefter Japans offentlige myndigheder skal samarbejde med PPC), finder generel anvendelse og omfatter dermed undersøgelser af alle former for efterforskningsforanstaltninger truffet af sådanne myndigheder, der samtidig har forpligtet sig til et sådant samarbejde gennem skriftlige tilsagn fra de kompetente ministerier og myndighedschefer som afspejlet i bilag II.
- (143) Hvis undersøgelsen viser, at en overtrædelse af gældende regler har fundet sted, »omfatter de berørte offentlige myndigheders samarbejde med PPC en forpligtelse til at afhjælpe overtrædelsen«, hvilket i tilfælde af ulovlig indsamling af personlige oplysninger indebærer sletning af sådanne oplysninger. Væsentligt er i den forbindelse, at denne forpligtelse gennemføres under tilsyn foretaget af PPC, som »inden afslutningen af vurderingen [vil] bekræfte, at overtrædelsen er afhjulpel fuldt ud«.
- (144) Når undersøgelsen er gennemført, skal PPC inden for en rimelig frist meddele den berørte person dennes resultat, herunder eventuelle korrigerende foranstaltninger, såfremt dette er relevant. Samtidig skal PPC også oplyse den berørte person om mulighederne for at anmode om bekræftelse af resultatet hos den kompetente offentlige myndighed, og om hvilken myndighed sådan en anmodning om bekræftelse skal rettes til. Muligheden for at

⁽¹¹⁵⁾ Betingelsen om en »specifik ulempe« indebærer blot, at klageren personligt skal være berørt af politiets adfærd (eller manglende handling), ikke at pågældende skal kunne påvise at have lidt skade.

⁽¹¹⁶⁾ Overholdelsen af loven, herunder de lovgivningsmæssige krav med hensyn til indsamling og anvendelse af personoplysninger, er en del af disse pligter. Jf. politilovens artikel 2, stk. 2, og artikel 3.

⁽¹¹⁷⁾ I forbindelse med gennemførelsen af sin undersøgelse vil PPC samarbejde med ministeriet for interne anliggender og kommunikation, som jf. betragtning 136 kan anmode om forklaringer og materialer og afgive udtalelser vedrørende det pågældende administrative organs håndtering af personlige oplysninger (artikel 50 og 51 i APPIHAO).

modtage en sådan bekræftelse, herunder begrundelsen for den kompetente myndigheds afgørelse, kan hjælpe den enkelte med henblik på at tage yderligere skridt, herunder i forbindelse med et søgsmål. Nærmere oplysninger om evalueringens resultat kan være omfattet af begrænsninger, så længe der er en rimelig formodning for, at en sådan underretning vil udgøre en risiko for den igangværende efterforskning.

- (145) For det tredje kan en person, som er uenig i rettens afgørelse om beslaglæggelse (ved kendelse) ⁽¹¹⁸⁾ af pågældendes oplysninger eller i de foranstaltninger, som politiet eller anklagemyndigheden har truffet ved fuldbyrdelsen af en sådan afgørelse, indgive anmodning om, at sådanne foranstaltninger annulleres eller ændres (strafferetsplejelovbogens artikel 429, stk. 1, og artikel 430, stk. 1 og 2, og aflytningslovens artikel 26) ⁽¹¹⁹⁾. Hvis appelretten finder, at enten selve kendelsen eller fuldbyrdelsen deraf (»beslaglæggelsesproceduren«) er ulovlig, gives den anmodende part medhold, og der gives pålæg om tilbagelevering af de beslaglagte genstande ⁽¹²⁰⁾.
- (146) Såfremt en person anser indsamlingen af sine personlige oplysninger i forbindelse med en strafferetlig efterforskning for ulovlig, kan denne for det fjerde, som en mere indirekte form for retslig kontrol, gøre dette gældende i forbindelse med retssagen. Hvis retten er enig, vil beviserne ikke blive tilladt i sagen.
- (147) Endelig kan en ret i henhold til artikel 1, stk. 1, i lov om statens erstatningsansvar tilkende erstatning, hvis en offentlig embedsmand under udøvelsen af statslig myndighed i forbindelse med sit hverv ulovligt og culpøst (forsætligt eller uagtsomt) har forvoldt den berørte person skade. I henhold til artikel 4 i lov om statens erstatningsansvar finder den borgerlige lovbogs bestemmelser anvendelse i sager om statens erstatningsansvar. I den forbindelse foreskrives det ved den borgerlige lovbogs artikel 710, at erstatningsansvaret ikke er begrænset til skader på ejendom, således at der også kan være tale om moralsk skade (f.eks. i form af »psykisk overlast«). Herunder falder også tilfælde, hvor en krænkelse af privatlivets fred har fundet sted ved ulovlig overvågning og/eller indsamling af personlige oplysninger (f.eks. ulovlig fuldbyrdelse af en kendelse) ⁽¹²¹⁾.
- (148) Ud over økonomisk erstatning kan fysiske personer under visse betingelser også få nedlagt forbud eller påbud (f.eks. i form af sletning af personoplysninger indsamlet af offentlige myndigheder) på grundlag af deres ret til privatlivets fred i henhold til forfatningens artikel 13 ⁽¹²²⁾.
- (149) For så vidt angår alle disse klage- og prøvelsesmuligheder fastlægges det ved den tvistbilæggelsesordning, som de japanske myndigheder har indført, at fysiske personer, der er utilfredse med resultatet af proceduren, kan henvende sig til PPC, »som skal oplyse pågældende om de forskellige muligheder og nærmere procedurer for klage- og søgsmål i henhold til japanske love og forskrifter«. Derudover vil PPC »støtte den enkelte, herunder gennem vejledning og bistand i forbindelse med eventuel opfølgning på sagen over for det relevante administrative eller retslige organ«.
- (150) Dette indebærer anvendelse af de processuelle rettigheder i henhold til strafferetsplejelovbogens. F.eks. gælder, at »[h]vis vurderingen viser, at en person er mistænkt i en straffesag, oplyser PPC pågældende herom« ⁽¹²³⁾, samt muligheden for i henhold til strafferetsplejelovbogens artikel 259 at anmode anklagemyndigheden om at blive underrettet, når myndigheden har besluttet ikke at indlede en straffesag. Viser det sig derudover i forbindelse med vurderingen, at en sag, som omfatter pågældendes personlige oplysninger, er blevet indledt, og at sagen siden er afsluttet, da meddeler PPC denne, at der kan gives indsigt i sagsakterne i henhold til strafferetsplejelovbogens artikel 53 (og artikel 4 i loven om endelige sagsakter i straffesager). For den berørte person er det vigtigt at få

⁽¹¹⁸⁾ Dette omfatter aflytningskendelser, som der i aflytningsloven er fastsat et særligt meddelelseskrav for (artikel 23). I henhold til denne bestemmelse skal de personer, hvis meddelelser er blevet opfanget (og derfor er blevet registreret i fortegnelserne over denne aflytning), af efterforskningsmyndigheden have skriftlig underretning herom. Et andet eksempel er strafferetsplejelovbogens artikel 100, stk. 3, hvori det fastlægges, at retten, når den har beslaglagt postforsendelser eller telegrammer sendt til eller af tiltalte, skal give afsender eller modtager meddelelse herom, medmindre der er risiko for, at en sådan meddelelse vil kunne gribe forstyrrende ind i retssagen. For så vidt angår ransagning og beslaglæggelse foretaget af en efterforskningsmyndighed henvises der i artikel 222, stk. 1, til denne bestemmelse.

⁽¹¹⁹⁾ Selv om en sådan anmodning ikke automatisk har opsættende virkning på fuldbyrdelsen af afgørelsen om beslaglæggelse, kan appelretten bestemme en sådan udsættelse, indtil den har truffet afgørelse i sagen. Jf. strafferetsplejelovbogens artikel 429, stk. 2, og artikel 432 sammenholdt med artikel 424.

⁽¹²⁰⁾ Jf. bilag II, afsnit II.C, punkt 1).

⁽¹²¹⁾ Jf. bilag II, afsnit II.C, punkt 2).

⁽¹²²⁾ Se f.eks. byretten i Tokyo, dom af 24. marts 1988 (nr. 2925); byretten i Osaka, dom af 26. april 2007 (nr. 2925). Ifølge byretten i Osaka skal en række faktorer afvejes, f.eks.: i) arten og indholdet af de pågældende personlige oplysninger, ii) den måde, hvorpå de er indsamlet, iii) de negative konsekvenser for den berørte person, hvis oplysningerne ikke slettes, og iv) den offentlige interesse, herunder de negative konsekvenser for den offentlige myndighed, hvis oplysningerne slettes.

⁽¹²³⁾ Under alle omstændigheder skal den tiltalte, efter at der er indledt en straffesag, have mulighed for at undersøge dette bevismateriale (se strafferetsplejelovbogens artikel 298-299). For så vidt angår ofre for forbrydelser henvises til strafferetsplejelovbogens artikel 316-333.

adgang til sagsakterne med henblik på bedre at kunne forstå den efterforskning, som pågældende har været genstand for, og således bedre kunne forberede et eventuelt søgsmål (f.eks. en erstatningssag), hvis pågældende anser indsamlingen eller anvendelsen af sine oplysninger for ulovlig.

3.3. De japanske myndigheders adgang og brug med henblik på nationale sikkerhedsformål

- (151) Ifølge de japanske myndigheder er der i Japan ingen lovgivning, som giver mulighed for at indhente oplysninger ved tvangsindgreb eller »administrativ aflytning«, når der ikke er tale om en strafferetlig efterforskning. Hvor det drejer sig om national sikkerhed, kan oplysninger således kun indhentes fra en informationskilde, som alle har fri adgang til, eller ved frivillig udlevering. Erhvervsdrivende, som modtager en anmodning om frivilligt samarbejde (i form af videregivelse af elektroniske oplysninger), er ikke retligt forpligtet til at videregive disse oplysninger ⁽¹²⁴⁾.
- (152) Ifølge de modtagne oplysninger er det derudover kun fire statslige organer, som har beføjelse til at indsamle elektroniske oplysninger hos japanske erhvervsdrivende på grundlag af nationale sikkerhedshensyn, nemlig: i) kabinettets efterretnings- og undersøgelseskontor, ii) forsvarsministeriet, iii) politiet (både det nationale politiagentur ⁽¹²⁵⁾ og præfekturpolitiet) og iv) efterretningsagenturet for offentlig sikkerhed. Kabinettets efterretnings- og undersøgelseskontor indsamler imidlertid aldrig oplysninger direkte fra erhvervsdrivende, heller ikke ved aflytning eller lignende af meddelelser. Hvis agenturet modtager oplysninger fra andre offentlige myndigheder med henblik på analyser til kabinettet, skal disse andre myndigheder i den forbindelse overholde loven, herunder de begrænsninger og garantier, der er analyseret i denne afgørelse. Dets aktiviteter er derfor ikke relevante i en overførsels-sammenhæng.

3.3.1. Retsgrundlag og gældende begrænsninger/garantier

- (153) Ifølge de modtagne oplysninger indsamler forsvarsministeriet (elektroniske) oplysninger på grundlag af loven om oprettelse af forsvarsministeriet. I henhold til lovens artikel 3 er forsvarsministeriets mission at stå for administration og ledelse af de militære styrker og at »varetagde de dermed forbundne anliggender med henblik på at sikre national fred og uafhængighed og nationens sikkerhed«. Det fastsættes ved artikel 4, stk. 4, at forsvarsministeriet har ansvaret for »forsvar og beskyttelse«, for foranstaltninger truffet af det japanske forsvar og for udsendelse af de militære styrker, herunder den indsamling af oplysninger, som er nødvendige for at varetage disse anliggender. Ministeriet har kun beføjelse til at indsamle (elektroniske) oplysninger fra erhvervsdrivende gennem frivilligt samarbejde.
- (154) Præfekturpolitiets opgaver og pligter omfatter »opretholdelse af offentlig sikkerhed og orden« (politilovens artikel 35, stk. 2, sammenholdt med artikel 2, stk. 1). Inden for dette kompetenceområde kan politiet indsamle oplysninger, men kun på frivillig basis (sanktionsfrit). Desuden skal politiets virksomhed være »strengt begrænset« til, hvad der er nødvendigt for at udføre dets opgaver. Derudover skal det handle på en »upartisk, fordomsfri og retfærdig« måde, og det må aldrig misbruge sine beføjelser »på en sådan måde, at det griber ind i en persons forfatningssikrede rettigheder og friheder« (politilovens artikel 2).
- (155) Endelig kan efterretningsagenturet for offentlig sikkerhed foretage undersøgelser i henhold til loven om forhindring af undergravende aktiviteter (»SAPA«) og loven om kontrol med organisationer, som har begået vilkårlige masse mord (»ACO«), såfremt sådanne undersøgelser er nødvendige for at forberede iværksættelsen af kontrolforanstaltninger mod visse organisationer ⁽¹²⁶⁾. I henhold til begge love kan kommissionen for undersøgelser vedrørende offentlig sikkerhed efter anmodning fra generaldirektøren for efterretningsagenturet for offentlig sikkerhed iværksætte visse »dispositioner« (overvågning/forbud efter ACO ⁽¹²⁷⁾ og opløsning/forbud efter SAPA ⁽¹²⁸⁾), og i den forbindelse kan efterretningsagenturet foretage undersøgelser ⁽¹²⁹⁾. Ifølge de modtagne oplysninger foretages disse undersøgelser altid på frivillig basis, hvilket vil sige, at efterretningsagenturet for offentlig

⁽¹²⁴⁾ Erhvervsdrivende kan således frit vælge ikke at samarbejde, uden at de risikerer sanktioner eller andre negative konsekvenser. Jf. bilag II, afsnit III.A, punkt 1).

⁽¹²⁵⁾ Ifølge de modtagne oplysninger er det nationale politiagenturs vigtigste rolle at koordinere efterforskninger foretaget af de forskellige kredse i præfekturpolitiet og udveksle oplysninger med udenlandske myndigheder. Selv i denne rolle er det nationale politiagentur underlagt tilsyn foretaget af den nationale kommission for den offentlige sikkerhed, der bl.a. har ansvar for at sikre beskyttelsen af fysiske personers rettigheder og frihed (politilovens artikel 5, stk. 1).

⁽¹²⁶⁾ Jf. bilag II, afsnit III.A, punkt 1), nr. 3) Det respektive anvendelsesområde for disse to love er begrænset, således omhandler SAPA »terroristisk undergravende aktivitet« og ACO »vilkårlige masse mord« (dvs. en »terroristisk undergravende aktivitet« i den i SAPA anvendte betydning, »hvorved et stort antal personer vilkårligt myrdes«).

⁽¹²⁷⁾ Jf. artikel 5 og 8 i ACO. En overvågningsdisposition omfatter også en rapporteringsforpligtelse for den organisation, der er omfattet af foranstaltningen. For så vidt angår de proceduremæssige sikkerhedsforanstaltninger, navnlig gennemsigtighedskrav og forudgående tilladelse fra kommissionen for undersøgelser vedrørende offentlig sikkerhed, se artikel 12, 13 og 15-27 i ACO.

⁽¹²⁸⁾ Jf. artikel 5 og 7 i SAPA. For så vidt angår de proceduremæssige sikkerhedsforanstaltninger, navnlig gennemsigtighedskrav og forudgående tilladelse fra kommissionen for undersøgelser vedrørende offentlig sikkerhed, jf. artikel 11-25 i ACO.

⁽¹²⁹⁾ Jf. artikel 27 i SAPA og artikel 29 og 30 i ACO.

sikkerhed ikke kan tvinge en indehaver af personlige oplysninger til at videregive sådanne oplysninger⁽¹³⁰⁾. I hvert tilfælde skal kontroller og undersøgelser kun foretages i det mindst mulige omfang for at opnå kontrollens formål, og de må under ingen omstændigheder gennemføres med henblik på »urimelig« begrænsning af de forfatnings-sikrede rettigheder og friheder (artikel 3, stk. 1, i SAPA/ACO). Derudover må efterretningsagenturet for offentlig sikkerhed i henhold artikel 3, stk. 2, i SAPA/ACO under ingen omstændigheder misbruge disse kontroller eller de undersøgelser, der foretages for at forberede sådanne kontroller. Hvis en af agenturets embedsmænd har misbrugt sin myndighed i henhold til den relevante lov ved at tvinge en person til at foretage sig noget, som denne ikke er forpligtet til at gøre, eller ved at gribe forstyrrende ind i udøvelsen af en persons rettigheder, kan pågældende idømmes strafferetlige sanktioner i henhold til artikel 45 i SAPA eller artikel 42 i ACO. Endelig foreskrives det ved begge retsakter udtrykkeligt, at bestemmelserne deri, herunder de derved tillagte beføjelser, »under ingen omstændigheder må gøres til genstand for en udvidende fortolkning« (artikel 2 i SAPA/ACO).

- (156) I alle tilfælde af offentlig adgang af hensyn til den nationale sikkerhed, der er beskrevet i dette afsnit, finder de af den japanske højesteret fastlagte begrænsninger for frivillige undersøgelser anvendelse, hvilket betyder, at indsamlingen af (elektroniske) oplysninger skal være i overensstemmelse med principperne om nødvendighed og proportionalitet (»egnet metode«)⁽¹³¹⁾. Som de japanske myndigheder udtrykkeligt har bekræftet, finder »indsamling og behandling af oplysninger kun sted i det omfang, det er nødvendigt for, at den kompetente offentlige myndighed kan udføre specifikke opgaver, samt på grundlag af specifikke trusler«. Derfor »udelukker dette massiv og vilkårlig indsamling af eller adgang til personlige oplysninger af hensyn til den nationale sikkerhed⁽¹³²⁾«.
- (157) Når de er indsamlet, vil personlige oplysninger, som opbevares af offentlige myndigheder med henblik på nationale sikkerhedsformål, desuden være omfattet og nyde godt af beskyttelsen i henhold til APPIHAO for så vidt angår efterfølgende opbevaring, anvendelse og videregivelse (jf. betragtning 118).

3.3.2. Uafhængigt tilsyn

- (158) Indsamlingen af personlige oplysninger til nationale sikkerhedsformål er omfattet af flere lag af tilsyn fra statsmagtens tre dele.
- (159) For det første kan det japanske parlament via sine særlige udvalg undersøge lovligheden af undersøgelser på grundlag af sine beføjelser til at foretage parlamentarisk kontrol (forfatningens artikel 62, parlamentslovens artikel 104; jf. betragtning 134). Denne tilsynsfunktion understøttes ved specifikke rapporteringsforpligtelser for de aktiviteter, der udføres i henhold til nogle af ovennævnte retsgrundlag⁽¹³³⁾.
- (160) For det andet findes der en række tilsynsmekanismer inden for den udøvende magt.
- (161) For forsvarsministeriets vedkommende udøves tilsynet af generalinspektørkontoret for overholdelse af lovkrav⁽¹³⁴⁾, som på grundlag af artikel 29 i loven om oprettelse af forsvarsministeriet er blevet oprettet som et kontor inden for ministeriet under forsvarsministerens tilsyn (som det rapporterer til), men som er uafhængigt af ministeriets operationelle afdelinger. Generalinspektørkontoret har til opgave at sikre overholdelsen af love og forskrifter samt at sikre forsvarsministeriets embedsmænds korrekte udførelse af deres pligter. Kontoret har bl.a. beføjelse til at foretage såkaldte »forsvarsinspektioner«, både med regelmæssige mellemrum (»regelmæssige forsvarsinspektioner«) og i særlige tilfælde (»særlige forsvarsinspektioner«), og disse har hidtil også omfattet den korrekte behandling af personlige oplysninger⁽¹³⁵⁾. I forbindelse med inspektionerne kan generalinspektørkontoret gå ind på steder

⁽¹³⁰⁾ Jf. bilag II, afsnit III.A, punkt 1), nr. 3)

⁽¹³¹⁾ Jf. bilag II, afsnit III.A, punkt 2), litra b). »Det følger af højesterets praksis, at der, for at en erhvervsdrivende kan anmodes om frivilligt samarbejde, skal være tale om en nødvendig anmodning med henblik på at efterforske en mistanke om en strafbar handling, og at anmodningen skal være rimelig for at nå formålet med efterforskningen. Selv om undersøgelser foretaget af efterforskningsmyndigheder på området national sikkerhed er forskellige fra undersøgelser foretaget af efterforskningsmyndigheder på retshåndhævelsesområdet, både hvad angår deres retsgrundlag og formål, finder de centrale principper om »undersøgelsens nødvendighed« og »metodens egnethed« ligeledes anvendelse på området national sikkerhed, og de skal overholdes under behørig hensyntagen til de særlige omstændigheder i hvert enkelt tilfælde«.

⁽¹³²⁾ Jf. bilag II, afsnit III.A, punkt 2), litra b).

⁽¹³³⁾ Jf. f.eks. artikel 36 i SAPA/artikel 31 i ACO (for efterretningsagenturet for offentlig sikkerhed).

⁽¹³⁴⁾ Chefen for generalinspektørkontoret er en tidligere offentlig anklager. Jf. bilag II, afsnit III.B, punkt 3).

⁽¹³⁵⁾ Jf. bilag II, afsnit III.B, punkt 3). Ifølge det forelagte eksempel omfattede den regelmæssige forsvarsinspektion 2016 vedrørende »bevidsthed om/parathed til overholdelse af lovkrav« bl.a. »status for beskyttelse af personlige oplysninger« (forvaltning, opbevaring, osv.). I den deraf følgende rapport blev der konstateret tilfælde af ukorrekt dataforvaltning og opfordret til forbedringer i denne henseende. Forsvarsministeriet offentliggjorde rapporten via sit websted.

(kontorer) og anmode om udlevering af dokumenter eller oplysninger, herunder om forklaringer fra den stedfortrædende viceforsvarsminister. Inspektionen færdiggøres med en rapport til forsvarsministeren, hvori resultater og forbedringstiltag forelægges (deres gennemførelse kan efterfølgende igen kontrolleres gennem yderligere inspektioner). Rapporten udgør endvidere grundlaget for forsvarsministerens instrukser om gennemførelse af de foranstaltninger, der er nødvendige for at håndtere situationen; den stedfortrædende viceminister får til opgave at gennemføre disse foranstaltninger og skal rapportere om opfølgningen.

- (162) For så vidt angår præfekturpolitiet sikres tilsynet af de uafhængige præfekturkommissioner for den offentlige sikkerhed, som beskrevet i betragtning 135 vedrørende retshåndhævelsen på det strafferetlige område.
- (163) Endelig kan efterretningsagenturet for offentlig sikkerhed som angivet kun foretage undersøgelser i det omfang, det er nødvendigt i forbindelse med dispositioner i form af forbud, opløsning eller overvågning foretaget i henhold til SAPA/ACO, og den uafhængige ⁽¹³⁶⁾ kommission for undersøgelser vedrørende offentlig sikkerhed har ansvaret for det forudgående tilsyn med disse dispositioner. Derudover foretages regelmæssige/periodiske inspektioner (som på en helhedsorienteret måde ser på efterretningsagenturet for offentlig sikkerheds aktiviteter) ⁽¹³⁷⁾ og særlige interne inspektioner ⁽¹³⁸⁾ vedrørende enkelte afdelinger/kontorer osv. af særligt udvalgte inspektører, og de kan føre til, at der udstedes instrukser til cheferne for de relevante afdelinger om at træffe foranstaltninger med henblik på korrektion eller forbedring.
- (164) Disse tilsynsmekanismer, som styrkes yderligere via den mulighed, som enkeltpersoner har for at få PPC til at gribe ind som uafhængig tilsynsmyndighed (jf. betragtning 168 nedenfor), giver tilstrækkelige garantier mod risikoen for, at de japanske myndigheders misbruger af deres beføjelser på området national sikkerhed, og mod enhver form for ulovlig indsamling af elektroniske oplysninger.

3.3.3. Individuel klage- eller prøvelsesadgang

- (165) For så vidt angår enkeltpersoners klage- og prøvelsesadgang med hensyn til personlige oplysninger, der er blevet indsamlet og således opbevares af administrative organer, er disse organer forpligtet til »bestræbe sig på hurtigt at behandle alle klager« vedrørende sådan behandling (artikel 48 i APPIHAO).
- (166) I modsætning til strafferetlige efterforskninger har enkeltpersoner (heriblandt udenlandske statsborgere med udenlandsk bopæl) derudover i princippet ret til indsigt ⁽¹³⁹⁾, berigtigelse (herunder sletning) og suspension af anvendelsen/videregivelsen i henhold til APPIHAO. Uanset dette kan chefen for det administrative organ afslå at give indsigt med hensyn til oplysninger, »for hvilke der er rimelig grund [...] til at antage, at denne indsigt sandsynligvis vil være til skade for den nationale sikkerhed« (artikel 14, nr. iv), i APPIHAO, og pågældende kan desuden gøre det uden at oplyse, om sådanne oplysninger forefindes (artikel 17 i APPIHAO). Selv om enkeltpersoner kan anmode om suspension af anvendelsen eller om sletning af oplysninger i henhold til artikel 36, stk. 1, nr. i), i APPIHAO, såfremt det administrative organ har erhvervet oplysningerne ulovligt eller opbevarer/anvender dem ud over, hvad der er nødvendigt for at opnå det angivne formål, har myndigheden ligeledes mulighed for at afslå anmodningen, hvis den finder, at en suspension af anvendelsen »sandsynligvis vil være til hinder for varetagelsen af de anliggender, som vedrører anvendelsesformålet for brugen af de opbevarede personlige oplysninger på grund af disse anliggendes karakter« (artikel 38 i APPIHAO). Såfremt det er muligt let at adskille og udelade dele, som er genstand for en undtagelse, har administrative organer imidlertid pligt til at give mindst delvis indsigt (jf. f.eks. artikel 15, stk. 1, i APPIHAO) ⁽¹⁴⁰⁾.

⁽¹³⁶⁾ I henhold til loven om oprettelse af kommissionen for undersøgelser vedrørende offentlig sikkerhed skal kommissionens formand og medlemmer »udøve deres myndighed i uafhængighed« (artikel 3). De udnævnes af premierministeren med samtykke fra begge kamre i parlamentet og kan kun afskediges med gyldig grund (f.eks. fængsling, embedsmisbrug, mental eller fysisk forstyrrelse, indledning af konkursbehandling).

⁽¹³⁷⁾ Regulering af efterretningsagenturet for offentlig sikkerheds periodiske inspektioner (generaldirektøren for efterretningsagenturet for offentlig sikkerhed, instruks nr. 4, 1986).

⁽¹³⁸⁾ Regulering af efterretningsagenturet for offentlig sikkerheds særlige inspektioner (generaldirektøren for efterretningsagenturet for offentlig sikkerhed, instruks nr. 11, 2008). Særlige inspektioner gennemføres, hvis generaldirektøren for efterretningsagenturet for offentlig sikkerhed finder det nødvendigt.

⁽¹³⁹⁾ Herved henvises til retten til at modtage en kopi af de »opbevarede personlige oplysninger«.

⁽¹⁴⁰⁾ Jf. også muligheden for »skønmæssig indsigt« selv i et tilfælde, hvor »hemmeligholdte oplysninger« indgår i de »opbevarede personlige oplysninger«, der søges om indsigt i (artikel 16 i APPIHAO).

- (167) Under alle omstændigheder skal det administrative organ træffe en skriftlig afgørelse inden for en bestemt frist (30 dage, som på visse betingelser kan forlænges med yderligere 30 dage). Hvis der gives afslag på anmodning, den kun delvis imødekommes, eller hvis den enkelte af andre grunde anser det administrative organs adfærd for »ulovlig eller uretfærdig«, kan pågældende anmode om administrativ prøvelse på grundlag af loven om administrativ rekurs⁽¹⁴¹⁾. I sådanne tilfælde skal chefen for det administrative organ, som træffer afgørelse i klagesagen, høre klagenævnet for indsigt og beskyttelse af personlige oplysninger (artikel 42 og 43 i APPIHAO), som er et specialiseret, uafhængigt nævn, hvis medlemmer er udpeget af premierministeren med samtykke fra begge kamre i parlamentet. Ifølge de modtagne oplysninger kan klagenævnet foretage en undersøgelse⁽¹⁴²⁾ og i den forbindelse anmode det administrative organ om at forelægge de opbevarede personlige oplysninger, herunder alt klassificeret indhold, og yderligere oplysninger og dokumenter. Selv om den endelige rapport, der sendes til klageren og det administrative organ og offentliggøres, ikke er retligt bindende, følges den næsten altid⁽¹⁴³⁾. Samtidig har den enkelte mulighed for at anfægte klageafgørelsen i ved domstolene på grundlag af loven om forvaltningsretssager. Derved banes vejen for en effektiv domstolskontrol af anvendelsen af nationale sikkerhedsundtagelser, herunder hvorvidt en sådan undtagelse er blevet misbrugt eller stadig er berettiget.
- (168) For at lette udøvelsen af ovennævnte rettigheder i henhold til APPIHAO har ministeriet for interne anliggender og kommunikation etableret 51 informationscentre, der står for oplysning om disse rettigheder, de gældende procedurer for anmodninger og muligheder for klage- og prøvelsesadgang⁽¹⁴⁴⁾. For de administrative organer gælder, at de er forpligtet til at meddele »oplysninger, som bidrager til nærmere bestemmelse af de opbevarede personlige oplysninger«⁽¹⁴⁵⁾ og til at træffe »andre hensigtsmæssige foranstaltninger med henblik på lettelse for personen, som har til hensigt fremsætte anmodningen« (artikel 47, stk. 1, i APPIHAO).
- (169) Som det er tilfældet for undersøgelser inden for retshåndhævelsen på det strafferetlige område, har borgerne også på området national sikkerhed mulighed for individuel klage ved direkte henvendelse til PPC. Dette vil udløse den særlige tvistbilæggelsesprocedure, som den japanske regering har indført for enkeltpersoner fra EU, hvis personoplysninger overføres i henhold til denne afgørelse (se nærmere beskrivelse i betragtning 141-144 og 149).
- (170) En borger kan desuden få sin sag prøvet ved domstolene gennem et erstatningssøgsmål i henhold til lov om statens erstatningsansvar, som også omfatter immateriel skade og under visse betingelser sletning af de indsamlede data (jf. betragtning 147).

4. KONKLUSION: ET TILSTRÆKKELIGT BESKYTTELSESNIVEAU FOR PERSONOPLYSNINGER, DER OVERFØRES FRA EU TIL ERHVERVSDRIVENDE I JAPAN

- (171) Kommissionen finder, at APPI suppleret ved de supplerende regler i bilag I sammen med de officielle redegørelser, forsikringer og tilsagn i bilag II sikrer et beskyttelsesniveau for personoplysninger overført fra Den Europæiske Union, der i det væsentlige svarer til det niveau, der er garanteret ved forordning (EU) 2016/679.
- (172) Kommissionen finder desuden ud fra en samlet betragtning, at tilsynsmekanismerne og domstolsadgangen i den japanske lovgivning i praksis gør det muligt at identificere og sanktionere overtrædelser begået af modtagende PIHBO'er, og at de sikrer den registrerede retsmidlerne til at opnå adgang til personoplysninger, som vedrører pågældende, og til efterfølgende at få sådanne oplysninger berigtiget eller slettet.

⁽¹⁴¹⁾ loven om administrativ rekurs (lov nr. 160 af 2014), særlig artikel 1, stk. 1.

⁽¹⁴²⁾ Jf. artikel 9 i lov om oprettelse af klagenævnet for indsigt og beskyttelse af personlige oplysninger (lov nr. 60 af 2003).

⁽¹⁴³⁾ Ifølge de modtagne oplysninger har de administrative organer i de 13 år siden 2005 (da APPIHAO trådte i kraft) kun i 2 ud af mere end 2000 sager undladt at følge rapporten, på trods af at administrative afgørelser er blevet modsagt af klagenævnet i en række sager. Derudover skal det administrative organ, hvis det træffer en afgørelse, der afviger fra rapportens resultater, klart begrunde, hvorfor den afviger herfra. Se bilag II, afsnit III.C, med henvisning til artikel 50, stk. 1, punkt iv), i loven om administrativ rekurs.

⁽¹⁴⁴⁾ Informationscentrene – hvoraf der findes et i hvert præfektur – giver borgerne forklaringer med hensyn til personlige oplysninger, der er indsamlet af offentlige myndigheder (f.eks. eksisterende databaser), og de gældende databeskyttelsesregler (APPIHAO), herunder hvordan de kan udøve rettighederne til indsigt, berigtigelse eller suspension af anvendelsen. Samtidig fungerer centrene som kontaktpunkter for forespørgsler/klager fra borgerne. Jf. bilag II, afsnit II.C, punkt 4), litra a).

⁽¹⁴⁵⁾ Jf. også artikel 10 og 11 i APPIHAO om »registret over sagsmapper med personlige oplysninger«, der imidlertid indeholder omfattende undtagelser med hensyn til »sagsmapper med personlige oplysninger«, der behandles eller opbevares med henblik på strafferetlige efterforskninger, eller som indeholder oplysninger vedrørende statens sikkerhed og øvrige vigtige interesser (jf. artikel 10, stk. 2, nr. i) og ii), i APPIHAO).

- (173) Endelig finder Kommissionen på grundlag af de tilgængelige oplysninger om den japanske retsorden, herunder de i bilag II indeholdte redegørelser, forsikringer og tilsagn fra den japanske regering, at eventuelle indgreb i de grundlæggende rettigheder for enkeltpersoner, hvis personoplysninger overføres fra Den Europæiske Union til Japan, som foretages af de japanske myndigheder i offentlighedens interesse, navnlig med henblik på retshåndhævelse på det strafferetlige område og af nationale sikkerhedshensyn, vil blive begrænset til det strengt nødvendige med henblik på at nå tilsigtede legitime mål, og at der er en effektiv retsbeskyttelse mod sådanne indgreb.
- (174) Ud fra hvad Kommissionen har konstateret i denne afgørelse, finder den derfor, at Japan sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger overført fra Den Europæiske Union til PIHBO'er i Japan, der er omfattet af APPI, undtagen i de tilfælde, hvor modtageren tilhører en af de i artikel 76, stk. 1, omhandlede kategorier og hele eller en del af formålet med behandlingen svarer til et af de i bestemmelsen angivne formål.
- (175) På dette grundlag konkluderer Kommissionen, at der leves op til standarden for tilstrækkelig beskyttelse i artikel 45 i forordning (EU) 2016/679 som fortolket i lyset af Den Europæiske Unions charter om grundlæggende rettigheder, navnlig i henhold til Schrems-dommen ⁽¹⁴⁶⁾.

5. DATABESKYTTELSESMYNDIGHEDERNES FORANSTALTNINGER OG OPLYSNINGER TIL KOMMISSIONEN

- (176) Ifølge Domstolens praksis ⁽¹⁴⁷⁾ og som anerkendt i artikel 45, stk. 4, i forordning (EU) 2016/679 bør Kommissionen løbende overvåge den relevante udvikling i tredjelandet efter vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet for at vurdere, hvorvidt Japan stadig sikrer et i det væsentlige tilsvarende beskyttelsesniveau. En sådan undersøgelse skal under alle omstændigheder foretages, når Kommissionen modtager oplysninger, der rejser begrundet tvivl i denne henseende.
- (177) Kommissionen bør derfor løbende overvåge situationen med hensyn til de retlige rammer og den faktiske praksis i behandlingen af personoplysninger, som er blevet vurderet i denne afgørelse, herunder om de japanske myndigheder holder sig til de redegørelser, forsikringer og tilsagn, der er indeholdt i bilag II. For at lette denne proces, forventes det af de japanske myndigheder, at de underretter Kommissionen om materiel udvikling, som er relevant for denne afgørelse, både hvad angår erhvervsdrivendes behandling af personoplysninger og de begrænsninger og garantier, som finder anvendelse med hensyn til offentlige myndigheders adgang til personoplysninger. Dette bør omfatte enhver afgørelse, som PPC vedtager i henhold til artikel 24 APPI om anerkendelse af, at et tredjeland har et beskyttelsesniveau svarende til det japanske.
- (178) Med henblik på at Kommissionen effektivt kan udføre sin overvågning bør medlemsstaterne underrette Kommissionen om alle relevante foranstaltninger, der træffes af de nationale databeskyttelsesmyndigheder, navnlig med hensyn til forespørgsler og klager fra registrerede i EU vedrørende overførsel af personoplysninger fra Den Europæiske Union til erhvervsdrivende i Japan. Kommissionen bør også underrettes om eventuelle indikationer på, at de japanske myndigheder med ansvar for forebyggelse, efterforskning, afsløring og retsforfølgelse på det strafferetlige område eller for national sikkerhed, herunder alle tilsynsmyndigheder, ikke handler på en måde, der sikrer det krævede beskyttelsesniveau.
- (179) Medlemsstaterne og deres organer er forpligtet til at træffe de nødvendige foranstaltninger for at overholde EU-institutionernes retsakter, da der gælder en formodning om, at disse retsakter er lovlige, og de afføder derfor retsvirkninger, så længe de ikke er blevet trukket tilbage, annulleret under et annullationssøgsmaal eller erklæret ugyldige som følge af en præjudiciel forelæggelse eller en ulovlighedsindsigelse. En afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 er således bindende for alle de organer i medlemsstaterne, som den er rettet til, herunder deres uafhængige tilsynsmyndigheder. Som Domstolen har redegjort for i Schrems-dommen ⁽¹⁴⁸⁾ og som anerkendt i forordningens artikel 58, stk. 5, er det samtidig således, at dersom en databeskyttelsesmyndighed, herunder på baggrund af en klage, tvivler på, om en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet er forenelig med beskyttelsen af den grundlæggende ret til privatliv og databeskyttelse, så skal der i national ret være retsmidler, der gør det muligt for myndigheden at gøre klagepunkterne gældende for en national domstol, og denne er i tvivlstilfælde forpligtet til at udsætte en sag og forelægge Domstolen et præjudicielt spørgsmål ⁽¹⁴⁹⁾.

⁽¹⁴⁶⁾ Se ovenstående fodnote 3.

⁽¹⁴⁷⁾ Schrems, præmis 76.

⁽¹⁴⁸⁾ Schrems, præmis 65.

⁽¹⁴⁹⁾ Schrems, præmis 65. »I denne henseende påhviler det den nationale lovgiver at fastsætte retsmidler, der gør det muligt for den pågældende nationale tilsynsmyndighed at gøre de klagepunkter, som den finder begrundede, gældende for de nationale domstole, således at disse, såfremt de deler myndighedens tvivl vedrørende gyldigheden af Kommissionens afgørelse, kan foretage en præjudiciel forelæggelse med henblik på en efterprøvelse af denne afgørelses gyldighed«.

6. REGELMÆSSIG EVALUERING AF KONSTATERINGEN AF ET TILSTRÆKKELIGT BESKYTTELSESNIVEAU

- (180) I medfør af artikel 45, stk. 3, i forordning (EU) 2016/679⁽¹⁵⁰⁾ og henset til den omstændighed, at det beskyttelsesniveau, som den japanske retsorden sikrer, kan ændre sig, vil Kommissionen efter vedtagelse af denne afgørelse med regelmæssige mellemrum undersøge, om konstateringen af det tilstrækkelige beskyttelsesniveau, som er sikret af Japan, stadig er faktisk og retligt begrundet.
- (181) Med henblik herpå bør første revision af denne afgørelse foretages to år efter dens ikrafttræden. Efter den første revision og afhængigt af dennes resultat vil Kommissionen i nært samråd med det udvalg, der er nedsat i henhold til artikel 93, stk. 1, i databeskyttelsesforordningen, beslutte, om den toårige cyklus bør opretholdes. Under alle omstændigheder bør de efterfølgende revisioner finde sted mindst hvert fjerde år⁽¹⁵¹⁾. Revisionen bør omfatte alle aspekter af denne afgørelses funktionsmåde, navnlig anvendelsen af de supplerende regler (med særlig opmærksomhed på den beskyttelse, der gives i tilfælde af videreoverførsler), anvendelsen af reglerne om samtykke, herunder ved tilbagetrukket samtykke, udøvelsen af individuelle rettigheder samt begrænsningerne og garantierne med hensyn til myndighedsadgang, herunder den i bilag II til denne afgørelse omhandlede prøvelsesmekanisme. Den bør også omfatte effektiviteten af tilsynet og håndhævelsen, både med hensyn til de regler, som finder anvendelse på PIHBO'er, og de regler, som finder anvendelse inden for retshåndhævelsen på det strafferetlige område og med hensyn til national sikkerhed.
- (182) Med henblik på at foretage revisionen bør Kommissionen mødes med PPC, som efter behov kan ledsages af andre japanske myndigheder med ansvar for myndighedsadgang, herunder de relevante tilsynsorganer. Deltagelsen i dette møde bør være åben for repræsentanter for medlemmerne af Det Europæiske Databeskyttelsesråd. Inden for rammerne af den fælles revision bør Kommissionen anmode PPC om omfattende oplysninger om alle aspekter, der er relevante for konstateringen af et tilstrækkeligt beskyttelsesniveau, herunder om begrænsningerne og garantierne vedrørende myndighedsadgang⁽¹⁵²⁾. Kommissionen bør også indhente redegørelser vedrørende eventuelle oplysninger med relevans for denne afgørelse, som den har modtaget, herunder offentlige rapporter fra japanske myndigheder eller andre interessenter i Japan, Det Europæiske Databeskyttelsesråd, individuelle databeskyttelsesmyndigheder, civilsamfundsgrupper, medierne eller andre tilgængelige informationskilder.
- (183) Kommissionen vil på grundlag af den fælles revision udarbejde en offentlig rapport til Europa-Parlamentet og Rådet.

7. SUSPENSION AF AFGØRELSEN OM TILSTRÆKKELIGHEDEN AF BESKYTTELSESNIVEAUET

- (184) Hvis Kommissionen på grundlag af kontrollerne eller andre tilgængelige oplysninger konkluderer, at det beskyttelsesniveau, som den japanske retsorden giver, ikke længere i det væsentlige svarer til beskyttelsesniveauet i Unionen, bør den underrette de kompetente japanske myndigheder herom og anmode om, at der træffes passende foranstaltninger inden for en fastlagt, rimelig frist. Dette omfatter reglerne for både erhvervsdrivende og Japans offentlige myndigheder med ansvar for retshåndhævelse på det strafferetlige område eller nationale sikkerhedsanliggender. En sådan procedure vil f.eks. skulle iværksættes i tilfælde, hvor videreoverførsler ikke længere finder sted under garantier, der sikrer den fortsatte beskyttelse i overensstemmelse med artikel 44 i databeskyttelsesforordningen, herunder tilfælde, hvor grundlaget er afgørelser vedtaget af PPC i henhold til artikel 24 i APPI om anerkendelse af, at et tredjeland har et beskyttelsesniveau svarende til det japanske.
- (185) Hvis de kompetente japanske myndigheder efter udløbet af den fastlagte frist ikke på tilfredsstillende vis kan dokumentere, at denne afgørelse fortsat er baseret på et tilstrækkeligt beskyttelsesniveau, bør Kommissionen ved anvendelse af artikel 45, stk. 5, i forordning (EU) 2016/679 indlede proceduren med henblik på hel eller delvis suspension eller ophævelse af denne afgørelse. Kommissionen bør alternativt indlede proceduren med henblik på ændring af denne afgørelse, navnlig ved at fastsætte yderligere betingelser for dataoverførsler eller ved at begrænse anvendelsesområdet for konstateringen af et tilstrækkeligt beskyttelsesniveau til dataoverførsler, for hvilke den fortsatte beskyttelse er sikret i overensstemmelse med artikel 44 i databeskyttelsesforordningen.

⁽¹⁵⁰⁾ Artikel 45, stk. 3, i forordning (EU) 2016/679: »[i] den pågældende gennemførelsesretsakt fastsættes en mekanisme for regelmæssig revision, som foretages mindst hvert fjerde år, og som inddrager enhver relevant udvikling i tredjelandet eller den internationale organisation«.

⁽¹⁵¹⁾ Artikel 45, stk. 3, i forordning (EU) 2016/679 foreskriver, at en regelmæssig revision skal finde sted mindst hvert fjerde år. Se også Det Europæiske Databeskyttelsesråd, Adequacy Referential, WP 254 rev. 01.

⁽¹⁵²⁾ Jf. også bilag II, afsnit IV: »Inden for rammerne af den regelmæssige revision af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vil PPC og Europa-Kommissionen udveksle oplysninger om behandlingen af oplysninger i henhold til betingelserne i konstateringen af et tilstrækkeligt beskyttelsesniveau, herunder dem, der er fastsat i denne redegørelse«.

- (186) Kommissionen bør navnlig indlede proceduren med henblik på suspension eller ophævelse i tilfælde af indikationer på, at de supplerende regler i bilag I ikke overholdes af erhvervsdrivende, der modtager personoplysninger i henhold til denne afgørelse, og/eller ikke håndhæves effektivt, eller at de japanske myndigheder ikke holder sig til de redegørelser, forsikringer og tilsagn, som er indeholdt i bilag II til denne afgørelse.
- (187) Kommissionen bør ligeledes overveje at indlede proceduren med henblik på ændring, suspension eller ophævelse af denne afgørelse, hvis de japanske myndigheder i forbindelse med den fælles revision eller på anden vis undlader at forelægge de oplysninger og præciseringer, der er nødvendige for at vurdere beskyttelsesniveauet for personoplysninger, der overføres fra Den Europæiske Union til Japan, eller for at vurdere overholdelsen af denne afgørelse. I den forbindelse bør Kommissionen tage hensyn til, i hvilket omfang de relevante oplysninger kan indhentes fra andre kilder.
- (188) Kommissionen bør i behørigt begrundede hastende tilfælde, f.eks. ved en risiko for alvorlig overtrædelse af registreredes rettigheder, overveje at vedtage en afgørelse om at suspendere eller ophæve nærværende afgørelse, og en sådan afgørelse bør finde anvendelse straks, jf. artikel 93, stk. 3, i forordning (EU) 2016/679 sammenholdt med artikel 8 i Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011⁽¹⁵³⁾.

8. AFSLUTTENDE BETRAGTNINGER

- (189) Det Europæiske Databeskyttelsesråd har offentliggjort sin udtalelse⁽¹⁵⁴⁾, som er blevet taget i betragtning ved udarbejdelsen af denne afgørelse.
- (190) Europa-Parlamentet har vedtaget en beslutning om en digital handelsstrategi, hvori Kommissionen opfordres til at prioritere og fremskynde vedtagelsen af afgørelser om et tilstrækkeligt beskyttelsesniveau med vigtige handelspartnere i henhold til betingelserne i forordning (EU) 2016/679, således at disse kan fungerer som en grundlæggende mekanisme til at sikre overførslen af personoplysninger fra EU⁽¹⁵⁵⁾. Europa-Parlamentet har også vedtaget en beslutning om tilstrækkeligheden af den beskyttelse af personoplysninger, der gives af Japan⁽¹⁵⁶⁾.
- (191) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 93, stk. 1, i databeskyttelsesforordningen —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. Med henblik på artikel 45 i forordning (EU) 2016/679 sikrer Japan et tilstrækkeligt beskyttelsesniveau for personoplysninger, som overføres fra Den Europæiske Union til erhvervsdrivende, der håndterer personlige oplysninger og er omfattet af loven om beskyttelse af personlige oplysninger som suppleret ved de supplerende regler i bilag I og de officielle redegørelser, forsikringer og tilsagn i bilag II.

⁽¹⁵³⁾ Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

⁽¹⁵⁴⁾ Udtalelse 28/2018 om Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i Japan, vedtaget den 5. december 2018.

⁽¹⁵⁵⁾ Europa-Parlamentets beslutning af 12. december 2017 om »Udvikling af en digital handelsstrategi« (2017/2065(INI)). Se især punkt 8 (»... minder om, at personoplysninger kan overføres til tredjelande uden, at der gøres brug af generelle discipliner i handelsaftaler, når kravene [...] i Kapitel V i forordning (EU) 2016/679 - både på nuværende tidspunkt og i fremtiden - er opfyldt; anerkender, at afgørelser om et tilstrækkeligt beskyttelsesniveau, herunder delvise og sektorspecifikke afgørelser, udgør en grundlæggende mekanisme for så vidt angår beskyttelse af overførsler af personoplysninger fra EU til et tredjeland; bemærker, at EU kun har vedtaget afgørelser om et tilstrækkeligt beskyttelsesniveau med fire af sine 20 største handelspartnere...«) og punkt 9 (»opfordrer Kommissionen til at prioritere og fremskynde vedtagelsen af afgørelser om et tilstrækkeligt beskyttelsesniveau, forudsat at tredjelande på grundlag af deres nationale lovgivning eller deres internationale forpligtelser sikrer et beskyttelsesniveau«reelt tilsvarende»det, der garanteres i EU...«).

⁽¹⁵⁶⁾ Europa-Parlamentets beslutning af 13. december 2018 om tilstrækkeligheden af den beskyttelse af personoplysninger, der gives af Japan (2018/2979(RSP)).

2. Denne afgørelse omfatter ikke personoplysninger, der overføres til modtagere, som tilhører en af følgende kategorier, for så vidt hele eller en del af formålet med behandlingen af personoplysningerne svarer til et af de anførte formål:

- a) radio- og tv-spredningsorganer, avisudgivere, kommunikationsbureauer og andre presseorganer (herunder personer, som udøver presseaktiviteter som erhverv) i det omfang, de behandler personoplysninger til presseformål
- b) personer, der er professionelle skribenter, i det omfang dette involverer personoplysninger
- c) universiteter og alle organisationer eller grupper, hvis formål er akademiske undersøgelser, eller enhver person, der tilhører en sådan organisation eller gruppe, i det omfang de behandler personoplysninger med henblik på akademiske undersøgelser
- d) religiøse organer, i det omfang de behandler personoplysninger med henblik på religiøse aktiviteter (herunder alle tilknyttede aktiviteter)
- e) politiske organer, i det omfang de behandler personoplysninger med henblik på deres politiske aktiviteter (herunder alle tilknyttede aktiviteter).

Artikel 2

Når de kompetente myndigheder i medlemsstaterne med henblik på at beskytte fysiske personer i forbindelse med behandlingen af deres personoplysninger udøver deres beføjelser i medfør af artikel 58 i forordning (EU) 2016/679, og dette fører til suspension eller definitivt forbud mod dataoverførsel til en specifik erhvervsdrivende i Japan inden for det anvendelsesområde, der er fastlagt i artikel 1, underretter den pågældende medlemsstat straks Kommissionen herom.

Artikel 3

1. Kommissionen overvåger løbende anvendelsen af den retlige ramme, som denne afgørelse er baseret på, herunder de betingelser, hvorunder der foretages videreoverførsler, med henblik på at vurdere, om Japan fortsat sikrer et tilstrækkeligt beskyttelsesniveau i henhold til artikel 1.

2. Medlemsstaterne og Kommissionen underretter hinanden om tilfælde, hvor kommissionen for beskyttelse af personlige oplysninger eller andre kompetente japanske myndigheder ikke sikrer overholdelsen af de retlige rammer, som denne afgørelse er baseret på.

3. Medlemsstaterne og Kommissionen underretter hinanden, hvis der er indikationer på, at de japanske myndigheders indgriben i den enkeltes ret til beskyttelse af sine personoplysninger går videre, end hvad der er strengt nødvendigt, eller på, at der ikke er en effektiv retsbeskyttelse mod sådanne indgreb.

4. Kommissionen foretager senest to år fra datoen for meddelelse af denne afgørelse til medlemsstaterne og herefter mindst hvert fjerde år en evaluering af konklusionen i artikel 1, stk. 1, på grundlag af alle tilgængelige oplysninger, herunder de oplysninger, der modtages som led i den årlige fælles revision, som foretages sammen med de japanske myndigheder.

5. Dersom Kommissionen har oplysninger om, at der ikke længere sikres et tilstrækkeligt beskyttelsesniveau, underretter den de kompetente japanske myndigheder herom. Den kan om nødvendigt beslutte at suspendere, ændre eller ophæve denne afgørelse eller begrænse dens anvendelsesområde, herunder når der er indikationer på:

- a) at erhvervsdrivende i Japan, som har modtaget personoplysninger fra Den Europæiske Union i henhold til denne afgørelse, ikke efterlever de yderligere garantier i de supplerende regler i bilag I til denne afgørelse, eller at der er utilstrækkeligt tilsyn i denne henseende
- b) at de japanske myndigheder ikke efterlever de redegørelser, forsikringer og tilsagn, som er indeholdt i bilag II til denne afgørelse, herunder med hensyn til betingelserne og begrænsningerne for de japanske myndigheders indsamling af og adgang til de i henhold til denne afgørelse overførte personoplysninger med henblik på retshåndhævelse på det strafferetlige område eller af hensyn til den nationale sikkerhed.

Kommissionen kan også fremsætte sådanne udkast til foranstaltninger, hvis de japanske myndigheders manglende samarbejdsvilje forhindrer den i at afgøre, om konklusionen i artikel 1, stk. 1, er berørt.

Artikel 4

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 23. januar 2019.

På Kommissionens vegne
Věra JOUROVÁ
Medlem af Kommissionen

BILAG I

SUPPLERENDE REGLER I HENHOLD TIL LOV OM BESKYTTELSE AF PERSONLIGE OPLYSNINGER VEDRØRENDE HÅNDBLÆRNINGEN AF PERSONOPPLYSNINGER, DER OVERFØRES FRA EU PÅ GRUNDLAG AF EN AFGØRELSE OM TILSTRÆKKELIGHEDEN AF BESKYTTELSESNIVEAUET

Indholdsfortegnelse

1) Følsomme personlige oplysninger (lovens artikel 2, stk. 3)	38
2) Opbevarede personoplysninger (lovens artikel 2, stk. 7).	39
3) Præcisering af et anvendelsesformål, begrænsning som følge af et anvendelsesformål (lovens artikel 15, stk. 1, artikel 16, stk. 1, og artikel 26, stk. 1 og 3)	40
4) Begrænsning af videregivelsen til tredjemand i et tredjeland (lovens artikel 24; reglernes artikel 11-2)	41
5) Anonymt behandlede oplysninger (lovens artikel 2, stk. 9, og artikel 36, stk. 1 og 2)	41

[Termer]

»loven«	Lov om beskyttelse af personlige oplysninger (lov nr. 57 af 2003).
»Kabinetsbekendtgørelsen«	Kabinetsbekendtgørelse om gennemførelse af loven om beskyttelse af personlige oplysninger (lov nr. 507 af 2003).
»reglerne«	Håndhævelsesregler til loven om beskyttelse af personlige oplysninger (kommissionen for beskyttelse af personlige oplysningers regler nr. 3, 2016).
»retningslinjer til de generelle regler«	Retningslinjer til loven om beskyttelse af personlige oplysninger (bind om generelle regler) (kommissionen for beskyttelse af personlige oplysningers cirkulære nr. 65, 2015).
»EU«	»EU«, herunder dets medlemsstater og, henset til EØS-aftalen, Island, Liechtenstein og Norge
»databeskyttelsesforordningen«	Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
»afgørelse om tilstrækkeligheden af beskyttelsesniveauet«	Europa-Kommissionens afgørelse om, at et tredjeland eller et område i dette tredjeland mv. sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger i henhold til databeskyttelsesforordningens artikel 45.

Med henblik på gensidig og smidig overførsel af personlige oplysninger mellem Japan og EU udpegede kommissionen for beskyttelse af personlige oplysninger EU som et tredjeland, der har indført et system til beskyttelse af personlige oplysninger, hvis standarder anerkendes som svarende til Japans med hensyn til beskyttelse af enkeltpersoners rettigheder og interesser på grundlag af artikel 24 i loven, og Europa-Kommissionen har samtidig besluttet, at Japan sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger i henhold til databeskyttelsesforordningens artikel 45.

Herved vil gensidig og smidig overførsel af personoplysninger mellem Japan og EU kunne foretages på en måde, der sikrer et højt niveau af beskyttelse af enkeltpersoners rettigheder og interesser. For at sikre dette høje beskyttelsesniveau for personlige oplysninger, der modtages fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og henset til at der på trods af den høje grad af konvergens mellem de to systemer er nogle relevante forskelle mellem dem, har kommissionen for beskyttelse af personlige oplysninger vedtaget disse supplerende regler på grundlag af lovens bestemmelser vedrørende gennemførelse mv. af samarbejde med myndighederne i andre lande og med henblik på at sikre passende håndtering af personlige oplysninger, som på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet modtages fra EU af en erhvervsdrivende, der håndterer personlige oplysninger, og den korrekte og effektive gennemførelse af de i sådanne regler fastsatte forpligtelser⁽¹⁾.

⁽¹⁾ Lovens artikel 4, 6, 8, 24, 60 og 78 og reglernes artikel 11.

Navnlig fastsættes der i lovens artikel 6 beføjelser til at træffe de nødvendige lovgivningsmæssige og øvrige foranstaltninger med henblik på at sikre den øgede beskyttelse af personlige oplysninger og konstruere et internationalt konsistent system vedrørende personlige oplysninger gennem strengere regler, som supplerer og er mere vidtgående end dem, der er fastlagt i loven og kabinetsbekendtgørelsen. Kommissionen for beskyttelse af personlige oplysninger har derfor, som den kompetente myndighed med hensyn til den overordnede forvaltning af loven, i medfør af lovens artikel 6 beføjelse til at indføre strengere regler ved at udarbejde nærværende supplerende regler, hvorved der fastsættes et højere beskyttelsesniveau for enkeltpersoners rettigheder og interesser vedrørende håndteringen af personoplysninger, der modtages fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, herunder med hensyn til definitionen af følsomme personlige oplysninger, jf. lovens artikel 2, stk. 3, og opbevarede personoplysninger, jf. lovens artikel 2, stk. 7 (herunder med hensyn til den relevante opbevaringsperiode).

På dette grundlag er de supplerende regler bindende for den erhvervsdrivende, der håndterer personlige oplysninger, som modtager personoplysninger, der overføres fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og pågældende er følgelig forpligtet til at overholde dem. Alle rettigheder og forpligtelser kan som retligt bindende regler håndhæves af kommissionen for beskyttelse af personlige oplysninger på samme måde som de af lovens bestemmelser, som de supplerer med strengere og/eller mere udførlige regler. I tilfælde af overtrædelse af de rettigheder og forpligtelser, som gælder i medfør af de supplerende regler, kan enkeltpersoner få prøvet deres sag ved domstolene på samme måde, som hvis der var tale om bestemmelser i loven, som de supplerer med strengere og/eller mere udførlige regler.

For så vidt angår kommissionen for beskyttelse af personlige oplysningers håndhævelse, har denne, såfremt en erhvervsdrivende, der håndterer personlige oplysninger, ikke overholder en eller flere forpligtelser i henhold til de supplerende regler, beføjelse til at træffe foranstaltninger i henhold til lovens artikel 42. Med hensyn til personlige oplysninger modtaget fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet vil det generelt, når en erhvervsdrivende, der håndterer personlige oplysninger, undlader at handle i overensstemmelse med en henstilling fremsat i henhold til lovens artikel 42, stk. 1, hvor dette sker uden angivelse af en legitime grunde⁽²⁾, blive betragtet som en alvorlig overtrædelse, der indebærer en overhængende fare for den enkeltes rettigheder og interesser, jf. lovens artikel 42, stk. 2.

1) Følsomme personlige oplysninger (lovens artikel 2, stk. 3)

Lovens artikel 2, stk. 3

3. »Følsomme personlige oplysninger« i denne lov forstås som personlige oplysninger såsom den berørtes race, tro, sociale status, sygdomshistorie, straffeattest, hvorvidt pågældende har lidt skader i forbindelse med en forbrydelse eller andre beskrivelser mv., som i henhold til en kabinetsbekendtgørelse er de beskrivelser, som kræver særlig håndtering, således at de ikke forårsager uretfærdig forskelsbehandling, fordomme eller andre ulemper for den berørte.

Kabinetsbekendtgørelsens artikel 2

De beskrivelser osv., som fastlægges i henhold til en kabinetsbekendtgørelse, jf. lovens artikel 2, stk. 3, er de beskrivelser mv., som indeholder ethvert af de forhold, der er fastsat i det følgende (undtaget dem, der hører under den berørtes sygdomshistorie eller strafferetlige forhold):

- i) det at have fysiske handicap, intellektuelle handicap, mentale handicap (herunder udviklingshandicap) eller andre fysiske og mentale funktionsnedsættelser som fastlagt i kommissionen for beskyttelse af personlige oplysningers regler
- ii) resultaterne af en lægeundersøgelse eller en andre undersøgelser (i det følgende nr. benævnt »lægeundersøgelse mv.«) til forebyggelse og tidlig opdagelse af en sygdom, som en læge eller en anden person, der varetager medicinske opgaver (i det følgende nr. benævnt »læge mv.«), foretager af den berørte
- iii) det forhold, at en berørt på grundlag af resultaterne af en lægeundersøgelse mv. eller på grund af sygdom, skade eller andre mentale eller fysiske ændringer af en læge mv. har modtaget vejledning med henblik på forbedring af sin mentale og fysiske tilstand eller medicinsk behandling eller en recept
- iv) Det forhold, at der er foretaget anholdelse, ransagning, beslaglæggelse, tilbageholdelse, indledt retsforfølgning eller andre procedurer i forbindelse med en straffesag mod den berørte som mistænkt eller tiltalt

⁽²⁾ Legitime grunde skal forstås som en begivenhed af ekstraordinær karakter uden for den erhvervsdrivende, der håndterer personlige oplysningers kontrol, som ikke med rimelighed har kunnet forudses (f.eks. naturkatastrofer), eller således at behovet for at træffe foranstaltninger med hensyn til en henstilling, der er fremsat af kommissionen for beskyttelse af personlige oplysninger i henhold til lovens artikel 42, stk. 1, ikke længere er til stede, fordi den erhvervsdrivende, der håndterer personlige oplysninger, har truffet alternative foranstaltninger, der fuldt ud afhjælper overtrædelser.

- v) det forhold, at en efterforskning, en foranstaltning med henblik på overvågning og beskyttelse, retsmøde og afgørelse, beskyttelsesforanstaltninger eller andre procedurer i forbindelse med en ungdomsbeskyttelsessag er iværksat eller truffet over for en berørt som ungdomskriminel eller som mistænkt herfor, jf. artikel 3, stk. 1, i loven om ungdomskriminelle.

Reglernes artikel 5

De fysiske og mentale handicap, som fastlægges i kommissionen for beskyttelse af personlige oplysningers regler, jf. artikel 2, nr. i), i bekendtgørelsen, er de i det følgende anførte handicap:

- i) fysiske handicap fastlagt i en vedlagt tabel i lov om velfærd for personer med fysiske handicap (lov nr. 283 af 1949)
- ii) intellektuelle handicap som omhandlet i lov om velfærd for personer med intellektuelle handicap (lov nr. 37 af 1960)
- iii) mentale handicap omhandlet i lov om mental sundhed og velfærd for personer med mentale handicap (lov nr. 123 af 1950) (herunder udviklingshandicap, jf. artikel 2, stk. 1, i lov om støtte til personer med udviklingshandicap, og undtaget intellektuelle handicap i henhold til lov om velfærd for personer med intellektuelle handicap)
- iv) en sygdom uden helbredelsesmetoder eller andre særlige sygdomme, hvis alvorlighed som fastlagt ved kabinetsbekendtgørelse i henhold til artikel 4, stk. 1, i lov om støtte til hverdagslivet og et socialt liv for personer med handicap (lov nr. 123 af 2005) svarer til den, der er fastlagt af ministeren for sundhed, arbejde og velfærd i henhold til nævnte stykke.

Hvis personoplysninger modtaget fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet indeholder oplysninger vedrørende en fysisk persons sexliv, seksuelle orientering eller fagforeningsmedlemskab, der er defineret som særlige kategorier af personoplysninger i databeskyttelsesforordningen, skal erhvervsdrivende, der håndterer personlige oplysninger, behandle disse på samme måde som følsomme personlige oplysninger i den i artikel 2, stk. 3, i loven anvendte betydning.

2) Opbevarede personoplysninger (lovens artikel 2, stk. 7).

Lovens artikel 2, stk. 7

7. »Opbevarede personoplysninger« i denne lov forstås som personlige oplysninger, som en erhvervsdrivende, der håndterer personlige oplysninger, har beføjelse til at videregive, rette, ændre eller slette indholdet af, indstille videregivelsen til tredjemand og anvendelsen af samt at slette, og der er hverken tale om de informationer, som i henhold til en kabinetsbekendtgørelse er potentielt til skade for offentlige eller andre interesser, hvis deres tilstedeværelse eller fravær bliver kendt, eller hvis sletning skal finde sted inden for en ved en kabinetsbekendtgørelse fastlagt periode på højst et år.

Kabinetsbekendtgørelsens artikel 4

De i henhold til lovens artikel 2, stk. 7, ved kabinetsafgørelse fastlagte informationer er følgende.

- i) dem, hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, potentielt vil være til skade for en berørt eller tredjemands liv, legeme eller formue
- ii) dem, hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, potentielt vil opmuntre eller foranledige til en ulovlig eller uretmæssig handling
- iii) dem, hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, muligvis vil undergrave den nationale sikkerhed, ødelægge et tillidsforhold til et andet land eller en international organisation, eller have ugunstig virkning i forhandlinger med et andet land eller en international organisation
- iv) dem, hvor det, såfremt disse personoplysningers tilstedeværelse eller fravær bliver kendt, muligvis vil være til hinder for opretholdelsen af den offentlige sikkerhed og orden, f.eks. forebyggelsen, bekæmpelsen og efterforskningen af kriminalitet.

Kabinetsbekendtgørelsens artikel 5

Den i henhold til lovens artikel 2, stk. 7, ved kabinetsbekendtgørelse fastlagte periode er seks måneder.

Personoplysninger modtaget fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet skal håndteres som opbevarede personoplysninger i den i artikel 2, stk. 7, i APPI anvendte betydning, uanset om sletningen skal finde sted efter en fastlagt periode.

Hvis personoplysninger modtaget fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet omfattes af de personoplysninger, som i henhold til en kabinetsbekendtgørelse er »potentielt til skade for offentlige eller andre interesser, hvis deres tilstedeværelse eller fravær bliver kendt«, skal sådanne oplysninger behandles som personoplysninger (jf. kabinetsbekendtgørelsens artikel 4; retningslinjer til de generelle regler, »2.-7. Opbevarede personoplysninger«).

- 3) Præcisering af et anvendelsesformål, begrænsning som følge af et anvendelsesformål (lovens artikel 15, stk. 1, artikel 16, stk. 1, og artikel 26, stk. 1 og 3)

Lovens artikel 15, stk. 1

1. En erhvervsdrivende, der håndterer personlige oplysninger, skal i forbindelse med håndteringen af personlige oplysninger specificere formålet med at anvende de personlige oplysninger (herefter »anvendelsesformål«) så udføreligt som muligt.

Lovens artikel 16, stk. 1

1. En erhvervsdrivende, der håndterer personlige oplysninger, må ikke uden på forhånd at indhente den berørtes samtykke håndtere personlige oplysninger, ud over hvad der er nødvendigt for at opnå et anvendelsesformål som fastlagt i bestemmelserne i foregående artikel.

Lovens artikel 26, stk. 1 og 3

1. En erhvervsdrivende, der håndterer personlige oplysninger, skal ved modtagelsen af personoplysninger fra tredje-mand, bekræfte nedenstående forhold i henhold til kommissionen for beskyttelse af personlige oplysningers regler. (udeladt)
- i) (udeladt)
- ii) de omstændigheder, hvorunder pågældende tredjemand erhvervede personoplysningerne
3. En erhvervsdrivende, der håndterer personlige oplysninger, skal efter at have foretaget bekræftelsen i henhold til stk. 1, i henhold til kommissionen for beskyttelse af personlige oplysningers regler registrere datoen for modtagelsen af personoplysningerne, omstændighederne vedrørende nævnte bekræftelse, og andre forhold fastlagt i kommissionen for beskyttelse af personlige oplysningers regler.

Hvis erhvervsdrivende håndterer personlige oplysninger, ud over hvad der er nødvendigt for at opnå et anvendelsesformål som fastlagt i lovens artikel 15, stk. 1, skal de på forhånd indhente den berørtes samtykke (lovens artikel 16, stk. 1) Ved modtagelsen af personoplysningerne fra tredjemand skal erhvervsdrivende, der håndterer personlige oplysninger, i henhold til reglerne bekræfte forhold som f.eks. de omstændigheder, hvorunder pågældende tredjemand erhvervede personoplysningerne, og registrere disse forhold (lovens artikel 26, stk. 1 og 3).

Dersom en erhvervsdrivende, der håndterer personlige oplysninger, modtager personoplysninger fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, omfatter omstændighederne vedrørende erhvervelsen af personoplysningerne, som skal bekræftes og registreres i henhold til artikel 26, stk. 1 og 3, det anvendelsesformål, som oplysningerne blev modtaget til fra EU.

Dersom en erhvervsdrivende, der håndterer personlige oplysninger, fra en anden erhvervsdrivende, der håndterer personlige oplysninger, modtager personoplysninger, som tidligere er overført fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, da omfatter omstændighederne vedrørende erhvervelsen af personoplysningerne, som bekræftes og registreres i henhold til artikel 26, stk. 1 og 3, ligeledes anvendelsesformålet, som oplysningerne blev modtaget til.

I ovennævnte tilfælde skal den erhvervsdrivende, der håndterer personlige oplysninger, specificere formålet med at anvende de nævnte personoplysninger inden for rammerne af anvendelsesformålet, således som dette er bekræftet og registreret i henhold til lovens artikel 26, stk. 1 og 3, og anvende oplysningerne inden for de nævnte rammer (som fastlagt ved lovens artikel 15, stk. 1, og artikel 16, stk. 1).

4) Begrænsning af videregivelsen til tredjemand i et tredjeland (lovens artikel 24; reglernes artikel 11-2)

Lovens artikel 24

En erhvervsdrivende, der håndterer personlige oplysninger, undtagen i de i foregående artikel, stk. 1, fastlagte tilfælde, skal ved videregivelse af personoplysninger til tredjemand (hertil medregnes ikke personer, som har etableret et system i overensstemmelse med standarder, der i henhold til kommissionen for beskyttelse af personlige oplysningers regler er nødvendige for løbende at træffe foranstaltninger svarende til dem, som en erhvervsdrivende, der håndterer personlige oplysninger, skal træffe vedrørende håndteringen af personoplysninger, jf. bestemmelserne i dette afsnit; herefter forstås det samme i denne artikel) i et tredjeland (dvs. et land eller en region uden for Japans område; herefter forstås det samme) (hertil medregnes ikke dem, som i henhold til kommissionen for beskyttelse af personlige oplysningers regler er tredjelande, der har indført et system til beskyttelse af personlige oplysninger, hvis standarder anerkendes som svarende til Japans med hensyn til beskyttelse af enkeltpersoners rettigheder og interesser; herefter forstås det samme i denne artikel) på forhånd indhentede den berørtes samtykke med henblik på dennes godkendelse af videregivelsen til en tredjemand i et tredjeland. I så fald finder bestemmelserne i den foregående artikel ikke anvendelse.

Reglernes artikel 11-2

Standarderne ifølge kommissionen for beskyttelse af personlige oplysningers regler i henhold til lovens artikel 24 henhører under hvert af nedenstående tilfælde.

- i) en erhvervsdrivende, der håndterer personlige oplysninger, og en person, der modtager personoplysninger, har i forbindelse med den pågældende modtagers håndtering af personoplysningerne sikret gennemførelsen af foranstaltninger i overensstemmelse med hovedindholdet i bestemmelserne i lovens kapitel IV, afsnit 1, via en passende og rimelig metode
- ii) en person, der modtager personoplysninger, har opnået en anerkendelse baseret på en international ramme for behandling af personlige oplysninger.

En erhvervsdrivende, der håndterer personlige oplysninger, skal, i de tilfælde hvor denne har videregivet personoplysninger til tredjemand i et tredjeland, som den erhvervsdrivende har modtaget fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, på forhånd indhentede den berørtes samtykke med henblik på dennes godkendelse af videregivelsen til en tredjemand i et tredjeland, jf. lovens artikel 24, efter at den berørte har fået oplysninger om omstændighederne i forbindelse med overførslen, således at det er muligt for denne at træffe sin samtykkebeslutning, undtagen i de tilfælde, der falder ind under følgende fra i) til iii).

- i) hvis tredjemanden befinder sig i et land, som i henhold til reglerne er et tredjeland, der har indført et system til beskyttelse af personlige oplysninger, hvis standarder anerkendes som svarende til Japans med hensyn til beskyttelse af enkeltpersoners rettigheder og interesser
- ii) hvis en erhvervsdrivende, der håndterer personlige oplysninger, og tredjemanden, som modtager personoplysningerne, i forbindelse med tredjemandens håndtering af personoplysningerne, sammen har gennemført foranstaltninger, der sikrer et beskyttelsesniveau svarende til lovens sammenholdt med reglerne, via en passende og rimelig metode (dvs. en kontrakt, andre former for bindende aftaler eller bindende ordninger inden for en koncern).
- iii) i tilfælde, der falder ind under lovens artikel 23, stk. 1.

5) Anonymt behandlede oplysninger (lovens artikel 2, stk. 9, og artikel 36, stk. 1 og 2)

Lovens artikel 2, stk. 9

- 9. »Anonymt behandlede oplysninger« i denne lov betyder oplysninger vedrørende en person, som fremkommer ved behandlingen af personlige oplysninger, således at det hverken er muligt at identificere en bestemt person som foreskrevet i hvert af følgende numre i overensstemmelse med opdelingerne af personlige oplysninger deri, eller at genskabe de personlige oplysninger.

- i) personlige oplysninger, der falder ind under stk. 1, nr. i);

sletning af en del af de beskrivelser mv., som er indeholdt i de pågældende personlige oplysninger (herunder erstatning af den pågældende del af beskrivelserne mv. med andre beskrivelser mv. ved hjælp af en metode uden regelbundethed, der umuliggør genskabelse af den pågældende del af beskrivelserne mv.)

- ii) personlige oplysninger, der falder ind under stk. 1, nr. ii);

sletning af alle de individuelle identifikationskoder, som er indeholdt i de pågældende personlige oplysninger (herunder erstatning af de pågældende individuelle identifikationskoder med andre beskrivelser mv. ved hjælp af en metode uden regelbundethed, der umuliggør genskabelsen af pågældende individuelle identifikationskode)

Lovens artikel 36, stk. 1

1. En erhvervsdrivende, der håndterer personlige oplysninger, som genererer anonymt behandlede oplysninger« (begrænset til dem, der udgør databaser over anonymt behandlede oplysninger mv.; herefter forstås det samme), skal behandle personlige oplysninger i overensstemmelse med de standarder, der i kommissionen for beskyttelse af personlige oplysningers regler er fastlagt som nødvendige for at gøre det umuligt at identificere en bestemt person eller genskabe de personlige oplysninger.

Reglernes artikel 19

De standarder, der er i henhold til lovens artikel 36, stk. 1, fastlægges ved kommissionen for beskyttelse af personlige oplysningers regler er følgende.

- i) sletning af helheden eller dele af beskrivelser mv., hvormed man kan identificere en bestemt person i de personlige oplysninger (herunder erstatning af sådanne beskrivelser mv. med andre beskrivelser mv. ved hjælp af en metode uden regelbundethed, der umuliggør genskabelse af helheden eller dele af beskrivelser mv.)
- ii) sletning af alle de individuelle identifikationskoder i de pågældende personlige oplysninger (herunder erstatning af sådanne koder med andre beskrivelser mv. ved hjælp af en metode uden regelbundethed, der umuliggør genskabelsen af de individuelle identifikationskoder)
- iii) sletning af de koder (begrænset til de koder, der gensidigt forbinder flere oplysninger, som faktisk håndteres af en erhvervsdrivende, der håndterer personlige oplysninger), som forbinder personlige oplysninger og oplysninger fremkommet ved at have truffet foranstaltninger med hensyn til de personlige oplysninger (herunder erstatning af de pågældende koder med andre koder, der ikke kan forbinde de nævnte personlige oplysninger og oplysninger fremkommet via foranstaltninger med hensyn til de nævnte personlige oplysninger, ved hjælp af en metode uden regelbundethed, der umuliggør genskabelse af pågældende identifikationskoder)
- iv) sletning af særegne beskrivelser mv. (herunder erstatning af sådanne beskrivelser mv. med andre beskrivelser mv. ved hjælp af en metode uden regelbundethed, der umuliggør genskabelse af de særegne beskrivelser mv.)
- v) ud over de i hvert foregående nummer omhandlede foranstaltninger også iværksættelse af foranstaltninger på grundlag af resultaterne af vurderingen af attributter mv. for databaser mv. med personlige oplysninger, f.eks. forskelle mellem beskrivelser mv. indeholdt i personlige oplysninger og beskrivelser mv. indeholdt i andre personlige oplysninger, der udgør databasen over personlige oplysninger mv., som omfatter nævnte personlige oplysninger.

Lovens artikel 36, stk. 2

2. En erhvervsdrivende, der håndterer personlige oplysninger og har genereret anonymt behandlede oplysninger, skal i overensstemmelse med standarder, der i henhold til kommissionen for beskyttelse af personlige oplysningers regler er fastlagt som nødvendige for at forhindre læk af oplysninger vedrørende sådanne beskrivelser mv. og af individuelle identifikationskoder slettet fra personlige oplysninger, som er blevet anvendt til at generere de anonymt behandlede oplysninger, samt oplysninger vedrørende en anvendt behandlingsmetode i henhold til bestemmelserne i foregående stykke, træffe foranstaltninger med henblik på sikkerhedskontrollen for sådanne oplysninger.

Reglernes artikel 20

De standarder, der er i henhold til lovens artikel 36, stk. 2, fastlægges ved kommissionen for beskyttelse af personlige oplysningers regler er følgende.

- i) klar fastlæggelse af myndigheden og ansvaret for en person, der håndterer personlige oplysninger vedrørende de beskrivelser mv. og de individuelle identifikationskoder, som er blevet slettet fra personlige oplysninger anvendt til at generere anonymt behandlede oplysninger, samt oplysningerne vedrørende en anvendt behandlingsmetode i henhold til bestemmelserne i artikel 36, stk. 1 (begrænset til dem, som kan genskabe de personlige oplysninger ved hjælp af sådanne relaterede oplysninger) (i denne artikel herefter »oplysninger vedrørende behandlingsmetoden mv.«)
- ii) fastlæggelse af regler og procedurer for håndtering af oplysninger vedrørende behandlingsmetoden mv., korrekt håndtering af oplysninger vedrørende behandlingsmetoden mv. i overensstemmelse med reglerne og procedurerne, evaluering af håndteringssituationen og på grundlag af resultaterne heraf iværksættelse af de nødvendige foranstaltninger med henblik på forbedring
- iii) iværksættelse af nødvendige og passende foranstaltninger med henblik på at forhindre en person uden legitim myndighed i at håndtere oplysninger vedrørende behandlingsmetoden

Personlige oplysninger, der modtages fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, betragtes kun som anonymt behandlede personlige oplysninger i den i lovens artikel 2, stk. 9, anvendte betydning, hvis den erhvervsdrivende, der håndterer personlige oplysninger, træffer foranstaltninger, som gør fornyet identifikation af den enkelte umulig for alle, herunder ved at slette oplysninger vedrørende behandlingsmetoden m.v. (dvs. oplysninger vedrørende de beskrivelser mv. og de individuelle identifikationskoder, som er blevet slettet fra personlige oplysninger anvendt til at generere anonymt behandlede oplysninger, samt oplysningerne vedrørende en anvendt behandlingsmetode i henhold til bestemmelserne i artikel 36, stk. 1 (begrænset til dem, som kan genskabe de personlige oplysninger ved hjælp af sådanne relaterede oplysninger)).

BILAG 2

Hendes Excellence Věra Jourová, kommissær for retlige anliggender, forbrugere og ligestilling mellem mænd og kvinder i Europa-Kommissionen

Deres Excellence

Jeg glæder mig over de konstruktive drøftelser mellem Japan og Kommissionen, der har til formål at skabe rammerne for gensidig overførsel af personoplysninger mellem Japan og EU.

Efter anmodning fra Kommissionen til Japans regering sender jeg hermed et dokument, der giver et overblik over de retlige rammer for de japanske myndigheders adgang til oplysninger.

Dette dokument vedrører mange ministerier og myndigheder i Japan, og for så vidt angår dokumentets indhold er de relevante ministerier og myndigheder (kabinetssekretariatet, det nationale politiagentur, kommissionen for beskyttelse af personlige oplysninger, ministeriet for interne anliggender og kommunikation, justitsministeriet, efterretningsagenturet for offentlig sikkerhed, forsvarsministeriet) ansvarlige for de passager, der falder inden for deres respektive kompetenceområder. De relevante ministerier og myndigheder er anført nedenfor.

Kommissionen for beskyttelse af personlige oplysninger modtager alle spørgsmål vedrørende dette dokument og koordinerer eventuelle besvarelser fra de relevante ministerier og myndigheder.

Jeg håber, at dette dokument vil være nyttigt med henblik på Europa-Kommissionens beslutningstagning.

Jeg sætter pris på det store bidrag, De har ydet i dette spørgsmål.

Med venlig hilsen

Yoko KAMIKAWA

Justitsminister

Dette dokument er udarbejdet af justitsministeriet og følgende berørte ministerier og myndigheder:

Koichi HAMANO

Rådgiver, kabinetssekretariatet

Schunichi KURYU

Kommissær for det nationale politiagentur

Mari SONODA

Generalsekretær for kommissionen for beskyttelse af personlige oplysninger

Mitsuru YASUDA

Viceminister, ministeriet for interne anliggender og kommunikation

Seimei NAKAGAWA

Efterretningsagenturet for offentlig sikkerhed

Kenichi TAKAHASHI

Administrativ viceforsvarsminister

14. september 2018

De japanske offentlige myndigheders indsamling og brug af personlige oplysninger med henblik på retshåndhævelse på det strafferetlige område og national sikkerhed

Følgende dokument indeholder et overblik over de retlige rammer for japanske offentlige myndigheders indsamling og anvendelse af personlige (elektroniske) oplysninger med henblik på retshåndhævelse på det strafferetlige område og national sikkerhed (herefter »myndighedsadgang«), navnlig med hensyn til det relevante retsgrundlag, gældende betingelser (begrænsninger) og garantier, herunder uafhængigt tilsyn og prøvelsesmuligheder for den enkelte. Denne fremstilling er rettet til Europa-Kommissionen for at give tilsagn og forsikre om, at myndighedsadgangen til personlige oplysninger overført fra EU til Japan vil være begrænset til, hvad der er nødvendigt og forholdsmæssigt, underlagt uafhængigt tilsyn, og at berørte personer vil kunne klage eller gå til domstolene i tilfælde af eventuelle overtrædelser af deres grundlæggende ret til privatliv og databeskyttelse. I medfør af denne fremstilling oprettes der ligeledes en ny prøvelsesmekanisme under forvaltning af kommissionen for beskyttelse af personlige oplysninger (PPC), og denne skal håndtere klager fra personer fra EU vedrørende myndighedsadgang til deres personoplysninger, som er blevet overført fra EU til Japan.

I. De generelle retsprincipper, der er relevante for myndighedsadgang

Som en udøvelse af offentlig myndighed skal myndighedsadgang finde sted i fuld overensstemmelse med loven (legalitetsprincippet). I Japan er personlige oplysninger beskyttet både i den private og offentlige sektor via en mekanisme med flere niveauer.

A. Forfatningsmæssige rammer og legalitetsprincippet

Forfatningens artikel 13 og retspraksis anerkender retten til privatlivets fred som en forfatningssikret ret. I den forbindelse har højesteret fastslået, at det er naturligt, at enkeltpersoner ikke ønsker, at andre skal kende deres personlige oplysninger uden god grund, og denne forventning skal beskyttes⁽¹⁾. Yderligere beskyttelse findes i forfatningens artikel 21, stk. 2, som sikrer meddeleleshemmeligheden, og artikel 35, som garanterer retten til ikke at blive udsat for ransagning og beslaglæggelse uden retskendelse, således at indsamling af personlige oplysninger, herunder adgang, via tvangsindgreb altid skal finde sted på grundlag af en kendelse. En sådan kendelse kan kun udstedes med henblik på efterforskning af allerede begåede forbrydelser. De retlige rammer i Japan tillader således ikke indsamling af oplysninger ved tvangsindgreb med henblik på national sikkerhed (som ikke er en strafferetlig efterforskning).

I overensstemmelse med legalitetsprincippet skal indsamling af oplysninger ved tvangsindgreb derudover have særlig lovhjemmel. I tilfælde indsamling, der ikke foregår ved tvangsindgreb/er frivillig, skal oplysningerne indhentes fra en kilde, som der er fri adgang til, eller modtages på grundlag af en anmodning om frivillig videregivelse, dvs. en anmodning, der ikke kan håndhæves over for den fysiske eller juridiske person, som har oplysningerne. Dette er imidlertid kun tilladt i det omfang den offentlige myndighed har beføjelse til at foretage undersøgelsen, eftersom hver enkelt offentlig myndighed kun kan handle indenfor sin administrative jurisdiktion i henhold til lovgivningen (uanset om myndighedens handlinger griber inde i den enkeltes rettigheder eller friheder eller ej). Dette princip finder anvendelse på myndighedens evne til at indsamle personlige oplysninger.

B. Særlige regler om beskyttelse af personlige oplysninger

Loven om beskyttelse af personlige oplysninger (APPI) og Loven om beskyttelse af personlige oplysninger i administrative organer (APPIHAO), som bygger på og udbygger bestemmelserne i forfatningen, sikrer retten til personlige oplysninger i både den private og offentlig sektor.

I medfør af artikel 7 i APPI skal PPC udarbejde den »grundlæggende politik om beskyttelse af personlige oplysninger« (grundlæggende politik). Den grundlæggende politik, der vedtages ved afgørelse truffet af det japanske regeringskabinet som det centrale organ for den japanske regering (statsministeren og ministrene), fastsætter retningen for beskyttelsen af personlige oplysninger i Japan. PPC, der er en uafhængig tilsynsmyndighed, fungerer således som »kommandocentralen« i Japans system for beskyttelse af personlige oplysninger.

Når administrative organer indsamler oplysninger, uanset om dette sker ved tvangsindgreb, skal de i princippet⁽²⁾ overholde kravene i APPIHAO. APPIHAO er en generel lov, som finder anvendelse på den behandling af »opbevarede personlige oplysninger«⁽³⁾ i »administrative organer« (som defineret i artikel 2, stk. 1, i APPIHAO). Den omfatter derfor

⁽¹⁾ Højesteret, dom af 12. september 2003 (2002 (Ju) nr. 1656).

⁽²⁾ For undtagelser med hensyn til kapitel 4 i APPIHAO, se side 16 nedenfor.

⁽³⁾ »Opbevarede personlige oplysninger« forstås ifølge artikel 2, stk. 5, i APPIHAO som personlige oplysninger udarbejdet eller indhentet af en ansat i et administrativt organ i forbindelse med udøvelsen af dennes pligter, der opbevares af dette administrative organ til organisatorisk brug for de ansatte.

også behandlingen af oplysninger inden for retshåndhævelsen på det strafferetlige område og området national sikkerhed. Blandt de offentlige myndigheder, der er bemyndiget til at gennemføre offentlig adgang, er alle myndigheder (undtagen præfekturpolitiet) nationale myndigheder, som falder ind under definitionen »administrative organer«. Præfekturpolitiets håndtering af personlige oplysninger finder sted i henhold til præfekturbekendtgørelser⁽⁴⁾, hvori der fastlægges principper til beskyttelse af personlige oplysninger og rettigheder og pligter svarende til APPIHAO's.

II. Myndighedsadgang med henblik på retshåndhævelse på det strafferetlige område

A. Retsgrundlag og begrænsninger

1) Indsamling af personlige oplysninger ved tvangsindgreb

a) Retsgrundlag

I henhold til forfatningens artikel 35 er retten til beskyttelse af boligen, dokumenter og ejendele mod adgang, ransagninger og beslaglæggelse ukrænkelig, undtagen ved en retskendelse afsagt på et »tilstrækkeligt grundlag«, som særligt beskriver stedet for ransagningen og de genstande, som skal beslaglægges. Følgelig kan offentlige myndigheders indsamling af oplysninger indhentet ved tvangsindgreb i forbindelse med en strafferetlig efterforskning kun finde sted på grundlag af en retskendelse. Dette gælder både indsamlingen af elektroniske fortegnelser, som indeholder (personlige) oplysninger, og aflytning af kommunikation. Den eneste undtagelse til denne regel (som imidlertid ikke er relevant i forbindelse med en elektronisk overførsel af personlige oplysninger fra udlandet) er strafferetsplejelovbogens artikel 220, stk. 1⁽⁵⁾, ifølge hvilken anklagemyndigheden eller politiet ved anholdelsen af en åbenlys lovovertræder om nødvendigt kan foretage ransagning og beslaglæggelse »på stedet for anholdelsen«.

I henhold til strafferetsplejelovbogens artikel 197, stk. 1, må tvangsindgreb i efterforskningen »ikke anvendes, medmindre særlige bestemmelser herom er fastsat i denne lovbog«. Med hensyn til offentlige myndigheders indsamling af elektroniske oplysninger ved tvangsindgreb er det relevante retsgrundlag strafferetsplejelovbogens artikel 218, stk. 1, (hvorefter anklagemyndigheden eller politiet, hvis det er nødvendigt for efterforskningen af et strafbart forhold, kan foretage ransagning eller beslaglæggelse på grundlag af en retskendelse) og artikel 222-2 (hvorefter tvangsindgreb med henblik på at opfange elektronisk kommunikation uden samtykke fra nogen af parterne skal gennemføres på grundlag af anden lovgivning). Sidstnævnte bestemmelse henviser til loven om aflytning i forbindelse med strafferetlig efterforskning (»aflytningsloven«), hvori der i artikel 3, stk. 1, fastlægges de betingelser, hvorunder meddelelser vedrørende alvorlige forbrydelser kan aflyttes på grundlag af en aflytningskendelse⁽⁶⁾.

For så vidt angår politiet ligger beføjelsen til at efterforske i alle tilfælde hos præfekturpolitiet, mens det nationale politiaгентur ikke foretager nogen strafferetlige efterforskninger, jf. strafferetsplejelovbogen.

b) Begrænsninger

Indsamlingen af elektroniske oplysninger ved tvangsindgreb begrænses af forfatningen og bemyndigende forskrifter, således som fortolket i retspraksis, som navnlig fastlægger de kriterier, som domstolene skal anvende ved afsigelse af kendelser. Ved APPIHAO pålægges desuden en række begrænsninger med hensyn til både indsamlingen og håndteringen af oplysninger (mens lokale bekendtgørelser mere eller mindre indeholder de samme kriterier for præfekturpolitiet).

1) Begrænsninger som følger af forfatningen og den bemyndigende forskrift

I henhold til strafferetsplejelovbogens artikel 197, stk. 1, må tvangsindgreb »ikke anvendes, medmindre særlige bestemmelser herom er fastsat i denne lovbog«. I strafferetsplejelovbogens artikel 218, stk. 1, fastslås efterfølgende, at beslaglæggelse mv. kræver en retskendelse og kun må foretages, »hvis det er nødvendigt for efterforskningen af et strafbart

⁽⁴⁾ Hvert præfektur har sit egen »præfekturbekendtgørelse«, der gælder for præfekturpolitiets beskyttelse af personlige oplysninger. Der findes ingen oversættelse til engelsk for disse præfekturbekendtgørelser.

⁽⁵⁾ I henhold til strafferetsplejelovbogens artikel 220, stk. 1, kan anklagemyndigheden eller politiet ved anholdelsen af en mistænkt om nødvendigt træffe følgende foranstaltninger: a) indtrængen på en andens bopæl osv. med henblik på eftersøgning af mistænkte; b) ransagning, beslaglæggelse eller inspektion på stedet for anholdelsen.

⁽⁶⁾ Denne bestemmelse forskriver nærmere bestemt at »anklagemyndigheden eller politiet kan aflytte telekommunikation relateret til forbrydelser, såfremt et af følgende forhold gør sig gældende: hvis der er tilstrækkeligt begrundet mistanke om, at telekommunikation finder sted om emner vedrørende begåelsen af en forbrydelse (de forbrydelser, der er fastlagt i ii) og iii)), planlægning med hensyn til forberedelsen af en forbrydelse, handlinger som f.eks. destruktion af bevismateriale efter en begået forbrydelse, eller instruktioner, andre interaktioner eller begåelsen af andre førnævnte forbrydelser (herefter »forbrydelsesrelateret telekommunikation«), og det er særligt vanskeligt at udrede detaljerne eller status for en forbrydelse eller at identificere de kriminelle ved hjælp af andre metoder, hvis telekommunikationsmetoden (herefter »telekommunikationsmetoden«) angives via numre og symboler (herefter »telefonnumre«) til at identificere telefonnumre eller dem, der foretager eller modtager opkald, og mistænkte anvender den på grundlag af kontrakter med teleselskaber (herfra undtaget tilfælde hvor der ikke fastslås nogen mistanke om, at metoden bruges til forbrydelsesrelateret telekommunikation af kriminelle), eller hvis der er tilstrækkeligt grundlag for en mistanke om, at kriminelle anvender telekommunikationsmetoden til forbrydelsesrelateret telekommunikation«.

forhold«. Selv om kriterierne for bedømmelsen af nødvendigheden ikke præciseres yderligere i den relevante lovgivning, har højesteret⁽⁷⁾ fastslået, at retten skal foretage en overordnet vurdering under hensyntagen til navnlig følgende elementer:

- a) alvoren af lovovertrædelsen, og hvordan den blev begået
- b) værdien og betydningen af de materialer, som skal beslaglægges som bevismateriale
- c) sandsynligheden for, at beslaglagte materialer skjules eller destrueres
- d) omfanget af ulemperne som følge af beslaglæggelsen
- e) andre relaterede betingelser.

Begrænsningerne følger også af kravet i forfatningens artikel 35 om, at der skal være et »tilstrækkeligt grundlag«. I henhold til standarden om »tilstrækkeligt grundlag« kan der afsiges kendelser, såfremt: [1] Der er behov for en strafferetlig efterforskning (jf. ovennævnte højesteretsdom af. marts 18, 1969 (1968 (Shi) nr. 100)), [2] der er en situation, hvor den mistænkte (den tiltalte) anses for at have begået en strafbar handling (strafferetsplejereglerne artikel 156, stk. 1)⁽⁸⁾ [3] kendelsen vedrørende efterforskning med hensyn til legeme, genstande, bopæl eller enhver anden person end den anklagedes bopæl, bør kun afsiges, når det er rimeligt at antage, at genstandene, der skal beslaglægges, eksisterer (strafferetsplejelovbogens artikel 102, stk. 2). Når retten finder, at det af efterforskningsmyndighedernes fremlagte bevismateriale ikke udgør et tilstrækkeligt grundlag for en mistanke om en forbrydelse, afslås anmodningen om en kendelse. Det skal i den forbindelse bemærkes, at »forberedelse med henblik på at begå« en planlagt forbrydelse henhold til loven om straf for organiseret kriminalitet og forvaltning af udbytte fra strafbare handlinger (f.eks. fremskaffelse af penge i forbindelse med terrorforbrydelser) i sig selv udgør en forbrydelse og således kan være genstand for efterforskning ved tvangsindgreb på grundlag af en retskendelse.

Endelig gælder, at såfremt kendelsen vedrører efterforskningen med hensyn til legeme, genstande, bopæl eller enhver anden person end den anklagedes bopæl, bør den kun afsiges, når det er rimeligt at antage, at genstandene, der skal beslaglægges, eksisterer (strafferetsplejelovbogens artikel 102, stk. 2, og artikel 222, stk. 1)

Hvad nærmere angår aflytningen af kommunikation med henblik på strafferetlig efterforskning baseret på aflytningsloven, bør en sådan kun foretages, når de strenge krav i dennes artikel 3, stk. 1, er opfyldt. Ifølge denne bestemmelse kræver aflytningen altid på forhånd en retskendelse, og denne må kun afsiges i et begrænset antal situationer⁽⁹⁾.

2) Begrænsninger som følger af APPIHAO

For så vidt angår administrative organers indsamling⁽¹⁰⁾ og videre håndtering (herunder navnlig opbevaring, forvaltning og anvendelse) af personlige oplysninger er der i APPIHAO navnlig fastsat følgende begrænsninger:

- a) I henhold til artikel 3, stk. 1, i APPIHAO kan administrative organer kun opbevare personlige oplysninger, når opbevaringen er nødvendig for at varetage de opgaver, som hører under deres kompetence i henhold til love og forskrifter. I forbindelse med opbevaringen skal de også (i videst muligt omfang) angive formålet med anvendelsen af personlige oplysninger. I henhold til artikel 3, stk. 2 og 3, i APPIHAO må administrative organer ikke opbevare personlige oplysninger ud over, hvad der er nødvendigt for at opfylde det således angivne formål med anvendelsen, og de må ikke ændre formålet med anvendelsen ud over, hvad der med rimelighed kan betragtes som relevant i forhold til det oprindelige formål.
- b) I henhold til artikel 5 i APPIHAO skal chefen for et administrativt organ bestræbe sig på at sikre, at de opbevarede personlige oplysninger er korrekte og ajourførte i det omfang, det er nødvendigt for at opfylde formålet med anvendelsen.
- c) I henhold til artikel 6, stk. 1, i APPIHAO skal chefen for et administrativt organ træffe de foranstaltninger, der er nødvendige for at forebygge læk, tab eller skade og for at sikre korrekt forvaltning af de opbevarede personlige oplysninger.
- d) I henhold til artikel 7 i APPIHAO må ingen (herunder tidligere) ansatte videregive erhvervede personlige oplysninger til en anden person uden forsvarlig grund eller anvende sådanne oplysninger til et urimeligt formål.

⁽⁷⁾ Dom af 18. marts 1969 (1968 (Shi) nr. 100).

⁽⁸⁾ Strafferetsplejereglerne artikel 156, stk. 1, fastsætter: »Ved indgivelse af den anmodning, der er omhandlet i stk. 1, fremlægger den anmodende part materialer, på hvis grundlag den mistænkte eller anklagede må anses at have begået en strafbar handling«.

⁽⁹⁾ Se fodnote 6.

⁽¹⁰⁾ Artikel 3, stk. 1 og 2, i APPIHAO begrænser omfanget af opbevaring og dermed også indsamlingen af personlige oplysninger.

- e) Endvidere er det i artikel 8, stk. 1, i APPIHAO fastsat, at chefen for et administrativt organ ikke må anvende opbevarede personlige oplysninger eller videregive sådanne oplysninger til en anden person til andre formål end det angivne anvendelsesformål, medmindre andet er fastsat i love og forskrifter. Selv om artikel 8, stk. 2, indeholder undtagelser fra denne regel i særlige situationer, finder disse kun anvendelse, hvis det er meget lidt sandsynligt, at en sådan ekstraordinær videregivelse vil medføre »uretmæssig« skade for den registreredes eller tredjemands rettigheder og interesser.
- f) I henhold til artikel 9 i APPIHAO skal chefen for et administrativt organ om nødvendigt indføre begrænsninger vedrørende anvendelsesformålet eller -metoden eller andre nødvendige begrænsninger, såfremt personlige oplysninger videregives til en anden person; vedkommende kan også anmode modtageren om at træffe de foranstaltninger, der er nødvendige for at forebygge læk og sikre korrekt forvaltning af oplysningerne.
- g) I henhold til artikel 48 i APPIHAO skal chefen for et administrativt organ bestræbe sig på at behandle klager over håndteringen af personlige oplysninger korrekt og hurtigt.

2) Indsamling af personlige oplysninger gennem anmodninger om frivilligt samarbejde (frivillig undersøgelse)

a) Retsgrundlag

Ud over ved tvangsindgreb indhentes personlige oplysninger enten fra en kilde, som frit kan tilgås, eller på basis af frivillig videregivelse, herunder foretaget af erhvervsdrivende, der er i besiddelse af sådanne oplysninger.

For så vidt angår sidstnævnte bemyndiger strafferetsplejelovbogens artikel 197, stk. 2, anklagemyndigheden og politiet til at foretage »skriftlige undersøgelser i efterforskningsøjemed« (såkaldte »undersøgelsesskemaer«). I henhold til strafferetsplejelovbogen anmodes de adspurgte personer om at rapportere til efterforskningsmyndighederne. Det er imidlertid ikke muligt at tvinge dem til at rapportere, hvis de offentlige kontorer eller de offentlige og/eller private organisationer, der har modtaget forespørgslerne, nægter at gøre det. Hvis de ikke rapporterer i forbindelse med forespørgslerne, kan der ikke pålægges nogen straf eller anden sanktion. Hvis efterforskningsmyndighederne vurderer, at de ønskede oplysninger er uundværlige, er de nødt til at indhente oplysningerne gennem ransagning og beslaglæggelse på grundlag af en retskendelse.

På baggrund af den voksende bevidsthed om den enkeltes rettigheder med hensyn til privatliv og den arbejdsbyrde, som sådanne anmodninger indebærer, er mange erhvervsdrivende mere og mere forsigtige med at imødekomme sådanne anmodninger ⁽¹¹⁾. Når de beslutter, om de ønsker at samarbejde, tager erhvervsdrivende navnlig hensyn til arten af de ønskede oplysninger, deres forhold til den person, hvis oplysninger står på spil, risici for deres omdømme, risici for retstvister osv.

b) Begrænsninger

Ligesom for indsamling af elektroniske oplysninger ved tvangsindgreb er den frivillige undersøgelse begrænset af forfatningen som fortolket i retspraksis og den bemyndigende forskrift. Desuden har erhvervsdrivende ikke lov til at videregive oplysninger i visse situationer. Endelig indeholder APPIHAO en række begrænsninger, der gælder både for indsamling og håndtering af oplysninger (mens lokale bekendtgørelser gengiver stort set de samme kriterier for præfekturpolitiet).

1) Begrænsninger som følger af forfatningen og den bemyndigende forskrift

Ved at tage hensyn til formålet med forfatningens artikel 13 har højesteret i to afgørelser af 24. december 1969 (1965A nr. 1187) og 15. april 2008 (2007A nr. 839) indført begrænsninger for efterforskningsmyndighedernes gennemførelse af frivillige undersøgelser. Selv om disse afgørelser vedrørte tilfælde, hvor personlige oplysninger (i form af billeder) blev indsamlet gennem fotografering/optagelse, er resultaterne relevante for frivillige undersøgelser (dvs. uden tvangsindgreb), der griber ind i privatlivets fred i almindelighed. De finder derfor anvendelse og skal overholdes, for så vidt angår indsamling af personlige oplysninger gennem frivillige undersøgelser, under hensyntagen til de særlige omstændigheder i hvert enkelt tilfælde.

I henhold til disse afgørelser afhænger lovligheden af frivillige undersøgelser af, hvorvidt tre kriterier er opfyldt, nemlig:

— »mistanke om en forbrydelse« (dvs. at det skal vurderes, om der er begået en forbrydelse)

— »undersøgelsens nødvendighed« (dvs. at det skal vurderes, om anmodningen holder sig inden for rammerne af, hvad der er nødvendigt i forbindelse med efterforskningen), samt

⁽¹¹⁾ Se også meddelelsen fra det nationale politiagentur den 7. december 1999 (side 9, herunder), hvor der gives udtryk for det samme.

— »metodernes hensigtsmæssighed« (dvs. at det skal vurderes, om frivillig undersøgelse er »passende« eller rimelig for at opfylde formålet med efterforskningen) ⁽¹²⁾.

Generelt vurderes lovligheden af frivillige undersøgelser, under hensyntagen til ovenstående tre kriterier, ud fra hvorvidt de kan anses for rimelige i overensstemmelse med socialt accepterede konventioner.

Kravet om, at undersøgelsen skal være »nødvendig«, følger også direkte af strafferetsplejelovbogens artikel 197 og er blevet bekræftet i de instrukser, der er udstedt af det nationale politiagentur til præfekturpolitiet vedrørende anvendelsen af »undersøgelsesskemaer«. I det nationale politiagenturs meddelelse af 7. december 1999 er der fastsat en række proceduremæssige begrænsninger, herunder kravet om kun at anvende »undersøgelsesskemaer«, hvis det er nødvendigt i forbindelse med efterforskningen. Desuden er strafferetsplejelovbogens artikel 197, stk. 1, begrænset til strafferetlige efterforskninger og kan derfor kun anvendes, hvis der er konkret mistanke om en allerede begået forbrydelse. Omvendt er dette retsgrundlag ikke tilgængeligt i forbindelse med indsamling og anvendelse af personlige oplysninger, hvis en lovovertrædelse endnu ikke har fundet sted.

2) Begrænsninger vedrørende visse erhvervsdrivende

Der gælder yderligere begrænsninger på visse områder på grundlag af den beskyttelse, der er fastsat i andre love.

For det første har efterforskningsmyndigheder og teleselskaber, der er i besiddelse af personlige oplysninger, pligt til at respektere meddelelseshemmeligheden, der er sikret ved forfatningens artikel 21, stk. 2 ⁽¹³⁾. Desuden har teleselskaberne samme pligt i henhold til teleselskabslovens artikel 4 ⁽¹⁴⁾. I henhold til retningslinjerne om beskyttelse af personlige oplysninger i telesektoren, som er udstedt af ministeriet for interne anliggender og kommunikation på grundlag af forfatningen og teleselskabsloven, må teleselskaberne i tilfælde, hvor meddelelseshemmeligheden står på spil, ikke videregive personlige oplysninger om meddelelseshemmeligheden til tredjemand, medmindre de har indhentet den pågældendes samtykke, eller de kan påberåbe sig en af de »berettigede årsager« til manglende overholdelse af straffelovbogens. Sidstnævnte vedrører »berettigede handlinger« (straffelovbogens artikel 35), »selvforsvar« (straffelovbogens artikel 36) og »afværge af aktuelle farer« (straffelovbogens artikel 37). »Berettigede handlinger« i henhold til straffelovbogens artikel 35 er kun de handlinger, som et teleselskab foretager med henblik på overholdelse af obligatoriske statslige foranstaltninger, hvilket ikke omfatter frivillige undersøgelser. Hvis efterforskningsmyndighederne derfor anmoder om personlige oplysninger på grundlag af et »undersøgelsesskema« (strafferetsplejelovbogens artikel 197, stk. 2), er det forbudt for et teleselskab at videregive oplysningerne.

For det andet er erhvervsdrivende forpligtet til at afvise anmodninger om frivilligt samarbejde, hvis loven forbyder dem at videregive personlige oplysninger. Dette omfatter eksempelvis tilfælde, hvor den erhvervsdrivende har pligt til at respektere fortroligheden af oplysninger, f.eks. i henhold til straffelovbogens artikel 134 ⁽¹⁵⁾.

3) Begrænsninger på grundlag af APPIHAO

For så vidt angår administrative organers indsamling og videre håndtering af personlige oplysninger er der i APPIHAO fastsat de begrænsninger, der er beskrevet ovenfor i afsnit II.A, punkt 1), litra b), nr. 2). Tilsvarende begrænsninger følger af de præfekturbekendtgørelser, der gælder for præfekturpolitiet.

B. Tilsyn

1) Retligt tilsyn

For så vidt angår indsamling af personlige oplysninger ved tvangsindgreb skal dette ske på grundlag af en kendelse ⁽¹⁶⁾ og er derfor betinget af en forudgående retslig undersøgelse. Hvis efterforskningen var ulovlig, kan retten udelukke sådanne beviser i den efterfølgende straffesag. En enkeltperson kan anmode om en sådan udelukkelse i vedkommendes straffesag med påstand om, at efterforskningen var ulovlig.

⁽¹²⁾ Forbrydelsens alvor og sagens uopsættelighed er relevante faktorer til vurdering af »metodernes hensigtsmæssighed«.

⁽¹³⁾ I forfatningens artikel 21, stk. 2, står der følgende: »Ingen form for censur må udøves, og meddelelseshemmeligheden må ikke krænkes for nogen form for kommunikationsmiddel.«

⁽¹⁴⁾ I teleselskabslovens artikel 4 står der følgende: »1) Meddelelseshemmeligheden for meddelelser, der håndteres af et teleselskab, må ikke krænkes. 2) Enhver person, der er aktiv inden for telekommunikation, må, så længe denne bestrider et sådant hverv, ikke videregive hemmeligheder, hvortil der er opnået kendskab gennem teleselskabets håndtering af meddelelser. Det samme gælder også, efter at vedkommende har forladt sin stilling.«

⁽¹⁵⁾ I straffelovbogens artikel 134 står der følgende: »1) Hvis en læge, farmaceut, lægemiddeldistributør, jordemor, advokat, forsvarsadvokat, notar eller enhver anden person, der tidligere var aktiv inden for et sådant erhverv, uden begrundelse videregiver en andens persons fortrolige oplysninger, hvortil vedkommende har fået kendskab gennem et sådant erhverv, vil vedkommende blive idømt fængsel med arbejde i højst seks måneder eller en bøde på højst 100 000 yen. 2) Det samme gælder i tilfælde, hvor en person, der bestrider eller har bestredet et religiøst hverv, uden begrundelse videregiver en andens persons fortrolige oplysninger, hvortil vedkommende har fået kendskab gennem udøvelsen af sådanne religiøse aktiviteter.«

⁽¹⁶⁾ For så vidt angår undtagelsen til denne regel henvises til fodnote 5.

2) Tilsyn på grundlag af APPIHAO

I Japan har ministeren eller lederen af hvert enkelt ministerium eller hver enkelt myndighed tilsyns- og håndhævelsesbeføjelser baseret på APPIHAO, mens ministeren for interne anliggender og kommunikation kan føre tilsyn med alle andre ministeriers håndhævelse af APPIHAO.

Hvis ministeren for interne anliggender og kommunikation — f.eks. på grundlag af tilsynet med håndhævelsen af APPIHAO ⁽¹⁷⁾, med behandlingen af klager eller med forespørgsler rettet til et af ministeriets informationscentre — finder det nødvendigt for at opfylde formålet med APPIHAO, kan vedkommende anmode chefen for et administrativt organ om materiale og forklaringer vedrørende det pågældende administrative organs håndtering af personlige oplysninger i medfør af artikel 50 i APPIHAO. Ministeren kan afgive udtalelser til chefen for det administrative organ vedrørende behandling af personlige oplysninger i det administrative organ, hvis han eller hun finder det nødvendigt for at opfylde lovens formål. Desuden kan ministeren f.eks. anmode om en revision af foranstaltningerne via de i lovens artikel 50 og 51 fastsatte tiltag, hvis der er mistanke om, at loven er blevet overtrådt eller anvendt uhensigtsmæssigt. Dette er med til at sikre en ensartet anvendelse og overholdelse af APPIHAO.

3) Tilsyn med politiet foretaget af kommissionerne for den offentlige sikkerhed

Med hensyn til politiets forvaltning fører den nationale kommission for den offentlige sikkerhed tilsyn med det nationale politiagentur, mens de præfekturkommissioner for den offentlige sikkerhed, der er nedsat i hvert præfektur, fører tilsyn med præfekturpolitiet. Hvert af disse tilsynsorganer sikrer demokratisk forvaltning og politisk neutralitet i politiets administration.

Den nationale kommission for den offentlige sikkerhed er ansvarlig for de anliggender, der hører under dens kompetenceområde i henhold til politiloven og anden lovgivning. Dette omfatter udnævnelser til stillingen som generalkommissær for det nationale politiagentur og lokale overordnede politistillinger såvel som fastlæggelse af omfattende politikker med grundlæggende retningslinjer eller foranstaltninger vedrørende forvaltningen af det nationale politiagentur.

Præfekturkommissionerne for den offentlige sikkerhed består af medlemmer, der repræsenterer befolkningen i det pågældende præfektur i henhold til politiloven, og forvalter præfekturpolitiet som et uafhængigt rådssystem. Medlemmerne udnævnes af præfekturguvernøren med præfekturforsamlingens samtykke i henhold til politilovens artikel 39. Deres embedsperiode er på tre år, og de kan kun afskediges mod deres vilje af specifikke grunde, der er fastsat i lovgivningen (såsom manglende evne til at udføre deres opgaver, tilsidesættelse af pligter, embedsmisbrug osv.), hvilket sikrer deres uafhængighed (jf. politilovens artikel 40 og 41). For at sikre deres politiske neutralitet er det i henhold til politilovens artikel 42 endvidere forbudt for et præfekturkommissionsmedlem samtidig at fungere som medlem af et lovgivende organ, blive ledende medlem af et politisk parti eller andre politiske organer eller deltage aktivt i politiske bevægelser. Hver præfekturkommission hører under den respektive præfekturguvernørs kompetenceområde, men dette giver ikke guvernøren beføjelser til at udstede instrukser for, hvordan dens funktioner udøves.

I henhold til politilovens artikel 38, stk. 3, sammenholdt med artikel 2 og artikel 36, stk. 2, har præfekturkommissionerne for den offentlige sikkerhed til opgave at sørge for »beskyttelsen af den enkeltes rettigheder og frihed«. Til dette formål modtager de rapporter fra præfekturpoliticheferne vedrørende aktiviteterne inden for deres jurisdiktion, herunder på regelmæssige møder, der afholdes tre til fire gange om måneden. Præfekturkommissionerne giver vejledning om disse anliggender ved at fastsætte omfattende politikker.

Desuden kan præfekturkommissionerne for den offentlige sikkerhed som led i deres tilsynsfunktion udstede instrukser til præfekturpolitiet i konkrete sager på særskilt basis, hvis de finder det nødvendigt i forbindelse med kontrol af præfekturpolitiets aktiviteter eller tjenestelige forseelser blandt personalet. Endvidere kan præfekturkommissionerne, når de finder det nødvendigt, pålægge et udpeget medlem at vurdere gennemførelsen af den udstedte instruks (politilovens artikel 43-2).

⁽¹⁷⁾ For at sikre gennemsigtighed og gøre det lettere for ministeriet for interne anliggender og kommunikation at føre tilsyn er chefen for et administrativt organ i henhold til artikel 11 i APPIHAO forpligtet til at registrere hvert punkt, der er foreskrevet i artikel 10, stk. 1, i APPIHAO, såsom navnet på det administrative organ, der opbevarer sagsmapper, anvendelsesformålet med sagsmapper, metoden til indsamling af de personlige oplysninger osv. (det såkaldte »register over sagsmapper med personlige oplysninger«). Imidlertid er sagsmapper med personlige oplysninger, der er omfattet af artikel 10, stk. 2, i APPIHAO, såsom dem, der er udarbejdet eller indhentet som led i en strafferetlig efterforskning eller vedrørende spørgsmål af relevans for den nationale sikkerhed, undtaget fra forpligtelsen til at underrette ministeriet for interne anliggender og kommunikation samt at inkludere dem i det offentlige register. I henhold til artikel 7 i loven om forvaltning af offentlige registre og arkiver er chefen for et administrativt organ imidlertid altid forpligtet til at registrere klassifikation, titel, opbevaringsperiode og opbevaringssted osv. for administrative dokumenter (»registret over forvaltning af sagsmapper med administrative dokumenter«). Indeksoplysningerne for begge registre offentliggøres på internettet og giver enkeltpersoner mulighed for at kontrollere, hvilken slags personlige oplysninger der er indeholdt i sagsmapper, og hvilket administrativt organ der opbevarer oplysningerne.

4) Parlamentets tilsyn

Det japanske parlament kan foretage undersøgelser af offentlige myndigheders aktiviteter og i denne forbindelse anmode om udlevering af dokumenter og vidneforklaringer (forfatningens artikel 62). I denne forbindelse kan det kompetente udvalg i parlamentet undersøge, om politiets aktiviteter med henblik på at indsamle oplysninger har været hensigtsmæssige.

Disse beføjelser er nærmere præciseret i parlamentsloven. I henhold til parlamentslovens artikel 104 kan parlamentet kræve, at kabinettet og de offentlige organer fremlægger de rapporter og fortegnelser, som er nødvendige for at gennemføre undersøgelsen. Endvidere kan parlamentsmedlemmer indgive »skriftlige forespørgsler« i henhold til parlamentslovens artikel 74. Disse forespørgsler skal godkendes af kammerets formand og skal i princippet besvares skriftligt af kabinettet inden for syv dage (hvis det er umuligt at svare inden for denne frist, skal dette begrundes, og der skal fastsættes en ny frist, jf. parlamentslovens artikel 75). Tidligere har det japanske parlaments skriftlige forespørgsler også omhandlet administrationens håndtering af personlige oplysninger ⁽¹⁸⁾.

C. Individuel klage- eller prøvelsesadgang

I henhold til artikel 32 i Japans forfatning må ingen nægtes ret til domstolsprøvelse. Desuden garanterer forfatningens artikel 17 enhver person retten til at sagsøge staten eller offentlige enheder med henblik på at opnå erstatning (som fastsat ved lov), hvis den pågældende person har lidt skade på grund af en ulovlig handling foretaget af en embedsmand.

1) Domstolsprøvelse af indsamling af oplysninger ved tvangsindgreb på grundlag af en retskendelse (strafferetsplejelovbogens artikel 430)

I henhold til strafferetsplejelovbogens artikel 430, stk. 2, kan en person, der er utilfreds med de foranstaltninger, der er truffet af politiet vedrørende beslaglæggelse af genstande (herunder hvis de indeholder personlige oplysninger) på grundlag af en retskendelse, indgive en anmodning til den kompetente domstol om, at sådanne foranstaltninger »annulleres eller ændres«.

Enkeltpersonen behøver ikke afvente sagens afslutning, før en sådan anfægtelse kan indgives. Hvis retten finder, at beslaglæggelsen ikke var nødvendig, eller at der er andre grunde til at betragte beslaglæggelsen som ulovlig, kan den kræve, at disse foranstaltninger annulleres eller ændres.

2) Domstolsprøvelse i henhold til retsplejelovbogen og loven om statens erstatningsansvar

Hvis enkeltpersoner mener, at deres ret til privatlivets fred i henhold til forfatningens artikel 13 er blevet krænket, kan de anlægge civilt søgsmål og anmode om, at personlige oplysninger, der er indsamlet i løbet af en strafferetlig efterforskning, slettes.

Desuden kan en enkeltperson anlægge erstatningssag i henhold til loven om statens erstatningsansvar i kombination med de relevante artikler i den borgerlige lovbog, hvis den pågældende person mener, at dennes ret til privatlivets fred er blevet krænket, og at personen har lidt skade som følge af indsamling af dennes personlige oplysninger eller overvågning ⁽¹⁹⁾. Da den »skade«, der er genstand for et krav om erstatning, ikke er begrænset til skader på ejendom (artikel 710 i den borgerlige lovbog), kan dette også omfatte »psykisk overlast«. Erstatningen for en sådan moralsk skade vurderes af retten på grundlag af en »frit skøn under hensyntagen til de forskellige faktorer i hvert enkelt tilfælde« ⁽²⁰⁾.

Artikel 1, stk. 1, i loven om statens erstatningsansvar omfatter retten til erstatning, i tilfælde hvor i) en offentlig embedsmand under udøvelsen af statslig myndighed eller et offentligt organs myndighed ii) i forbindelse med sit hverv iii) forsætligt eller uagtsomt iv) ulovligt v) har forvoldt en anden person skade.

Den pågældende person skal anlægge sagen i overensstemmelse med retsplejelovbogen. I henhold til de gældende regler kan personen anbringe sagen for den domstol, der har kompetence på det sted, hvor den skadevoldende handling blev begået.

⁽¹⁸⁾ Se f.eks. overhusets skriftlige forespørgsel nr. 92 af 27. marts 2009 vedrørende håndtering af oplysninger, der er indhentet i forbindelse med strafferetlig efterforskning, herunder politiets og anklagemyndighedens overtrædelser af tavshedspligten.

⁽¹⁹⁾ Et eksempel på en sådan sag er »sagen om forsvarsagenturets liste« (byretten i Niigata, afgørelse af 11. maj 2006, (2002(Wa) nr. 514)). I denne sag havde en embedsmand i forsvarsagenturet udarbejdet, ajourført og distribueret en liste over de personer, der havde indgivet anmodninger om indsigt i administrative dokumenter til forsvarsagenturet. Listen indeholdt beskrivelser af sagsøgers personlige oplysninger. Sagsøger insisterede på, at hans privatliv, ret til information osv. var blevet krænket, og anmodede sagsøgte om at betale erstatning i henhold til artikel 1, stk. 1, i loven om statens erstatningsansvar. Denne anmodning blev delvist imødekommet af domstolen, der tildelte sagsøger en delvis erstatning.

⁽²⁰⁾ Højesteret, afgørelse af 5. april 1910 (1910(O) nr. 71).

- 3) Individuelle klage- eller prøvelsesmuligheder i forbindelse med ulovlig/uretmæssig efterforskning foretaget af politiet: klage til præfekturkommissionen for den offentlige sikkerhed (politilovens artikel 79)

I henhold til politilovens artikel 79 ⁽²¹⁾, som blev præciseret yderligere i en instruks fra chefen for det nationale politiagentur til præfekturpolitiet og præfekturkommissionerne for den offentlige sikkerhed ⁽²²⁾, kan enkeltpersoner indgive en skriftlig klage ⁽²³⁾ til den kompetente præfekturkommission for den offentlige sikkerhed vedrørende enhver form for ulovlig eller uhensigtsmæssig adfærd fra en politiembedsmand i udførelsen af dennes pligter. Dette omfatter forpligtelser med hensyn til indsamling og anvendelse af personlige oplysninger. Kommissionen behandler loyalt sådanne klager i overensstemmelse med lovgivningen og lokale bekendtgørelser, og den skal skriftligt meddele klageren undersøgelsens resultat.

Præfekturkommissionen for den offentlige sikkerhed skal på grundlag af sin funktion som tilsynsmyndighed i henhold til politilovens artikel 38, stk. 3, udstede en instruks til præfekturpolitiet om at undersøge de faktiske omstændigheder, gennemføre de nødvendige foranstaltninger alt efter resultatet af undersøgelsen og meddele præfekturkommissionen resultaterne heraf. Hvis præfekturkommissionen finder det nødvendigt, kan den også udstede instrukser om behandlingen af klagen, f.eks. hvis den finder, at politiets efterforskning er utilstrækkelig. Denne fremgangsmåde er beskrevet i det cirkulære, som det nationale politiagentur har udsendt til præfekturpoliticheferne.

Klageren underrettes også om resultatet af undersøgelsen på grundlag af undersøgelsesrapporterne fra politiet og de foranstaltninger, der er truffet efter anmodning fra præfekturkommissionen.

- 4) Individuel klage- eller prøvelsesadgang i henhold til APPIHAO og strafferetsplejelovbogen

a) APPIHAO

I henhold til artikel 48 i APPIHAO skal administrative organer bestræbe sig på at behandle klager over håndteringen af personlige oplysninger korrekt og hurtigt. Som et middel til videregivelse af konsoliderede oplysninger til enkeltpersoner (f.eks. om deres rettigheder til indsigt, berigtigelse eller suspension af anvendelsen i medfør af APPIHAO) og som et kontaktpunkt til forespørgsler har ministeriet for interne anliggender og kommunikation i hvert præfektur på grundlag af artikel 47, stk. 2, i APPIHAO etableret informationscentre til indsigt i oplysninger og beskyttelse af personlige oplysninger. Personer uden bopæl i Japan kan også rette forespørgsler dertil. F.eks. besvarede informationscentrene i alt 5186 forespørgsler mv. i regnskabsåret 2017 (april 2017 til marts 2018).

I henhold til artikel 12 og 27 i APPIHAO har enkeltpersoner ret til at anmode om indsigt i og berigtigelse af opbevarede personlige oplysninger. Herudover kan de i henhold til artikel 36 i APPIHAO anmode om suspension af anvendelsen eller sletning af deres opbevarede personlige oplysninger, såfremt det administrative organ har erhvervet de opbevarede personlige oplysninger ulovligt eller opbevarer eller anvender oplysningerne i strid med lovgivningen.

Hvad angår personlige oplysninger, der er blevet indsamlet (enten på grundlag af en kendelse eller via et »undersøgelses-skema«) og opbevaret med henblik på strafferetlig efterforskning ⁽²⁴⁾, falder sådanne oplysninger normalt ind under kategorien »personlige oplysninger registreret i dokumenter vedrørende retssager og beslaglagte genstande«. Disse personlige oplysninger er derfor i henhold til strafferetsplejelovbogens artikel 53-2 udelukket fra anvendelsesområdet for de individuelle rettigheder i kapitel 4 i APPIHAO ⁽²⁵⁾. Behandlingen af sådanne personlige oplysninger og den enkelte persons ret til adgang og berigtigelse er i stedet underlagt særlige regler i medfør af strafferetsplejelovbogen og loven

⁽²¹⁾ Politilovens artikel 79 (uddrag):

1. Enhver, der er utilfreds med præfekturpolitiets personales udførelse af deres pligter, kan indgive en skriftlig klage til præfekturkommissionen for den offentlige sikkerhed i henhold til den procedure, der er fastsat i bekendtgørelsen om den nationale kommission for den offentlige sikkerhed.
2. Præfekturkommissioner for den offentlige sikkerhed, der modtager klager i henhold til det foregående stykke, skal behandle dem loyalt i overensstemmelse med lovgivningen og lokale forskrifter og underrette klageren herom skriftligt, undtagen i følgende tilfælde:
 - 1) Hvis klagen opfattes som indgivet med henblik på at hindre præfekturpolitiets lovlige udførelse af deres pligter
 - 2) Hvis klagerens nuværende bopæl er ukendt
 - 3) Hvis klagen opfattes som indgivet i fællesskab med andre klagere, og de andre klagere allerede er blevet underrettet om resultatet af den fælles klage.

⁽²²⁾ Det nationale politiagentur, cirkulære vedrørende korrekt behandling af klager vedrørende politiembedsmænds udførelse af deres pligter, den 13. april 2001, med tillæg 1, »Standarder for fortolkning/gennemførelse af politilovens artikel 79«.

⁽²³⁾ Ifølge cirkulæret fra det nationale politiagentur (jf. foregående fodnote) skal personer, der har vanskeligt ved at indgive klager skriftligt, modtage bistand. Dette omfatter udtrykkeligt udlændinge.

⁽²⁴⁾ På den anden side vil der være dokumenter, som ikke er klassificeret som »dokumenter vedrørende retssager«, da de i sig selv ikke er oplysninger, der er erhvervet på grundlag af en kendelse eller skriftlige undersøgelser i efterforskningsøjemed, men derimod er oprettet på basis af sådanne dokumenter. Dette ville være tilfældet, hvor private oplysninger ikke er omfattet af artikel 45, stk. 1, i APPIHAO, hvorfor disse oplysninger ikke vil være undtaget fra anvendelsen af kapitel 4 i APPIHAO.

⁽²⁵⁾ I henhold til strafferetsplejelovbogens artikel 53-2, stk. 2, finder bestemmelserne i kapitel IV i APPIHAO ikke anvendelse på personlige oplysninger registreret i dokumenter vedrørende retssager og beslaglagte genstande.

om endelige sagsakter i straffesager (se nedenfor) ⁽²⁶⁾. Denne udelukkelse begrundes af forskellige faktorer som f.eks. beskyttelsen af de berørte personers privatliv, efterforskningens fortrolighed og den korrekte gennemførelse af straffesagen. Bestemmelserne i kapitel 2 i APPIHAO om principperne for håndtering af sådanne oplysninger finder dog fortsat anvendelse.

b) strafferetsplejelovbogen

I henhold til strafferetsplejelovbogen afhænger mulighederne for at få adgang til personlige oplysninger, der er blevet indsamlet med henblik på en strafferetlig efterforskning, af både tidspunktet under proceduren og personens rolle i efterforskningen (mistænkt, tiltalt, offer osv.).

Som en undtagelse fra reglen i strafferetsplejelovbogens artikel 47 om, at dokumenter, der vedrører retssagen, ikke må offentliggøres forud for indledningen af retssagen (da dette vil kunne udgøre en krænkelse af de berørte personers ære og/eller privatliv og hindre efterforskningen/retssagen), har offeret for en forbrydelse i princippet lov til at få indsigt i sådanne oplysninger, for så vidt det anses for rimeligt under hensyntagen til formålet med bestemmelsen i strafferetsplejelovbogens artikel 47 ⁽²⁷⁾.

Hvad angår mistænkte får de normalt kendskab til, at de er genstand for en strafferetlig efterforskning, når de afhøres af enten politiet eller anklagemyndigheden. Hvis anklagemyndigheden efterfølgende beslutter ikke at indlede retsforfølgning, underrettes den mistænkte straks herom på dennes egen anmodning (strafferetsplejelovbogens artikel 259).

Herudover skal anklagemyndigheden efter indledningen af retsforfølgningen give den tiltalte eller dennes advokat mulighed for på forhånd at få indsigt i beviserne, inden der anmodes om at få dem efterprøvet af retten (strafferetsplejelovbogens artikel 299). Dette giver den tiltalte mulighed for at få indsigt i de af pågældendes personlige oplysninger, der er blevet indsamlet som led i en strafferetlig efterforskning.

Endelig er beskyttelsen af personlige oplysninger, der er blevet indsamlet som led i en strafferetlig efterforskning, hvad enten de tilhører en mistænkt, den tiltalte eller en anden person (f.eks. et offer for en forbrydelse), sikret ved fortrolighedsforpligtelsen (artikel 100 i lov om den nationale offentlige tjeneste) og truslen om straf i tilfælde af offentliggørelse af fortrolige oplysninger i forbindelse med varetagelsen af offentlige opgaver (artikel 109, nr. xii), i lov om den nationale offentlige tjeneste).

5) Individuelle klagemuligheder i forbindelse med ulovlig/uretmæssig efterforskning foretaget af offentlige myndigheder: klager til PPC

I henhold til artikel 6 i APPI skal regeringen træffe de nødvendige foranstaltninger i samarbejde med regeringerne i tredjelande for at konstruere et internationalt konsistent system vedrørende personlige oplysninger ved at fremme samarbejde med internationale organisationer og andre internationale rammer. Med udgangspunkt i denne bestemmelse gives PPC i den grundlæggende politik om beskyttelse af personlige oplysninger (der er vedtaget ved kabinetsafgørelse) som den kompetente myndighed i forbindelse med den overordnede forvaltning af APPI beføjelse til at træffe de nødvendige foranstaltninger til at slå bro over forskellene mellem systemerne og aktiviteterne mellem Japan og det pågældende tredjeland med henblik på at sikre passende håndtering af personlige oplysninger fra et sådant land.

Desuden er PPC i medfør af artikel 61, nr. i) og ii), i APPI ansvarlig for at udforme og fremme en grundlæggende politik samt for at mægle i forbindelse med klager indgivet mod erhvervsdrivende. Endelig skal de administrative organer kommunikere og samarbejde tæt med hinanden (artikel 80 i APPI).

På grundlag af disse bestemmelser vil PPC behandle klager indgivet af enkeltpersoner på følgende vis:

- a) En person, som har mistanke om, at pågældendes oplysninger, der er blevet overført fra EU, er blevet indsamlet eller anvendt af offentlige myndigheder i Japan – herunder de myndigheder, som har ansvaret for de aktiviteter, der er omhandlet i kapitel II og kapitel III i nærværende redegørelse – i strid med gældende regler, herunder de regler, der er omfattet af denne redegørelse, kan indgive en klage til PPC (som enkeltperson eller via pågældendes databeskyttelsesmyndighed).
- b) PPC håndterer klagen, bl.a. ved at gøre brug af sine beføjelser i henhold artikel 6, artikel 61, nr. ii), og artikel 80 i APPI, og underretter de kompetente myndigheder, herunder de relevante tilsynsorganer, om klagen.

⁽²⁶⁾ Ifølge strafferetsplejelovbogen og loven om endelige sagsakter i straffesager er adgangen til og berigtigelsen af beslaglagte genstande samt dokumenter/personlige oplysninger vedrørende straffesager underlagt et unikt og særligt regelsæt, der har til formål at beskytte de berørte personers privatliv, efterforskningens fortrolighed og den korrekte gennemførelse af straffesagen osv.

⁽²⁷⁾ Mere specifikt er indsigten i oplysninger vedrørende objektive beviser i princippet tilladt for ofre for forbrydelser med hensyn til fortegnelser vedrørende sager, hvor der ikke er foretaget retsforfølgning, dersom der i henhold til strafferetsplejelovbogens artikel 316-33ff. gives mulighed for deltagelse af ofre, og herved gøres beskyttelsen af ofre for forbrydelser mere tilfredsstillende.

Disse myndigheder har i henhold til artikel 80 i APPI pligt til at samarbejde med PPC, herunder ved at fremsende de nødvendige oplysninger og relevant materiale, således at PPC kan vurdere, om indsamlingen eller den efterfølgende anvendelse af personlige oplysninger har fundet sted i overensstemmelse med gældende regler. I forbindelse med gennemførelsen af denne vurdering vil PPC samarbejde med ministeriet for interne anliggender og kommunikation.

- c) Hvis vurderingen viser, at en overtrædelse af gældende regler har fundet sted, omfatter de berørte offentlige myndigheders samarbejde med PPC en forpligtelse til at afhjælpe overtrædelser.

I tilfælde af ulovlig indsamling af personlige oplysninger i henhold til gældende regler skal dette omfatte sletning af de indsamlede personlige oplysninger.

I tilfælde af en overtrædelse af gældende regler vil PPC ligeledes inden afslutningen af vurderingen bekræfte, at overtrædelserne er afhjulpes fuldt ud.

- d) Når vurderingen er gennemført, skal PPC inden for en rimelig frist meddele den berørte person dennes resultat, herunder eventuelle korrigerende foranstaltninger, såfremt dette er relevant. Via denne meddelelse skal PPC også oplyse den berørte person om mulighederne for at anmode om bekræftelse af resultatet hos den kompetente offentlige myndighed, og om hvilken myndighed sådan en anmodning om bekræftelse skal rettes til.

Nærmere oplysninger om evalueringens resultat kan være omfattet af begrænsninger, så længe der er en rimelig formodning for, at en sådan underretning vil udgøre en risiko for den igangværende efterforskning.

Hvis klagen vedrører indsamling eller anvendelse af personoplysninger på det strafferetlige område, vil PPC i tilfælde af, at det i forbindelse med vurderingen viser sig, at en sag, som omfatter pågældendes personlige oplysninger, er blevet indledt, og at sagen siden er afsluttet, meddele denne, at der kan gives indsigt i sagsakterne i henhold til strafferetsplejebogens artikel 53 og artikel 4 i loven om endelige sagsakter i straffesager.

Hvis vurderingen viser, at en person er mistænkt i en straffesag, vil PPC oplyse pågældende herom og om muligheden for at indgive en anmodning i henhold til strafferetsplejebogens artikel 259.

- e) Hvis en person stadig er utilfreds med resultatet af denne procedure, kan denne henvende sig til PPC, som skal oplyse pågældende om de forskellige muligheder og nærmere procedurer for klage- og søgsmål i henhold til japanske love og forskrifter. PPC vil støtte den enkelte, herunder gennem vejledning og bistand i forbindelse med eventuel opfølgning på sagen over for det relevante administrative eller retslige organ.

III. Myndighedsadgang af hensyn til den nationale sikkerhed

A. Retsgrundlag og begrænsninger for indsamling af personlige oplysninger

1) Retsgrundlag for det berørte ministeriums/den berørte myndigheds indsamling af oplysninger

Som angivet ovenfor skal de administrative organers indsamling af personlige oplysninger under henvisning til den nationale sikkerhed være omfattet af deres administrative beføjelser.

I Japan findes der ingen love, der muliggør indsamling af oplysninger ved tvangsindgreb udelukkende af hensyn til den nationale sikkerhed. I henhold til forfatningens artikel 35 er det kun muligt at indsamle personlige oplysninger ved tvangsindgreb, hvis der foreligger en retskendelse til efterforskning af en lovovertrædelse. En sådan kendelse kan derfor kun afsiges med henblik på en strafferetlig efterforskning. Dette betyder, at det i henhold til japansk ret ikke er tilladt at indsamle/tilgå oplysninger ved tvangsindgreb under henvisning til den nationale sikkerhed. I stedet kan de berørte ministerier eller myndigheder, når det drejer sig om den nationale sikkerhed, kun indhente oplysninger fra kilder, som alle har fri adgang til, eller modtage oplysninger fra erhvervsdrivende eller enkeltpersoner gennem frivilligt samarbejde. Erhvervsdrivende, som modtager en anmodning om frivilligt samarbejde, er ikke retligt forpligtet til at videregive disse oplysninger, og det har derfor ingen negative konsekvenser for dem, hvis de nægter at samarbejde.

En række forskellige ministerielle kontorer og agenturer har beføjelser på området national sikkerhed.

1) Kabinetssekretariatet

Kabinetssekretariatet beskæftiger sig med indsamling og undersøgelse af oplysninger om væsentlige kabinetspolitikker ⁽²⁸⁾, jf. kabinetslovens artikel 12-2 ⁽²⁹⁾. Kabinetssekretariatet har imidlertid ikke beføjelse til at indsamle personlige oplysninger direkte fra erhvervsdrivende. Det indsamler, indarbejder, analyserer og vurderer oplysninger fra bl.a. åbne kilder og andre offentlige myndigheder.

2) Det nationale politiagentur/præfekturpolitiet

I hvert præfektur har præfekturpolitiet beføjelse til at indsamle oplysninger inden for sit kompetenceområde i henhold til lovens artikel 2. Det kan ske, at det nationale politiagentur indsamler oplysninger direkte inden for sit kompetenceområde som fastsat i politiloven. Dette vedrører navnlig de aktiviteter, der udføres af det nationale politiagents sikkerhedskontor og af afdelingen for udenrigsanliggender og efterretning. I henhold til politilovens artikel 24 er sikkerhedskontoret ansvarligt for sikkerhedspolitiske spørgsmål ⁽³⁰⁾, mens afdelingen for udenrigsanliggender og efterretning er ansvarlig for spørgsmål vedrørende udlændinge og japanske statsborgere, der befinder sig i udlandet.

3) Efterretningsagenturet for offentlig sikkerhed

Anvendelsen af loven om forhindring af undergravende aktiviteter (SAPA) og loven om kontrol med organisationer, som har begået vilkårlige masse mord (ACO), henhører primært under efterretningsagenturet for offentlig sikkerhed, der sorterer under justitsministeriet. Dette er en myndighed under justitsministeriet.

Ifølge SAPA og ACO kan der inden for rammerne af forfatningen på strenge betingelser vedtages administrative bestemmelser (dvs. foranstaltninger til begrænsning af sådanne organisationers aktiviteter, deres opløsning osv.) mod organisationer, der begår visse alvorlige handlinger (»terroristisk undergravende aktivitet« eller »vilkårlige masse mord«) i strid med »den offentlige sikkerhed« eller »det grundlæggende samfundssystem«. »Terroristisk undergravende aktivitet« falder ind under anvendelsesområdet for SAPA (jf. artikel 4 om aktiviteter som f.eks. oprør, tilskyndelse til aggression udefra, politisk motiveret mord osv.), mens ACO omhandler »vilkårlige masse mord« (jf. artikel 4 i ACO). Bestemmelserne i SAPA eller ACO finder kun anvendelse på nøje identificerede organisationer, som udgør specifikke interne eller eksterne trusler mod den offentlige sikkerhed.

I den forbindelse udgør SAPA og ACO retsgrundlag for efterforskning. De grundlæggende undersøgelsesbeføjelser, der er tillagt personalet i efterretningsagenturet for offentlig sikkerhed, er fastsat i artikel 27 i SAPA og artikel 29 i ACO. Efterforskning i efterretningsagenturet for offentlig sikkerhed i henhold til hertil gennemføres, for så vidt den er nødvendige for overholdelsen af ovennævnte bestemmelser om kontrol med organisationer (radikale grupper på venstrefløjen, Aum Shinrikyo-sekten og visse indenlandske grupper med tætte forbindelser til Nordkorea er eksempler på organisationer, der tidligere har været genstand for efterforskning). Disse efterforskninger kan dog ikke bero på tvangsindgreb, og en organisation, der ligger inde med personlige oplysninger, kan således ikke tvinges til at videregive sådanne oplysninger.

Indsamlingen og anvendelsen af oplysninger, der videregives til efterretningsagenturet for offentlig sikkerhed på frivillig basis, er underlagt lovbestemte garantier og begrænsninger som bl.a. den forfatningssikrede meddelelseshemmelighed og de i APPIHAO fastsatte regler for håndtering af personlige oplysninger.

4) Forsvarsministeriet

Hvad angår forsvarsministeriets indsamling af oplysninger indsamler det oplysninger på grundlag af artikel 3 og 4 i loven om oprettelse af forsvarsministeriet, for så vidt det er nødvendigt for udførelsen af de administrative opgaver, der er omfattet af dets kompetence, bl.a. med hensyn til forsvar og beskyttelse, foranstaltninger truffet af forsvarsstyrkerne og udsendelsen af land-, sø- og luftforsvarsstyrkerne. Forsvarsministeriet kan kun indsamle oplysninger til disse formål gennem frivilligt samarbejde og fra kilder, som alle har fri adgang til. Det indsamler ikke oplysninger om offentligheden.

2) Begrænsninger og garantier

a) Lovbestemte begrænsninger

1) Generelle begrænsninger på grundlag af APPIHAO

APPIHAO er en almindelig lov, der finder anvendelse på administrative organers indsamling og håndtering af personlige oplysninger inden for et hvilket som helst af disse organers aktivitetsområder. Derfor finder de i afsnit II.A, punkt 1), litra b), nr. 2, beskrevne begrænsninger og garantier ligeledes anvendelse på bl.a. opbevaringen, lagringen og anvendelsen af personlige oplysninger på området national sikkerhed.

⁽²⁸⁾ Disse aktiviteter udføres af kabinettets efterretnings- og undersøgelseskontor på grundlag af artikel 4 i bekendtgørelsen om forvaltning af kabinetssekretariatet.

⁽²⁹⁾ Dette omfatter »indsamling og undersøgelse af efterretningsoplysninger om væsentlige kabinetspolitikker«.

⁽³⁰⁾ Sikkerhedspolitiet er ansvarligt for kriminalitetsbekæmpende aktiviteter vedrørende den offentlige sikkerhed og nationens interesse. Dette omfatter bekæmpelse af kriminalitet og indsamling af oplysninger om ulovlige handlinger forbundet med grupper på den yderste venstre- og højrefløj og aktiviteter til skade for Japan.

2) Særlige begrænsninger, der gælder for politiet (både det nationale politiagentur og præfekturpolitiet)

Som anført ovenfor i afsnittet om indsamling af oplysninger med henblik på retshåndhævelse på det strafferetlige område må politiet kun indsamle oplysninger inden for sit kompetenceområde, og i så fald skal det i henhold til politilovens artikel 2, stk. 2, kun være »strengt begrænset« til, hvad der er nødvendigt for at udføre dets opgaver, og på en »upartisk, fordomsfri og retfærdig« måde. Desuden må det »aldrig misbruge sine beføjelser på en sådan måde, at det griber ind i en persons forfatningssikrede rettigheder og friheder«.

3) Særlige begrænsninger, der gælder for efterretningsagenturet for offentlig sikkerhed

I henhold til artikel 3 i SAPA såvel som artikel 3 i ACO må de efterforskninger, som gennemføres i medfør af disse love, kun foretages i det mindst mulige omfang for at opnå det tilstræbte formål, og de må ikke gennemføres på en måde, der udgør en urimelig begrænsning af de grundlæggende menneskerettigheder. Dertil kommer, at hvis en medarbejder i efterretningsagenturet for offentlig sikkerhed misbruger sit embede, udgør dette i henhold til artikel 45 i SAPA og artikel 42 i ACO en forbrydelse, som straffes med højere strafferetlige sanktioner end »generel« embedsmisbrug inden for andre områder af den offentlige sektor.

4) Særlige begrænsninger, der gælder for forsvarsministeriet

Hvad angår forsvarsministeriets indsamling/tilrettælgelse af oplysninger, jf. artikel 4 i lov om oprettelse af forsvarsministeriet, er ministeriets aktiviteter på dette område begrænset til, hvad der er »nødvendigt« for at udføre dets opgaver vedrørende 1) forsvar og beskyttelse, 2) foranstaltninger truffet af forsvarsstyrkerne og 3) land-, sø- og luftforsvarsstyrkernes organisering, personaleantal, struktur, udrustning og udsendelse.

b) Andre begrænsninger

Som forklaret ovenfor i afsnit II.A, punkt 2), litra b), nr. 1), følger det af højesterets praksis, at der, for at en erhvervsdrivende kan anmodes om frivilligt samarbejde, skal være tale om en nødvendig anmodning med henblik på at efterforske en mistanke om en strafbar handling, og at anmodningen skal være rimelig for at nå formålet med efterforskningen.

Selv om undersøgelser foretaget af efterforskningsmyndigheder på området national sikkerhed er forskellige fra undersøgelser foretaget af efterforskningsmyndigheder på retshåndhævelsesområdet, både hvad angår deres retsgrundlag og formål, finder de centrale principper om »undersøgelsens nødvendighed« og »metodens egnethed« ligeledes anvendelse på området national sikkerhed, og de skal overholdes under behørig hensyntagen til de særlige omstændigheder i hvert enkelt tilfælde.

Kombinationen af ovennævnte begrænsninger sikrer, at indsamling og behandling af oplysninger kun finder sted i det omfang, det er nødvendigt for, at den kompetente offentlige myndighed kan udføre specifikke opgaver, samt på grundlag af specifikke trusler. Dette udelukker massiv og vilkårlig indsamling af eller adgang til personlige oplysninger af hensyn til den nationale sikkerhed.

B. Tilsyn

1) Tilsyn på grundlag af APPIHAO

Som forklaret ovenfor i afsnit II.B, punkt 2), har ministeren eller lederen af hvert enkelt ministerium eller hver enkelt myndighed i den japanske offentlige sektor beføjelse til at føre tilsyn med og sikre overholdelsen af APPIHAO i sit ministerium eller sin myndighed. Desuden kan ministeren for interne anliggender og kommunikation føre tilsyn med håndhævelsen af loven, anmode hver minister om materiale og forklaringer i medfør af lovens artikel 49 og 50 samt afgive udtalelser til hver minister i medfør af lovens artikel 51. For eksempel kan pågældende anmode om en revision af foranstaltningerne via de i lovens artikel 50 og 51 fastsatte tiltag.

2) Tilsyn med politiet foretaget af kommissionerne for den offentlige sikkerhed

Som forklaret ovenfor i afsnit II om indsamling af oplysninger med henblik på retshåndhævelse på det strafferetlige område fører præfekturkommissionerne for den offentlige sikkerhed tilsyn med præfekturpolitiets aktiviteter.

For det nationale politiagents vedkommende udøves tilsynet af den nationale kommission for den offentlige sikkerhed. I henhold til politilovens artikel 5 er denne kommission særlig ansvarlig for »beskyttelsen af den enkeltes rettigheder og frihed«. Med henblik herpå skal den navnlig udarbejde omfattende politikker, som fastsætter bestemmelser for forvaltning af de i henhold til hvert punkt i politilovens artikel 5, stk. 4, foreskrevne anliggender, og som udgør grundlæggende retningslinjer eller foranstaltninger, som der bør gøres brug af med henblik udførelsen af nævnte aktiviteter. Den nationale kommission for den offentlige sikkerhed har samme grad af uafhængighed som præfekturkommissionerne for den offentlige sikkerhed.

3) Tilsyn med forsvarsministeriet foretaget af generalinspektørkontoret for overholdelse af lovkrav

Generalinspektørkontoret for overholdelse af lovkrav er et uafhængigt kontor inden for forsvarsministeriet, som er direkte underlagt forsvarsministeren i henhold til artikel 29 i loven om oprettelse af forsvarsministeriet. Generalinspektørkontoret kan ved inspektion undersøge, hvorvidt forsvarsministeriets embedsmænd overholder love og forskrifter. Disse inspektioner kaldes »forsvarsinspektioner«.

Generalinspektørkontoret foretager inspektioner ud fra et uafhængigt kontors synspunkt for at sikre overholdelse af lovkrav i hele ministeriet, herunder forsvarsstyrkerne. Det varetager sine opgaver uafhængigt af forsvarsministeriets operationelle afdelinger. Efter en inspektion rapporterer generalinspektørkontoret straks sine observationer sammen med fornødne afhjælpende foranstaltninger direkte til forsvarsministeren. På grundlag af generalinspektørkontorets rapport kan forsvarsministeren udstede påbud om at gennemføre de foranstaltninger, som er nødvendige for at afhjælpe situationen. Den stedfortrædende viceminister er ansvarlig for at gennemføre disse foranstaltninger og skal aflægge rapport til forsvarsministeren om status for gennemførelsen.

Som en frivillig gennemsigthedsforanstaltning offentliggøres resultaterne af forsvarsinspektionerne nu på forsvarsministeriets websted (selv om det ikke er et lovkrav).

Der er tre kategorier af forsvarsinspektioner:

- i) regelmæssige forsvarsinspektioner, som foretages med jævne mellemrum ⁽³¹⁾
- ii) forsvarsinspektioner med henblik på kontrol, som foretages for at kontrollere, om der er truffet effektive afhjælpende foranstaltninger, og
- iii) særlige forsvarsinspektioner, som foretages i forbindelse med særlige spørgsmål på forsvarsministerens anmodning.

I forbindelse med sådanne inspektioner kan generalinspektøren bl.a. anmode det berørte kontor om rapporter, anmode om at få fremsendt dokumenter, foretage inspektion på stedet og anmode den stedfortrædende viceminister om at afgive forklaringer. I betragtning af arten af generalinspektørkontorets inspektionsopgaver ledes dette kontor af meget højstående juridiske eksperter (tidligere statsadvokater).

4) Tilsyn i efterretningsagenturet for offentlig sikkerhed

Efterretningsagenturet for offentlig sikkerhed foretager både regelmæssige og særlige inspektioner af aktiviteterne i sine enkelte afdelinger og kontorer på alle niveauer. I forbindelse med de regelmæssige inspektioner udpeges der en vicegeneralinspektør og/eller en direktør som inspektør(er). Sådanne inspektioner omfatter ligeledes forvaltning af personlige oplysninger.

5) Parlamentets tilsyn

Hvad angår indsamling af oplysninger med henblik retshåndhævelse kan det japanske parlament via sit kompetente udvalg undersøge lovligheden af indsamlingen af oplysninger under henvisning til den nationale sikkerhed. Parlamentets undersøgelsesbeføjelser er baseret på forfatningens artikel 62 og parlamentslovens artikel 74 og 104.

C. Individuel klage- eller prøvelsesadgang

Individuelle klager indgives på samme måde som i forbindelse med retshåndhævelsen på det strafferetlige område. Dette omfatter også de nye klagemekanismer, der forvaltes og overvåges af PPC, til håndtering og bilæggelse af klager indgivet af EU-borgere. I den forbindelse henvises til de relevante underafsnit i afsnit II.C.

Herudover er der specifikke individuelle klagemuligheder på området national sikkerhed.

Personlige oplysninger, der er blevet indsamlet af et administrativt organ af hensyn til den nationale sikkerhed, er underlagt bestemmelserne i kapitel 4 i APPIHAO. Dette omfatter retten til at anmode om indsigt i (artikel 12) og berigtigelse (herunder tilføjelse eller sletning) (artikel 27) af den berørte persons opbevarede personlige oplysninger og retten til at anmode om suspension af anvendelsen af de personlige oplysninger, såfremt det administrative organ har

⁽³¹⁾ Som et eksempel på en inspektion af relevans for de af denne redegørelse omfattede spørgsmål kan der for så vidt angår oplysning om/forberedelse til overholdelse af lovkrav henvises til den regelmæssige forsvarsinspektion for 2016, idet beskyttelsen af personlige oplysninger var et af inspektionens fokusområder. Mere specifikt vedrørte inspektionen status for bl.a. forvaltningen, opbevaringen osv. af personlige oplysninger. I sin rapport konstaterede generalinspektørkontoret adskillige u hensigtsmæssige aspekter i forvaltningen af personlige oplysninger, som skulle forbedres, f.eks. den manglende beskyttelse af oplysninger ved hjælp af et password. Rapporten er tilgængelig på forsvarsministeriets websted.

indhentet de pågældende oplysninger på ulovlig vis (artikel 36). Dog er udøvelsen af disse rettigheder underlagt visse begrænsninger af hensyn til den nationale sikkerhed. Anmodninger om indsigt, berigtigelse eller suspension imødekommes ikke, hvis de vedrører »oplysninger, for hvilke lederen af et administrativt organ har rimelig grund til at antage, at denne indsigt sandsynligvis vil være til skade for den nationale sikkerhed, skade tillidsforholdet til et andet land eller en international organisation eller have ugunstig virkning i forhandlinger med et andet land eller en international organisation« (artikel 14, nr. iv)). Det er derfor ikke al frivillig indsamling af oplysninger vedrørende den nationale sikkerhed, der er omfattet af denne undtagelse, eftersom sidstnævnte altid kræver en konkret vurdering af de risici, der er forbundet med videregivelsen af oplysningerne.

Hertil kommer, at hvis anmodningen fra den berørte person afvises med den begrundelse, at de pågældende oplysninger ikke betragtes som egnede til videregivelse, jf. artikel 14, nr. iv), kan den berørte person indgive en administrativ klage om, at de i artikel 14, nr. iv), fastsatte betingelser ikke var opfyldt i den foreliggende sag, for at få taget afgørelsen op til fornyet overvejelse. I dette tilfælde skal lederen af det pågældende administrative organ, inden han eller hun træffer afgørelse, høre klagenævnet for indsigt og beskyttelse af personlige oplysninger. Dette klagenævnet vil behandle klagen på et uafhængigt grundlag. Klagenævnet er et yderst specialiseret og uafhængigt organ, hvis medlemmer med samtykke fra begge kamre i parlamentet udpeges af premierministeren blandt personer med den største sagkundskab ⁽³²⁾. Klagenævnet har omfattende undersøgelsesbeføjelser, bl.a. mulighed for at anmode om dokumenter og få indsigt i de pågældende personlige oplysninger, forhandle bag lukkede døre og gøre brug af »Vaughn index«-proceduren ⁽³³⁾. Derefter udarbejder det en skriftlig rapport, som videreformidles til den berørte person ⁽³⁴⁾. Konklusionerne i rapporten offentliggøres. Selv om rapporten formelt set ikke er retligt bindende, overholdes næsten alle rapporter af det berørte administrative organ ⁽³⁵⁾.

Endelig kan den berørte person i henhold til artikel 3, stk. 3, i loven om forvaltningsretssager anlægge sag med henblik på at få tilbagekaldt den af det administrative organ trufne afgørelse om ikke at videregive personlige oplysninger.

IV. Regelmæssig revision

Inden for rammerne af den regelmæssige revision af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vil PPC og Europa-Kommissionen udveksle oplysninger om behandlingen af oplysninger i henhold til betingelserne i konstateringen af et tilstrækkeligt beskyttelsesniveau, herunder dem, der er fastsat i denne redegørelse.

⁽³²⁾ Jf. artikel 4 i lov om oprettelse af klagenævnet for indsigt og beskyttelse af personlige oplysninger.

⁽³³⁾ Jf. artikel 9 i lov om oprettelse af klagenævnet for indsigt og beskyttelse af personlige oplysninger.

⁽³⁴⁾ Jf. artikel 16 i lov om oprettelse af klagenævnet for indsigt og beskyttelse af personlige oplysninger.

⁽³⁵⁾ I de seneste tre år har der ikke været tilfælde, hvor det berørte administrative organ traf en afgørelse, der afveg fra klagenævnets konklusioner. Der har i årenes løb været meget få tilfælde, hvor dette er sket: kun to ud af i alt 2 000 sager siden 2005 (året for ikrafttrædelsen af APPIHAO). Hvis det administrative organ træffer en afgørelse, der i henhold til artikel 50, stk. 1, nr. 4, i loven om administrativ rekurs, som anvendes til erstatning af artikel 42, stk. 2, i APPIHAO, afviger fra klagenævnets konklusioner, skal det tydeligt angive årsagerne hertil.