Databeskyttelsesrådets udtalelser (artikel 70, stk. 1, litra s)

Udtalelse 28/2018

vedrørende Kommissionens udkast til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger i Japan

Vedtaget den 5. december 2018

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Indholdsfortegnelse

1 SAMMENFATNING ... 4

1.1 Konvergensområder ... 5

1.2 Generelle udfordringer ... 5

1.3 Specifikke kommercielle aspekter ... 6

1.3.1 Det Europæiske Databeskyttelsesråds betænkeligheder med hensyn til centrale databeskyttelsesprincipper ... 6

1.3.2 Behov for præcisering ... 7

1.4 Om offentlige myndigheders adgang til data overført til Japan ... 7

1.5 Konklusion ... 8

2 INDLEDNING ... 9

2.1 Den japanske ramme for databeskyttelse ... 9

2.2 Anvendelsesområdet for Det Europæiske Databeskyttelsesråds vurdering ... 9

2.3 Generelle bemærkninger og betænkeligheder ... 11

2.3.1 Særlige kendetegn ved denne type afgørelse om tilstrækkeligheden af beskyttelsesniveauet ... 11

2.3.2 Pålideligheden af oversættelser ... 11

2.3.3 Sektorspecifik tilstrækkelighed ... 12

2.3.4 Bindende karakter af tillægsreglementet og PPC's retningslinjer ... 12

2.3.5 Regelmæssig gennemgang af afgørelsen om tilstrækkeligt beskyttelsesniveau ... 13

2.3.6 Internationale forpligtelser indgået af Japan ... 13

2.3.7 Databeskyttelsesmyndighedernes beføjelser til at anlægge sag ved en domstol vedrørende gyldigheden af en afgørelse om tilstrækkeligt beskyttelsesniveau ... 14

3 KOMMERCIELLE ASPEKTER ... 14

3.1 Indholdsprincipper ... 14

3.1.1 Begreber ... 15

3.1.2 Grunde til lovlig og rimelig behandling til lovlige formål ... 18

3.1.3 Gennemsigtighedsprincippet ... 19

3.1.4 Begrænsninger for videreoverførsler ... 20

3.1.5 Direkte markedsføring ... 23

3.1.6 Automatisk beslutningstagning og profilering ... 23

3.2 Procedurer og håndhævelsesmekanismer ... 24

3.2.1 Kompetent uafhængig tilsynsmyndighed ... 24

3.2.2 Databeskyttelsessystemet skal sikre en høj grad af overholdelse ... 25

3.2.3 Databeskyttelsessystemet skal yde støtte og bistand til individuelle registrerede i forbindelse med udøvelsen af deres rettigheder og omfatte passende klagemekanismer. ... 26

4 OM OFFENTLIGE MYNDIGHEDERS ADGANG TIL DATA OVERFØRT TIL JAPAN 27
4.1 Retshåndhævende myndigheders adgang til data 27
4.1.1 Procedurer for adgang til data på det strafferetlige område 27
4.1.2 Tilsyn på det strafferetlige område 30
4.1.3 Klageadgang på det strafferetlige område 33
4.2 Adgang af hensyn til national sikkerhed 40
4.2.1 Omfanget af overvågning 40
4.2.2 Frivillig fremlæggelse af oplysninger i tilfælde af national sikkerhed 42
4.2.3 Tilsyn 42
4.2.4 Klagemekanisme 45

Det Europæiske Databeskyttelsesråd

Under henvisning til artikel 70, stk. 1, litra s), i Europa-Parlamentets og Rådets forordning 2016/679/EU 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 (i det følgende benævnt "den generelle forordning om databeskyttelse").

Under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 til EØS-aftalen som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018.

Under henvisning til forretningsordenens artikel 12 og artikel 22 af 25. maj 2018.

HAR VEDTAGET FØLGENDE UDTALELSE:

1 SAMMENFATNING

1. Europa-Kommissionen godkendte udkastet til gennemførelsesafgørelse om tilstrækkelig beskyttelse af personoplysninger fra Japan i henhold til den generelle forordning om databeskyttelse (i det følgende benævnt: Den generelle forordning om databeskyttelse) [1]den 5. september 2018[2] . Herefter indledte Europa-Kommissionen proceduren for den formelle vedtagelse.

2. Den 25. september 2018 anmodede Kommissionen Det Europæiske Databeskyttelsesråd om en udtalelse[3]. Kommissionen blev anmodet om at give Det Europæiske Databeskyttelsesråd al den nødvendige dokumentation vedrørende dette land, herunder al relevant korrespondance med den japanske regering.

3. I lyset af drøftelserne med Det Europæiske Databeskyttelsesråd ændrede Kommissionen to gange sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet og sendte sin sidste udgave den 13. november 2018[4]. Det Europæiske Databeskyttelsesråd har baseret sin nuværende udtalelse på denne seneste udgave af udkastet til gennemførelsesafgørelse (i det følgende benævnt "udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet").

4. Det Europæiske Databeskyttelsesråds vurdering af det beskyttelsesniveau, der sikres ved Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau, er foretaget på grundlag af en gennemgang af selve afgørelsen og på grundlag af en analyse af den dokumentation, som [5]Kommissionen[6] har stillet til rådighed .

---

[1] 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.
[2] Se pressemeddelelse http://europa.eu/rapid/press-release_IP-18-5433_en.htm.
[3] I henhold til artikel 70, stk. 1, litra s), i den generelle forordning om databeskyttelse.
[4] Se bilag I til Det Europæiske Databeskyttelsesråds udtalelse om den ajourførte udgave af Kommissionens udkast til gennemførelsesafgørelse.
[5] Det Europæiske Databeskyttelsesråd baserede sin analyse på oversættelser fra de japanske myndigheder, som blev verificeret af Kommissionen.
[6] Se bilag II til Det Europæiske Databeskyttelsesråds udtalelse om listen over dokumenter, som Kommissionen ikke har sendt til Det Europæiske Databeskyttelsesråd.

5. Det Europæiske Databeskyttelsesråd fokuserede på vurderingen af både de kommercielle aspekter af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet og på regeringens adgang til personoplysninger, der overføres fra EU med henblik på retshåndhævelse og national sikkerhed, herunder de retsmidler, der er til rådighed for EU-borgere. Det Europæiske Databeskyttelsesråd vurderede også, om de garantier, der blev givet i henhold til de japanske retlige rammer, er indført og effektive.

6. Det Europæiske Databeskyttelsesråd har anvendt referencen vedrørende et tilstrækkeligt beskyttelsesniveau, der blev vedtaget i februar 2018, som [7]hovedreference for dette arbejde.

1.1 Konvergensområder

7. Det Europæiske Databeskyttelsesråds vigtigste mål er at afgive en udtalelse til Kommissionen om det beskyttelsesniveau, der tilbydes enkeltpersoner inden for de japanske rammer. Det er vigtigt at erkende, at Det Europæiske Databeskyttelsesråd ikke forventer, at de japanske retsregler er en kopi af den europæiske lovgivning om databeskyttelse.

8. Det Europæiske Databeskyttelsesråd minder imidlertid om, at for at blive anset for at frembyde et tilstrækkeligt beskyttelsesniveau kræver EU-Domstolens retspraksis samt artikel 45 i den generelle forordning om databeskyttelse, at tredjelandets lovgivning tilpasses til det væsentligste indhold i de grundlæggende principper i den generelle forordning om databeskyttelse. På databeskyttelsesområdet bemærker Det Europæiske Databeskyttelsesråd endvidere, at der er centrale områder med tilpasning mellem rammen for den generelle forordning om databeskyttelse og de japanske rammer for visse centrale bestemmelser såsom datanøjagtighed og -minimering, -begrænsning, datasikkerhed, formålsbegrænsning og en uafhængig tilsynsmyndighed, Japans kommission for beskyttelse af personoplysninger (PPC).

9. Ud over ovennævnte glæder Det Europæiske Databeskyttelsesråd sig over de bestræbelser, som Kommissionen og de japanske myndigheder har gjort for at sikre, at Japan sikrer et tilstrækkeligt beskyttelsesniveau svarende til den generelle forordning om databeskyttelse, navnlig ved at udfylde hullerne mellem den generelle forordning om databeskyttelse og de japanske databeskyttelsesrammer gennem vedtagelse af yderligere regler fra PPC, som finder anvendelse på personoplysninger, der overføres fra EU til Japan, tillægsreglementet. For eksempel bemærker Det Europæiske Databeskyttelsesråd, at PPC gik med til at behandle yderligere kategorier af data som følsomme oplysninger (følsomme oplysninger i henhold til den japanske lovgivning omfatter ikke seksuel orientering eller et medlemskab af en fagforening). Desuden sikrer tillægsreglementet, at de registreredes rettigheder finder anvendelse på alle personoplysninger, der videregives fra EU, uanset deres opbevaringsperiode (hvorimod det japanske retssystem foreskriver, at den registreredes rettigheder ikke finder anvendelse på personoplysninger, der er fastsat til at blive slettet inden for en periode på seks måneder).

10. Det Europæiske Databeskyttelsesråd noterer sig også Kommissionens bestræbelser på at styrke afgørelsen om tilstrækkeligheden af beskyttelsesniveauet på baggrund af de betænkeligheder, som Det Europæiske Databeskyttelsesråd har givet udtryk for.

1.2 Generelle udfordringer

11. Ikke desto mindre er der stadig udfordringer, og Det Europæiske Databeskyttelsesråd foreslår følgende som de hovedområder, der bør styrkes og overvåges nøje i det japanske system.

[7] WP254, reference vedrørende et tilstrækkeligt beskyttelsesniveau, 6. februar 2018.

12. Den første udfordring vedrører overvågningen af denne nye struktur for tilstrækkelighed, som består i at kombinere en eksisterende retlig ramme med et specifikt tillægsreglement for at sikre, at det bliver et bæredygtigt og pålideligt system, der ikke vil give anledning til **praktiske problemer med hensyn til den konkrete og effektive overholdelse** fra de japanske enheders side og håndhævelse fra PPC's side.

13. For det andet noterer Det Europæiske Databeskyttelsesråd sig Kommissionens og de japanske myndigheders gentagne tilsagn og forsikringer om tillægsreglementets bindende og eksigible karakter og opfordrer Kommissionen til **løbende at overvåge dets bindende karakter og en effektiv anvendelse i Japan**, da dets juridiske værdi er en absolut nødvendig del af EU's og Japans afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Med hensyn til PPC's retningslinjer bifalder Det Europæiske Databeskyttelsesråd præciseringer i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet med hensyn til **deres bindende karakter, og anmoder Kommissionen om nøje at overvåge dette aspekt**[8].

1.3 Specifikke kommercielle aspekter

14. For så vidt angår de kommercielle aspekter af udkastet til EU's og Japans afgørelse om tilstrækkeligheden af beskyttelsesniveauet har Det Europæiske Databeskyttelsesråd visse bekymringer og ønsker at anmode om præciseringer vedrørende visse vigtige spørgsmål.

1.3.1 Det Europæiske Databeskyttelsesråds betænkeligheder med hensyn til centrale databeskyttelsesprincipper

15. Det Europæiske Databeskyttelsesråd glæder sig over, at tillægsreglementet udelukker, at personoplysninger, der overføres fra EU, videregives til et tredjeland på grundlag af reglerne om grænseoverskridende databeskyttelse i APEC-landene. Desuden anerkender Det Europæiske Databeskyttelsesråd, at Kommissionen i sit nye udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet har forpligtet sig til at ophæve afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, når videregivelser ikke længere sikrer kontinuiteten i beskyttelsen.

16. I henhold til den japanske lovgivning er en del af retsgrundlaget for videregivelser anerkendelsen af et tredjeland som værende i stand til sikre et tilstrækkeligt højt beskyttelsesniveau svarende til det i Japan. Vurderingen af et tredjeland som tilstrækkelig af Japan synes imidlertid ikke at omfatte det specifikke "tillægsreglement", der er forhandlet mellem Kommissionen og PPC, og som kun finder anvendelse på personoplysninger fra EU for at sikre et beskyttelsesniveau, der i det væsentlige svarer til standarderne i den generelle forordning om databeskyttelse. Det følger heraf, at personoplysninger fra EU, der overføres fra Japan til et andet tredjeland, som ikke anerkendes som havende en grundlæggende ækvivalent databeskyttelsesramme svarende til den generelle forordning om databeskyttelse, på grundlag af et japansk grundlag for tilstrækkelighed ikke længere nødvendigvis vil være omfattet af den specifikke beskyttelse af EU's personoplysninger.

17. **Det bør imidlertid erindres, at videregivelse af personoplysninger kan finde sted til tredjelande, som bliver genstand for en eventuel senere japansk afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Disse tredjelande har muligvis ikke været genstand for en tidligere vurdering eller afgørelse om et tilstrækkeligt beskyttelsesniveau af EU. På dette tidspunkt bør Kommissionen overtage sin overvågningsrolle og sikre, at beskyttelsesniveauet for EU's data fastholdes, eller overveje at ophæve denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet.**

18. Endvidere er Det Europæiske Databeskyttelsesråd bekymret over de dataansvarliges **forpligtelser med hensyn til samtykke og gennemsigtighed** (PIHBO'er). Det Europæiske Databeskyttelsesråd foretog en

[8] Se afsnit 1.3.4 i denne udtalelse for yderligere oplysninger.

omhyggelig kontrol af disse elementer med den begrundelse, at anvendelsen af samtykke som grundlag for behandling og videregivelse af personoplysninger spiller en central rolle i det japanske retssystem, der er forskellig fra den europæiske databeskyttelseslovgivning. Det Europæiske Databeskyttelsesråd er f.eks. bekymret over begrebet samtykke, som ikke er defineret på en måde, der omfatter fortrydelsesretten, som er et væsentligt element i henhold til EU-retten for at sikre den registreredes reelle kontrol over vedkommendes personoplysninger. For så vidt angår de gennemsigtighedsforpligtelser, der påhviler et PIHBO, er der tvivl om, hvorvidt der gives proaktiv information til de registrerede.

19. Det Europæiske Databeskyttelsesråd er bekymret for, at det **japanske klagesystem** ikke nødvendigvis er let at tilgå for enkeltpersoner i EU, der har brug for støtte, eller som ønsker at indgive en klage i betragtning af, at PPC's støtte kun er tilgængelig via en telefonisk hjælpetjeneste og udelukkende på japansk. Det samme problem gør sig gældende med hensyn til den mæglingstjeneste, der stilles til rådighed af PPC, da systemet ikke offentliggøres på den engelske udgave af PPC's websted. Desuden er vigtige informative dokumenter, som f.eks. ofte stillede spørgsmål om APPI, ligeledes kun tilgængelige på japansk. I denne forbindelse ville Det Europæiske Databeskyttelsesråd bifalde, hvis Kommissionen med PPC kunne drøfte muligheden for at oprette en onlinetjeneste, i det mindste på engelsk, med henblik på at yde støtte til og behandle klager fra enkeltpersoner i EU — svarende til den, der er fastsat i bilag II til denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Kommissionen vil også være nødt til nøje at overvåge effektiviteten af sanktionerne og de relevante afhjælpende foranstaltninger.

1.3.2 Behov for præcisering

20. Det Europæiske Databeskyttelsesråd ønsker garantier for visse aspekter af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, som der stadig er behov for yderligere afklaring af.

21. Det drejer sig f.eks. om visse nøglebegreber i den japanske lovgivning. Mere specifikt er der mangel på klarhed om **status for den såkaldte "administrator"** - et begreb, der svarer til databehandler i henhold til den generelle forordning om databeskyttelse, men hvis evne til at bestemme og ændre formålet med og metoderne til behandling af personoplysninger stadig er tvetydig.

22. Det Europæiske Databeskyttelsesråd skal også have garantier på grund af manglende relevante dokumenter om, hvorvidt **begrænsningerne i enkeltpersoners rettigheder** (navnlig retten til indsigt, berigtigelse og indsigelse) er nødvendige og forholdsmæssige i et demokratisk samfund og respekterer kernen i de grundlæggende rettigheder.

23. Det Europæiske Databeskyttelsesråd forventer også, at Kommissionen nøje overvåger den effektive beskyttelse af **personoplysninger, der overføres fra EU til Japan, på grundlag af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet gennem hele deres "livscyklus"** , selv om den japanske lovgivning pålægger en forpligtelse til at holde oplysningerne oprindelsesregistreret i højst tre år.

1.4 Om offentlige myndigheders adgang til data overført til Japan

24. Det Europæiske Databeskyttelsesråd har også analyseret de retlige rammer for japans statslige enheder, når de har adgang til personoplysninger, der er overført fra EU til Japan med henblik på retshåndhævelse eller national sikkerhed. I erkendelse af den japanske regerings forsikringer, som der henvises til som bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, har Det Europæiske Databeskyttelsesråd peget på en række aspekter, der skal afklares, og som giver anledning til bekymring. Heraf skal følgende fremhæves.

25. Inden for retshåndhævelse bemærker Det Europæiske Databeskyttelsesråd, at de juridiske principper, der gælder for adgang til data, ofte synes at svare til reglerne i EU, i det omfang de er tilgængelige. Manglen på oversættelser af flere lovtekster og relevant retspraksis gør det imidlertid vanskeligt at konkludere, at alle procedurer for adgang til data er nødvendige og forholdsmæssige, og at anvendelsen af disse principper anvendes på en måde, som "i det væsentlige svarer" til EU-retten.

26. Inden for området national sikkerhed anerkender Det Europæiske Databeskyttelsesråd, at den japanske regering har gentaget, at der kun kan indhentes oplysninger fra frit tilgængelige kilder eller gennem virksomheders frivillige udlevering af oplysninger, og at den ikke indsamler oplysninger om den brede offentlighed. Den er imidlertid klar over, at der blandt eksperter og i medierne er givet udtryk for bekymring, og den imødekommer en yderligere præcisering af Japans statslige enheders tilsynsforanstaltninger.

27. Hvad angår EU-borgeres ret til domstolsprøvelse på området for retshåndhævelse og national sikkerhed, glæder Det Europæiske Databeskyttelsesråd sig over, at Kommissionen og den japanske regering har forhandlet sig frem til en yderligere mekanisme, som gør det muligt for EU's borgere at give dem en yderligere klagemulighed, og dermed udvide den japanske databeskyttelsesmyndigheds beføjelser. Det giver dog fortsat anledning til bekymring, at denne nye mekanisme ikke fuldt ud kompenserer for manglerne i forbindelse med tilsyn og klageadgang i henhold til den japanske lovgivning. Det Europæiske Databeskyttelsesråd søger derfor yderligere præciseringer for at sikre, at denne nye mekanisme fuldt ud kompenserer for disse mangler.

1.5 Konklusion

28. Det Europæiske Databeskyttelsesråd er af den opfattelse, at denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet er af afgørende betydning. I sin egenskab af første tilstrækkelighedsbeslutning siden ikrafttrædelsen af den generelle forordning om databeskyttelse vil den danne **præcedens for fremtidige ansøgninger om et tilstrækkeligt beskyttelsesniveau samt for revisionen af de afgørelser om tilstrækkeligheden af beskyttelsesniveauet, der er truffet i henhold til direktiv 95/46**[9]. Det er også vigtigt at understrege, at enkeltpersoner er mere og mere bevidste om globaliseringens indvirkning på deres privatliv og henvender sig til deres tilsynsmyndigheder for at sikre, at der findes passende garantier, når deres personoplysninger overføres til udlandet. I lyset af disse konsekvenser mener Det Europæiske Databeskyttelsesråd, at Kommissionen bør sikre, at der ikke er mangler i den beskyttelse, der ydes af EU/Japan, og at denne specifikke type tilstrækkelighed er tilpasset kravene i artikel 45 i den generelle forordning om databeskyttelse.

29. Det Europæiske Databeskyttelsesråd glæder sig over den indsats, som Kommissionen og den japanske PPC har gjort for så vidt muligt at tilpasse den japanske lovramme til den europæiske. **De forbedringer**, der er indført med tillægsreglementet for at slå bro over nogle af forskellene mellem de to rammer, er meget vigtige og godt modtaget.

30. Som følge af en omhyggelig analyse af Kommissionens udkast til en afgørelse om tilstrækkeligheden af beskyttelsesniveauet og af den japanske databeskyttelsesramme, er Det Europæiske Databeskyttelsesråd imidlertid af den opfattelse, at **en række bekymringer sammen med behovet for yderligere præciseringer fortsat består**. Desuden rejser denne specifikke type tilstrækkelighed, der kombinerer en eksisterende national ramme med yderligere specifikke regler, også spørgsmål om den operationelle gennemførelse. I lyset af ovenstående henstiller Det Europæiske Databeskyttelsesråd, at Kommissionen tager hånd om de bekymringer og anmodninger om præcisering, der er rejst af Det

[9] Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Europæiske Databeskyttelsesråd, og fremlægger yderligere dokumentation og forklaringer vedrørende de spørgsmål, der rejses. Det Europæiske Databeskyttelsesråd opfordrer også Kommissionen til at foretage en gennemgang af denne afgørelse om et tilstrækkeligt beskyttelsesniveau (mindst) hvert andet år og ikke hvert fjerde år som foreslået i det nuværende udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

2 INDLEDNING

2.1 Den japanske ramme for databeskyttelse

31. Den japanske ramme for databeskyttelse blev for nylig moderniseret i 2017. Denne ramme omfatter flere søjler, hvor der findes en generel lov, nemlig loven om beskyttelse af personoplysninger (APPI). En anden vigtig retsakt er kabinettets bekendtgørelse om at håndhæve APPI ("kabinetsbekendtgørelsen"), som fastsætter visse centrale principper i APPI.

32. Baseret på en regeringsafgørelse, der blev vedtaget den 12. juni 2018[10], og artikel 6 i APPI, fik PPC beføjelse til at *"tage de nødvendige skridt til at slå bro over forskellene mellem systemer og operationer mellem Japan og det pågældende andet land med henblik på at sikre en hensigtsmæssig håndtering af de personoplysninger, der modtages fra hvert land"*[11]. Regeringsafgørelsen tyder også på, at de regler, der er vedtaget af PPC, og som supplerer eller er mere vidtgående end dem, der er fastsat i APPI, vil være bindende og kunne håndhæves over for de japanske virksomhedsledere[12].

33. I overensstemmelse hermed indledte PPC forhandlinger med Kommissionen og vedtog i juni 2018 strengere regler end dem i APPI og kabinettets bekendtgørelse, som skal anvendes på data, der overføres fra EU. Dette er tillægsbestemmelser til loven om beskyttelse af personoplysninger til håndtering af personoplysninger, der overføres fra EU på grundlag af en afgørelse om tilstrækkeligt beskyttelsesniveau, i det følgende benævnt "tillægsreglement"[13]. Dette tillægsreglement er også vedlagt som bilag til udkastet til Kommissionens gennemførelsesafgørelse, der blev offentliggjort i juli 2018.

34. Det er vigtigt at bemærke, at tillægsreglementet kun finder anvendelse på personoplysninger, der videregives fra Den Europæiske Union til Japan på grundlag af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet og har til formål at forbedre den gældende beskyttelse af disse oplysninger. Som sådan finder de ikke anvendelse på personoplysninger om fysiske personer i Japan eller fra andre lande end EØS.

35. Endvidere ønsker Det Europæiske Databeskyttelsesråd at gøre opmærksom på, at den ændrede APPI trådte i kraft den 30. maj 2017, og at PPC blev etableret i 2016 i sin nuværende form. Desuden er tillægsreglementet, som PPC har forhandlet med Kommissionen, endnu ikke trådt i kraft, da dette vil afhænge af, om Kommissionen anerkender Japan som en jurisdiktion, der svarer til den i EU.

2.2 Anvendelsesområdet for Det Europæiske Databeskyttelsesråds vurdering

[10] Det Europæiske Databeskyttelsesråd bemærker, at i henhold til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet blev denne regeringsafgørelse vedtaget den 12. juni 2018. Imidlertid blev Det Europæiske Databeskyttelsesråd kun forsynet med udkastet til regeringsafgørelsen fra april 2018.
[11] Regeringsafgørelse af 25. april 2018.
[12] (Der er yderligere oplysninger i afsnit 1.3.4 nedenfor).
[13] Tillægsreglementet, bilag I til Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, der blev sendt til Det Europæiske Databeskyttelsesråd i september 2018.

36. Kommissionens udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet er resultatet af en vurdering af de japanske databeskyttelsesregler, efterfulgt af forhandlinger med de japanske myndigheder. Resultatet af disse forhandlinger afspejles i de to bilag, der er vedlagt udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet: det første giver yderligere beskyttelse, som japanske virksomhedsledere skal anvende på behandlingen af personoplysninger, der overføres fra EU, mens det andet indeholder forsikringer og tilsagn fra den japanske regering om offentlige myndigheders adgang til data.

37. Det Europæiske Databeskyttelsesråd har undersøgt den japanske databeskyttelsesramme, tillægsreglementet, som Kommissionen har forhandlet sig frem til, og den japanske regerings garantier og tilsagn. Det Europæiske Databeskyttelsesråd forventes at afgive en uafhængig udtalelse om Kommissionens resultater, identificere eventuelle mangler i rammen for tilstrækkeligheden af beskyttelsesniveauet og bestræbe sig på at foreslå rettelser eller ændringer af disse.

38. Som nævnt i Det Europæiske Databeskyttelsesråds reference vedrørende et tilstrækkeligt beskyttelsesniveau, bør *"oplysningerne fra Kommissionen være udtømmende og sætte Det Europæiske Databeskyttelsesråd i stand til at foretage en egen vurdering af databeskyttelsesniveauet i tredjelandet"*[14].

39. De fleste dokumenter, som udgør en væsentlig del af det japanske retssystem, og som der henvises til i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, modtog Det Europæiske Databeskyttelsesråd imidlertid på engelsk. Det Europæiske Databeskyttelsesråd afgiver derfor nærværende udtalelse på grundlag af analysen af tilgængelige dokumenter på engelsk. Det Europæiske Databeskyttelsesråd tog hensyn til den gældende databeskyttelsesramme i Den Europæiske Union, herunder artikel 8 i den europæiske menneskerettighedskonvention (i det følgende benævnt: EMRK), der beskytter retten til privatliv og familieliv samt artikel 7, 8 og 47 i Den Europæiske Unions charter om grundlæggende rettigheder (i det følgende benævnt "charteret"), til beskyttelse af henholdsvis retten til privatliv og familieliv, retten til beskyttelse af personoplysninger og retten til effektive retsmidler og til en upartisk domstol. Ud over ovenstående gennemgik Det Europæiske Databeskyttelsesråd kravene i den generelle forordning om databeskyttelse samt så på den relevante retspraksis.

40. Formålet med denne øvelse er at sikre, at den japanske databeskyttelsesramme i det væsentlige svarer til Den Europæiske Unions ramme. Domstolen har videreudviklet begrebet "tilstrækkeligt beskyttelsesniveau", som allerede fandtes i direktiv 95/46. Det er vigtigt at minde om den standard, der er fastsat af Domstolen i Schrems, navnlig at de midler, som tredjelandet benytter i denne forbindelse med henblik på et sådant beskyttelsesniveau, kan afvige fra dem, der anvendes inden for [EU]", selvom "beskyttelsesniveauet" i tredjelandet "i alt væsentligt skal svare" til det, der garanteres i EU[15]. Målet er derfor ikke at afspejle den europæiske lovgivning, men at fastlægge de væsentlige og grundlæggende krav i den lovgivning, der undersøges. Et tilstrækkeligt beskyttelsesniveau kan opnås gennem en kombination af rettigheder for de registrerede og forpligtelser for dem, der behandler data, eller som udøver kontrol over en sådan behandling og tilsyn gennem uafhængige organer. Reglerne om databeskyttelse er imidlertid kun effektive, hvis de kan håndhæves og følges i praksis. Det er derfor nødvendigt at overveje ikke blot indholdet af de regler, der finder anvendelse på personoplysninger, der videregives til et tredjeland eller en international organisation, men også af det

[14] WP254, s. 3.
[15] Sag C362/14, Maximillian Schrems mod Data Protection Commissioner, af 6. oktober 2015 (præmis 73 og 74).

system, der er indført for at sikre sådanne reglers effektivitet. Effektive håndhævelsesmekanismer er af afgørende betydning for databeskyttelsesreglernes effektivitet[16].

2.3 Generelle bemærkninger og betænkeligheder

2.3.1 Særlige kendetegn ved denne type afgørelse om tilstrækkeligheden af beskyttelsesniveauet

41. Aftalen om et tilstrækkeligt beskyttelsesniveau mellem EU og Japan er den første, der skal undersøges i forhold til den nye retslige baggrund i den generelle forordning om databeskyttelse. Dette gør Det Europæiske Databeskyttelsesråds arbejde så meget desto vigtigere i lyset af de virkninger, som dette udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet vil få for fremtidige ansøgninger om et tilstrækkeligt beskyttelsesniveau.

42. Aftalen om tilstrækkeligt beskyttelsesniveau mellem EU og Japan vil også være den første gensidige aftale af sin art. Når og hvis EU anerkender Japan som værende i stand til at sikre et beskyttelsesniveau, der i det væsentlige svarer til beskyttelsesniveauet i den generelle forordning om databeskyttelse, vil Japan også udstede sin egen afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 24 i APPI, idet Japan anerkender, at EU tilbyder et tilstrækkeligt beskyttelsesniveau i henhold til den japanske databeskyttelsesramme. Således har denne påtænkte aftale om tilstrækkeligt beskyttelsesniveau mellem EU og Japan en særlig karakter, som Det Europæiske Databeskyttelsesråd har taget hensyn til i sin vurdering. Som nævnt ovenfor har den japanske PPC forhandlet specifikke, strengere regler med Kommissionen, som kun gælder for personoplysninger, der overføres fra EU. Disse strengere regler er bindende og kan håndhæves i henhold til kabinetsafgørelsen og skal overholdes af alle virksomheder, der håndterer personoplysninger i Japan (i det følgende benævnt PIHBO'er), når de behandler personoplysninger, der kommer fra EU i henhold til dette udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

43. Kommissionen har derfor baseret sin bedømmelse af et tilstrækkeligt beskyttelsesniveau ikke kun på den eksisterende generelle japanske databeskyttelsesramme, men også på disse specifikke regler. Det forhold, at tillægsreglementet var nødvendigt for at supplere APPI, er et tegn på, at Kommissionen anerkender, at den japanske databeskyttelseslovgivning ikke i sig selv i det væsentlige svarer til den generelle forordning om databeskyttelse.

44. **På baggrund af ovennævnte spørgsmål opfordrer Det Europæiske Databeskyttelsesråd Kommissionen til at sikre, at denne nye struktur for tilstrækkelighed, som er den første, der vedtages i henhold til den generelle forordning om databeskyttelse, og som bygger på tillægsreglementet, bliver et bæredygtigt og pålideligt system, der ikke vil give anledning til praktiske problemer med hensyn til den konkrete og effektive overholdelse fra de japanske instansers side og håndhævelse fra PPC's side.**

2.3.2 Pålideligheden af oversættelser

45. Som Kommissionen har Det Europæiske Databeskyttelsesråd arbejdet på grundlag af engelske oversættelser fra de japanske myndigheder[17]. Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til at præcisere, at den har baseret sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet på de modtagne engelske oversættelser og kontrollerer kvaliteten og pålideligheden af disse oversættelser regelmæssigt.

[16] WP254, s. 2.
[17] Kommissionen har kontrolleret disse oversættelser.

2.3.3 Sektorspecifik tilstrækkelighed

46. Afgørelsen om tilstrækkeligheden af beskyttelsesniveauet i dette udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet er begrænset til beskyttelsen af personoplysninger af PIHBO'er som omhandlet i APPI. Dette betyder, at tilstrækkeligheden er sektorspecifik, da den kun gælder for den private sektor, idet overførsel af personoplysninger mellem offentlige myndigheder og organer ikke er omfattet. Kommissionen nævner i øjeblikket kort dette særlige aspekt af tilstrækkeligheden i betragtning 10 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

47. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til udtrykkeligt at nævne den sektorspecifikke karakter af denne afgørelse om tilstrækkeligt beskyttelsesniveau i titlen til gennemførelsesafgørelsen samt i dens artikel 1 i overensstemmelse med artikel 45, stk. 3, i den generelle forordning om databeskyttelse.**

2.3.4 Bindende karakter af tillægsreglementet og PPC's retningslinjer

48. Artikel 6 i APPI nævner, at "regeringen... skal vedtage nødvendige lovgivningsmæssige og andre foranstaltninger for at kunne træffe diskretionære foranstaltninger til beskyttelse af personoplysninger, hvis korrekte behandling kræver en nøje gennemførelse for at opnå en forstærket beskyttelse af personers rettigheder og interesser, og skal træffe de nødvendige foranstaltninger i samarbejde med regeringerne i andre lande med henblik på at opbygge et internationalt tilpasset system til behandling af personoplysninger gennem fremme af samarbejdet med en international organisation og andre internationale rammer". Selv om regeringen i denne artikel i APPI klart er udpeget som kompetent til at træffe sådanne retlige foranstaltninger, henviser den ikke direkte til PPC som kompetent organ til at vedtage specifikke regler[18]. På grund af tidspres var Det Europæiske Databeskyttelsesråd ikke i stand til at indsamle, gennemgå og undersøge eksisterende beviser i den henseende.

49. **I lyset af betydningen af dette spørgsmål noterer Det Europæiske Databeskyttelsesråd sig Kommissionens og de japanske myndigheders gentagne forpligtelser og tilsagn vedrørende tillægsreglementets bindende og eksigible karakter. Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til løbende at overvåge dets retskraft og effektive anvendelse i Japan, da dets retslige status udgør en væsentligt bestanddel af det tilstrækkelige beskyttelsesniveau mellem EU og Japan.**

50. Desuden henviser Kommissionen i flere afsnit i sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet til PPC's retningslinjer.

51. Selv om Kommissionen præciserer, at retningslinjerne giver en autoritativ fortolkning af APPI i betragtning 16 i sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, henviser den i samme betragtning til disse retningslinjers retskraft: "Ifølge de oplysninger, der er modtaget fra PPC, betragtes disse retningslinjer som bindende regler, der udgør en integreret del af den retlige ramme, som skal læses sammen med teksten til APPI, kabinetsbekendtgørelsen, PPC-reglerne og et sæt Q & A udarbejdet af PPC."[19]

---

[18] Ifølge en artikel, der blev offentliggjort i juli 2018, hvori der var et udkast til tillægsreglementet, ville den retlige bindende karakter af dette reglement sandsynligvis blive genstand for en intern debat i landet. Se Fujiwara S., ., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (juli 2018): s. 19.

[19] Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november 2018, betragtning 16.

52. Imidlertid er Det Europæiske Databeskyttelsesråds opfattelse, baseret på de samme oplysninger fra PPC, at retningslinjerne ikke er juridisk bindende. De giver snarere en "autoritativ fortolkning" af loven. PPC hævder, at retningslinjerne følges af PIHBO'er i praksis og anvendes af PPC til at håndhæve loven over for PIHBO'er og af domstolene, når de afsiger dom. Disse elementer udgør imidlertid ikke tilstrækkeligt bevis for, at retningslinjerne er retligt bindende standarder.

53. **Det Europæiske Databeskyttelsesråd ønsker en præcisering af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet i forhold til PPC's retningslinjernes bindende karakter og anmoder Kommissionen om nøje at overvåge dette aspekt.**

54. I henhold til PPC følges retningslinjerne i praksis, da det er et spørgsmål om lokal sædvane. PPC nævner, at de japanske domstole anvender PPC-retningslinjerne til at gøre deres domme gældende, når de anvender APPI-regler. Kommissionen henviser til en retsafgørelse[20], der er afsagt i 2006, og som indeholder dokumentation for, at de japanske domstole baserer sig på retningslinjer for deres konklusioner. Til trods for at Det Europæiske Databeskyttelsesråd ikke fik denne domstolsafgørelse, ville Det Europæiske Databeskyttelsesråd sætte pris på, om Kommissionen kunne fremlægge en nyere domstolsafgørelse, hvis det er muligt, enten inden for databeskyttelse eller i en anden sektor, hvor de japanske domstole har anvendt PPC-retningslinjerne eller andre tilsvarende retningslinjer som grundlag for deres afgørelse.

2.3.5 Regelmæssig gennemgang af afgørelsen om tilstrækkeligt beskyttelsesniveau

55. I henhold til artikel 45, stk. 3, i den generelle forordning om databeskyttelse skal der foretages en periodisk revision mindst hvert fjerde år. Ifølge Det Europæiske Databeskyttelsesråds reference vedrørende et tilstrækkeligt beskyttelsesniveau[21] er der tale om en generel tidsramme, som skal tilpasses til det enkelte tredjeland eller den enkelte internationale organisation med en afgørelse om tilstrækkeligheden af beskyttelsesniveauet. Afhængigt af de særlige omstændigheder kan der være behov for kortere revisionsintervaller. Hændelser eller andre oplysninger om eller ændringer af de retlige rammer i det pågældende tredjeland eller den pågældende internationale organisation kan udløse et behov for en revision forud for tidsplanen. Det forekommer også hensigtsmæssigt først at foretage en første revision af en helt ny afgørelse om tilstrækkeligheden af beskyttelsesniveauet forholdsvis hurtigt og gradvist tilpasse revisionsintervallerne afhængigt af resultatet.

56. Under hensyntagen til en række faktorer, herunder det forhold, at APPI trådte i kraft i 2017, at PPC blev etableret i 2016, og at der ikke foreligger nogen oplysninger eller dokumentation om den praktiske anvendelse af tillægsreglementet, **opfordrer Det Europæiske Databeskyttelsesråd Kommissionen til at foretage en revision af denne afgørelse (mindst) hvert andet år og ikke hvert fjerde år som foreslået i det nuværende udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet**.

2.3.6 Internationale forpligtelser indgået af Japan

57. I henhold til artikel 45, stk. 2, litra c), i den generelle forordning om databeskyttelse og tilstrækkeligheden af beskyttelsesniveauet[22], skal Kommissionen, når den vurderer tilstrækkeligheden af beskyttelsesniveauet i et tredjeland, bl.a. tage hensyn til de internationale forpligtelser, som tredjelandet har påtaget sig, eller andre forpligtelser, der følger af tredjelandets deltagelse i multilaterale eller regionale systemer, navnlig i forbindelse med beskyttelse af personoplysninger,

[20] Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november 2018, side 5, fodnote 16, "distriktsdomstolen i Osaka, beslutning af 19. maj 2006, Hanrei Jiho, bd. 1948, s. 122.
[21] WP254, s. 3.
[22] WP254, s. 2.

samt gennemførelsen af sådanne forpligtelser. Endvidere bør tredjelandets tiltrædelse af Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger ("konvention 108 +"[23] og tillægsprotokollen hertil tages i betragtning.

58. **I denne henseende bemærker Det Europæiske Databeskyttelsesråd, at Japan er observatør for det rådgivende udvalg om konvention 108 +.**

2.3.7 Databeskyttelsesmyndighedernes[24] beføjelser til at anlægge sag ved en domstol vedrørende gyldigheden af en afgørelse om tilstrækkeligt beskyttelsesniveau

59. Det Europæiske Databeskyttelsesråd understreger, at selv om betragtning 179 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet kun nævner tilfælde, hvor en databeskyttelsesmyndighed har modtaget en klage, der stiller spørgsmålstegn ved, om en afgørelse om tilstrækkeligheden af beskyttelsesniveauet er forenelig med privatlivets fred og databeskyttelse, skal denne erklæring forstås som et eksempel på situationer, hvor en databeskyttelsesmyndighed kan indbringe sagen for en national domstol, hvilket også kunne være muligt, hvis der ikke blev indgivet en klage, snarere end som en begrænsning af de beføjelser, der er tillagt databeskyttelsesmyndighederne i henhold til den generelle forordning om databeskyttelse og medlemsstaternes nationale lovgivning i denne henseende. Bestemmelserne i den generelle forordning om databeskyttelse omfatter nemlig både beføjelsen til at suspendere dataoverførsler, selv når de er baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og til at anlægge sag vedrørende gyldigheden af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og er ikke begrænset til tilfælde, hvor de har modtaget en klage, hvis deres nationale lovgivning giver dem beføjelse til at gøre dette mere generelt og uafhængigt af en klage i overensstemmelse med de relevante bestemmelser i den generelle forordning om databeskyttelse.

60. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til i sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet at præcisere, at tilsynsmyndighedernes beføjelser til at anlægge sag mod gyldigheden af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet på grundlag af en klage blot er en illustration af databeskyttelsesmyndighedernes bredere beføjelser i henhold til den generelle forordning om databeskyttelse, som omfatter beføjelsen til at suspendere overførsler og anlægge sag vedrørende gyldigheden af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, såfremt der ikke foreligger en klage, hvis deres nationale lovgivning giver mulighed herfor.**

3 KOMMERCIELLE ASPEKTER

3.1 Indholdsprincipper

61. Kapitel 3 i referencen vedrørende et tilstrækkeligt beskyttelsesniveau omhandler "indholdsprincipper". Et tredjelands eller en international organisations system skal indeholde disse principper, for at det beskyttelsesniveau, der tilvejebringes, i det væsentlige svarer til det beskyttelsesniveau, der er fastsat i EU-lovgivningen. Det Europæiske Databeskyttelsesråd anerkender, at det japanske retssystem følger en anden tilgang end den i den generelle forordning om databeskyttelse for at give retten til privatlivets fred virkning. Selv om retten til privatlivets fred ikke

[23] Konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108+, 18. maj 2018).
[24] Sag C362/14, Maximillian Schrems mod Data Protection Commissioner, af 6. oktober 2015.

er nedfældet i den japanske forfatning i sig selv, er den i kraft af retspraksis blevet anerkendt som en forfatningsmæssig rettighed, hvilket også fremgår af Kommissionens afgørelse[25].

62. Især fordi den japanske tilgang markant afviger fra den europæiske tilgang, skal det nøje overvåges, om ikke kun enkelte aspekter, men systemet som helhed i sidste ende giver et beskyttelsesniveau, der "i det væsentlige er tilsvarende". Dette betyder, at potentielle "mangler" med hensyn til et enkelt indholdsprincip kan opvejes af visse andre aspekter, der skaber hensigtsmæssige kontrolforanstaltninger.

3.1.1 Begreber

63. På grundlag af referencen vedrørende et tilstrækkeligt beskyttelsesniveau bør de grundlæggende databeskyttelsesbegreber og/eller principper være defineret i tredjelandets retlige rammer. Selv om disse ikke skal afspejle terminologien i den generelle forordning om databeskyttelse, bør de afspejle og være i overensstemmelse med de begreber, der er nedfældet i den europæiske databeskyttelseslovgivning. Den generelle forordning om databeskyttelse indeholder f.eks. følgende vigtige begreber: "personoplysninger", "behandling af personoplysninger", "dataansvarlig", "databehandler", "modtager" og "følsomme oplysninger"[26].

64. APPI indeholder også en række definitioner, som f.eks. "personlig information", "personoplysninger", "virksomhedsleder, der håndterer personoplysninger". **Det ser dog ud til, at APPI ikke indeholder en definition af udtrykket "behandling af personoplysninger", som svarer til udtrykket "håndtering af personoplysninger".**

65. Med hensyn til definitionen af udtrykket "behandling af personoplysninger" indgav PPC skriftlige svar til Det Europæiske Databeskyttelsesråds spørgsmål om denne definition. Kommissionen henviste til dette svar på udkastet til Kommissionens afgørelse. *"Selv om APPI ikke anvender udtrykket "behandling", bygger den på det tilsvarende begreb "håndtering", som ifølge de oplysninger, der modtages af PPC, dækker "enhver form for behandling af personoplysninger", herunder erhvervelse, input, akkumulering, organisering, lagring, redigering/forarbejdning, fornyelse, produktion, forsikring, produktion, anvendelse eller tilvejebringelse af personoplysninger.[27]"*

66. Da henvisningen til denne definition ikke er blevet udarbejdet, opfordrer Det Europæiske Databeskyttelsesråd **Kommissionen til nøje at overvåge, at definitionen af ovennævnte begreb, som fastsat af PPC, reelt følges i praksis.**

3.1.1.1 Begrebet databehandler og forpligtelser for en "administrator"

67. Som nævnt ovenfor kræver referencen vedrørende et tilstrækkeligt beskyttelsesniveau, at de grundlæggende databeskyttelsesbegreber og/eller principper er defineret i tredjelandets retlige rammer.

68. APPI omfatter en definition af en "virksomhedsleder, der håndterer personoplysninger", og som ifølge Kommissionen omfatter både begrebet dataansvarlig og databehandler, jf. den generelle forordning

[25] Det Europæiske Databeskyttelsesråd har ikke modtaget den engelske oversættelse af denne retsafgørelse. Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november 2018, fodnote 9.
[26] WP254, s. 4.
[27] Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november 2018, betragtning 17.

om databeskyttelse, og skelner ikke mellem de to[28]. Imidlertid omfatter APPI også en "administrator" i sin artikel 22, som på visse måder ligner udtrykket en databehandler i henhold til den generelle forordning om databeskyttelse.

69. Som PPC har forklaret i sine svar til Det Europæiske Databeskyttelsesråd og ligeledes medtaget i Kommissionens udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, betragtes en administrator som ækvivalent med en databehandler i henhold til den generelle forordning om databeskyttelse, som har fået til opgave at behandle personoplysninger af en PIHBO. Denne administrator har samme forpligtelser og rettigheder som enhver PIHBO, herunder de rettigheder i tillægsreglementet for personoplysninger, der overføres fra EU. Den PIHBO, der overdrager behandlingen af personoplysninger til en administrator, er forpligtet til at "føre det nødvendige og passende tilsyn"[29] med administratoren.

70. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til at redegøre for administratorens status og forpligtelser, når administratoren ændrer formålet med og metoderne til behandling af oplysninger og præciserer, om den registreredes samtykke fortsat er en nødvendig betingelse for en sådan ændring af formål eller fastlæggelse af midler[30].**

3.1.1.2 Begrebet opbevarede personoplysninger

71. APPI indeholder begrebet "opbevarede personoplysninger", der betragtes som en underkategori af personoplysninger. Ifølge APPI finder bestemmelserne om den registreredes rettigheder[31] kun anvendelse på opbevarede personoplysninger. Definitionen af opbevarede personoplysninger er indeholdt i artikel 2, stk. 7, i APPI.

72. Opbevarede personoplysninger er andre personoplysninger end dem, der i) skal slettes inden for en periode på højst 6 måneder[32], eller ii) som falder ind under undtagelserne i artikel 4 i kabinetsbekendtgørelsen, og som sandsynligvis vil skade offentligheden eller andre interesser, hvis deres tilstedeværelse eller fravær offentliggøres.

73. Punkt 2 i tillægsreglementet fastsætter, at "personoplysninger, der modtages fra EU på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, skal behandles som opbevarede personoplysninger, uanset den frist inden for hvilken disse er fastsat til at blive slettet."

74. Det er imidlertid ikke et krav, at personoplysninger, der falder ind under artikel 4 i kabinetsbekendtgørelsen, skal behandles som værende opbevarede personoplysninger, og at de registreredes rettigheder ikke finder anvendelse.

75. Af artikel 23 i den generelle forordning om databeskyttelse fremgår det, at ligesom artikel 4 i kabinetsbekendtgørelsen kan EU-retten eller medlemsstaternes nationale ret begrænse de forpligtelser, der gælder for den registrerede, og de rettigheder, der er tilgængelige for den registrerede. Dette kan gøres ved hjælp af en lovgivningsmæssig foranstaltning. Disse begrænsninger skal respektere kernen i de grundlæggende rettigheder og friheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund.

---

[28] Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november 2018, betragtning 35.

[29] Artikel 22 i den ændrede lov om beskyttelse af personoplysninger (APPI) trådte i kraft den 30. maj 2017.

[30] Artikel 23, stk. 5, litra i), i APPI. Se også afsnittet om gennemsigtighedsprincippet nedenfor.

[31] Artikel 27 til 30 i APPI.

[32] Ændring af kabinetsbekendtgørelsen om ikrafttræden af lov om beskyttelse af personoplysninger (kabinetsbekendtgørelsen), som trådte i kraft den 30. maj 2017, artikel 5.

76. Med hensyn til indholdet af de undtagelser, der er fastsat i kabinetsbekendtgørelsens artikel 4, er Det Europæiske Databeskyttelsesråd ikke blevet forsynet med tilstrækkelig dokumentation om disse begrænsninger eller yderligere elementer for at præcisere anvendelsesområdet for disse bestemmelser[33]. Det Europæiske Databeskyttelsesråd er ikke i stand til at vurdere, om disse begrænsninger af registreredes rettigheder er begrænset til, hvad der ville blive betragtet som strengt nødvendigt og forholdsmæssigt i henhold til EU-retten, og at det derfor i det væsentlige ville svare til de rettigheder, der gives til registrerede i EU.

77. **På grund af manglende relevante dokumenter vil Det Europæiske Databeskyttelsesråd også gerne have garantier fra Kommissionen, om begrænsninger af enkeltpersoners rettigheder (navnlig retten til indsigt, berigtigelse og indsigelse) er nødvendige og forholdsmæssige i et demokratisk samfund og respekterer kernen i de grundlæggende rettigheder.**

78. Et væsentligt krav i henhold til den generelle forordning om databeskyttelse er, at personoplysninger beskyttes gennem hele deres "livscyklus".

79. Under hensyntagen til, at tillægsreglementet kun finder anvendelse på personoplysninger, der overføres fra EU, vil Det Europæiske Databeskyttelsesråd sætte pris på at modtage yderligere oplysninger om den praktiske gennemførelse af disse regler fra PIHBO'er, navnlig når disse data videregives til en anden PIHBO, efter at de er overført til Japan første gang.

80. Kommissionen har i betragtning 15 i sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet præciseret, at PIHBO'er, der modtager og/eller viderebehandler personoplysninger fra EU, vil være underlagt en retlig forpligtelse til at overholde tillægsreglementet, og at de for at gøre dette skal sikre, at de kan identificere sådanne personoplysninger i hele deres "livscyklus".

81. PPC[34] har i sine svar forklaret, at en sådan identifikation vil blive foretaget ved hjælp af tekniske metoder (mærkning) eller organisatoriske metoder (lagring af data fra EU i en særlig database).

82. I fodnote 14 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet forklarer Kommissionen, at PIHBO'er skal registrere oplysningerne om oprindelsen af EU-data, så længe det er nødvendigt for at kunne overholde tillægsreglementet. Dette er også nedfældet i artikel 26, stk. 1, 3, og 4, i APPI, hvoraf det fremgår, at en PIHBO er forpligtet til at bekræfte og registrere kilden til disse oplysninger og alle forhold i forbindelse med erhvervelsen af disse data.

83. Det Europæiske Databeskyttelsesråd bemærker imidlertid, at artikel 18 i PPC's regler[35] fastsætter, at kravet om dataregistrering for PIHBO'er er begrænset til maksimalt tre år for sager, der falder uden for de specifikke registreringsmetoder, der er beskrevet i artikel 16 i PPC's regler (ved hjælp af et skriftligt dokument, elektromagnetisk registrering eller mikrofilm). Dette fremgår også af betragtning 71 i Kommissionens udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet: *"Som anført i artikel 18 i PPC's regler skal disse optegnelser opbevares i en periode på et til tre år, afhængigt af omstændighederne".*

84. Selv om PIHBO'er, som anført af Kommissionen i fodnote 14 til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, ikke har forbud mod at føre fortegnelser over dataenes

[33] Det Europæiske Databeskyttelsesråd er ikke blevet tildelt de højesteretsafgørelser, der er omhandlet i betragtning 53 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet.
[34] Bilag III til denne udtalelse.
[35] Fuldbyrdelsesregler for lov om beskyttelse af personoplysninger (kabinetsbekendtgørelsen), som trådte i kraft den 30. maj 2017, artikel 16.

oprindelse i mere end tre år for at være i stand til at opfylde deres forpligtelser i henhold til punkt 2 i tillægsreglementet, er dette hverken klart afspejlet i den japanske lovgivning eller i tillægsreglementet. Det Europæiske Databeskyttelsesråd mener, at der er en risiko for, at PIHBO'er i realiteten vil følge artikel 18 i PPC's regler, selv når de behandler oplysninger fra EU. Dette skyldes hovedsagelig, at der for øjeblikket — efter Det Europæiske Databeskyttelsesråds opfattelse og baseret på tilgængelige dokumenter — ikke er nogen bestemmelser, der forpligter PIHBO'er til at overholde tillægsreglementet i stedet for. Dette ville resultere i, at data, der overføres fra EU, ikke længere er beskyttet af den yderligere beskyttelse i tillægsreglementet.

85. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til nøje at overvåge den effektive beskyttelse af personoplysninger, der overføres fra EU til Japan, på grundlag af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet gennem hele deres livscyklus, selv om den japanske lovgivning pålægger en forpligtelse til at holde oplysningerne oprindelsesregistreret i højst tre år.**

3.1.2 Grunde til lovlig og rimelig behandling til lovlige formål

86. Ifølge referencen vedrørende et tilstrækkeligt beskyttelsesniveau skal data behandles på en lovlig, rimelig og legitim måde[36] i overensstemmelse med den generelle forordning om databeskyttelse. Retsgrundlaget, hvorunder personoplysninger behandles på en lovlig, rimelig og berettiget måde, bør fastlægges på en tilstrækkelig klar måde. Den europæiske ramme anerkender flere sådanne legitime grunde, herunder f.eks. bestemmelser i national ret, samtykke fra den registrerede, opfyldelse af en kontrakt eller den dataansvarliges eller en tredjemands legitime interesser, når den enkeltes interesser ikke har forrang.

87. Under APPI spiller samtykke en central rolle i det japanske retssystem for databeskyttelse. Samtykke er det centrale retsgrundlag for behandling af personoplysninger i Japan og et af de vigtigste retsgrundlag for overførsel af personoplysninger fra Japan til et tredjeland. Desuden kræves der samtykke i forbindelse med en ændring af formålet med behandlingen.

88. I henhold til punkt 3 i tillægsreglementet er retsgrundlaget for behandling af personoplysninger, der overføres fra EU til Japan, det retsgrundlag, for hvilket der overføres data til Japan. Hvis PIHBO'en ønsker at behandle disse oplysninger yderligere til et andet formål, skal vedkommende indhente den registreredes samtykke på forhånd.

89. Det Europæiske Databeskyttelsesråd mener, at kvaliteten af samtykke, navnlig på grund af dets centrale rolle i de japanske retlige rammer, skal opfylde de grundlæggende krav til begrebet samtykke, dvs. i henhold til EU-retten, en *"frivillig, specifik, informeret og utvetydig angivelse af den registreredes ønsker... "*. Den registrerede kan trække sit samtykke tilbage som en væsentlig sikkerhedsforanstaltning for at sikre den registreredes frie vilje hele tiden[37]. Retten til at trække samtykket tilbage, som et obligatorisk samtykke, synes at mangle i de japanske retlige rammer. Ifølge PPC-retningslinjerne[38] er en tilbagetrækning af samtykket blot "ønskelig" og betinget af "forretningsaktiviteternes karakteristika, størrelse og status".

---

[36] WP254, s. 4.

[37] Den generelle forordning om databeskyttelse, artikel 4, stk. 11. For yderligere oplysninger se også de relevante retningslinjer fra Det Europæiske Databeskyttelsesråd om samtykke (WP259 af 10. april 2018).

[38] Konsortium for databeskyttelse, juridisk og teknisk forskning og analyse (DPC), en vurdering af beskyttelsesniveauet for personoplysninger, der stilles til rådighed i henhold til japansk lovgivning, s. 46: "Med hensyn til beskyttelse af berørte personers rettigheder og interesser som f.eks. forbrugere er det ønskeligt, at der, hvis der kommer en anmodning fra den berørte person vedrørende de opbevarede personoplysninger, yderligere tages hensyn til den berørte persons anmodning på en sådan måde, at der ophøres med at sende

3.1.3 Gennemsigtighedsprincippet

90. På grundlag af artikel 5 i den generelle forordning om databeskyttelse er gennemsigtighed et grundlæggende princip i EU's databeskyttelsessystem[39]. Referencen vedrørende et tilstrækkeligt beskyttelsesniveau nævner udtrykkeligt "gennemsigtighed" som et af de principper, der skal tages hensyn til ved vurderingen af det i det væsentlige ækvivalente beskyttelsesniveau, der er fastsat af et tredjeland. Princippet om gennemsigtighed og rimelighed tilstræber at sikre, at den registrerede har kontrol over sine data, og med henblik herpå skal oplysningerne som hovedregel gives til den registrerede på en proaktiv måde. For så vidt angår værnet om privatlivets fred henviste artikel 29-Gruppen[40] i sin udtalelse 1/2016 til bilag II, II 1, litra b), i aftalen om værnet om privatlivets fred (meddelelse til den enkelte) og anførte, at en organisation, hvis oplysningerne ikke indsamles direkte, bør underrette den registrerede "på det tidspunkt, hvor oplysningerne registreres af foretagendet, der indgår i værnet om privatlivets fred" (afsnit 2.2.1.a). En offentligt tilgængelig politik for beskyttelse af privatlivets fred er et yderligere kriterium (se afsnit 2.2.1.b). Det blev derfor allerede i henhold til direktiv 95/46/EF anset for nødvendigt at underrette den registrerede direkte.

91. En første bekymring kommer til udtryk over den måde, oplysningerne leveres til den registrerede under APPI. I henhold til artikel 27, stk. 1, i APPI er en PIHBO forpligtet til at give de oplysninger, der er beskrevet i artikel 27, stk. 1, i APPI, ved at sørge for, at de er "i en tilstand, så den berørte person kan få kendskab til dem". Denne formulering gør det imidlertid ikke klart, i hvilket omfang PIHBO'en skal træffe positive foranstaltninger for reelt at informere den registrerede.

92. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til at præcisere betydningen af udtrykket "kan få kendskab til" og om, hvorvidt APPI generelt fastsætter en forpligtelse til reelt at informere de registrerede.**

93. Desuden kan der i henhold til referencen vedrørende et tilstrækkeligt beskyttelsesniveau eksistere begrænsninger for de oplysninger, der skal stilles til rådighed for den registrerede, svarende til artikel 23 i den generelle forordning om databeskyttelse. På samme måde indeholder artikel 14, stk. 5, i den generelle forordning om databeskyttelse en undtagelse fra retten til at blive informeret, når oplysningerne sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre gennemførelsen af behandlingen. Men selv i dette tilfælde skal den dataansvarlige stille en eller anden form for information til rådighed, f.eks. ved at gøre "generelle" oplysninger offentligt tilgængelige. Endvidere skal den registrerede underrettes, når risikoen ophører med at eksistere[41]. Disse aspekter er vigtige for at sikre det grundlæggende princip om retfærdighed.

94. I henhold til artikel 23 i APPI skal en PIHBO på forhånd give den registrerede oplysninger om, hvorvidt han/hun videregiver vedkommendes oplysninger til en tredjepart, enten implicit ved at få vedkommendes samtykke eller udtrykkeligt ved en fritagelsesmeddelelse. Det er Europæiske Databeskyttelsesråds forståelse, at den registrerede ikke underrettes om, at vedkommendes data ikke er opbevarede personoplysninger under APPI, fordi de er omfattet af undtagelserne i kabinetsbekendtgørelsens artikel 4. Som følge heraf vil de ikke kunne drage fuld fordel af deres

---

direct mail, eller at der frivilligt ophøres med udnyttelsen osv. under hensyntagen til forretningsaktiviteternes karakteristika, størrelse og status".

[39] WP 254, kapitel 3, punkt 7, s. 5; se også betragtning (39) i den generelle forordning om databeskyttelse.

[40] Denne arbejdsgruppe blev nedsat ved artikel 29 i direktiv 95/46/EF. Det var et uafhængigt europæisk rådgivende organ for databeskyttelse og privatlivets fred. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF. Artikel 29-Gruppen er nu blevet til Det Europæiske Databeskyttelsesråd.

[41] Tele2, forenede sager C 203/15 og C 698/15, Domstolens dom af 21. december 2016, Sml. 121 og Digital Rights Ireland, forenede sager C-293/12 og C-594/12, Domstolens dom af 8. april 2014, Sml. 54-62.

rettigheder. De registrerede er heller ikke informeret i de tilfælde, der er omhandlet i artikel 18, stk. 4, i APPI.

95. **Det Europæiske Databeskyttelsesråd anerkender, at rettighederne kan være begrænset på grund af legitime mål, der forfølges af PIHBO og de statslige myndigheder. Samtidig mener Det Europæiske Databeskyttelsesråd, at der som minimum bør være generelle oplysninger om muligheden for at begrænse rettighederne for de mål, der er omhandlet i loven, og at den registrerede bør underrettes, når de risici, som oplysningerne er begrænset til, ophører med at eksistere.**

96. Endelig behandles andre aspekter af gennemsigtighed yderligere nedenfor. Disse vedrører de risici, som overførslen til et tredjeland indebærer[42], og oplysninger om formålet med behandling i forbindelse med den automatiserede beslutningstagning, herunder profilering.[43]

3.1.4 Begrænsninger for videreoverførsler

97. Det Europæiske Databeskyttelsesråd glæder sig over den indsats, som de japanske myndigheder og Kommissionen har gjort for at øge beskyttelsesniveauet for videregivelser i punkt 4 i tillægsreglementet, hvilket udelukker, at personoplysninger, der overføres fra EU, yderligere videregives til et tredjeland på grundlag af APEC-CBPR. Desuden anerkender Det Europæiske Databeskyttelsesråd, at Kommissionen i betragtning 177 og 184 i sit nye udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet har forpligtet sig til at ophæve afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, når videregivelse ikke længere sikrer kontinuiteten i beskyttelsen. Det Europæiske Databeskyttelsesråd vil dog gerne rejse to punkter vedrørende disse overførsler af EU-personoplysninger fra Japan til tredjelande.

98. **Anvendelsen af samtykke som grundlag for videregivelse af oplysninger fra Japan til et tredjeland i det japanske retssystem giver anledning til bekymring, da Det Europæiske Databeskyttelsesråd mener, at de oplysninger, der gives til den registrerede i EU forud for samtykke, ikke synes at være fyldestgørende.**

99. Artikel 24 i APPI forbyder videregivelse af personoplysninger til en tredjepart uden for Japans område uden den pågældende persons forudgående samtykke. Punkt 4 i tillægsreglementet fastsætter, at registrerede i EU skal informeres om omstændighederne omkring den overførsel, der kræves for at træffe en afgørelse om samtykke.

100. Kommissionen konkluderer i sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, at punkt 4 i tillægsreglementet sikrer et særligt godt informeret samtykke fra den registrerede i EU[44], idet vedkommende vil blive underrettet om, at oplysningerne vil blive overført til udlandet og til det specifikke bestemmelsesland. Dette vil gøre det muligt for den registrerede at vurdere risikoen for privatlivets fred i forbindelse med overførslen.

101. I henhold til gennemsigtighedsprincippet i forbindelse med tilstrækkeligheden af beskyttelsesniveauet skal der sikres en vis grad af retfærdighed, når enkeltpersoner underrettes. I forbindelse med videregivelse af oplysninger, der er baseret på samtykke, er Det Europæiske Databeskyttelsesråd af den opfattelse, at de registrerede for at sikre en så passende grad af retfærdighed bør underrettes udtrykkeligt om de mulige risici for sådanne overførsler som følge af manglen på tilstrækkelig beskyttelse i tredjelandet og manglen på passende sikkerhedsforanstaltninger forud for samtykke. En

[42] Se afsnit 2.1.4.
[43] Se afsnit 2.1.6.
[44] Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november, betragtning 76.

sådan meddelelse bør f.eks. indeholde oplysninger om, at der i tredjelandet muligvis ikke er en tilsynsmyndighed og/eller databehandlingsprincipper, og/eller at den registreredes rettigheder måske slet ikke er tilgodeset i tredjelandet[45]. For Det Europæiske Databeskyttelsesråd er det afgørende at give disse oplysninger, for at den registrerede kan give sit samtykke med fuldt kendskab til de specifikke forhold i forbindelse med overførslen[46].

102. Informeret samtykke er også vigtigt med hensyn til sektorspecifikke undtagelser. Afgørelsen om tilstrækkeligheden af beskyttelsesniveauet omfatter ikke visse typer af behandling, der foretages af visse organer såsom universiteter med henblik på behandling af personoplysninger til akademiske formål. Det Europæiske Databeskyttelsesråd berører her det specifikke scenarie, hvor data, der overføres fra EU i henhold til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet — f.eks. HR-data fra Erasmus-studerende i Japan — anvendes til et andet formål, der falder uden for anvendelsesområdet for afgørelsen om tilstrækkeligheden af beskyttelsesniveauet (f.eks. forskningsformål) med den registreredes samtykke — og derfor ikke længere er omfattet af den yderligere beskyttelse, som tillægsreglementet giver.

103. Kommissionen anfører i betragtning 38 i sit udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, at et sådant scenario vil falde ind under yderligere videregivelse, og at PIHBO, hvis det finder sted, skal give den registrerede alle de nødvendige oplysninger, inden vedkommendes samtykke indhentes, herunder at personoplysningerne ikke vil falde ind under den beskyttelse, der ligger i APPI-reglerne.

104. Punkt 4 i tillægsreglementet kræver kun, at PIHBO'en indhenter den registreredes samtykke efter at have fået information om omstændighederne omkring den overførsel, der er nødvendig for, at den berørte person kan træffe afgørelse om samtykke.

105. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til at sikre, at de oplysninger, der skal gives til den registrerede "om omstændighederne omkring overførslen", omfatter oplysninger om de mulige risici for overførsler, der opstår som følge af manglen på tilstrækkelig beskyttelse i tredjelandet, og manglen på passende garantier, eller i tilfælde af sektorspecifikke undtagelser, om den manglende beskyttelse, der ligger i tillægsreglementet og APPI.**

106. **Videregivelse af personoplysninger kan finde sted til tredjelande, som bliver genstand for en eventuel senere japansk afgørelse om tilstrækkeligheden af beskyttelsesniveauet.**

107. Uden at det berører de undtagelser, der er fastsat i artikel 23, stk. 1, i APPI, kan data, der oprindeligt blev overført fra EU til Japan, derefter overføres fra Japan til et tredjeland uden samtykke i to tilfælde:

- Hvis PIHBO'en og tredjepartsmodtageren sammen har gennemført foranstaltninger, der giver et beskyttelsesniveau svarende til APPI sammenholdt med tillægsreglementet ved hjælp af en kontrakt, andre former for bindende aftaler eller bindende aftaler inden for en koncern[47].

[45] Det Europæiske Databeskyttelsesråds retningslinjer 2/2018 om undtagelser i artikel 49 i forordning 2016/679, 25. maj 2018, s. 8.
[46] Det Europæiske Databeskyttelsesråds retningslinjer 2/2018 om undtagelser i artikel 49 i forordning 2016/679, 25. maj 2018, s. 7.
[47] Tillægsreglement, punkt 4, nr. ii.

- Hvis det er blevet anerkendt af PPC i henhold til artikel 24 i APPI og artikel 11 i PPC's regler[48], at tredjelandet giver det samme beskyttelsesniveau som det, der garanteres i Japan.

108. Det Europæiske Databeskyttelsesråd evaluerer artikel 24 i APPI som den mere specifikke regel, der indeholder en undtagelse fra den generelle regel i henhold til artikel 23 i APPI. Derfor deler Det Europæiske Databeskyttelsesråd ikke Kommissionens vurdering i den nye sidste sætning i betragtning 78 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, hvor det fastslås, at overførslen til tredjepart selv i disse tilfælde fortsat er betinget af kravet om at indhente samtykke i henhold til artikel 23, stk. 1, i APPI.

109. I henhold til artikel 11, stk. 1, i PPC's regler, kræver en afgørelse om tilstrækkeligheden af beskyttelsesniveauet af PPC, at der findes væsentlige standarder, der svarer til dem i APPI, hvis gennemførelse er sikret i tredjelandet, og som effektivt overvåges af en uafhængig håndhævende myndighed. Endvidere kan PPC pålægge de nødvendige betingelser for at beskytte enkeltpersoners rettigheder og interesser i Japan, jf. artikel 11, stk. 2, i PPC-reglerne.

110. Punkt 4 i tillægsreglementet fastsætter, at personoplysninger fra EU kan overføres til et tredjeland i henhold til en japansk afgørelse om tilstrækkeligheden af beskyttelsesniveauet uden yderligere begrænsninger. Artikel 44 i den generelle forordning om databeskyttelse foreskriver imidlertid, at enhver overførsel af personoplysninger til et tredjeland skal opfylde betingelserne i kapitel V i den generelle forordning om databeskyttelse, herunder yderligere videregivelse af personoplysninger fra et tredjeland til et andet tredjeland. Beskyttelsesniveauet for fysiske personer, hvis oplysninger overføres, må ikke undermineres af yderligere videregivelse[49]. Selv om denne fortolkning i princippet også deles af Kommissionen i dens udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet[50], synes den ikke at blive fuldstændig fulgt. Kommissionen har ført forhandlinger om et forbud mod, at data, der stammer fra EU, overføres til et tredjeland på grundlag af APEC's CBPR-bestemmelser. I lyset af det komparative værktøj, der blev udviklet i 2014 inden for rammerne af EU-direktivet mellem bindende virksomhedsregler (Binding Corporate Rules, BCR) og CBPR, som viser kravene til begge systemer, deres konvergens og forskelle (WP29's udtalelse 02/2014), har Det Europæiske Databeskyttelsesråd betænkeligheder ved anvendelsen af CBPR som et redskab til yderligere videregivelse af personoplysninger, der overføres fra EU til lande uden for Japan.

111. I modsætning hertil synes yderligere videregivelse af personoplysninger, der overføres fra EU til Japan på grundlag af en japansk afgørelse om tilstrækkeligheden af beskyttelsesniveauet, at være accepteret af Kommissionen, uden at PPC har mulighed for at indføre tillægsreglementet som betingelse for at beskytte EU-borgeres rettigheder og interesser, om nødvendigt. Det Europæiske Databeskyttelsesråd udleder fra artikel 44 i den generelle forordning om databeskyttelse, at den øgede beskyttelse af data, der overføres fra EU til Japan i henhold til tillægsreglementet, altid skal udvides, når personoplysninger, der overføres fra EU til Japan, yderligere videregives til et tredjeland, hvis databeskyttelsesrammen i det pågældende land ikke anerkendes som værende i det væsentlige svarende til den generelle forordning om databeskyttelse.

---

[48] Håndhævelsesregler for lov om beskyttelse af personoplysninger, 30. maj 2017. Kommissionen sendte en engelsk oversættelse af den nye artikel 11 til Det Europæiske Databeskyttelsesråd, men denne artikel er endnu ikke blevet offentliggjort.

[49] WP 254, s. 5.

[50] Kommissionens gennemførelsesafgørelse af XXXX i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 2016/679 om tilstrækkelig beskyttelse af personoplysninger i Japan, som blev sendt til Det Europæiske Databeskyttelsesråd den 13. november, betragtning 75.

112. **Derfor opfordrer Det Europæiske Databeskyttelsesråd Kommissionen til at påtage sig sin overvågningsrolle og sikre niveauet for beskyttelse af EU's data, eller at overveje at ophæve denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet, hvis personoplysninger, der overføres fra EU til Japan, yderligere videregives til tredjelande med forbehold af en eventuel senere japansk afgørelse om tilstrækkeligheden af beskyttelsesniveauet, når disse tredjelande ikke har været genstand for en tidligere vurdering eller afgørelse vedrørende et tilstrækkeligt beskyttelsesniveau i EU.**

3.1.5 Direkte markedsføring

113. I henhold til punkt 3 i tillægsreglementet er det forbudt for en PIHBO at behandle oplysningerne med henblik på direkte markedsføring, hvis disse er blevet overført fra Den Europæiske Union til et andet formål, og den registrerede i EU ikke har givet sit samtykke til ændringen i udnyttelsen.

114. Ifølge referencen vedrørende et tilstrækkeligt beskyttelsesniveau skal den registrerede, hvis personoplysninger behandles med henblik på direkte markedsføring, til enhver tid uden omkostninger kunne gøre indsigelse mod at få sine oplysninger behandlet til sådanne formål. I henhold til artikel 16 i APPI må en PIHBO kun behandle personoplysninger, hvis den registrerede giver sit samtykke. Tilbagetrækning af samtykke skal kunne give det samme resultat som den privilegerede ret til at gøre indsigelse mod direkte markedsføring.

115. Den japanske databeskyttelsesramme giver ikke en privilegeret indsigelsesret, og som forklaret ovenfor i afsnittet om samtykke er tilbagetrækning af samtykke i henhold til PPC's retningslinjer kun ønskelig og betinget og kan derfor ikke anses for at være ensbetydende med en ret til at gøre indsigelse på et hvilket som helst tidspunkt, som der anmodes om i henhold til referencen vedrørende et tilstrækkeligt beskyttelsesniveau. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til at give forsikringer om retten til at trække samtykke tilbage og til at overvåge sager vedrørende direkte markedsføring.**

3.1.6 Automatisk beslutningstagning og profilering

116. I henhold til referencen vedrørende et tilstrækkeligt beskyttelsesniveau kan afgørelser, der udelukkende er baseret på automatisk behandling (automatiseret individuel beslutningstagning), herunder profilering, som har retsvirkning eller væsentlig berører den registrerede, kun træffes på visse betingelser, der er fastsat inden for tredjelandets retlige ramme. Derfor skal der, hver gang der foretages automatisk beslutningstagning og udarbejdelse af profilering under ovennævnte omstændigheder, være et retligt grundlag for dette.

117. Inden for de europæiske rammer gælder det, at betingelserne for automatiseret beslutningstagning f.eks. omfatter behovet for at indhente et udtrykkeligt samtykke fra den registrerede[51], eller at det er nødvendigt, at en sådan aftale træffes for at kunne indgå en aftale. Hvis afgørelsen ikke opfylder sådanne betingelser som fastsættes i tredjelandets retlige ramme, skal den registrerede have ret til ikke at blive omfattet af den. Endvidere bør tredjelandets lovgivning under alle omstændigheder indeholde nødvendige beskyttelsesgarantier, herunder retten til at blive underrettet om de specifikke grunde, der ligger til grund for afgørelsen, og det logiske system, der ligger bag for at rette urigtige eller ufuldstændige oplysninger og gøre indsigelse mod en afgørelse, som er truffet på et fejlagtigt grundlag.

[51] Med hensyn til kritiske bemærkninger til begrebet samtykke i den japanske databeskyttelseslovgivning henvises til: 2.1. Generelt og 2.2.8. Direkte markedsføring.

118. Kommissionens afgørelse vedrører kun banksektoren, hvor sektorspecifikke regler[52] vedrørende automatiske afgørelser finder anvendelse. I henhold til de omfattende retningslinjer for tilsyn med større banker, der er nævnt i betragtning 93 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, skal den pågældende person have specifikke forklaringer på, hvorfor en anmodning om indgåelse af en låneaftale er blevet afvist.

119. De argumenter, Kommissionens henviser til i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet (betragtning 94), om at manglen på specifikke regler om automatiseret beslutningstagning i APPI ikke kan forventes at påvirke beskyttelsesniveauet, tager (for eksempel) ikke højde for det tilfælde, hvor overførte personoplysninger fra EU efterfølgende behandles af en anden japansk dataansvarlig (forskellig fra den oprindelige japanske dataimportør).

120. Det ser derfor ud til, at der ikke findes generelle regler, der finder anvendelse på tværs af sektorer i Japan, for så vidt angår automatisk beslutningstagning og profilering.

121. **Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til at overvåge sager vedrørende automatisk beslutningstagning og profilering.**

3.2 Procedurer og håndhævelsesmekanismer

122. På grundlag af kriterierne i referencen vedrørende et tilstrækkeligt beskyttelsesniveau har Det Europæiske Databeskyttelsesråd analyseret følgende aspekter af den japanske databeskyttelse og retlige ramme, som er omfattet af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet: om der findes en uafhængig tilsynsmyndighed, der fungerer effektivt, forekomsten af et system, der sikrer et højt niveau af overensstemmelse og et system med adgang til passende klageordninger, der giver EU-borgerne midler til at udøve deres rettigheder og ret til at klage uden at støde på besværlige hindringer for administrative og retlige klagemuligheder.

123. På grundlag af de parametre, der er fastlagt af EU-Domstolen i Schrems-sagen[53], og de parametre, der er beskrevet i betragtning 104 og artikel 45 i den generelle forordning om databeskyttelse, finder Det Europæiske Databeskyttelsesråd, at selv om der findes et system i Japan, der er i overensstemmelse med det europæiske system, kan dette system være vanskeligt at få adgang til i praksis for EU-borgere, hvis data vil blive overført i henhold til denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet på baggrund af eksistensen af sproglige og institutionelle barrierer.

124. I afsnittene nedenfor gennemgås ovennævnte aspekter af den japanske ramme, inden der fremlægges nogle henstillinger til Kommissionen.

3.2.1 Kompetent uafhængig tilsynsmyndighed

125. PPC blev oprettet den 1. januar 2016 efter ændringerne af APPI i 2015 og afløste forgængeren — den særlige kommission til beskyttelse af personoplysninger (oprettet i 2013 i henhold til "My Number Act"). Selv om PPC er en ung organisation, har den siden oprettelsen gjort en betydelig indsats for at opbygge den nødvendige infrastruktur for at tage højde for gennemførelsen af den ændrede APPI. I den forbindelse kan nævnes udarbejdelsen af PPC's regler, PPC's retningslinjer som giver vejledning til PIHBO'er om fortolkningen af APPI, offentliggørelsen af et PPC-dokument[54] med spørgsmål og svar og etablering af en hjælpetjeneste, der kan rådgive virksomhedsledere og borgere om bestemmelser om databeskyttelse samt en mæglingstjeneste til behandling af klager.

[52] Disse sektorspecifikke regler blev ikke givet til Det Europæiske Databeskyttelsesråd.

[53] Sag 362/14 (2015) Maximilian Schrems mod Data Protection Commissioner (præmis 73 og 74).

[54] Det Europæiske Databeskyttelsesråd har ikke modtaget dette dokument fra Kommissionen på engelsk.

126. PPC's oprettelse og funktion er reguleret i APPI's kapitel V. Selv om PPC hører under premierministeren, er det fastsat i artikel 62, at PPC udøver sin funktion uafhængigt. Det Europæiske Databeskyttelsesråd glæder sig over Kommissionens præcisering i det ændrede udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, der blev udsendt den 13. november 2018, for yderligere at beskrive, i hvor høj grad PPC er fri for interne og eksterne påvirkninger.

3.2.2 Databeskyttelsessystemet skal sikre en høj grad af overholdelse

127. Udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet indeholder en omfattende undersøgelse af de beføjelser, som PPC er tillagt i henhold til artikel 40, 41 og 42 i APPI for at sikre overvågning og håndhævelse af lovgivningen. I henhold til artikel 40 kan PPC anmode om, at PIHBO'er indsender rapporter og dokumentation vedrørende behandlingsaktiviteter samt gennemfører kontrolbesøg på stedet. I henhold til artikel 42 har PPC beføjelser— når PPC fastslår, at det er nødvendigt at beskytte individuelle rettigheder, eller at der er tale om en overtrædelse af lovens bestemmelser — til at udstede henstillinger og, hvis det ikke giver noget resultat, udstede påbud til PIHBO'er om at ophøre med overtrædelsen eller træffe de foranstaltninger, der er nødvendige for at rette op på overtrædelsen.

128. I oktober 2018 traf PPC en af sine første foranstaltninger i henhold til artikel 41 i den ændrede APPI og udstedte en "vejledning" til en PIHBO, der rådgiver virksomheden med henblik på at styrke dens sikkerhedsforanstaltninger og effektivt føre tilsyn med applikationsudbydere, samtidig med at den giver klare og letforståelige oplysninger til brugerne om, hvordan deres personoplysninger anvendes, og indhenter samtykke på forhånd, når oplysningerne deles med en tredjepart, samt besvarer brugernes anmodning om sletning af deres oplysninger. I de svar, der afgives til Det Europæiske Databeskyttelsesråd[55], meddelte embedsmænd fra PPC, at virksomheden har meddelt, at den vil samarbejde, og at den, når virksomheden ikke gør det, vil give virksomheden en "henstilling" i henhold til artikel 42, stk. 1, i APPI.

129. Den undersøgelse, som PPC har foretaget af ovennævnte PIHBO, er en meget positiv indikator for den japanske tilsynsmyndigheds bestræbelser på at sikre en god efterlevelse i landet.

130. Selv om der er sket forbedringer med hensyn til den eksisterende ramme forud for 2015-ændringerne, bemærker Det Europæiske Databeskyttelsesråd, at PPC har færre beføjelser end europæiske databeskyttelsesmyndigheder i henhold til den generelle forordning om databeskyttelse, navnlig i forbindelse med **håndhævelse**. Administrative bøder[56] er f.eks. ret milde. Kommissionens beslutning understreger i betragtning 108, at i tilfælde af manglende overholdelse eller visse overtrædelser af APPI er der indført strafferetlige sanktioner, og at PPC's formand kan fremsende sager til den offentlige anklager. Kommissionens beslutning tager imidlertid ikke højde for det forhold, at offentlig påtale i Japan bygger på en skønsmæssig bedømmelse og undertiden er genstand for langvarige klageprocedurer[57]. Desuden kan straffen for fængsel (med eller uden straffearbejde) i forbindelse med overtrædelser af APPI i henhold til bestemmelserne i kapitel VII være vanskelig at gennemføre, fordi

[55] Bilag III.

[56] Disse findes i kapitel VII i APPI. Den maksimale sanktion er fastsat i artikel 83 (brug eller udnyttelse af en database med personoplysninger til brug for egen eller tredjemands ulovlige fortjeneste) og svarer til enten et års fængsel med straffearbejde eller en bøde på højst 500 000 yen (ca. 3 900 EUR). Ifølge Kommissionens forklaringer er bøderne kumulative pr. overtrædelse. Selv om dette kan være tilfældet, bemærker Det Europæiske Databeskyttelsesråd, at selv om der anvendes kumulative bøder, vil det samlede beløb sandsynligvis forblive meget lavt sammenlignet med europæiske standarder.

[65] Oda H., japansk lov, Oxford University Press (III-udgave), 2009: 439-440.

det er rettet mod fysiske personer og under alle omstændigheder ikke straffer PIHBO'en som en juridisk enhed, der ikke udøver sine forpligtelser med hensyn til ansvarlighed.

131. **I lyset af ovenstående opfordrer Det Europæiske Databeskyttelsesråd Kommissionen til nøje at overvåge effektiviteten af sanktioner og relevante retsmidler i det japanske databeskyttelsessystem.**

3.2.3 Databeskyttelsessystemet skal yde støtte og bistand til individuelle registrerede i forbindelse med udøvelsen af deres rettigheder og omfatte passende klagemekanismer.

132. PPC giver omfattende oplysninger og retningslinjer på sit websted med henblik på at øge bevidstheden blandt PIHBO'er i forhold til deres forpligtelser og ansvar i henhold til rammen for databeskyttelse samt en hjælpetjeneste for at give oplysninger og støtte til japanske statsborgere med hensyn til deres individuelle rettigheder i henhold til APPI. Webstedet har også et afsnit, der kaldes "Children's room", og som udtrykkeligt henvender sig til børn og unge. Det Europæiske Databeskyttelsesråd bemærker, at disse oplysninger — sammen med hjælpetjenesten, vejledning og Q & A-dokumentation — er tilgængelig på japansk[58]. Derfor er Det Europæiske Databeskyttelsesråd overbevist om, at det vil være gavnligt, hvis PPC kan udarbejde en særlig side på den engelske udgave af sit websted til borgere i EU, hvis oplysninger vil blive overført til Japan i henhold til Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet, med det formål at give oplysninger om deres individuelle rettigheder i henhold til den japanske databeskyttelsesramme og i henhold til tillægsreglerne.

133. Det Europæiske Databeskyttelsesråd glæder sig over Kommissionens præcisering i betragtning 104 i det ændrede udkast til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, der blev sendt ud den 13. november 2018, vedrørende den mæglingstjeneste, der forvaltes af PPC i henhold til artikel 61, nr. ii), i APPI. Det Europæiske Databeskyttelsesråd vil dog gerne rejse tre punkter i den forbindelse. For det første offentliggøres mæglingstjenesten ikke på den engelske udgave af PPC's websted. For det andet er tjenesten kun tilgængelig via telefon og tilgængelig på japansk. Endelig er mægling blot en faciliterende proces, der ikke fører til en bindende aftale mellem parterne, hvilket har konsekvenser for effektiviteten, når det gælder de klagemuligheder, der er til rådighed for de registrerede[59].

134. Endelig bemærker Det Europæiske Databeskyttelsesråd, at der i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet lægges vægt på de retsmidler, der er tilgængelige gennem civilretlige foranstaltninger, samt straffesager, men gør ikke opmærksom på, at der findes **institutionelle hindringer for retstvister** i Japan, såsom retsomkostninger (retsgebyrer fordeles ligeligt mellem sagsøger og sagsøgte, uanset hvilken part der vinder sagen[60]), manglen på advokater i landet[61], det forhold, at udenlandske advokater ikke har lov til at praktisere national lovgivning, samt bevisbyrden i henhold til erstatningsretten. Det Europæiske Databeskyttelsesråd frygter, at disse forhold — i praksis — kan lægge hindringer i vejen for enkeltpersoners adgang til domstolsprøvelse og hurtigt bringe deres ret i fare til at udnytte retsmidler uden urimelige omkostninger.

---

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; og Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashport (2003) (ed.).

[60] Wagatsuma (2012), "Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure" i Reimann (ed.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice bd. 11, s. 195-200.

[61] Ifølge de seneste tal er antallet af advokater i Japan 38 980 (ca. 290 advokater pr. mio. indbyggere[Japan Federation of Bar Association] (2017), hvidbog om advokater: s. 8-9.

135. I lyset af ovenstående er **Det Europæiske Databeskyttelsesråd bekymret over, at der er en risiko for, at enkeltpersoner i EU har problemer med at få adgang til administrativ og retlig prøvelse**, og det ville derfor være ønskeligt, hvis Kommissionen kunne drøfte med PPC, om der var mulighed for at oprette en onlinetjeneste, i det mindste på engelsk, **med henblik på at yde støtte til og behandle klager fra EU-borgere**[62]. Desuden vil Det Europæiske Databeskyttelsesråd glæde sig over muligheden for at give EU's databeskyttelsesmyndigheder mulighed for at fungere som formidlere af klager fra registrerede i EU med organisationer, der opererer i Japan, og PPC.

4 OM OFFENTLIGE MYNDIGHEDERS ADGANG TIL DATA OVERFØRT TIL JAPAN

136. Kommissionens hensigt er gennem afgørelsen om tilstrækkeligheden af beskyttelsesniveauet at anerkende, at "Japan sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der videregives fra Den Europæiske Union til virksomheder, der håndterer personoplysninger i Japan", jf. artikel 1 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet. I overensstemmelse med artikel 45, stk. 2, i den generelle forordning om databeskyttelse har Kommissionen også analyseret begrænsningerne og garantierne i forbindelse med offentlige myndigheders adgang til personoplysninger. Dette kapitel fokuserer på en vurdering af de retshåndhævende myndigheders og andre offentlige enheders adgang til personoplysninger med henblik på national sikkerhed. Det Europæiske Databeskyttelsesråds analyse er baseret på bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, hvori den japanske regering giver et overblik over den relevante retlige ramme og de japanske retsakter, i det omfang Kommissionen har stillet dem til rådighed. Det Europæiske Databeskyttelsesråd har derfor på baggrund af den konkrete sammenhæng i denne vurdering taget hensyn til elementer vedrørende japanske love, som ikke indgår i Kommissionens bedømmelse, men som er relevante for at vurdere de betingelser og sikkerhedsforanstaltninger, hvorunder japanske offentlige myndigheder kan få adgang til personoplysninger, der er overført fra EU.

4.1 Retshåndhævende myndigheders adgang til data

4.1.1 Procedurer for adgang til data på det strafferetlige område

137. Udkastet til afgørelse om tilstrækkeligt beskyttelsesniveau indeholder tre måder, hvorpå de retshåndhævende myndigheder i Japan kan få adgang til data i Japan:

4.1.1.1 Begæringer om aktindsigt med en dommerkendelse

138. I udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet fastslås det, at for så vidt angår aktindsigt for statslige myndigheder i Japan, og især hvad angår de strafferetlige håndhævende myndigheder, der skal anmode om adgang til elektronisk bevismateriale i forbindelse med strafferetlige efterforskninger, kræves der altid, at de har en dommerkendelse, medmindre de benytter proceduren med frivillig fremlæggelse af oplysninger — se nedenfor.

4.1.1.1.1 Krav om "tilstrækkelig grund" samt at dommerkendelser er nødvendige og proportionale

139. Det Europæiske Databeskyttelsesråd anerkender, at enhver indsamling af personoplysninger i henhold til den japanske forfatning skal ske på grundlag af en dommerkendelse. Mere specifikt fremgår det af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, at der i alle tilfælde af

[62] Svarende til det, der er fastsat i bilag II til denne afgørelse om tilstrækkeligheden af beskyttelsesniveauet for klager fra EU-borgere vedrørende de japanske offentlige myndigheders adgang til deres oplysninger.

"ransagninger og beslaglæggelser" skal udstedes en dommerkendelse af en "tilstrækkelig grund". Ifølge højesteret foreligger en sådan grund kun, når den pågældende person (den mistænkte eller tiltalte) anses for at have begået en lovovertrædelse, og ransagning og beslaglæggelse er nødvendig for den strafferetlige efterforskning. Kommissionen henviser her til højesterets dom af 18. marts 1969, sag N. 100 (1968(Shi)).). Det Europæiske Databeskyttelsesråd minder om, at det i henhold til EU-Domstolens retspraksis[63] kun er en domstol, og ikke anklagere, der kan tillade indsamling af trafikdata og lokaliseringsdata i særdeleshed.

140. Det Europæiske Databeskyttelsesråd beklager, også set i lyset af EU-Domstolens retspraksis, hvorefter adgang til data kan gøres betinget af en dommerkendelse, som i sagen vedrørende Tele2, at der ikke blev fremlagt yderligere oplysninger for at vurdere, hvordan kriterierne for vurdering af nødvendigheden af en dommerkendelse — lovovertrædelsens alvor, og hvordan den blev begået, det beslaglagte materiales værdi og betydning som bevis, sandsynligheden for hemmeligholdelse eller ødelæggelse af beslaglagte materialer, omfanget af ulemperne forårsaget af en beslaglæggelse, andre relaterede forhold — og begrebet "tilstrækkelig grund", der udspringer af forfatningen, anvendes i praksis. Derfor opfordrer Det Europæiske Databeskyttelsesråd Kommissionen til at overvåge, om udstedelsen af dommerkendelser opfylder de kriterier, som Domstolen har fastsat i praksis.

4.1.1.1.2 Typer af forbrydelser, for hvilke der kan udstedes dommerkendelser

141. Proceduren for udstedelse af dommerkendelse finder kun anvendelse, når der foretages en "obligatorisk undersøgelse". Disse dommerkendelser kan i princippet kun udstedes i tilfælde, hvor der er tale om en overtrædelse. I den forbindelse noterer Det Europæiske Databeskyttelsesråd sig den nyligt vedtagne "lov om straf for organiseret kriminalitet og kontrol med strafbare handlinger" af 15. juni 2017 i forbindelse med Japans tiltrædelse af FN's internationale konvention om bekæmpelse af grænseoverskridende organiseret kriminalitet (UNTOC)[64]. I mangel af en engelsk udgave af denne lovgivning og i betragtning af kravet i EU-lovgivningen om, at visse oplysninger kun indsamles i forbindelse med efterforskning, afsløring eller retsforfølgning af alvorlige forbrydelser[65], og i betragtning af de betænkeligheder, der er givet udtryk for af flere kommentatorer, herunder FN's særlige rapportør, Joseph Cannaataci[66], vedrørende det brede anvendelsesområde, hvilket skyldes en definition af "organiserede kriminelle grupper", der angiveligt er vag og for bred, er Det Europæiske Databeskyttelsesråd ikke i stand til at konkludere, om adgang til elektronisk bevismateriale i henhold til den relevante japanske lovgivning er begrænset til de tærskler, der er fastsat i EU-retten.

142. Det skal også bemærkes, at i forbindelse med visse typer lovovertrædelser er det det regionale politi, der er kompetent, og at det har sine egne politiforordninger. Det Europæiske Databeskyttelsesråd har ikke haft adgang til de interne regler for det regionale politi.

143. Ifølge udkastet til beslutning om tilstrækkeligheden af beskyttelsesniveauet, henhører indsamlingen af elektroniske oplysninger på det strafferetlige område under det regionale politi.

4.1.1.2 Dommerkendelser vedrørende aflytning

144. I bilag II til udkastet om tilstrækkeligheden af beskyttelsesniveauet anføres, at særlige vilkår for aflytning af kommunikation foreskives i loven om aflytning med henblik på kriminalefterforskning. Denne lovgivning blev vedtaget meget sent, hvilket ikke gav mulighed for en tilbundsgående analyse. Selv om der synes at være mange sikkerhedsforanstaltninger inden for denne retlige ramme, er Det Europæiske Databeskyttelsesråd derfor ikke i stand til at vurdere, om de betingelser, der er fastsat i

[63] Se sag 203/15 og sag C 293/12 og C 594/12 fra EU-Domstolen.
[64] Se: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .
[65] Se forenede sager 293/12 og C 594/12 og sag C 203/15 fra EU-Domstolen.
[66] FN's særlige rapportør om retten til privatlivets fred, samt Graham Greenleaf, forsker på UNSW.

denne retsakt, er omgivet af garantier, der i alt væsentligt svarer til dem, der kræves i EU, både i chartret, som det er fortolket af EU-Domstolen, og i den europæiske menneskerettighedskonvention, som det er fortolket af domstolen i Strasbourg.

4.1.1.3 Proceduren for "frivillig fremlæggelse af oplysninger" på grundlag af spørgeskema

145. Denne ikke-obligatoriske form for samarbejde gør det muligt for offentlige myndigheder at bede de dataansvarlige (undtagen teleoperatører) om at give dem de oplysninger, de har adgang til. Manglende overholdelse af anmodningen kan ikke håndhæves. Det er fortsat uklart, hvilke myndigheder der kan anvende denne procedure, men den forekommer begrænset til dem, der efterforsker forbrydelser.

4.1.1.3.1 Betingelser for udstedelse af "spørgeskemaer"

146. Det Europæiske Databeskyttelsesråd anerkender, at den japanske højesteret med henvisning til forfatningen har fastlagt begrænsninger for anvendelsen af "frivillige oplysninger"[67]. Det fremgår af udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, at i praksis kan de kompetente myndigheder kun anmode om en "frivillig fremlæggelse af oplysninger" gennem udfærdigelsen af et "spørgeskema". Det siges kun at være tilladt at sende et sådant "spørgeskema" som led i en strafferetlig efterforskning, hvilket altid forudsætter en konkret mistanke om en allerede begået kriminel handling. Sådanne efterforskninger udføres normalt af det regionale politi, hvor begrænsningerne i henhold til artikel 2, stk. 2, i politiloven finder anvendelse, hvilket betyder, at det skal være relevant for politiets aktiviteter. Det Europæiske Databeskyttelsesråd ønsker imidlertid en yderligere præcisering af den konkrete udforming af de kriterier, der gør det muligt at udfærdige et spørgeskema (f.eks. retspraksis, der illustrerer anvendelsen af disse kriterier), og forholdet mellem proceduren for frivillig fremlæggelse af oplysninger og beslaglæggelse af data på grundlag af en dommerkendelse. Det ser således ud til, at selv om der ikke kunne indhentes oplysninger gennem den frivillige procedure, kunne de stadig indhentes med en dommerkendelse, hvis det er nødvendigt for efterforskningsmyndighederne[68].

4.1.1.3.2 Gældende retspraksis vedrørende begrænsning af brugen af frivillig fremlæggelse af oplysninger

147. De sager, der er anført i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet[69], for at illustrere begrænsningerne i anvendelsen af proceduren med frivillig fremlæggelse af oplysninger, vedrører tilfælde, hvor den anklagede enten blev fotograferet eller filmet i det offentlige rum direkte af politiet, og giver derfor kun begrænsede oplysninger om situationer, hvor de kompetente myndigheder kan anmode en dataansvarlig om at videregive oplysninger, navnlig med hensyn til de kriterier, der er anført i bilag II, om "hensigtsmæssigheden af metoder", som synes at vedrøre vurderingen af, hvorvidt frivillige undersøgelser er "passende" eller rimelige med henblik på at opfylde målet med efterforskningen. Det samme kan siges om de generelle kriterier for "hvorvidt det kan anses for rimeligt i overensstemmelse med socialt accepterede konventioner" at vurdere, om de frivillige efterforskninger er lovlige. Endvidere har det nationale politiagentur, som er den føderale myndighed med ansvar for alle spørgsmål vedrørende kriminalpolitiet, udsendt instrukser til det regionale politi om "den korrekte anvendelse ved skriftlige henvendelser i efterforskningsmæssige undersøgelser". Efterforskningslederen skal bl.a. modtage intern godkendelse fra en højtstående embedsmand. Det Europæiske Databeskyttelsesråd har ikke kendskab til, hvorvidt disse instrukser er

[67] Se bilag II, s. 8.
[68] Se bilag II, s. 7.
[69] Se bilag II, side 8 — to højesteretsafgørelser af 24. december 1969 (1965 (A) nr. 1187) og 15. april 2008 (2007 (A) nr. 839).

bindende. Ikke desto mindre fastslår Det Europæiske Databeskyttelsesråd, at anvendelsen af denne procedure skal være forholdsmæssig eller nødvendig.

4.1.1.3.3 De dataansvarliges rettigheder og forpligtelser i forbindelse med frivillig fremlæggelse af oplysninger

148. Det er desuden de dataansvarlige, der skal give samtykke til at levere data (men der synes ikke at være nogen forpligtelse for dem til at indhente samtykke fra de registrerede eller informere dem), hvis disse anmodninger ikke er i strid med andre retlige forpligtelser (såsom fortrolighedsforpligtelser). Det fremgår af Kommissionens rapport, at de dataansvarlige efter en høj grad af efterlevelse er begyndt at tage hensyn til deres kunders databeskyttelse og således er begyndt at svare mindre hyppigt på disse anmodninger.

149. Det er også fortsat uklart, om de dataansvarlige har noget incitament til at efterkomme anmodningerne (f.eks. om de har en fordel, når de overholder reglerne, eller om de er fritaget for retsforfølgelse osv.). Navnlig nævnes der ikke noget lignende princip som "princippet om ikke at vidne mod sig selv".

150. Det Europæiske Databeskyttelsesråd ønsker yderligere oplysninger, hvis de foreligger, taloplysninger om antallet og typen af anmodninger samt om svarene fra de adspurgte dataansvarlige. I mangel af retspraksis og tal opfordrer Det Europæiske Databeskyttelsesråd Kommissionen til at overvåge effektiviteten og den konkrete anvendelse af denne procedure i praksis.

151. Det Europæiske Databeskyttelsesråd mangler imidlertid retspraksis og tal om denne procedure med henblik på at fastlægge disse elementer. Det Europæiske Databeskyttelsesråd kan derfor ikke bedømme, om denne procedure er effektiv, eller dens konkrete anvendelse uden yderligere elementer vedrørende praksis.

4.1.1.4 Konklusion om procedurer for adgang til oplysninger med henblik på retshåndhævelse

152. Som konklusion anerkender Det Europæiske Databeskyttelsesråd, at princippet om, at personoplysninger kun kan tilgås af de kompetente myndigheder, når det er nødvendigt og står i et rimeligt forhold til formålet og på grundlag af en dommerkendelse, svarer til de vigtigste grundlæggende garantier i EU-lovgivningen og den europæiske menneskerettighedskonvention. I overensstemmelse med ovenstående anmoder Det Europæiske Databeskyttelsesråd Kommissionen om at overvåge anvendelsesområdet for disse foranstaltninger, omfanget af proceduren med frivillig fremlæggelse af oplysninger og det regionale politis anvendelse af dette princip og domstolenes anvendelse i den relevante retspraksis samt at overvåge, om den japanske retlige ramme indeholder de væsentlige garantier, som Domstolen har fastslået på grundlag af chartret og Den Europæiske Menneskerettighedsdomstol på grundlag af konventionen.

4.1.2 Tilsyn på det strafferetlige område

153. Udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet samt bilag II indeholder fire typer tilsyn, som gennemføres af politi, ministerier og offentlige organer.

4.1.2.1 Retsligt tilsyn

4.1.2.1.1 I tilfælde, hvor elektroniske oplysninger indsamles ved brug af tvangsmidler (ransagning og beslaglæggelse)

154. Ifølge udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet skal politiet i alle tilfælde, hvor der indsamles elektronisk information ved brug af tvangsmidler (ransagning og beslaglæggelse), indhente en forudgående dommerkendelse. Der er dog en undtagelse fra denne regel[70]. I henhold til

[70] Se bilag II.

artikel 220, stk. 1, i strafferetsplejeloven kan en offentlig anklager, dennes assistent eller en embedsmand fra kriminalpolitiet, der pågriber en mistænkt person, søge eller beslaglægge elektroniske oplysninger på stedet for pågribelsen. I denne situation er der mulighed for, at disse oplysninger udelukkes som bevismateriale af en dommer.

155. Det Europæiske Databeskyttelsesråd er opmærksom på, at der også findes lignende undtagelser i henhold til EU-retten. Det bemærker, at der ikke altid er en domstolskontrol i tilfælde, hvor elektroniske oplysninger indsamles ved hjælp af tvangsmidler, sådan som det er fastsat i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet. I denne forbindelse minder Det Europæiske Databeskyttelsesråd om retspraksis fra den europæiske menneskerettighedskonvention om efterfølgende kontrol.[71]

4.1.2.1.2 I tilfælde af anmodninger om frivillig fremlæggelse af oplysninger

156. I henhold til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet er der i forbindelse med anmodninger om frivillig fremlæggelse af oplysninger ikke foretaget nogen forudgående kontrol af en dommer. I dette tilfælde arbejder det regionale politi under den offentlige anklagers tilsyn. Udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet nævner artikel 192, stk. 1, og artikel 246 om det gensidige samarbejde mellem og koordineringen af anklagere, den regionale kommission for offentlig sikkerhed og embedsmænd fra kriminalpolitiet og udveksling af oplysninger mellem dem. Det henviser også til artikel 193, stk. 1, i henhold til hvilken den offentlige anklager kan give kriminalpolitiet de nødvendige instrukser og fastsætte standarder for en retfærdig efterforskning. Endelig nævnes artikel 194 i henhold til hvilken den nationale eller regionale kommission for offentlig sikkerhed kan træffe disciplinære sanktioner over for kriminalpolitiet for manglende respekt for de offentlige anklagere.

157. Det Europæiske Databeskyttelsesråd anerkender vedtagelsen af ovennævnte foranstaltninger og det tilsyn med kriminalpolitiet, som gennemføres af den nationale eller regionale kommission for offentlig sikkerhed (se nedenfor).

4.1.2.2 Tilsyn med politiet gennem kommissionerne for offentlig sikkerhed

158. I henhold til bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet fører to typer kommissioner tilsyn med politiet. Begge har til formål at sikre demokratisk forvaltning og politisk neutralitet i politiforvaltningen.

4.1.2.2.1 Tilsyn gennem den nationale kommission for offentlig sikkerhed

159. I bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet nævnes det tilsyn, som den nationale kommission for offentlig sikkerhed har ført med NPA. Politiloven indeholder en liste over kommissionens opgaver, ud fra hvilke den har udøvet sine tilsynsbeføjelser (se artikel 5).

160. I henhold til artikel 4 i politiloven er den nationale kommission for offentlig sikkerhed etableret under premierministeren og består af en formand og fem medlemmer. I artikel 7 fastsættes visse begrænsninger for udnævnelsen af kommissionens medlemmer. Mandatet for kommissionens medlemmer er fem år og kan kun gentages én gang, jf. artikel 8. Hertil kommer, at parlamentet (Diet) ser ud til at have stor indflydelse på udnævnelsen og afskedigelsen af kommissionens medlemmer, som sikrer den nationale offentlige sikkerhedskommissions uafhængighed.

161. Sådanne retlige bestemmelser øger den nationale offentlige sikkerhedskommissions politiske neutralitet.

[71] EMRK, Modestou mod Grækenland, nr. 51693/13.

4.1.2.2.2 Tilsyn gennem de regionale kommissioner for offentlig sikkerhed

162. Det regionale politi er underlagt de regionale kommissioner for offentlige sikkerhed, der er oprettet i hver region. I henhold til artikel 2 og 36, stk. 2, i politiloven er de regionale kommissioner for offentlig sikkerhed ansvarlige for "beskyttelse af individets rettigheder og frihed". Artikel 38 og artikel 42 i politiloven indeholder en liste over de opgaver, de regionale kommissioner for offentlig sikkerhed varetager. Disse kommissioner har også til formål at sikre politiets demokratiske ledelse og politiske neutralitet som anført i artikel 43, stk. 2, ved at henvise individuelle sager til det regionale politi, når de finder det nødvendigt i forbindelse med en undersøgelse af det regionale politis aktiviteter eller dets personales adfærd.

163. Det er imidlertid uklart, om disse kommissioner har andre beføjelser end undersøgelse af politiets adfærd. Det Europæiske Databeskyttelsesråd vil gerne vide, om udtrykket "tjenesteforseelse" omfatter ulovlig adgang til oplysninger og i så fald, om disse kommissioner kan beordre sletning af oplysninger eller ej.

164. Med hensyn til neutraliteten og uafhængigheden af disse kommissioner som anført i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet[72] hører den regionale kommission for offentlig sikkerhed under den regionale guvernørs jurisdiktion. Guvernøren udpeger medlemmer af kommissionen med godkendelse fra den regionale forsamling. Medlemmerne af den regionale kommission for offentlig sikkerhed har en mandatperiode på tre år og kan genudnævnes op til to gange. Artikel 39 i politiloven har sat begrænsninger for udnævnelsen af medlemmerne. I udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet nævnes også den regionale forsamlings tilsyn med det regionale politi, med henvisning til artikel 100 i loven om lokalt selvstyre. Denne retsakt fik Det Europæiske Databeskyttelsesråd imidlertid ikke stillet til rådighed[73].

165. I henhold til artikel 42, stk. 2 og 3, i politiloven må "intet medlem af kommissionen samtidig være et medlem af forsamlingen eller det personale, der arbejder på fuld tid i lokale offentlige enheder, eller være deltidsansat som foreskrevet i bestemmelsen i § 1, artikel 28, stk. 5, i lov om lokalt selvstyre.

166. I henhold til ovennævnte oplysninger og i betragtning af samarbejdet mellem de regionale kommissioner for offentlig sikkerhed og den nationale kommission for offentlig sikkerhed Det Europæiske Databeskyttelsesråd bifalder udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og det glæder sig over, at medlemmerne af de regionale kommissioner for offentlig sikkerhed er neutrale og uafhængige. Det er Det Europæiske Databeskyttelsesråds forståelse, at de regionale kommissioner for offentlig sikkerhed har beføjelse til at undersøge politiets adfærd og ikke har andre tilsynsbeføjelser, herunder til sletning af oplysninger, der er indsamlet af det regionale politi. Det ser derfor ud til, at der er behov for en yderligere præcisering af, om det tilsyn, der føres af de regionale kommissioner for offentlig sikkerhed, er tilstrækkeligt i henhold til de standarder, der er fastsat i EU-retten.

4.1.2.2.3 Tilsyn gennem parlamentet

167. Udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet[74] og bilag II[75] giver visse oplysninger om det tilsyn, der føres af parlamentet i forhold til regeringen, herunder med hensyn til lovligheden af politiets indsamling af oplysninger. Begge nævner således forfatningens artikel 62, hvorefter parlamentet kan anmode om fremlæggelse af dokumenter og vidneforklaringer. Begge nævner ligeledes de retlige bestemmelser i loven om parlamentet, navnlig artikel 104, vedrørende

[72] Se udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, s. 31.
[73] Se udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, s. 33.
[74] Se udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, s. 30.
[75] Se bilag II, s. 12.

parlamentets beføjelser og artikel 74 om indgivelse af skriftlige forespørgsler, som skal besvares skriftligt af regeringen inden for syv dage som fastsat i artikel 75. Forslaget til en afgørelse om tilstrækkeligheden af beskyttelsesniveauet tilføjer også "parlamentets rolle i forbindelse med tilsynet med den udøvende magt unerstøttes af indberetningsforpligtelser, f.eks. i henhold til artikel 29 i loven om aflytning".

168. Det Europæiske Databeskyttelsesråd anerkender parlamentets betydning for tilsynet med regeringen og politiet i forbindelse med lovligheden af dataindsamling.

4.1.2.2.4 Tilsyn udført af den udøvende magt

169. I henhold til bilag II til udkastet om tilstrækkeligheden af beskyttelsesniveauet har ministeren eller chefen for hvert ministerium eller agentur på den ene side beføjelse til at føre tilsyn med og håndhæve reglerne på grundlag af APPIHAO[76]. På den anden side har ministeren for indre anliggender og kommunikation (MIC) en efterforskningsbeføjelse i forbindelse med alle andre ministeriers håndhævelse af APPIHAO, herunder justitsministeren for politiet som nævnt i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet[77].

170. Ministeren kan anmode chefen for et administrationsorgan om at indgive materiale og forklaringer vedrørende det pågældende administrationsorgans behandling af personoplysninger på grundlag af artikel 50 i APPIHAO. Den kan anmode om en revision af foranstaltningerne, hvis der er mistanke om, at en overtrædelse eller uhensigtsmæssig anvendelse af loven har fundet sted, og afgive udtalelser om de berørte administrationsorganers behandling af personoplysninger i henhold til artikel 50 og 51 i APPIHAO.

171. Udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet og bilag II indeholder også en omtale af oprettelsen af 51 omfattende informationscentre, der "sikrer en gnidningsløs gennemførelse af denne lov" i henhold til artikel 47 i APPIHAO. Det Europæiske Databeskyttelsesråd bemærker, at APPIHAO ikke uddyber disse informationscentres rolle og beføjelser, men at udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet giver nogle præciseringer.

172. Derfor glæder Det Europæiske Databeskyttelsesråd sig over, at ministeren for indre anliggender og kommunikation fører tilsyn med ministeriernes og de administrative organers efterlevelse af APPIHAO.

173. Som konklusion fastsættes der i EU-lovgivningen og den europæiske menneskerettighedskonvention gennem deres respektive domstoles retspraksis standarder og garantier, ifølge hvilke tilsynet skal være fuldstændigt, neutralt og uafhængigt. Det Europæiske Databeskyttelsesråd bemærker, at PPC ikke har tilsynsbeføjelser i spørgsmål vedrørende retshåndhævelse. Hvis det tilsyn, der udføres af parlamentet, den nationale og regionale sikkerhedskommission desuden lader til at være neutral og uafhængig, er der behov for en yderligere præcisering af tilsynsbeføjelserne for de regionale kommissioner for offentlig sikkerhed.

4.1.3 Klageadgang på det strafferetlige område

174. Udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, suppleret med bilag II, indeholder flere muligheder, hvorigennem enkeltpersoner kan indgive deres klager, både til de uafhængige myndigheder og til dommerne.

175. Disse muligheder og kerneelementerne i disse procedurer, som hidrører fra den tilgængelige dokumentation, fremlægges her efter en kort oversigt over de rettigheder, der er til rådighed, for at

[76] Se bilag II, s. 10.
[77] Se bilag II, s. 11.

præcisere, hvad de registrerede kan forvente af offentlige myndigheder i forbindelse med databehandling på det strafferetlige område.

4.1.3.1 De registreredes rettigheder i forbindelse med strafferetlige procedurer

176. For at opnå erstatning skal de registrerede have rettigheder i henhold til loven for at kunne gøre krav på, at de ikke blev overholdt. Derfor vurderede Det Europæiske Databeskyttelsesråd også de disponible rettigheder i forbindelse med de strafferetlige procedurer, der blev fremlagt i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

4.1.3.1.1 Generelle begrænsninger af de registreredes rettigheder i henhold til APPIHAO

177. I udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet henviser Kommissionen til og baserer sig på generelle databeskyttelsesprincipper, som de offentlige myndigheder skal overholde, når de har indsamlet personoplysninger. Disse principper er også nærmere beskrevet i bilag II, hvorfor Det Europæiske Databeskyttelsesråd også har besluttet at fremsætte bemærkninger til dem.

178. Hvad angår de rettigheder, der er til rådighed, bemærker Det Europæiske Databeskyttelsesråd, at nogle af de generelle rettigheder, der gives til registrerede i forbindelse med oplysninger, der behandles af administrative organer, fortsat er tilgængelige i henhold til bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, også i forbindelse med strafferetlige efterforskninger. Yderligere begrænsninger med hensyn til indsamling og yderligere behandling af personoplysninger i denne sammenhæng følger imidlertid også af APPIHAO selv.

179. Disse begrænsninger, som også finder anvendelse både i forbindelse med oplysninger, der er indsamlet på grundlag af en dommerkendelse, samt på grundlag af et spørgeskema i forbindelse med frivillig fremlæggelse af oplysninger, rejser spørgsmål vedrørende flere aspekter.

180. For så vidt angår princippet om formålsbegrænsning gælder det, at selv om administrative organer i princippet skal angive det formål, til hvilket de opbevarer personoplysninger, og de ikke må beholde dem uden for det anvendelsesområde, der er nødvendigt for at opfylde det angivne formål, kan de ændre formålet, hvis det er "hvad der med rimelighed kan anses for hensigtsmæssigt til det oprindelige formål".

181. APPIHAO fastsætter også princippet om fortrolighed, i henhold til hvilken en arbejdstager ikke må videregive de erhvervede personoplysninger til en anden person uden gyldig grund eller anvende sådanne oplysninger til et urimeligt formål. Der gives imidlertid ingen yderligere oplysninger om fortolkningen af, hvad "gyldig grund" eller "urimeligt formål" kan dække, så det er nødvendigt med en yderligere præcisering i forbindelse med vurderingen.

182. Artikel 8, stk. 1, i APPHAAO fastsætter også forbuddet mod at anvende eller videregive oplysninger, "medmindre andet er fastsat i love og bestemmelser". Selv om denne bestemmelse i princippet ikke er i strid med det beskyttelsesniveau, der ydes i henhold til EU-lovgivningen, mangler Det Europæiske Databeskyttelsesråd yderligere elementer vedrørende det omfang, hvori et tilsyn eller en kontrol udøves, når videregivelse er omfattet af love eller bestemmelser. Desuden finder der i henhold til artikel 8, stk. 2, yderligere undtagelser fra denne regel, når "en sådan ekstraordinær videregivelse ikke vil kunne skade den registreredes eller tredjemands rettigheder og interesser". Uden yderligere elementer på dette punkt er der behov for en yderligere præcisering af, om denne undtagelse, som bygger på det uklare begreb "uretfærdig" skade, er tilstrækkeligt snæver.

183. Endelig indeholder artikel 9 i APPIHAO yderligere begrænsninger for den påtænkte anvendelse eller anvendelsesmetoden eller andre begrænsninger, som skal pålægges af lederen af et administrativt organ, hvis der videregives opbevarede personoplysninger til en anden person. Da begreberne "andre

nødvendige begrænsninger" og "videregivet til en anden person" er meget brede, giver disse yderligere begrænsninger til de registreredes rettigheder anledning til betænkeligheder uden yderligere præciseringer af anvendelsesområdet for denne bestemmelse.

184. Selv om Det Europæiske Databeskyttelsesråd er fuldt ud klar over, at adgangsrettigheder og andre databeskyttelsesprincipper også er begrænset i straffesager i henhold til EU-retten, gives der yderligere garantier, når der er fastsat sådanne begrænsninger, herunder med hensyn til overvågning, tilsyn og klageadgang. I mangel af tilstrækkelig retspraksis vedrørende disse begrænsninger eller yderligere elementer for at præcisere anvendelsesområdet for disse bestemmelser er Det Europæiske Databeskyttelsesråd ikke i stand til at vurdere, om disse begrænsninger af registreredes rettigheder er begrænset til, hvad der ville blive betragtet som strengt nødvendigt og forholdsmæssigt i henhold til EU-retten, og at det derfor i det væsentlige ville svare til de rettigheder, der gives til registrerede i EU.

4.1.3.1.2 Yderligere begrænsninger af rettighederne i APPIHAO i medfør af strafferetsplejeloven og det regionale politis forordninger

185. Det Europæiske Databeskyttelsesråd bemærker, at selv om APPIHAO synes at finde anvendelse på al behandling foretaget af administrative organer i Japan, er der nogle vigtige begrænsninger i registreredes rettigheder som følge af specifik lovgivning. Navnlig hedder det i artikel 53, stk. 2, i strafferetsplejeloven[78]: "personoplysninger, der registreres i dokumenter vedrørende retssager og beslaglagte genstande", er ikke omfattet af anvendelsesområdet for de individuelle rettigheder i kapitel IV i APPIHAO. Konkret forstår Det Europæiske Databeskyttelsesråd derfor, at registrerede i forbindelse med straffesager ikke er omfattet af retten til information, indsigt, berigtigelse eller sletning af personoplysninger, der er registreret i dokumenter vedrørende retssager og beslaglagte genstande.

186. Med hensyn til disse begrænsninger er det Det Europæiske Databeskyttelsesråds forståelse, at de finder anvendelse i forbindelse med oplysninger, der er indsamlet på grundlag af dommerkendelser, samt i forbindelse med oplysninger, der er indsamlet i forbindelse med frivillig fremlæggelse af oplysninger, ved hjælp af spørgeskemaer (se nedenfor). Retsgrundlaget for de to procedurer for adgang til data (gennem en dommerkendelse og gennem et spørgeskema) er fastsat i strafferetsplejeloven. Artikel 53-2 i denne lov synes at finde anvendelse på begge typer indsamling. Da artikel 53-2 imidlertid henviser til de "beslaglagte" genstande, kan det afklares, om begrænsningerne af de rettigheder, der er fastsat i denne bestemmelse, også gælder i forbindelse med frivillig fremlæggelse af oplysninger.

187. Det Europæiske Databeskyttelsesråd beklager ikka at have haft adgang til det regionale politis forordninger, som siges at beskytte personoplysninger, rettigheder og forpligtelser, der svarer til APPIHAO's. I betragtning af uklarhederne med hensyn til fortolkningen af APPIHAO og den manglende adgang til det regionale politis forordninger stiller Det Europæiske Databeskyttelsesråd spørgsmålstegn ved, om de rettigheder, der gives til enkeltpersoner i denne sammenhæng, og om de yderligere tilsyns- og/eller klagemekanismer er tilstrækkelige til at kompensere for manglen på rettigheder.

4.1.3.2 Klageadgang ved hjælp af uafhængige myndigheder

4.1.3.2.1 Administrativ klageadgang

188. Det Europæiske Databeskyttelsesråd bemærker, at de administrative organer, der indsamler data, som f.eks. det regionale politi, har kompetence til at behandle anmodninger fra enkeltpersoner om deres

[78] Findes her http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 og citeret i bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, fodnote 25.

— begrænsede — rettigheder i forbindelse med oplysninger om dem, der er indsamlet som led i strafferetlige efterforskninger (se ovenfor om de tilgængelige rettigheder), hvilket synes at omfatte både indsamling af oplysninger på grundlag af en dommerkendelse og på grundlag af spørgeskemaer. Konkret synes disse rettigheder at være begrænset til generelle principper, som f.eks. nødvendigheden af datalagring i forbindelse med formålet (se artikel 3.1 i APPIHAO), princippet om formålsbegrænsning (artikel 4) eller oplysningernes nøjagtighed (artikel 5), mens individuelle rettigheder, såsom retten til information, indsigt, berigtigelse eller sletning, er udelukket for personoplysninger, der er registreret i dokumenter vedrørende retssager og beslaglagte genstande[79]. Selv om disse organer ikke kan betragtes som uafhængige og derfor som uafhængige klagemuligheder eller tilsyn, bifalder Det Europæiske Databeskyttelsesråd denne mulighed. Det understreger imidlertid, at de klager, der indgives i denne forbindelse, fortsat er begrænset til de registreredes meget få rettigheder i betragtning af de begrænsninger, der er forbundet med de rettigheder, der er fastsat i APPIHAO.

189. Da "personoplysninger, der er registreret i dokumenter vedrørende retssager og beslaglagte genstande", er udelukket fra anvendelsesområdet for de individuelle rettigheder i kapitel IV i APPIHAO i henhold til artikel 53-2 i strafferetsplejeloven, er mulighederne for at anmode om adgang til personoplysninger også begrænset til de procedurer, der er fastsat i andre bestemmelser i nærværende strafferetsplejelov. Det ser ud til, at kun ofre, mistænkte eller tiltalte personer, kan handle i denne forbindelse og stadig afhængigt af straffesagens stadium. Det Europæiske Databeskyttelsesråd er derfor bekymret for, at ingen generel ret til indsigt i og/eller berigtigelse eller sletning af oplysninger er til rådighed for registrerede i henhold til japansk lovgivning i forbindelse med en straffesag, og at alle tilgængelige klagemuligheder er forbundet med at være offer (i hvilket tilfælde personen sandsynligvis ville vide, at vedkommendes oplysninger blev indsamlet) eller en mistænkt eller tiltalt, eller påvisning af en skade. Registrerede bør imidlertid også have ret til at få adgang til deres oplysninger og eventuelt få deres oplysninger berigtiget eller slettet, når de ikke er blevet påført skade (endnu), og/eller når de hverken er ofre, mistænkte eller tiltalte, men vidner for eksempel.

4.1.3.2.2 Administrativ klageadgang gennem de regionale kommissioner for offentlig sikkerhed

190. Desuden synes de regionale kommissioner for offentlig sikkerhed at være kompetente til at behandle klager. På grundlag af artikel 79 i den politilov, der henvises til i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, kan enkeltpersoner klage over en agents ulovlige eller uretmæssige adfærd i forbindelse med udførelsen af dennes opgaver.

191. Det Europæiske Databeskyttelsesråd ønsker at få afklaret, om en "ulovlig" behandling af personoplysninger udgør en "ulovlig eller ukorrekt adfærd hos en agent", og om påvisningen af en ulempe, som synes påkrævet af den registrerede. Den meddelelse, som NPA udsendte til politiet og de regionale kommissioner for offentlig sikkerhed om korrekt behandling af klager over politibetjentes udførsel af opgaver, begrænser klager til konkrete krav om "korrektion for eventuelle særlige ulemper, der er blevet påført som følge af ulovlig eller uhensigtsmæssig adfærd, eller undladelse af at træffe de nødvendige foranstaltninger, af en politibetjent i forbindelse med udførelsen af sine opgaver" og muligheden for at "indgive klage over upassende måde at udføre arbejdsopgaver på af en politibetjent". Det præciseres udtrykkeligt, at "klager vedrørende en politibetjents manglende opfyldelse af sine forpligtelser i spørgsmål, der ikke anses for at være omfattet af en politibetjents arbejde, samt dem, der udtrykker en generel udtalelse eller et forslag, og som ikke direkte berører den klagende part selv, udelukkes".

[79] Se ovenfor vedrørende begrænsningerne i APPIHAO, jf. navnlig artikel 53-2 i strafferetsplejeloven (som der ikke er stillet til rådighed, men som der henvises til i bilag II til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, fodnote 25).

192. Hvad angår de proceduremæssige krav til at indgive en klage, og selv om de skal indgives skriftligt, bemærker Det Europæiske Databeskyttelsesråd, at der i denne forbindelse gives bistand til at skrive klagen i henhold til den japanske lovgivning, herunder for udlændinge. Desuden synes den japanske regering også at have betroet PPC at yde bistand til de registrerede i EU med henblik på at behandle og løse klager på dette område, hvilket Det Europæiske Databeskyttelsesråd glæder sig over. Det Europæiske Databeskyttelsesråd understreger, at PPC i denne forbindelse kun vil fungere som kontaktpunkt mellem de registrerede i EU og de kompetente myndigheder i Japan.

193. Resultaterne af en klage fra den regionale kommission for offentlig sikkerhed meddeles ikke i de tilfælde, der er nævnt i artikel 79-2 i politiloven, som omfatter det tilfælde, hvor den nuværende "klagers bopæl er ukendt". Det Europæiske Databeskyttelsesråd anerkender, at henvisningen til bopæl ikke indebærer, at registrerede i EU i alle tilfælde vil blive udelukket fra meddelelsen af resultaterne af deres klager på den baggrund, at de ikke har bopæl i Japan.

4.1.3.2.3 Ad hoc-mekanisme, der omfatter PPC

194. I lyset af de resultater, der er beskrevet ovenfor, bifalder Det Europæiske Databeskyttelsesråd, at den japanske regering og Kommissionen er nået til enighed om en yderligere klagemekanisme, der giver EU-borgere en yderligere klagemulighed i Japan, hvorigennem enkeltpersoner også kan klage over ulovlige eller uretmæssige undersøgelser fra offentlige myndigheders side. Det Europæiske Databeskyttelsesråd bemærker og glæder sig over, at anmodningerne kan indgives til PPC i stedet for en anden offentlig embedsmand, hvilket udvider PPC's kompetence til at omfatte retshåndhævelse og national sikkerhed.

195. Det Europæiske Databeskyttelsesråds fokus, når den nye mekanisme analyseres, har været at forstå de beføjelser, som PPC har i denne sammenhæng.

196. Selv om sproget ikke er helt klart, forstår Det Europæiske Databeskyttelsesråd, at den yderligere klagemekanisme ikke kræver "søgsmålskompetence" i den forstand, at ansøgeren ikke skal bevise, at vedkommendes personoplysninger sandsynligvis er blevet overvåget af en japansk myndighed. Det Europæiske Databeskyttelsesråd ønsker stadig at anmode om en bekræftelse fra Kommissionen.

197. I overensstemmelse med sin vurdering af ombudsmandsmekanismen, der blev oprettet under værnet om privatlivets fred, understreger Det Europæiske Databeskyttelsesråd, at det er nødvendigt med effektive beføjelser for modtageren af anmodningen, i dette tilfælde PPC, med henblik på at tage hensyn til klagemekanismen, der i det væsentlige svarer til et effektivt retsmiddel i henhold til artikel 47 i chartret om grundlæggende rettigheder.

198. Når den japanske regering forklarer klagemekanismen, henviser den til artikel 6, stk. 61, nr. ii), og artikel 80 i APPI og fastsætter disse beføjelser i bilag II. Det er Det Europæiske Databeskyttelsesråds opfattelse, at proceduren som beskrevet i bilag II specificerer eller udvider PPC's beføjelser, da sproget i artikel 6, stk. 61, nr. ii), og artikel 80 i APPI er temmelig vagt og generelt. I det omfang, hvor bilag II specificerer eller udvider PPC's beføjelser, anmoder Det Europæiske Databeskyttelsesråd om en præcisering af, om de øvrige agenturer i den japanske regering er bundet af dem.

199. På grundlag af proceduren i bilag II bemærker Det Europæiske Databeskyttelsesråd, at de kompetente offentlige myndigheder i Japan er forpligtet til at samarbejde med PPC, "herunder ved at forsyne dem med de nødvendige oplysninger og relevant materiale, så PPC kan vurdere, om indsamlingen eller den efterfølgende anvendelse af personoplysninger har fundet sted i overensstemmelse med de gældende regler". For at vurdere systemets effektivitet er det derfor vigtigt igen at henvise til de beføjelser, som de kompetente myndigheder, som PPC samarbejder med, har. Det er Det Europæiske Databeskyttelsesråds opfattelse, at disse beføjelser ikke vil blive udvidet gennem forsikringer i bilag II.

200. Det Europæiske Databeskyttelsesråd bemærker også, at hvis der er blevet identificeret en overtrædelse af reglerne, omfatter "det samarbejde, som de berørte offentlige myndigheder samarbejder med PPC om, en forpligtelse til at afhjælpe overtrædelsen", der udtrykkeligt omfatter sletning af de oplysninger, der er indsamlet i strid med de gældende regler. Det Europæiske Databeskyttelsesråd forstår, at den kompetente myndigheds forpligtelser stammer fra "samarbejdet med PPC" snarere end fra en beslutning truffet af PPC.

201. Endelig informerer PPC den anmodende part om "resultatet af evalueringen, herunder eventuelle korrigerende foranstaltninger, der er truffet." Desuden informerer PPC den anmodende part om "muligheden for at søge en bekræftelse af resultatet fra den kompetente offentlige myndighed og om den myndighed, til hvilken en sådan anmodning om bekræftelse skal fremsættes."

202. Desuden har PPC forpligtet sig til at bistå den anmodende part med at træffe yderligere foranstaltninger i henhold til japansk lovgivning, hvis den anmodende part er utilfreds med resultatet af proceduren.

203. I lyset af behovet for at have en effektiv klagemekanisme, som i det væsentlige svarer til EU's standarder, undrer Det Europæiske Databeskyttelsesråd sig alligevel over, om PPC har andre specifikke beføjelser end at vurdere, om indsamlingen eller den efterfølgende anvendelse af personoplysninger har fundet sted i overensstemmelse med de gældende regler, og opfordrer de kompetente myndigheder til at gøre brug af deres respektive beføjelser og til at behandle klager, som PPC fremsender til dem. Hvis PPC kun fungerer som kontaktpunkt for privatpersoner i EU, mener Det Europæiske Databeskyttelsesråd, at dette er utilstrækkeligt til at sikre en effektiv klagemekanisme, som i det væsentlige svarer til EU's standarder. Det Europæiske Databeskyttelsesråd opfordrer derfor Kommissionen til at præcisere de punkter, der er nævnt i dette underkapitel, navnlig om, hvorvidt og hvordan mekanismen udvider de kompetente myndigheders forpligtelser, hvordan de er bundet af den, og hvordan PPC effektivt kan sikre overholdelse og ikke kun fungere som et kontaktpunkt for EU-borgere.

4.1.3.3 Retslig prøvelse

4.1.3.3.1 Kvasiklagemekanisme

204. Den såkaldte "kvasiklage"-procedure gør det muligt at gøre en indsats mod obligatorisk indsamling af oplysninger, der er baseret på en dommerkendelse, for at få omstødt eller ændret en ulovlig beslaglæggelse.

205. Denne mulighed indebærer, at personen er bekendt med de oplysninger, der beslaglægges. Det Europæiske Databeskyttelsesråd forstår imidlertid, at proceduren for indsamling af oplysninger baseret på en dommerkendelse ikke meddeles den registrerede. Det forstår ligeledes, at frivillig fremlæggelse af oplysninger ikke indebærer, at selskaber skal have pligt til at underrette de registrerede om de modtagne og opfyldte anmodninger. Selv om det i bilag II understreges, at "en sådan anfægtelse kan indbringes uden at skulle vente på, at sagen afsluttes", er det i praksis, bortset fra dommerkendelser, der giver ret til aflytning, således at loven foreskriver, at der kræves underretningspligt[80], men denne mulighed synes kun at være konkret til rådighed, når den registrerede har fået kendskab til indsamlingen gennem en sag, der er anlagt mod den pågældende.

[80] Artikel 23 i loven om aflytning nævner side 33 i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet, men det Europæiske Databeskyttelsesråd blev ikke forsynet med denne tekst, og det er derfor ikke i stand til at vurdere, i hvilket omfang denne underretningspligt finder anvendelse, og i hvilke tilfælde den kan være begrænset.

4.1.3.3.2 Påbud

206. For at opnå sletning af oplysninger, der er indsamlet gennem en straffesag (det såkaldte "pålæg eller forbud"), eller for at opnå skadeserstatning, kan enkeltpersoner også indbringe civile søgsmål for en dommer.

207. Med hensyn til kompensation bemærker Det Europæiske Databeskyttelsesråd, at proceduren synes at være begrænset til situationer, hvor en offentligt ansat i udøvelsen af sit hverv ulovligt og culpøst (forsætligt eller uagtsomt) har påført den pågældende person skade. Efter hvad Det Europæiske Databeskyttelsesråd har forstået, synes skaden at omfatte moralsk skade. Det er imidlertid ikke fastsat nærmere, hvad der skal bevises af den enkelte med hensyn til den skade han eller hun har lidt. Det Europæiske Databeskyttelsesråd var ikke i stand til at vurdere retspraksis vedrørende tildeling af erstatning og er derfor ikke i stand til at vurdere, om denne mulighed giver adgang til effektive retsmidler i tilfælde af skader.

208. Med hensyn til "påbud" bemærker Det Europæiske Databeskyttelsesråd også, at for at indgive en anmodning skal den enkelte først være opmærksom på, at hans/hendes oplysninger blev indsamlet, og at de stadig opbevares. I betragtning af den begrænsede ret til information og adgang for enkeltpersoner i forbindelse med strafferetlige undersøgelser og procedurer synes procedurens effektivitet derfor også at være ret begrænset.

4.1.3.4 Samlet vurdering af klagemuligheder

209. Efter at have vurderet alle muligheder for at klage til PPC, der er til rådighed for enkeltpersoner i henhold til den japanske lovgivning, samt for de registrerede i EU, glæder Det Europæiske Databeskyttelsesråd sig over den ad hoc-tvistbilæggelsesmekanisme, der involverer PPC. Den har en merværdi for de registrerede i EU, navnlig fordi den giver dem mulighed for at forstå, hvilke muligheder de har for at opnå hjælp og/eller erstatning, samt for at fremsætte deres anmodninger i overensstemmelse med de gældende proceduremæssige krav i den japanske lovgivning. Der er imidlertid behov for yderligere præciseringer, navnlig om, hvorvidt og hvordan mekanismen udvider de kompetente myndigheders forpligtelser, hvordan de er bundet af den, og hvordan PPC effektivt kan sikre overholdelse for at sikre, at denne nye mekanisme sikrer effektiv klageadgang.

210. Denne vurdering viser, at ingen klagemekanisme i japansk lovgivning synes at tillade adgang, berigtigelse eller sletning af oplysninger for registrerede, der ikke er ofre, mistænkte eller tiltalte i forbindelse med en straffesag, f.eks. for at afhjælpe ulovlig indsamling eller opbevaring af deres oplysninger. Den viser også, at alle de klage- og kompensationsmekanismer og -procedurer, der er til rådighed i henhold til den japanske lovgivning for ofre, mistænkte eller tiltalte, indebærer kendskab til indsamling af oplysninger, som synes at være begrænset i praksis, da der gives begrænsede adgangsrettigheder og få oplysninger til dem. Endvidere synes der at være behov for yderligere præcisering, for så vidt angår påvisning af en ulovlig adfærd fra myndighedernes side, navnlig om en sådan adfærd omfatter enhver form for ulovlig behandling af personoplysninger eller en skade, som den enkelte har lidt.

211. Uden yderligere dokumentation og yderligere elementer er Det Europæiske Databeskyttelsesråd derfor bekymret for, hvorvidt klageadgang i henhold til den japanske lovgivning og udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet er tilstrækkeligt effektiv i forhold til standarderne i EU-lovgivningen.

4.2 Adgang af hensyn til national sikkerhed

4.2.1 Omfanget af overvågning

212. I udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet indføres kapitlet om "de japanske offentlige myndigheders adgang til og brug af hensyn til national sikkerhed" i overensstemmelse med den forsikring, den japanske regering har givet i bilag II, i henhold til hvilken ingen japansk lovgivning ville give og dermed tillade "obligatoriske anmodninger om oplysninger eller "administrativ aflytning" uden for strafferetlig efterforskning". Som konklusion anføres det, at "på grundlag af nationale sikkerhedsforskrifter kan oplysninger kun indhentes fra en informationskilde, der frit kan tilgås af alle, eller ved frivillig fremlæggelse af oplysninger. Dette udelukker hemmelige overvågningsaktiviteter på dette område. Virksomhedsledere, der modtager en anmodning om frivilligt samarbejde (i form af videregivelse af elektroniske oplysninger), er ikke retligt forpligtede til at fremlægge sådanne oplysninger."[81]

213. Inden for disse begrænsninger angives fire statslige enheder, som har beføjelse til at indsamle elektroniske oplysninger, som japanske virksomhedsledere har i deres besiddelse af hensyn til den nationale sikkerhed. Med hensyn til forsvarsministeriet, som er en af de fire enheder, siges det, at det "kun har beføjelser til at indsamle (elektroniske) oplysninger gennem frivillig fremlæggelse af oplysninger".[82]

214. I sin vurdering af det generelle system til indsamling af oplysninger med henblik på national sikkerhed ønsker Det Europæiske Databeskyttelsesråd at minde om den første af de fire såkaldte "væsentlige garantier", hvori det hedder, at "behandling bør baseres på klare, præcise og tilgængelige regler"[83]. Mere specifikt har Den Europæiske Menneskerettighedsdomstol gjort det klart, at overvågningsprogrammer kun er "i overensstemmelse med loven", hvis overvågningsforanstaltningerne "har en vis hjemmel i national ret". Domstolen har præciseret, at forenelighed med retsstatsprincippet kræver, at den lov, som tillader foranstaltningen, skal være tilgængelig og kunne forventes at have virkninger. Med henvisning til risikoen for vilkårlighed har domstolen krævet "klare detaljerede regler for hemmelige overvågningsforanstaltninger", som er "tilstrækkeligt klare til at give borgerne en passende tilkendegivelse af de omstændigheder og betingelser, under hvilke de offentlige myndigheder har beføjelser til at gøre brug af en sådan foranstaltning".[84]

215. Med hensyn til anvendelsen af disse væsentlige garantier i Japans retssystem er Det Europæiske Databeskyttelsesråd ikke kun bekendt med, at stater i spørgsmål om national sikkerhed har en bred fortolkningsmargen, som er anerkendt af Den Europæiske Menneskerettighedsdomstol. De nationale sikkerhedsbeføjelser afspejler også de historiske erfaringer, som landene har gjort. Det Europæiske Databeskyttelsesråd forstår således som understreget af den japanske regering, at de japanske nationale efterretningstjenester efter Anden Verdenskrig har fået mere begrænsede beføjelser end i andre stater.

216. Sådan som Det Europæiske Databeskyttelsesråd har tolket udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet på linje med den japanske regerings tilsagn, tyder det på, at de japanske myndigheder ikke gennemfører programmer, som strategisk overvåger eller generelt overvåger

---

[81] Afgørelse om tilstrækkeligt beskyttelsesniveau, punkt 151.

[82] Afgørelse om tilstrækkeligt beskyttelsesniveau, punkt 153.

[83] WP29, WP 237: Arbejdsdokument 01/2016 om begrundelse for indgreb i de grundlæggende rettigheder til privatlivets fred og databeskyttelse gennem overvågningsforanstaltninger ved overførsel af personoplysninger (europæiske væsentlige garantier).

[84] Se f.eks. Big Brother Watch m.fl. mod Det Forenede Kongerige, præmis 305.

(internet) kommunikation. Som nævnt ovenfor har den japanske regering i et brev, som justitsministeren har underskrevet, givet tilsagn om, at "der af hensyn til den nationale sikkerhed kun kan indhentes oplysninger fra en informationskilde, der frit kan tilgås af alle eller ved frivillig fremlæggelse af oplysninger".

217. For så vidt angår retsgrundlaget for forsvarsministeriet, bemærker Det Europæiske Databeskyttelsesråd, at udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet omfatter generelle oplysninger om forsvarsministeriets beføjelser og henviser til dets mission, der er"at gennemføre sådanne anliggender, som er knyttet hertil, for at sikre national fred og uafhængighed og nationens sikkerhed". Det Europæiske Databeskyttelsesråd har midlertidig ikke modtaget den engelske oversættelse af denne afgørelse.

218. Samtidig er Det Europæiske Databeskyttelsesråd vidende om rapporter, der er offentliggjort i forskellige medier, og som antyder, at direktoratet for signalefterretninger under det japanske forsvarsministerium administrerer overvågningsprogrammer [85]. I rapporten hævdes det også, at det japanske forsvarsministerium, selv om det nægter at drøfte specifikke spørgsmål i rapporten, har "anerkendt, at Japan har "kontorer i hele landet", der aflytter kommunikation", og at disse "vil fokusere på militære aktiviteter og "cybertrusler" og "ikke indsamle oplysninger om offentligheden". Sidstnævnte erklæring (at MOD ikke indsamler oplysninger om offentligheden) indgår som en del af den japanske regerings tilpasning.

219. Det står klart, at den japanske regering i et brev underskrevet af justitsministeren har gentaget, at MOD ikke indsamler oplysninger om den brede offentlighed.

220. Det ligger uden for Det Europæiske Databeskyttelsesråds opgave at foretage en generel vurdering af den japanske regerings mulige overvågningskapacitet. Disse aktiviteter er kun vigtige for vurderingen, hvis de er relevante for overførslen af personoplysninger mellem EU og Japan. I den forbindelse ønsker Det Europæiske Databeskyttelsesråd at bekræfte sin tilgang, som allerede blev vedtaget af sin forgænger, da det blev anmodet om at udtale sig om EU's og USA's værn om privatlivets fred. I forbindelse med udarbejdelsen af en udtalelse om værnet om privatlivets fred medtog artikel 29-Gruppen i sin analyse de amerikanske myndigheders beføjelser og begrænsninger til at foretage overvågning af data "på vej" til USA[86]. Med anvendelse af den samme standard for afgørelsen om tilstrækkeligheden af beskyttelsesniveauet for Japan er Det Europæiske Databeskyttelsesråd af den opfattelse, at oplysninger om de japanske myndigheders beføjelser til at overvåge data "på vej" til Japan er relevante. Hvis disse overvågningsbeføjelser findes, ser det ud til, at Den Europæiske Menneskerettighedsdomstols afgørelse i Big Brother Watch synes at antyde, at sådanne beføjelser skal reguleres i overensstemmelse med de standarder, der er fastsat af Den Europæiske Menneskerettighedsdomstol.

221. Hvis aflytninger som følge heraf var begrænset til "bistand til militære aktioner", kan de heller ikke være relevante for vurderingen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet. Det er

[85] I maj 2018 offentliggjorde internettidsskriftet "The Intercept" en rapport med titlen "Den ufortalte historie om Japans hemmelige efterretningstjeneste".

[86] Se WP255, EU's og USA's værn om privatlivets fred — den første årlige fælles undersøgelse, som blev vedtaget den 28. november 2017, s. 16: "artikel 29-Gruppen er af den opfattelse, at analysen af lovgivningen i det tredjeland, for hvilket et tilstrækkeligt beskyttelsesniveau tages i betragtning, ikke bør begrænses til den lov og praksis, der giver mulighed for overvågning inden for det pågældende lands fysiske grænser, men også bør omfatte en analyse af de retlige grunde i det pågældende tredjelands lovgivning, som gør det muligt for landet at foretage overvågning uden for sit område, for så vidt angår EU-data. Som allerede understreget i sin tidligere udtalelse, bør det klart fremgå, at principperne til værn om privatlivets fred finder anvendelse fra det tidspunkt, hvor dataoverførslen finder sted, hvilket betyder, at det omfatter data "på vej" til det pågældende land."

således Det Europæiske Databeskyttelsesråds interesse at få nærmere oplysninger om de japanske statslige enheders overvågningsforanstaltninger. I denne forbindelse ville en sådan præcisering være velkommen med henblik på at fastslå, om de data, der overføres i henhold til denne ramme om tilstrækkeligheden af beskyttelsesniveauet, kan gøres til genstand for adgang af hensyn til den nationale sikkerhed af de kompetente japanske myndigheder på dette område.

4.2.2 Frivillig fremlæggelse af oplysninger i tilfælde af national sikkerhed

222. I udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet fastslås det, at de fire statslige enheder kun har beføjelse til at indsamle (elektroniske) oplysninger ved frivillig fremlæggelse af oplysninger. I henhold til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet og bilag II er der visse begrænsninger af lovbestemte grunde, hvilket betyder, at indsamlingen af data er begrænset til, hvad der er nødvendigt for enhedernes udførelse af opgaverne.

223. På det strafferetlige område som nævnt i afsnittet om retshåndhævelse er frivillig fremlæggelse af oplysninger kun tilladt som led i en strafferetlig efterforskning og forudsætter således en konkret mistanke om en forbrydelse, der allerede er begået. Undersøgelser på området national sikkerhed adskiller sig fra undersøgelser på retshåndhævelsesområdet. Det Europæiske Databeskyttelsesråd anerkender, at ifølge bilag II gælder de centrale principper for "undersøgelsens nødvendighed" og "metodens hensigtsmæssighed" på samme måde på området for national sikkerhed og skal overholdes under behørig hensyntagen til de særlige omstændigheder i hvert enkelt tilfælde[87]. Det beklager, at anvendelsen ikke præciseres yderligere, herunder ved hjælp af en yderligere henvisning til retspraksis. Ikke desto mindre fastslår Det Europæiske Databeskyttelsesråd, at anvendelsen af denne procedure skal være forholdsmæssig eller nødvendig.

224. I henhold til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet gælder det, at når der er indsamlet personoplysninger ("indhentet"), er styres behandlingen af APPIHAO, med undtagelse af det regionale politi[88]. I bilag II fastsættes det, at det regionale politis håndtering af personoplysninger bestemmes af regionale forordninger, der fastsætter principper for beskyttelse af personoplysninger, rettigheder og forpligtelser, der svarer til dem i APPIHAO[89]. Da der ikke findes engelske oversættelser af disse forordninger, er Det Europæiske Databeskyttelsesråd ikke i stand til at vurdere, om principperne svarer til principperne i APPIHAO.

225. Hvad angår de øvrige bemærkninger om frivillig fremlæggelse af oplysninger, henvises der til afsnittet om retshåndhævelse.

4.2.3 Tilsyn

4.2.3.1 Generelt

226. De fire statslige enheder, der er bemyndiget til at indsamle elektroniske oplysninger, som japanske virksomhedsledere er i besiddelse af af hensyn til den nationale sikkerhed, er: (i) kabinettets efterretnings- og forskningskontor (CIRO); ii) forsvarsministeriet ("MOD") (iii) politiet (både den nationale politimyndighed (NPA)[90] og det regionale politi og (iv) efterretningstjenesten for offentlig sikkerhed ("PSIA").

---

[87] Se bilag II, s. 23.

[88] Afgørelse om tilstrækkeligt beskyttelsesniveau, punkt 118 og 157.

[89] Se bilag II, s. 3.

[90] Ifølge de modtagne oplysninger er den nationale politimyndigheds vigtigste opgave imidlertid at koordinere efterforskningen i de forskellige afdelinger inden for det regionale politi, og dens aktiviteter vedrørende indsamling af oplysninger er begrænset til udvekslinger med udenlandske myndigheder.

227. I henhold til udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet er disse offentlige enheder genstand for flere lag af tilsyn fra tre dele af regeringen[91]. Det Europæiske Databeskyttelsesråd bemærker, at der findes en tilsynsmekanisme inden for den lovgivende magt (det japanske parlament) og den udøvende magt (generalinspektørens kontor for overholdelse af love (IGO), de regionale kommissioner for offentlig sikkerhed og den offentlige sikkerhedsundersøgelseskommission). Det Europæiske Databeskyttelsesråd understreger, at Kommissionen bør afklare det retslige tilsyn (ex officio/garanti C i WP 237; med hensyn til klageadgang er der et særskilt kapitel i udkastet til afgørelse om tilstrækkeligheden af beskyttelsesniveauet og en ekstra garanti i WP 237) for ovennævnte statsorganer, da det er uklart, om der er et sådant retsligt tilsyn på området for indsamling af personoplysninger af hensyn til den nationale sikkerhed uden tvangsmidler.

4.2.3.2 Tilsyn gennem det japanske parlament

228. Det Europæiske Databeskyttelsesråd bemærker, at det japanske parlament kan foretage undersøgelser i forbindelse med offentlige myndigheders aktiviteter og derfor også for alle ovennævnte statslige enheder. Desuden kan parlamentet også anmode om fremlæggelse af dokumenter og vidneforklaringer (artikel 62 i den japanske forfatning, artikel 104 i lov om parlamentet). Det Europæiske Databeskyttelsesråd bemærker også, at parlamentet i henhold til artikel 74 og 75 i lov om parlamentet kan stille skriftlige spørgsmål til kabinettet, der kan ende med et svar fra kabinettet (artikel 75 i lov om parlamentet). Endelig skal det bemærkes, at der findes specifikke rapporteringsforpligtelser for f.eks. efterretningstjenesten for offentlig sikkerhed (PSIA) (artikel 36 i SAPA/artikel 31 i ACO) i form af en årlig rapport til parlamentet. Denne rapport blev imidlertid ikke givet til Det Europæiske Databeskyttelsesråd.

4.2.3.3 IGO's tilsyn

229. Det Europæiske Databeskyttelsesråd bemærker, at der er et tilsynsorgan for MOD, kaldet IGO. Det Europæiske Databeskyttelsesråd fik ikke adgang til loven om oprettelse af MOD, men kun til repræsentationerne i bilag II til udkastet til afgørelse. I henhold til bilag II er IGO et uafhængigt kontor i MOD, som er underlagt forsvarsministerens direkte tilsyn i henhold til artikel 29 i loven om oprettelse af MOD. IGO har beføjelser til at føre tilsyn med, at embedsmænd fra MOD (de såkaldte "forsvarsinspektioner") overholder love og bestemmelser på tværs af hele ministeriet, herunder selvforsvarsstyrkerne.

230. I henhold til bilag II udfører IGO sine opgaver uafhængigt af MOD's operationelle afdelinger. Det Europæiske Databeskyttelsesråd bemærker, at IGO er et *internt* tilsynsorgan.

231. Inspektioner fører til resultater og, med henblik på at sikre overholdelse, foranstaltninger, som rapporteres direkte til forsvarsministeren. På grundlag af IGO's rapport kan forsvarsministeren udstede påbud om at gennemføre de foranstaltninger, der er nødvendige for at rette op på situationen. Viceforsvarsministeren er ansvarlig for gennemførelsen af disse foranstaltninger og skal rapportere til forsvarsministeren om status for en sådan gennemførelse.

232. Ved at analysere bilag II glæder Det Europæiske Databeskyttelsesråd sig over muligheden for at sikre de nødvendige foranstaltninger til at afhjælpe situationen uden at have adgang til lovbestemmelserne (loven om oprettelse af MOD). Det Europæiske Databeskyttelsesråd rejser imidlertid tvivl om, hvorvidt IGO'en er uafhængig, da det er et kontor i MOD og er under direkte tilsyn af forsvarsministeren i henhold til bilag II (i henhold til *WP 237* er det ikke "*tilstrækkelig funktionel uafhængig i sig selv til at beskytte tilsynsmyndigheden mod al ekstern indflydelse*").

[91] Se bilag II, s. 39.

233. I overensstemmelse med retspraksis i henholdsvis den europæiske menneskerettighedskonvention og WP 237 og det, der angives i i bilag II, kan generalinspektøren anmode om rapporter fra det pågældende kontor (dokumenter, websteder, forklaringer). Det Europæiske Databeskyttelsesråd finder, at det er nødvendigt at præcisere, om de pågældende kontorer er forpligtet til at følge disse anmodninger eller ikke, og om de anmodede dokumenter indeholder lukkede materialer, sådan som det nævnes i WP 237.

234. Selv om Det Europæiske Databeskyttelsesråd glæder sig over, at meget højtstående juridiske eksperter (tidligere anklager) leder IGO, synes det nødvendigt at præcisere måden, hvorpå dette tilsynsorgan udpeges.

4.2.3.4 Tilsyn gennem kommissionen til undersøgelse af den offentlige sikkerhed

235. I henhold til bilag II (side 25) foretager PSIA regelmæssige og særlige inspektioner af driften af de enkelte tjenester og kontorer (efterretningstjenesten for offentlig sikkerhed, efterretningskontorerne for offentlig sikkerhed og underafdelinger osv.). Med henblik på det regelmæssige tilsyn udpeges der en vicegeneraldirektør og/eller en direktør som tilsynsførende. Sådanne inspektioner bør også vedrøre forvaltningen af personoplysninger.

236. I henhold til betragtning 163 i udkastet til afgørelse fungerer *kommissionen til undersøgelse af den offentlige sikkerhed* som et uafhængigt ex ante-tilsynsorgan for PSIA med hensyn til spørgsmål vedrørende ACO[92] og SAPA[93]. Det Europæiske Databeskyttelsesråd glæder sig over dette.

237. Selv om det japanske justitsministeriums websted indeholder nogle oplysninger[94], er Det Europæiske Databeskyttelsesråd ikke i stand til at foretage en omhyggelig vurdering af, i hvilket omfang kommissionen til undersøgelse af den offentlige sikkerhed er uafhængig, da den ikke har fået tilsendt loven om etablering af kommissionen til undersøgelse af den offentlige sikkerhed[95] og reglerne for kommissionen til undersøgelse af den offentlige sikkerhed[96].

4.2.3.5 Tilsyn gennem den nationale kommission for offentlig sikkerhed, de regionale kommissioner for offentlig sikkerhed og APPIHAO (den udøvende myndighed)

238. Se 3.1.2.2.1 (den nationale kommission for offentlig sikkerhed), 3.1.2.2.2. (de regionale kommissioner for offentlig sikkerhed) og 3.1.2.2.4. (Den udøvende myndighed).

4.2.3.6 PPC's tilsyn

239. Det Europæiske Databeskyttelsesråd opfordrer Kommissionen til i betragtning 164 at nævne, at PPC ikke er et tilsynsorgan for ovennævnte statslige enheder, og at det kun er kompetent med hensyn til den enkeltes muligheder for at klage eller at flytte passagen i betragtning 164 vedrørende PPC til afsnittet "individuel klageadgang".

---

[92] Lov om kontrol af organisationer, som har begået vilkårlig massemord (lov nr. 147 af 7. december 1999).
[93] Lov om forebyggelse af undergravende virksomhed (lov nr. 240 af 21. juli 1952).
[94] Se http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (september 2018): Det ikke-ministerielle organ *"består af en formand og seks medlemmer. De udvælges blandt personer med god karakter, som er i stand til at træffe en retfærdig afgørelse om kontrol med organisationer og som har omfattende viden og erfaring inden for både jura og samfund. De udnævnes af premierministeren og skal godkendes af begge kamre i parlamentet. Med hensyn til anvendelsen af ovennævnte love (SAPA/ACO) udfører medlemmerne deres opgaver helt uafhængigt og uden nogen form for styring eller tilsyn af premierministeren eller justitsministeren."*
[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (september 2018).
[96] Artikel 28 i ACO.

4.2.4 Klagemekanisme

240. Hvad angår analysen af de nyligt forhandlede klagemekanismer, henvises der til afsnittet om retshåndhævelse.

241. Det er desuden værd at bemærke, at den japanske lov indeholder bestemmelser om en specifik individuel klageadgang inden for den nationale sikkerhed. Det er Det Europæiske Databeskyttelsesråds opfattelse, at alle personer, herunder enkeltpersoner i EU, generelt kan anmode om fremlæggelse, berigtigelse (herunder sletning) eller suspension af anvendelsen fra de administrative organer, også hvis de behandles af hensyn til den nationale sikkerhed. Hvis en sådan anmodning "afvises med den begrundelse, at de pågældende oplysninger betragtes som uanfægtelige", kan der indgives klage, og "undersøgelsesudvalget for videregivelse af oplysninger og beskyttelse af personoplysninger" skal høres. Bestyrelsen består af medlemmer udpeget af premierministeren med samtykke fra begge kamre, der er udstyret med undersøgelsesbeføjelser, og konkluderer med en skriftlig rapport for den pågældende person, som ikke er juridisk bindende, men næsten altid følges[97]. I henhold til bilag II var der kun to ud af 2000 tilfælde, hvor en administrativ myndighed traf en afgørelse, som afveg fra udvalgets konklusion.[98]

242. Det lader til at fremgå af forklaringen, at gennemgangen ikke er tilgængelig, hvis oplysningerne kan "videregives", men den enkelte er utilfreds med resultatet. Det Europæiske Databeskyttelsesråd anerkender denne mulighed for at klage, men ønsker at søge yderligere afklaring af sidstnævnte aspekt, hvilket i høj grad vil begrænse dets anvendelsesområde.

For Det Europæiske Databeskyttelsesråd

Formand

(Andrea Jelinek)

[97] Se bilag II, s. 25-26. Lov om oprettelse af undersøgelsesudvalget for videregivelse af oplysninger og beskyttelse af personoplysninger, artikel 4, 9 og 11.
[98] Bilag II, fodnote 35.