

Advies van de EDPB (artikel 70, lid 1, onder s)



Advies 28/2018
over het ontwerpuitvoeringsbesluit van de Europese
Commissie
betreffende de adequate bescherming van
persoonsgegevens in Japan

Goedgekeurd op 5 december 2018

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

Inhoudsopgave

1	SAMENVATTING	4
1.1	Punten van overeenstemming	5
1.2	Algemene uitdagingen	5
1.3	Specifieke commerciële aspecten	6
1.3.1	Punten van zorg van het EDPB met betrekking tot belangrijke beginselen inzake gegevensbescherming	6
1.3.2	Noodzaak van verduidelijking	7
1.4	Over de inzage van overheidsinstanties in gegevens die aan Japan zijn doorgegeven	7
1.5	Conclusie	8
2	INLEIDING	9
2.1	Japans kader voor gegevensbescherming	9
2.2	Reikwijdte van de beoordeling van het EDPB	9
2.3	Algemene opmerkingen en bezorgdheden	11
2.3.1	Bijzonderheden van dit type adequaatheidsbesluit	11
2.3.2	Betrouwbaarheid van vertalingen	11
2.3.3	Sectorale adequaatheid	11
2.3.4	Bindend karakter van de aanvullende regels en de richtsnoeren van de CBP	12
2.3.5	Periodieke herziening van de vaststelling van adequaatheid	13
2.3.6	Door Japan aangegane internationale verbintenissen	13
2.3.7	Bevoegdheden van gegevensbeschermingsautoriteiten om bij een rechtbank rechtsvorderingen in te stellen betreffende de geldigheid van een adequaatheidsbesluit	14
3	COMMERCIELE ASPECTEN	14
3.1	Inhoudelijke beginselen	14
3.1.1	Begrippen	15
3.1.2	Gronden voor een rechtmatige en behoorlijke verwerking voor gerechtvaardigde doeleinden	18
3.1.3	Het transparantiebeginsel	18
3.1.4	Beperkingen op verdere doorgifte	20
3.1.5	Direct marketing	23
3.1.6	Geautomatiseerde besluitvorming en profilering	23
3.2	Procedurele en handhavingsmechanismen	24
3.2.1	Bevoegde onafhankelijke toezichthoudende autoriteit	24
3.2.2	Het systeem voor gegevensbescherming moet een goede naleving waarborgen	25
3.2.3	Het gegevensbeschermingsstelsel moet individuele betrokkenen ondersteunen en helpen bij de uitoefening van hun rechten en passende verhaalsmogelijkheden.	26

4	OVER DE INZAGE VAN OVERHEIDSINSTANTIES IN NAAR JAPAN DOORGEGEVEN GEGEVENS.....	27
4.1	Inzage van rechtshandhavingsinstanties in gegevens.....	27
4.1.1	Procedures voor inzage in gegevens in strafrechtelijke context.....	27
4.1.2	Toezicht op strafrechtelijk gebied.....	30
4.1.3	Verhaal in strafrechtelijke context.....	33
4.2	Inzage ten behoeve van de nationale veiligheid.....	40
4.2.1	Reikwijdte van het toezicht.....	40
4.2.2	Vrijwillige informatieverstrekking in geval van nationale veiligheid.....	42
4.2.3	Toezicht.....	42
4.2.4	Verhaalmechanisme.....	45

Het Europees Comité voor gegevensbescherming

Gelet op artikel 70, lid 1, onder s), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "de AVG"),

Gelet op de EER-Overeenkomst en met name bijlage XI en Protocol 37, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018,

Gelet op artikel 12 en artikel 22 van zijn reglement van orde van 25 mei 2018,

BRENGT HET VOLGENDE ADVIES UIT:

1 SAMENVATTING

1. Op 5 september 2018 heeft de Europese Commissie haar ontwerpuitvoeringsbesluit over de adequate bescherming van persoonsgegevens door Japan overeenkomstig de algemene verordening gegevensbescherming (hierna "de AVG")¹ bekrachtigd². Vervolgens heeft de Europese Commissie de procedure voor de formele goedkeuring ervan ingeleid.
2. Op 25 september 2018 heeft de Europese Commissie het Europees Comité voor gegevensbescherming (hierna "het EDPB") om advies gevraagd³. De Commissie werd verzocht het EDPB alle nodige documentatie met betrekking tot Japan te verstrekken, met inbegrip van alle relevante correspondentie met de Japanse overheid.
3. In het licht van de besprekingen met het EDPB heeft de Europese Commissie haar ontwerpadequaateheidsbesluit tweemaal gewijzigd. Op 13 november 2018 heeft zij haar laatste versie ervan toegezonden⁴. Het EDPB heeft zijn onderhavige advies gebaseerd op deze laatste versie van het ontwerpuitvoeringsbesluit (hierna "het ontwerpadequaateheidsbesluit").
4. De beoordeling door het EDPB van het beschermingsniveau dat door het adequaateheidsbesluit van de Commissie wordt gewaarborgd, is uitgevoerd op basis van het onderzoek van het besluit zelf en op basis van een analyse van de door de Commissie ter beschikking gestelde documentatie⁵.
5. Het EDPB heeft zich gericht op de beoordeling van zowel de commerciële aspecten van het ontwerpadequaateheidsbesluit als de inzage van de overheid in vanuit de EU doorgegeven

¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

² Zie het persbericht op http://europa.eu/rapid/press-release_IP-18-5433_nl.htm.

³ Overeenkomstig artikel 70, lid 1, onder s), van de AVG.

⁴ Zie bijlage I bij het advies van het EDPB voor de bijgewerkte versie van het ontwerpuitvoeringsbesluit van de Europese Commissie.

⁵ Het EDPB heeft zijn analyse gebaseerd op door de Japanse autoriteiten verstrekte vertalingen die door de Europese Commissie zijn geverifieerd.

⁶ Zie bijlage II van het advies van het EDPB voor de lijst van documenten die niet door de Europese Commissie aan het EDPB zijn verstrekt.

persoonsgegevens met het oog op rechtshandhaving en nationale veiligheid, met inbegrip van de rechtsmiddelen die natuurlijke personen uit de EU ter beschikking staan. Het EDPB heeft ook beoordeeld of de waarborgen die het Japanse rechtskader biedt operationeel en doeltreffend zijn.

6. Het EDPB heeft als belangrijkste referentie voor deze werkzaamheden zijn in februari 2018 goedgekeurde adequaatheidsreferentiedocument⁷ gebruikt.

1.1 Punten van overeenstemming

7. De belangrijkste doelstelling van het EDPB is het geven van een advies aan de Europese Commissie over het niveau van de bescherming die natuurlijke personen in het Japanse rechtskader genieten. Het is belangrijk in te zien dat het EDPB niet verwacht dat het Japanse rechtskader de Europese wetgeving inzake gegevensbescherming kopieert.
8. Het EDPB herinnert er echter aan dat de wetgeving van het derde land krachtens de jurisprudentie van het Hof van Justitie van de EU (hierna "het HvJ") en krachtens artikel 45 van de AVG in lijn moet zijn met de essentie van de fundamentele beginselen die in de AVG zijn verankerd om te kunnen worden geacht een adequaat beschermingsniveau te bieden. Wat gegevensbescherming betreft, merkt het EDPB voorts op dat er belangrijke gebieden zijn waar het AVG-kader en het Japanse kader op één lijn zitten over bepaalde kernbepalingen, zoals nauwkeurigheid van gegevens, minimale gegevensverwerking, opslagbeperking, gegevensbeveiliging, doelbinding en een onafhankelijke toezichthoudende autoriteit (de Japanse Commissie Bescherming Persoonsgegevens (CBP)).
9. Daarnaast verwelkomt het EDPB de inspanningen van de Europese Commissie en de Japanse autoriteiten om ervoor te zorgen dat Japan een adequaat beschermingsniveau biedt dat gelijkwaardig is aan het door de AVG geboden beschermingsniveau, met name door de leemten tussen de AVG en het Japanse gegevensbeschermingskader op te vullen met door de CBP vast te stellen aanvullende regels die alleen van toepassing zijn op vanuit de EU naar Japan doorgegeven persoonsgegevens (de "aanvullende regels"). Het EDPB merkt bijvoorbeeld op dat de CBP ermee heeft ingestemd om meer soorten gegevens als gevoelige gegevens te behandelen (gegevens met betrekking tot seksuele gerichtheid of het lidmaatschap van een vakbond zijn volgens de Japanse wetgeving geen gevoelige gegevens). Daarnaast zorgen de aanvullende regels ervoor dat de rechten van betrokkenen van toepassing zullen zijn op alle vanuit de EU doorgegeven persoonsgegevens, ongeacht de bewaartermijn (terwijl in het Japanse rechtssysteem is bepaald dat de rechten van betrokkenen niet van toepassing zijn op persoonsgegevens die binnen een periode van zes maanden worden gewist).
10. Het EDPB neemt ook nota van de inspanningen van de Europese Commissie om het adequaatheidsbesluit te versterken in reactie op de door het EDPB geuite punten van zorg.

1.2 Algemene uitdagingen

11. Toch blijven er nog uitdagingen. Het EDPB stelt voor met name de volgende gebieden in het Japanse systeem te versterken en nauwlettend te monitoren.
12. De eerste uitdaging betreft het toezicht op deze nieuwe adequaatheidsarchitectuur, waarbij een bestaand rechtskader wordt gecombineerd met specifieke aanvullende regels, om ervoor te zorgen dat het systeem duurzaam en betrouwbaar wordt en geen aanleiding geeft tot **praktische problemen met betrekking tot de concrete en efficiënte naleving** door Japanse entiteiten en handhaving door de CBP.

⁷ WP254, Adequaatheidsreferentiedocument, 6 februari 2018.

13. Ten tweede neemt het EDPB nota van de herhaalde toezeggingen en garanties van de Europese Commissie en de Japanse autoriteiten met betrekking tot het bindende en afdwingbare karakter van de aanvullende regels en verzoekt het EDPB de Europese Commissie om **voortdurend toe te zien op het bindende karakter en de daadwerkelijke toepassing ervan in Japan**, aangezien de juridische waarde van de aanvullende regels een absoluut essentieel element van het EU-Japan-adequaateitsbesluit vormt. Wat de richtsnoeren van de CBP betreft, zou het EDPB in het ontwerpadequaateitsbesluit graag verduidelijkingen zien met betrekking tot **het bindende karakter ervan. Het EDPB verzoekt de Commissie om nauwlettend op dit aspect toe te zien**⁸.

1.3 Specifieke commerciële aspecten

14. Wat de commerciële aspecten van het EU-Japan-ontwerpadequaateitsbesluit betreft, heeft het EDPB enkele specifieke punten van zorg en zou het graag opheldering krijgen over een aantal belangrijke kwesties.

1.3.1 Punten van zorg van het EDPB met betrekking tot belangrijke beginselen inzake gegevensbescherming

15. Het EDPB verwelkomt dat de aanvullende regels uitsluiten dat vanuit de EU doorgegeven persoonsgegevens verder worden doorgegeven aan een derde land op basis van grensoverschrijdende privacyregels van de economische samenwerking Azië-Stille Oceaan (APEC). Daarnaast erkent het EDPB dat de Europese Commissie zich in haar nieuwe ontwerp van het adequaateitsbesluit ertoe heeft verbonden het adequaateitsbesluit op te schorten wanneer bij verdere doorgifte de bescherming niet langer is gewaarborgd.
16. Volgens de Japanse wetgeving is een van de rechtsgronden voor verdere doorgifte de erkenning van een derde land als land dat een adequaat beschermingsniveau biedt dat gelijkwaardig is aan het door Japan geboden beschermingsniveau. De beoordeling door Japan van een derde land als een land dat een adequaat beschermingsniveau biedt, lijkt echter niet de specifieke "aanvullende regels" te omvatten waarover de Europese Commissie en de CBP hebben onderhandeld en die alleen van toepassing zijn op persoonsgegevens uit de EU om een beschermingsniveau te bieden dat in wezen gelijkwaardig is aan het door de normen van de AVG geboden beschermingsniveau. Hieruit volgt dat persoonsgegevens uit de EU die op basis van een Japans adequaateitsbesluit vanuit Japan worden doorgegeven aan een derde land waarvan niet wordt erkend dat het een gegevensbeschermingskader heeft dat in wezen gelijkwaardig is aan dat van de AVG, niet langer noodzakelijkerwijs de specifieke bescherming voor persoonsgegevens uit de EU genieten.
17. **Er zij evenwel op gewezen dat persoonsgegevens verder kunnen worden doorgegeven aan derde landen die het voorwerp van een eventueel later Japans adequaateitsbesluit worden. Het is mogelijk dat deze derde landen niet het voorwerp zijn geweest van een eerdere beoordeling of vaststelling van adequaateit door de EU. Op dit punt moet de Commissie haar controlerende rol vervullen en ervoor zorgen dat het niveau van bescherming van gegevens uit de EU wordt gehandhaafd, of moet zij overwegen dit adequaateitsbesluit op te schorten.**
18. Bovendien heeft het EDPB punten van zorg met betrekking tot de **toestemming en de transparantieplichtingen** van verwerkingsverantwoordelijken (ondernemers die persoonlijke informatie behandelen, hierna "OPIB's"). Het EDPB heeft deze elementen zorgvuldig gecontroleerd omdat het gebruik van toestemming als basis voor de verwerking en doorgifte een centrale rol speelt in het Japanse rechtstelsel, anders dan in de Europese wetgeving inzake gegevensbescherming. Het EDPB maakt zich bijvoorbeeld zorgen over het begrip "toestemming", dat niet zodanig is gedefinieerd

⁸ Zie punt 1.3.4 van het onderhavige advies voor meer informatie.

dat het herroepingsrecht eronder valt, een essentieel element in het EU-recht om ervoor te zorgen dat de betrokkene daadwerkelijk controle heeft over zijn persoonsgegevens. Wat de transparantieverplichtingen van OPIB's betreft, bestaat er twijfel over de vraag of aan de betrokkenen proactieve informatie wordt verstrekt.

19. Het EDPB maakt zich zorgen over het feit dat het **Japane verhaalsysteem** mogelijk niet gemakkelijk toegankelijk is voor natuurlijke personen in de EU die ondersteuning nodig hebben of een klacht willen indienen, aangezien de steun van de CBP beschikbaar is via een hulplijn en alleen in het Japans. Hetzelfde probleem doet zich voor met de bemiddelingsdienst van de CBP aangezien het systeem niet wordt bekendgemaakt op de Engelse versie van de website van de CBP. Ook belangrijke informatieve documenten, zoals het document met vaak gestelde vragen over de Japanse wet op de bescherming van persoonsgegevens (hierna "WBP"), zijn alleen in het Japans beschikbaar. In dat verband zou het EDPB graag zien dat de Commissie met de CBP de mogelijkheid bespreekt om een onlinedienst op te zetten, ten minste in het Engels, die gericht is op het verlenen van ondersteuning aan en de behandeling van klachten van natuurlijke personen in de EU – vergelijkbaar met de in bijlage II van dit adequaatheidsbesluit bedoelde dienst. De Europese Commissie zal ook nauwlettend moeten toezien op de doeltreffendheid van de sancties en de relevante rechtsmiddelen.

1.3.2 Noodzaak van verduidelijking

20. Het EDPB zou graag garanties krijgen met betrekking tot een aantal aspecten van het ontwerpadequaatheidsbesluit die nog verder moeten worden verduidelijkt.
21. Deze hebben bijvoorbeeld betrekking op een aantal sleutelbegrippen van de Japanse wetgeving. Meer specifiek is er een gebrek aan duidelijkheid over de **status van de zogenaamde "beheerder"** – die vergelijkbaar is met de "verwerker" in de AVG maar wiens vermogen om het doel van en de middelen voor de verwerking van persoonsgegevens te bepalen en te wijzigen onduidelijk blijft.
22. Het EDPB zou ook garanties moeten krijgen – vanwege het ontbreken van de relevante documenten – over de vraag of de **bepalingen van de rechten van natuurlijke personen** (met name het recht van inzage, recht op rectificatie en recht van bezwaar) noodzakelijk en evenredig zijn in een democratische samenleving en of zij in overeenstemming zijn met de essentie van grondrechten.
23. Het EDPB verwacht ook dat de Europese Commissie er nauwlettend op toeziet dat **persoonsgegevens die op basis van het ontwerpadequaatheidsbesluit vanuit de EU naar Japan worden doorgegeven** effectief worden beschermd **gedurende de gehele "levenscyclus" van die gegevens**, ook al is in de Japanse wetgeving bepaald dat informatie over de oorsprong van de gegevens maximaal drie jaar moet worden bewaard.

1.4 Over de inzage van overheidsinstanties in gegevens die aan Japan zijn doorgegeven

24. Het EDPB heeft ook een analyse gemaakt van het rechtskader voor Japanse overheidsinstanties wanneer zij om redenen van rechtshandhaving of nationale veiligheid inzage hebben in persoonsgegevens die vanuit de EU aan Japan zijn doorgegeven. Het EDPB erkent de garanties van de Japanse overheid, waarnaar wordt verwezen als bijlage II bij het ontwerpadequaatheidsbesluit, maar heeft een aantal aspecten geïdentificeerd die verduidelijking behoeven en aanleiding geven tot bezorgdheid, waarvan de volgende moeten worden benadrukt.
25. Wat rechtshandhaving betreft, merkt het EDPB op dat de rechtsbeginselen die van toepassing zijn op de inzage in gegevens vaak vergelijkbaar lijken met de regels in de EU, voor zover deze bestaan. Het gebrek aan beschikbare vertalingen van verschillende wetteksten en van relevante jurisprudentie maakt het echter moeilijk om te concluderen dat alle procedures voor inzage in gegevens noodzakelijk

en evenredig zijn en dat deze beginselen worden toegepast op een wijze die "in wezen gelijkwaardig" is aan de in het EU-recht voorgeschreven wijze.

26. Wat nationale veiligheid betreft, erkent het EDPB dat de Japanse overheid heeft herhaald dat informatie alleen kan worden verkregen uit vrij toegankelijke bronnen of door vrijwillige bekendmaking door bedrijven, en dat zij geen informatie over het grote publiek verzamelt. Het EDPB is echter op de hoogte van punten van zorg die door deskundigen en in de media zijn geuit en zou graag meer duidelijkheid krijgen over de toezichtsmaatregelen van Japanse overheidsinstanties.
27. Wat de juridische verhaalsmogelijkheden van natuurlijke personen uit de EU betreft, verwelkomt het EDPB dat de Europese Commissie en de Japanse overheid hebben onderhandeld over een aanvullend mechanisme om natuurlijke personen uit de EU op het gebied van rechtshandhaving en nationale veiligheid een extra verhaalsmogelijkheid te bieden, waardoor de bevoegdheden van de Japanse gegevensbeschermingsautoriteit worden uitgebreid. Een punt van zorg blijft echter dat dit nieuwe mechanisme de tekortkomingen van de toezichts- en verhaalmechanismen overeenkomstig de Japanse wetgeving niet volledig compenseert. Het EDPB vraagt dus verdere verduidelijking om ervoor te zorgen dat dit nieuwe mechanisme deze tekortkomingen wel volledig compenseert.

1.5 Conclusie

28. Het EDPB is van mening dat dit adequaatheidsbesluit van het grootste belang is. Het is het eerste adequaatheidsbesluit sinds de inwerkingtreding van de AVG en zal **een precedent vormen voor toekomstige verzoeken om een adequaatheidsbesluit en voor de herziening van de overeenkomstig Richtlijn 95/46/EG⁹ genomen adequaatheidsbesluiten**. Het is ook belangrijk te onderstrepen dat mensen zich steeds meer bewust zijn van de gevolgen van de globalisering voor hun privacy en dat zij hun toezichthoudende autoriteiten vragen om ervoor te zorgen dat er voldoende waarborgen zijn wanneer hun persoonsgegevens naar het buitenland worden doorgegeven. In het licht van deze gevolgen is het EDPB van mening dat de Europese Commissie ervoor moet zorgen dat er geen tekortkomingen zijn in de bescherming die wordt geboden door het EU-Japan-adequaatheidsbesluit en dat dit specifieke type adequaatheid in overeenstemming is met de vereisten van artikel 45 van de AVG.
29. Het EDPB verwelkomt de inspanningen van de Europese Commissie en de Japanse CBP om het Japanse rechtskader zo veel mogelijk op het Europese rechtskader af te stemmen. **De verbeteringen** die met de aanvullende regels zijn geïntroduceerd om enkele van de verschillen tussen de twee kaders te overbruggen, zijn zeer belangrijk en zijn goed onthaald.
30. Na een zorgvuldige analyse van het ontwerpadequaatheidsbesluit van de Commissie en van het Japanse kader voor gegevensbescherming merkt het EDPB echter op dat **er nog een aantal punten van zorg bestaan en dat er nog steeds behoefte is aan verdere verduidelijking**. Verder roept dit specifieke type adequaatheid, waarbij een bestaand nationaal kader wordt gecombineerd met aanvullende specifieke regels, ook vragen op over de operationele implementatie ervan. In het licht van het bovenstaande beveelt het EDPB de Europese Commissie aan, de door het EDPB geformuleerde punten van zorg en verzoeken om verduidelijking aan te pakken en verdere bewijzen en uitleg te verschaffen over de aan de orde gestelde kwesties. Het EDPB nodigt de Europese Commissie ook uit om deze vaststelling van adequaatheid (ten minste) om de twee jaar te herzien, en niet om de vier jaar zoals in het huidige ontwerpadequaatheidsbesluit voorgesteld.

⁹ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

2 INLEIDING

2.1 Japans kader voor gegevensbescherming

31. Het Japanse kader voor gegevensbescherming is zeer recentelijk, in 2017, geactualiseerd. Dit kader bestaat uit een aantal pijlers, waarvan een algemene wet, namelijk de wet op de bescherming van persoonsgegevens (WBP), de kern vormt. Een ander belangrijk stuk wetgeving is het Regeringsdecreet tot handhaving van de WBP ("het Regeringsdecreet"), waarin bepaalde kernbeginselen van de WBP zijn gespecificeerd.
32. Op basis van een regeringsbesluit van 12 juni 2018¹⁰ en artikel 6 van de WBP kreeg de CBP de bevoegdheid om *"de nodige maatregelen te nemen om de verschillen tussen de systemen en activiteiten van Japan en die van het betrokken derde land te overbruggen teneinde te zorgen voor een passende behandeling van persoonsgegevens die vanuit elk land worden ontvangen"*¹¹. In het regeringsbesluit wordt ook gesuggereerd dat de door de CBP vastgestelde regels die een aanvulling vormen op of verder gaan dan de regels van de WBP, bindend en afdwingbaar zouden zijn voor Japanse ondernemers¹².
33. De CBP is daarom in onderhandeling getreden met de Europese Commissie en heeft in juni 2018 strengere regels dan die van de WBP en het Regeringsdecreet vastgesteld die op vanuit de EU doorgegeven gegevens moeten worden toegepast. Dit zijn de aanvullende regels onder de Wet op de bescherming van persoonsgegevens bij de verwerking van persoonsgegevens die op basis van een adequaatheidsbesluit vanuit de EU zijn doorgegeven, hierna "aanvullende regels"¹³ genoemd. Deze aanvullende regels zijn ook opgenomen in de bijlage bij het ontwerpuitvoeringsbesluit van de Commissie dat in juli 2018 is gepubliceerd.
34. Het is belangrijk op te merken dat de aanvullende regels alleen van toepassing zijn op persoonsgegevens die op basis van het adequaatheidsbesluit vanuit de EU naar Japan zijn doorgegeven en dat zij tot doel hebben die gegevens beter te beschermen. De aanvullende regels zijn dus niet van toepassing op persoonsgegevens van natuurlijke personen in Japan noch op persoonsgegevens van natuurlijke personen uit een niet-EER-land.
35. Verder wil het EDPB de aandacht vestigen op het feit dat de gewijzigde WBP op 30 mei 2017 in werking is getreden en dat de CBP in zijn huidige vorm in 2016 is opgericht. Bovendien moeten de aanvullende regels waarover de CBP met de Europese Commissie heeft onderhandeld nog in werking treden, aangezien die inwerkingtreding afhankelijk is van de erkenning door de Europese Commissie van Japan als een rechtsgebied waar persoonsgegevens even adequaat worden beschermd als in de EU.

2.2 Reikwijdte van de beoordeling van het EDPB

36. Het ontwerpadequaatheidsbesluit van de Europese Commissie is het resultaat van een beoordeling van de Japanse regels inzake gegevensbescherming, gevolgd door onderhandelingen met de Japanse autoriteiten. Het resultaat van deze onderhandelingen is met name weerspiegeld in de twee bijlagen bij het ontwerpadequaatheidsbesluit. De eerste bijlage voorziet in aanvullende bescherming die Japanse ondernemers zullen moeten bieden bij de verwerking van persoonsgegevens die vanuit de EU

¹⁰ Het EDPB merkt op dat dit regeringsbesluit volgens het ontwerpadequaatheidsbesluit op 12 juni 2018 werd vastgesteld. Het EDPB heeft echter alleen de ontwerpversie van het regeringsbesluit van april 2018 ontvangen.

¹¹ Regeringsbesluit van 25 april 2018.

¹² Zie punt 1.3.4 voor meer informatie.

¹³ Aanvullende regels, bijlage I bij het uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, die op september 2018 aan het EDPB zijn toegezonden.

zijn doorgegeven. De tweede bijlage bevat garanties en toezeggingen van de Japanse overheid met betrekking tot de inzage van overheidsinstanties in gegevens.

37. Het EDPB heeft het Japanse gegevensbeschermingskader, de aanvullende regels waarover de Europese Commissie heeft onderhandeld en de garanties en toezeggingen van de Japanse overheid onderzocht. Van het EDPB wordt verwacht dat het een onafhankelijk advies over de bevindingen van de Europese Commissie uitbrengt, eventuele tekortkomingen in het adequaatheidskader identificeert en wijzigingen of aanpassingen voorstelt om die tekortkomingen aan te pakken.
38. Zoals in het adequaatheidsreferentiedocument van het EDPB vermeld, moet "*de door de Europese Commissie verstrekte informatie uitputtend zijn en het EDPB in staat stellen het niveau van gegevensbescherming in het derde land zelf te beoordelen*"¹⁴.
39. Het EDPB heeft evenwel Engelse vertalingen ontvangen van de meeste documenten waarnaar wordt verwezen in het ontwerpadequaateitsbesluit en die een essentieel onderdeel van het Japanse rechtstelsel vormen. Het EDPB brengt het onderhavige advies derhalve uit op basis van de analyse van in het Engels beschikbare documenten. Het EDPB heeft rekening gehouden met het toepasselijke gegevensbeschermingskader in de Europese Unie, waaronder artikel 8 van het Europees Verdrag voor de rechten van de mens (hierna "het EVRM") tot bescherming van het recht op eerbiediging van het privéleven en het familie- en gezinsleven alsmede de artikelen 7, 8 en 47 van het Handvest van de grondrechten van de Europese Unie (hierna "het Handvest") tot bescherming van respectievelijk het recht op eerbiediging van het privéleven en het familie- en gezinsleven, het recht op bescherming van persoonsgegevens en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht. Daarnaast heeft het EDPB rekening gehouden met de vereisten van de AVG en met de relevante jurisprudentie.
40. Het doel daarvan is ervoor te zorgen dat het Japanse kader voor gegevensbescherming in wezen gelijkwaardig is aan dat van de Europese Unie. Het HvJ heeft het begrip "adequaate beschermingsniveau", dat reeds bestond in Richtlijn 95/46/EG, verder uitgewerkt. Het is belangrijk te herinneren aan de norm die het HvJ in het arrest-Schrems heeft vastgesteld, namelijk dat het "beschermingsniveau" in het derde land "in wezen gelijkwaardig" moet zijn aan het in de EU gewaarborgde niveau – "de middelen waarmee dat derde land in dit verband voor een dergelijk beschermingsniveau kan zorgen, kunnen verschillen van die welke binnen de EU worden ingezet"¹⁵. Het doel is dus niet om de Europese wetgeving punt per punt te weerspiegelen, maar om de essentiële en kernvereisten van de onderzochte wetgeving vast te stellen. Adequaateit kan worden bereikt door een combinatie van rechten voor de betrokkenen en verplichtingen voor degenen die gegevens verwerken of die controle uitoefenen over die verwerking, en toezicht door onafhankelijke instanties. Regels inzake gegevensbescherming zijn echter alleen doeltreffend als ze afdwingbaar zijn en in de praktijk worden nageleefd. Daarom moet niet alleen worden gekeken naar de inhoud van regels die van toepassing zijn op persoonsgegevens die aan een derde land of aan een internationale organisatie worden doorgegeven, maar ook naar het bestaande systeem om de doeltreffendheid van die regels te waarborgen. Efficiënte handhavingsmechanismen zijn van het grootste belang voor de doeltreffendheid van gegevensbeschermingsregels¹⁶.

¹⁴ WP254, blz. 3.

¹⁵ Zaak C- 362/14, Maximilian Schrems/Data Protection Commissioner, 6 oktober 2015 (§§ 73 en 74).

¹⁶ WP254, blz. 2.

2.3 Algemene opmerkingen en bezorgdheden

2.3.1 Bijzonderheden van dit type adequaatheidsbesluit

41. Het EU-Japan-adequaateitsbesluit is het eerste dat wordt onderzocht tegen de nieuwe juridische achtergrond van de AVG. Dit maakt het werk van het EDPB des te belangrijker gezien de gevolgen van dit ontwerpadequaateitsbesluit voor toekomstige verzoeken om een adequaatheidsbesluit.
42. Het EU-Japan-adequaateitsbesluit zou ook het eerste wederzijdse adequaatheidsbesluit zijn. Wanneer en indien de EU erkent dat Japan een beschermingsniveau biedt dat in wezen gelijkwaardig is aan het door de AVG geboden beschermingsniveau, zal Japan ook zijn eigen adequaatheidsbesluit uitvaardigen overeenkomstig artikel 24 van de WBP, waarin wordt erkend dat de EU een adequaat beschermingsniveau biedt overeenkomstig het Japanse kader voor gegevensbescherming. Dit beoogde Japan-EU-adequaateitsbesluit is dus van bijzondere aard, en het EDPB heeft daarmee rekening gehouden bij zijn beoordeling. Zoals hierboven vermeld, heeft de Japanse CBP met de Europese Commissie onderhandeld over specifieke, strengere regels die alleen van toepassing zijn op vanuit de EU doorgegeven persoonsgegevens. Deze strengere regels zijn bindend en afdwingbaar overeenkomstig het regeringsbesluit en moeten door alle ondernemers die persoonlijke informatie behandelen (hierna "OPIB's") in Japan worden nageleefd bij de verwerking van persoonsgegevens uit de EU in het kader van dit ontwerpadequaateitsbesluit.
43. De Europese Commissie heeft haar vaststelling van adequaatheid daarom niet alleen op het bestaande algemene Japanse gegevensbeschermingskader maar ook op deze specifieke regels gebaseerd. Het feit dat aanvullende regels nodig waren om de WBP aan te vullen, geeft aan dat de Europese Commissie erkent dat de Japanse wetgeving inzake gegevensbescherming op zich niet in wezen gelijkwaardig is aan de AVG.
44. **In het licht van de bovengenoemde kwesties verzoekt het EDPB de Europese Commissie ervoor te zorgen dat deze nieuwe, op aanvullende regels gebaseerde adequaatheidsarchitectuur, de eerste die in het kader van de AVG zal worden vastgesteld, een duurzaam en betrouwbaar systeem zal zijn dat geen praktische vragen oproept over de concrete en efficiënte naleving door Japanse entiteiten en handhaving door de CBP.**

2.3.2 Betrouwbaarheid van vertalingen

45. Net als de Europese Commissie heeft het EDPB gewerkt op basis van Engelse vertalingen die door de Japanse autoriteiten waren verstrekt¹⁷. Het EDPB verzoekt de Europese Commissie te verduidelijken dat zij haar ontwerpadequaateitsbesluit heeft gebaseerd op de ontvangen Engelse vertalingen, en de kwaliteit en betrouwbaarheid van deze vertalingen regelmatig te controleren.

2.3.3 Sectorale adequaatheid

46. De vaststelling van adequaatheid in dit ontwerpadequaateitsbesluit is beperkt tot de bescherming van persoonsgegevens door OPIB's in de zin van de WBP. Dat betekent dat de adequaatheid sectoraal is, aangezien zij alleen van toepassing is op de particuliere sector – doorgiften van persoonsgegevens tussen overheidsinstanties en -organen van het toepassingsgebied worden uitgesloten. De Europese Commissie vermeldt in overweging 10 van het ontwerpadequaateitsbesluit kort deze specificiteit van het toepassingsgebied van de adequaatheid.
47. **Het EDPB verzoekt de Europese Commissie om in de titel van het uitvoeringsbesluit en in artikel 1 ervan uitdrukkelijk te vermelden dat deze vaststelling van adequaatheid sectoraal van aard is overeenkomstig artikel 45, lid 3, van de AVG.**

¹⁷ De Europese Commissie heeft deze vertalingen gecontroleerd.

2.3.4 Bindend karakter van de aanvullende regels en de richtsnoeren van de CBP

48. In artikel 6 van de WBP is bepaald dat "de overheid de nodige wetgevende en andere maatregelen moet nemen om discrete actie te kunnen ondernemen ter bescherming van persoonsgegevens die met name een strikte toepassing van de correcte behandeling ervan vereisen teneinde te streven naar een betere bescherming van de rechten en belangen van betrokkenen, en dat de overheid in samenwerking met de overheden van andere landen de nodige maatregelen moet nemen om een internationaal conform systeem met betrekking tot persoonsgegevens op te zetten door samenwerking met een internationale organisatie en een ander internationaal kader te bevorderen". Hoewel in dit artikel van de WBP duidelijk wordt aangegeven dat de overheid bevoegd is om dergelijke juridische maatregelen te nemen, verwijst het niet rechtstreeks naar de CBP als het bevoegde orgaan om specifieke regels vast te stellen¹⁸. Wegens tijdgebrek was het EDPB niet in staat bestaand bewijsmateriaal over dit punt te verzamelen en te onderzoeken.
49. **Gezien het belang van deze kwestie neemt het EDPB nota van de herhaalde toezeggingen en garanties van de Europese Commissie en de Japanse autoriteiten betreffende het bindende en afdwingbare karakter van de aanvullende regels. Het EDPB verzoekt de Europese Commissie om voortdurend toe te zien op het bindende karakter en de daadwerkelijke toepassing van de aanvullende regels in Japan, aangezien de juridische waarde ervan een essentieel element van het EU-Japan-adequaateitsbesluit is.**
50. Bovendien verwijst de Europese Commissie in verschillende delen van haar ontwerpadequaateitsbesluit naar de richtsnoeren van de CBP (hierna "de richtsnoeren").
51. Hoewel de Europese Commissie in overweging 16 van haar ontwerpadequaateitsbesluit verduidelijkt dat de richtsnoeren een gezaghebbende interpretatie van de WBP geven, verwijst zij in dezelfde overweging naar het bindende karakter van die richtsnoeren: "Volgens de van de CBP ontvangen informatie worden deze richtsnoeren beschouwd als bindende regels die integraal deel uitmaken van het rechtskader en die samen met de tekst van de WBP, het Regeringsdecreet, de CBP-regels en een door de CBP opgesteld vraag-en-antwoorddocument moeten worden gelezen."¹⁹
52. Op basis van dezelfde informatie die door de CBP is verstrekt, is het EDPB echter van mening dat de richtsnoeren niet juridisch bindend zijn. Ze verschaffen veeleer een "gezaghebbende interpretatie" van de wet. De CBP voert aan dat de richtsnoeren in de praktijk door OPIB's worden gevolgd, door de CBP worden gebruikt om de wet te handhaven tegen OPIB's en door rechters worden gebruikt bij het wijzen van vonnissen. Deze elementen vormen echter onvoldoende bewijs dat de richtsnoeren juridisch bindende normen zijn.
53. **Het EDPB zou in het adequaateitsbesluit graag verduidelijkingen zien met betrekking tot het bindende karakter van de richtsnoeren van de CBP en verzoekt de Europese Commissie dit aspect nauwlettend in het oog te houden.**
54. Volgens de CBP worden de richtsnoeren in de praktijk toch gevolgd, omdat het een lokaal gebruik is. De CBP vermeldt dat de Japanse rechtbanken de richtsnoeren van de CBP gebruiken om hun vonnissen te wijzen bij toepassing van de regels van de WBP. De Europese Commissie verwijst naar een

¹⁸ Volgens een artikel dat in juli 2018, toen de aanvullende regels nog in de ontwerpfase zaten, werd gepubliceerd, was het juridisch bindende karakter van deze regels waarschijnlijk onderwerp van intern debat in Japan. Zie Fujiwara S., 'Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (juli 2018): blz. 19.

¹⁹ Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, overweging 16.

rechterlijke uitspraak²⁰ uit 2006 om aan te tonen dat de Japanse rechtbanken zich voor hun bevindingen baseren op richtsnoeren. Het EDPB heeft deze rechterlijke uitspraak niet ontvangen maar zou het op prijs stellen als de Europese Commissie een recentere rechterlijke uitspraak, indien beschikbaar, zou kunnen verstrekken, hetzij op het gebied van gegevensbescherming, hetzij in een andere sector waar de Japanse rechtbanken hun uitspraak op de richtsnoeren van de CBP of andere soortgelijke richtsnoeren hebben gebaseerd.

2.3.5 Periodieke herziening van de vaststelling van adequaatheid

55. In artikel 45, lid 3, van de AVG is bepaald dat ten minste om de vier jaar een periodieke herziening moet plaatsvinden. Volgens het adequaatheidsreferentiedocument van het EDPB²¹ is dit een algemene termijn die aan elk derde land of elke internationale organisatie met een adequaatheidsbesluit moet worden aangepast. Afhankelijk van de specifieke omstandigheden kan een kortere herzieningscyclus gerechtvaardigd zijn. Ook kunnen incidenten of andere informatie over of wijzigingen in het rechtskader van het derde land of de internationale organisatie in kwestie aanleiding geven tot een vervroegde herziening. Het lijkt ook passend om in het geval van een geheel nieuw adequaatheidsbesluit vrij snel over te gaan tot een eerste evaluatie en de herzieningscyclus geleidelijk aan te passen, afhankelijk van het resultaat van de evaluatie.
56. Rekening houdend met een aantal factoren, zoals het feit dat de WBP in 2017 in werking is getreden, dat de CBP in 2016 is opgericht en dat er nog geen informatie of bewijs is over de praktische toepassing van de aanvullende regels, **verzoekt het EDPB de Europese Commissie om deze vaststelling van adequaatheid (ten minste) om de twee jaar te evalueren, en niet om de vier jaar zoals in het huidige ontwerpadequaatheidsbesluit voorgesteld.**

2.3.6 Door Japan aangegane internationale verbintenissen

57. Overeenkomstig artikel 45, lid 2, onder c), van de AVG en het adequaatheidsreferentiedocument²² moet de Europese Commissie bij de beoordeling van de adequaatheid van het beschermingsniveau van een derde land onder meer rekening houden met de internationale verbintenissen die het derde land is aangegaan, of andere verplichtingen die voortvloeien uit de deelname van het derde land aan multilaterale of regionale systemen, met name met betrekking tot de bescherming van persoonsgegevens, alsmede met de nakoming van die verplichtingen. Voorts moet rekening worden gehouden met de toetreding van het derde land tot het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens ("Verdrag 108+"²³ en het bijbehorende Aanvullend Protocol.
58. **In dit verband merkt het EDPB op dat Japan een waarnemer van het Raadgevend Comité van Verdrag 108+ is.**

²⁰ Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, bladzijde 5, voetnoot 16: "Districtsrechtbank van Osaka, uitspraak van 19 mei 2006, Hanrei Jiho, vol. 1948, blz. 122".

²¹ WP254, blz. 3.

²² WP254, blz. 2.

²³ Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Verdrag 108+, 18 mei 2018.

2.3.7 Bevoegdheden van gegevensbeschermingsautoriteiten²⁴ om bij een rechtbank rechtsvorderingen in te stellen betreffende de geldigheid van een adequaatheidsbesluit

59. Hoewel in overweging 179 van het ontwerpadequaateheidsbesluit alleen gevallen worden genoemd waarin een gegevensbeschermingsautoriteit een klacht heeft ontvangen waarin de verenigbaarheid van een adequaatheidsbesluit met het grondrecht op privacy en het grondrecht op gegevensbescherming in twijfel wordt getrokken, benadrukt het EDPB dat deze verklaring moet worden opgevat als een voorbeeld van situaties waarin een gegevensbeschermingsautoriteit de zaak voor een nationale rechtbank kan brengen, wat ook zonder een klacht mogelijk zou zijn, in plaats van als een beperking van de bevoegdheden van de gegevensbeschermingsautoriteiten krachtens de AVG en de nationale wetgeving van de lidstaten op dit gebied. De bepalingen van de AVG omvatten immers zowel de bevoegdheid om doorgiften van gegevens op te schorten, zelfs indien de doorgifte op een adequaatheidsbesluit is gebaseerd, als de bevoegdheid om een rechtsvordering in te stellen met betrekking tot de geldigheid van een adequaatheidsbesluit, en zijn niet beperkt tot gevallen waarin zij een klacht hebben ontvangen, indien hun nationale wetgeving hun de bevoegdheid verleent om dit ruimer en onafhankelijk van een klacht te doen, overeenkomstig de relevante bepalingen van de AVG.
60. **Het EDPB verzoekt de Europese Commissie om in haar ontwerpadequaateheidsbesluit te verduidelijken dat de bevoegdheid van toezichthoudende autoriteiten om naar aanleiding van een klacht een rechtsvordering tegen de geldigheid van een adequaatheidsbesluit in te stellen slechts een illustratie is van de ruimere bevoegdheden van gegevensbeschermingsautoriteiten die voortvloeien uit de AVG, waaronder de bevoegdheid om doorgiften op te schorten en om een rechtsvordering in te stellen met betrekking tot de geldigheid van een adequaatheidsbesluit bij gebrek aan een klacht indien hun nationale wetgeving daarin voorziet.**

3 COMMERCIEËLE ASPECTEN

3.1 Inhoudelijke beginselen

61. Hoofdstuk 3 van het adequaatheidsreferentiedocument is gewijd aan de "inhoudelijke beginselen". Het systeem van een derde land of een internationale organisatie moet deze beginselen bevatten opdat het geboden beschermingsniveau zou kunnen worden beschouwd als in wezen gelijkwaardig aan het door de EU-wetgeving gewaarborgde niveau. Het EDPB erkent het feit dat in het Japanse rechtstelsel een andere benadering wordt gevolgd dan die van de AVG om uitvoering te geven aan het recht op privacy. Hoewel het recht op privacy niet in de Japanse grondwet is vastgelegd, is dit recht via de jurisprudentie erkend als een grondwettelijk recht, zoals ook in het besluit van de Europese Commissie is vermeld²⁵.
62. Vooral wegens het feit dat de Japanse aanpak merkbaar verschilt van de Europese moet zorgvuldig worden nagegaan of niet alleen afzonderlijke aspecten een beschermingsniveau bieden dat "in wezen gelijkwaardig" is, maar of het systeem als geheel uiteindelijk een beschermingsniveau biedt dat "in wezen gelijkwaardig" is. Dat betekent dat mogelijke "tekortkomingen" met betrekking tot één

²⁴ Zaak C- 362/14, Maximilian Schrems/Data Protection Commissioner, 6 oktober 2015.

²⁵ Het EDPB heeft geen Engelse vertaling van deze rechterlijke uitspraak ontvangen. Zie Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, voetnoot 9

inhoudelijk beginsel kunnen worden gecompenseerd door een aantal andere aspecten die voor adequate teugels en tegenwichten zorgen.

3.1.1 Begrippen

63. Op basis van het adequaatheidsreferentiedocument moeten in het rechtskader van het derde land basisbegrippen en/of -beginselen inzake gegevensbescherming bestaan. Hoewel deze geen afspiegeling van de terminologie in de AVG hoeven te zijn, moeten zij in overeenstemming zijn met de begrippen die in de Europese wetgeving inzake gegevensbescherming zijn vastgelegd. De AVG omvat bijvoorbeeld de volgende belangrijke begrippen: "persoonsgegevens", "verwerking van persoonsgegevens", "verwerkingsverantwoordelijke", "verwerker", "ontvanger" en "gevoelige gegevens"²⁶.
64. De WBP bevat ook een aantal definities, zoals die van de termen "persoonlijke informatie", "persoonsgegevens", "ondernemer die persoonlijke informatie behandelt". **Het lijkt er echter op dat de WBP geen definitie van de term "behandeling van persoonsgegevens" bevat die vergelijkbaar is met de term "verwerking van persoonsgegevens".**
65. De CBP heeft schriftelijk geantwoord op de vraag van het EDPB over de definitie van de term "behandeling van persoonsgegevens". De Europese Commissie heeft dit antwoord in haar ontwerpbesluit geciteerd: *"De term "verwerking" wordt niet in de WBP gebruikt, maar de WBP hanteert het equivalente begrip "behandeling", dat volgens de door de CBP ontvangen informatie betrekking heeft op "elke handeling met betrekking tot persoonsgegevens", met inbegrip van het verkrijgen, invoeren, verzamelen, organiseren, bewaren, bewerken, verwerken, vernieuwen, uitvoeren, bevestigen, gebruiken of verstrekken van persoonlijke informatie".*²⁷
66. Aangezien de referentietekst voor deze definitie echter niet is verstrekt, verzoekt het EDPB **de Europese Commissie er nauwlettend op toe te zien dat de door de CBP verstrekte definitie van bovengenoemd begrip in de praktijk daadwerkelijk wordt gevolgd.**

3.1.1.1 Het begrip "verwerker" en verplichtingen van een "beheerder"

67. Zoals hierboven vermeld, is in het adequaatheidsreferentiedocument bepaald dat er in het rechtskader van het derde land basisbegrippen en/of -beginselen inzake gegevensbescherming moeten bestaan.
68. De WBP bevat de definitie van een "ondernemer die persoonlijke informatie behandelt". Deze term omvat volgens de Europese Commissie zowel de term "verwerkingsverantwoordelijke" als de term "verwerker" zoals die in de AVG zijn opgenomen en maakt geen onderscheid tussen beide²⁸. In artikel 22 van de WBP staat echter ook de term "beheerder", die in bepaalde opzichten lijkt op de term "verwerker" in de AVG.
69. Zoals de CBP heeft toegelicht in zijn aan het EDPB verstrekte antwoorden, die ook in het ontwerpadequaathedenbesluit van de Europese Commissie zijn opgenomen, wordt een beheerder beschouwd als het equivalent van een verwerker in de AVG, met name de persoon aan wie een OPIB de behandeling van persoonsgegevens heeft toevertrouwd. Deze beheerder heeft dezelfde verplichtingen en rechten als elke OPIB en moet zich ook houden aan de aanvullende regels voor

²⁶ WP254, blz. 4.

²⁷ Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, overweging 17.

²⁸ Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, overweging 35.

persoonsgegevens die vanuit de EU zijn doorgegeven. De OPIB die de behandeling van persoonsgegevens aan een beheerder toevertrouwt, is verplicht "noodzakelijk en passend toezicht"²⁹ op de beheerder uit te oefenen.

70. **Het EDPB verzoekt de Europese Commissie om de status en verplichtingen van de beheerder toe te lichten wanneer de beheerder het doel van en de middelen voor de verwerking wijzigt en om te verduidelijken of de toestemming van de betrokkene een noodzakelijke voorwaarde blijft voor die wijziging van het doel van of de middelen voor de verwerking³⁰.**

3.1.1.2 Term "bewaarde persoonsgegevens"

71. De WBP bevat de term "bewaarde persoonsgegevens". Deze gegevens worden als een subcategorie van persoonsgegevens beschouwd. Volgens de WBP zijn de bepalingen met betrekking tot de rechten van betrokkenen³¹ alleen van toepassing op bewaarde persoonsgegevens. De definitie van bewaarde persoonsgegevens is opgenomen in artikel 2, lid 7, van de WBP.
72. Bewaarde persoonsgegevens zijn andere persoonsgegevens dan die welke (i) binnen een termijn van maximaal 6 maanden worden gewist³² of (ii) onder de uitzonderingen van artikel 4 van het Regeringsdecreet vallen en de publieke of andere belangen kunnen schaden indien hun aanwezigheid of afwezigheid wordt bekendgemaakt.
73. In Aanvullende Regel (2) is bepaald dat "*persoonsgegevens die op basis van een adequaatheidsbesluit vanuit de EU zijn ontvangen, moeten worden behandeld als bewaarde persoonsgegevens, ongeacht de termijn waarbinnen zij moeten worden gewist*".
74. Persoonsgegevens die onder de uitzonderingen van artikel 4 van het Regeringsdecreet vallen, hoeven echter niet als bewaarde persoonsgegevens te worden behandeld en de rechten van betrokkenen zijn er niet op van toepassing.
75. In artikel 23 van de AVG is bepaald dat, net als in artikel 4 van het Regeringsdecreet, de wetgeving van de Unie of de lidstaat waaraan de verwerkingsverantwoordelijke/verwerker is onderworpen bepalingen kan bevatten die de reikwijdte van de op hem toepasselijke verplichtingen en de rechten van de betrokkene kunnen beperken. Dat kan door middel van een wetgevende maatregel. Deze beperkingen moeten de essentie van de grondrechten en fundamentele vrijheden eerbiedigen en vormen een noodzakelijke en evenredige maatregel in een democratische samenleving.
76. Wat de inhoud van de uitzonderingen betreft waarin artikel 4 van het Regeringsdecreet voorziet, heeft het EDPB onvoldoende documentatie over deze beperkingen of aanvullende elementen ontvangen om de werkingssfeer van deze bepalingen te verduidelijken³³. Het EDPB kan niet beoordelen of deze beperkingen van de rechten van betrokkenen beperkt zijn tot wat in het EU-recht strikt noodzakelijk en evenredig wordt geacht, en of deze rechten dus in wezen gelijkwaardig zouden zijn aan de rechten die betrokkenen uit de EU genieten.
77. **Bij gebrek aan een aantal relevante documenten zou het EDPB ook graag garanties van de Europese Commissie krijgen met betrekking tot de vraag of beperkingen van de rechten van betrokkenen (met**

²⁹ Artikel 22 van de gewijzigde wet op de bescherming van persoonsgegevens (WBP), in werking getreden op 30 mei 2017.

³⁰ Artikel 23, lid 5, onder i), WBP. Zie ook het deel over het transparantiebeginsel hieronder.

³¹ Artikelen 27 tot en met 30 van de WBP.

³² Wijziging van het Regeringsdecreet tot handhaving van de wet op de bescherming van persoonsgegevens (Regeringsdecreet), in werking getreden op 30 mei 2017, artikel 5.

³³ De in overweging 53 van het ontwerpadequaathheidsbesluit bedoelde uitspraken van het Hooggerechtshof zijn niet ter beschikking van het EDPB gesteld.

name het recht van inzage, recht op rectificatie en recht van bezwaar) in een democratische samenleving noodzakelijk en evenredig zijn en de essentie van de grondrechten eerbiedigen.

78. Een essentiële vereiste in de AVG is dat persoonsgegevens gedurende hun gehele "levenscyclus" worden beschermd.
79. Rekening houdend met het feit dat de aanvullende regels alleen van toepassing zijn op persoonsgegevens die vanuit de EU zijn doorgegeven, zou het EDPB graag meer informatie ontvangen over de praktische toepassing van deze regels door OPIB's, met name wanneer deze gegevens na de eerste doorgifte ervan naar Japan aan een andere OPIB worden doorgegeven.
80. De Europese Commissie heeft in overweging 15 van haar ontwerpadequaateitsbesluit verduidelijkt dat OPIB's die persoonsgegevens uit de EU ontvangen en/of verder verwerken, wettelijk verplicht zijn om de aanvullende regels na te leven en dat zij daartoe ervoor moeten zorgen dat zij die persoonsgegevens gedurende de hele "levenscyclus" ervan kunnen identificeren.
81. In zijn antwoorden heeft de CBP uitgelegd³⁴ dat een dergelijke identificatie zal plaatsvinden door middel van technische methoden (taggen) of organisatorische methoden (bewaren van gegevens uit de EU in een speciale database).
82. In voetnoot 14 van haar ontwerpadequaateitsbesluit legt de Europese Commissie uit dat OPIB's de informatie over de oorsprong van de EU-gegevens zo lang moeten bewaren als nodig is om aan de aanvullende regels te kunnen voldoen. Dit is ook vastgelegd in artikel 26, leden 1, 3 en 4, van de WBP, waarin is bepaald dat een OPIB verplicht is de bron van deze gegevens en alle omstandigheden waaronder deze gegevens zijn verkregen, te bevestigen en te registreren.
83. Het EDPB merkt echter op dat in artikel 18 van de CBP-regels³⁵ is bepaald dat de registratieverplichtingen van OPIB's maximaal drie jaar gelden voor gevallen die buiten de in artikel 16 van de CBP-regels beschreven specifieke registratiemethoden vallen (met behulp van een schriftelijk document, elektromagnetische registratie of een microfilm). De Europese Commissie heeft dit ook vermeld in overweging 71 van haar ontwerpadequaateitsbesluit: "*Zoals in artikel 18 van de CBP-regels bepaald, moeten deze geregistreerde gegevens worden bewaard voor een periode van één tot drie jaar, afhankelijk van de omstandigheden*".
84. Zelfs indien, zoals de Europese Commissie in voetnoot 14 van haar ontwerpadequaateitsbesluit stelt, het OPIB's niet verboden is om informatie over de oorsprong van de gegevens langer dan drie jaar te bewaren teneinde aan hun verplichtingen uit hoofde van Aanvullende Regel (2) te kunnen voldoen, is dat noch in de Japanse wetgeving, noch in de aanvullende regels duidelijk weerspiegeld. Het EDPB is van mening dat er een risico bestaat dat OPIB's in feite zullen voldoen aan artikel 18 van de CBP-regels, zelfs wanneer zij gegevens uit de EU verwerken. Dat komt vooral omdat er momenteel, naar het inzicht van het EDPB en op basis van de beschikbare documenten, geen bepaling is die OPIB's ertoe verplicht de aanvullende regels na te leven. Dat zou ertoe leiden dat vanuit de EU doorgegeven gegevens niet langer worden beschermd door de bijkomende bescherming die in de aanvullende regels is opgenomen.
85. **Het EDPB verzoekt de Europese Commissie om de effectieve bescherming van persoonsgegevens die op basis van het ontwerpadequaateitsbesluit vanuit de EU naar Japan zijn doorgegeven gedurende**

³⁴ Bijlage III bij dit advies.

³⁵ Handhavingsregels voor de wet op de bescherming van persoonsgegevens (CBP-regels), in werking getreden op 30 mei 2017, artikel 16.

de gehele levenscyclus ervan nauwlettend te monitoren, ook al is in de Japanse wetgeving bepaald dat informatie over de oorsprong van de gegevens maximaal drie jaar moet worden bewaard.

3.1.2 Gronden voor een rechtmatige en behoorlijke verwerking voor gerechtvaardigde doeleinden

86. Volgens het adequaatheidsreferentiedocument moeten gegevens overeenkomstig de AVG op een rechtmatige, billijke en gerechtvaardigde wijze worden verwerkt³⁶. De rechtsgrond op basis waarvan persoonsgegevens op een rechtmatige, billijke en gerechtvaardigde wijze mogen worden verwerkt, moet op voldoende duidelijke wijze worden vastgesteld. In het Europese kader worden verschillende gerechtvaardigde gronden erkend, waaronder bepalingen in nationale wetgeving, de toestemming van de betrokkene, de uitvoering van een overeenkomst of een gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde dat niet zwaarder weegt dan de belangen van de betrokkene.
87. Overeenkomstig de WBP speelt toestemming een centrale rol in het Japanse rechtstelsel voor gegevensbescherming. Toestemming is de centrale rechtsgrond voor de verwerking van persoonsgegevens in Japan en tevens een van de belangrijkste rechtsgronden voor de doorgifte van persoonsgegevens vanuit Japan naar een derde land. Daarnaast is toestemming vereist voor een wijziging van het doel van de verwerking.
88. Volgens Aanvullende Regel (3) is de rechtsgrond voor de verwerking van persoonsgegevens die vanuit de EU naar Japan zijn doorgegeven de rechtsgrond op basis waarvan de gegevens naar Japan zijn doorgegeven. Indien de OPIB deze gegevens voor een ander doel verder wil verwerken, moet hij vooraf de toestemming van de betrokkene verkrijgen.
89. Het EDPB is van mening dat de kwaliteit van de toestemming, met name vanwege de centrale rol ervan in het Japanse rechtskader, moet voldoen aan de fundamentele vereisten van het begrip toestemming, d.w.z. volgens het EU-recht, een *"vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene [...] hem betreffende verwerking van persoonsgegevens aanvaardt"*. De betrokkene kan deze toestemming intrekken als een essentiële waarborg om te verzekeren dat er op elk moment sprake is van vrije wil³⁷. Het recht op intrekking, als verplicht element van toestemming, lijkt in het Japanse rechtskader te ontbreken. Volgens de richtsnoeren van de CBP³⁸ is de intrekking immers slechts "wenselijk" en afhankelijk van "de kenmerken, de omvang en de status van de bedrijfsactiviteiten".

3.1.3 Het transparantiebeginsel

90. Krachtens artikel 5 van de AVG is transparantie een fundamenteel beginsel van het EU-systeem voor gegevensbescherming³⁹. In het adequaatheidsreferentiedocument wordt "transparantie" uitdrukkelijk genoemd als een van de inhoudelijke beginselen waarmee rekening moet worden gehouden bij de beoordeling of het door een derde land geboden beschermingsniveau in wezen gelijkwaardig is. Het

³⁶ WP254, blz. 4.

³⁷ Artikel 4, lid 11, van de AVG. Zie voor meer informatie ook de relevante richtsnoeren van het EDPB inzake toestemming, WP259, 10 april 2018.

³⁸ Data Protection Legal and Technical Research and Analysis Consortium (DPC), An assessment of the level of protection of personal data provided under Japanese law, blz. 46: "Voorts is het vanuit het oogpunt van de bescherming van de rechten en belangen van een betrokkene, zoals een consument, wenselijk om, indien een betrokkene om de bewaarde persoonsgegevens heeft verzocht, zodanig verder in te gaan op zijn verzoek dat de verzending van direct mail wordt stopgezet enz. of dat het gebruik van zijn persoonsgegevens vrijwillig wordt beëindigd enz. rekening houdend met de kenmerken, de omvang en de status van de bedrijfsactiviteiten".

³⁹ WP254, hoofdstuk 3, punt 7, blz. 5; zie ook overweging 39 van de AVG.

transparantie- en billijkheidsbeginsel is erop gericht te waarborgen dat de betrokkene controle heeft over zijn gegevens, wat vereist dat als vuistregel proactief informatie aan de betrokkene moet worden verstrekt. In het geval van het privacyshield heeft de Groep gegevensbescherming artikel 29⁴⁰ in haar advies 1/2016 verwezen naar bijlage II, II 1 b van de overeenkomst betreffende het privacyshield (kennisgeving aan de betrokkene) en verklaard dat, indien de gegevens niet rechtstreeks worden verzameld, een organisatie de betrokkene in kennis moet stellen "op het moment dat de gegevens door de privacyshieldorganisatie worden geregistreerd" (punt 2.2.1.a). Een aanvullend criterium is dat het privacybeleid publiek toegankelijk moet zijn (zie punt 2.2.1.b). Daarom werd het reeds in Richtlijn 95/46/EG noodzakelijk geacht de betrokkene rechtstreeks te informeren.

91. Een eerste punt van zorg betreft de wijze van informatieverstrekking aan de betrokkene overeenkomstig de WBP. Volgens artikel 27, lid 1, van de WBP is een OPIB verplicht de in artikel 27, lid 1, van de WBP beschreven informatie te verstrekken door deze "in een staat te brengen waarin een betrokkene ze kan begrijpen". Uit deze formulering blijkt echter niet duidelijk in hoeverre de OPIB positieve maatregelen moet nemen om de betrokkene daadwerkelijk te informeren.
92. **Het EDPB verzoekt de Commissie om de betekenis van "kan begrijpen" te verduidelijken en om te verduidelijken of de WBP als vuistregel voorziet in de verplichting om betrokkenen daadwerkelijk te informeren.**
93. Bovendien kunnen er volgens het adequaatheidsreferentiedocument beperkingen bestaan op de informatie die aan de betrokkene moet worden verstrekt, vergelijkbaar met artikel 23 van de AVG. In dezelfde geest voorziet artikel 14, lid 5, van de AVG in een uitzondering op het recht om te worden geïnformeerd wanneer de informatie de verwerking waarschijnlijk onmogelijk maakt of ernstig belemmert. Maar zelfs in dat geval moet de verwerkingsverantwoordelijke een of andere informatie verstrekken, bijvoorbeeld door "gegeneraliseerde" informatie openbaar te maken. Wanneer het risico ophoudt te bestaan, moet de betrokkene daarvan in kennis worden gesteld⁴¹. Deze aspecten zijn belangrijk om het fundamentele billijkheidsbeginsel te waarborgen.
94. Volgens artikel 23 van de WBP moet een OPIB de betrokkene in het algemeen vooraf informeren over de doorgifte van zijn gegevens aan een derde, hetzij impliciet bij het verkrijgen van zijn toestemming, hetzij expliciet door middel van een opt-outkennisgeving. Het EDPB heeft begrepen dat er geen kennisgeving aan de betrokkene is waarin hij wordt geïnformeerd over het feit dat zijn gegevens geen bewaarde persoonsgegevens zijn overeenkomstig de WBP omdat ze onder de uitzonderingen van artikel 4 van het Regeringsdecreet vallen. Bijgevolg zal de betrokkene zijn rechten niet ten volle kunnen genieten. Ook in de gevallen van artikel 18, lid 4, van de WBP worden de betrokkenen niet geïnformeerd.
95. **Het EDPB erkent dat de rechten kunnen worden beperkt voor legitieme doelstellingen die de OPIB en overheidsinstanties nastreven. Tegelijkertijd is het EDPB van mening dat er ten minste vooraf algemene informatie moet worden verstrekt over de mogelijkheid dat de rechten worden beperkt voor de in de wet genoemde doelstellingen en dat de betrokkene in kennis moet worden gesteld wanneer de risico's waarvoor de informatie wordt beperkt ophouden te bestaan.**

⁴⁰ Deze Groep was opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Zij was een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en privacy. De taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG. De WP29 is inmiddels het EDPB geworden.

⁴¹ Tele2, gevoegde zaken C 203/15 en C 698/15, arrest van het Hof van 21 december 2016, overweging 121 en Digital Rights Ireland, gevoegde zaken C-293/12 en C-594/12, arrest van het Hof van 8 april 2014, overwegingen 54 tot 62.

96. Tot slot worden hieronder nog andere aspecten van transparantie verder uitgewerkt. Deze hebben betrekking op de risico's die verbonden zijn aan de doorgifte naar een derde land⁴² en de informatie over de methode van verwerking in het kader van geautomatiseerde besluitvorming, met inbegrip van profilering.⁴³

3.1.4 Beperkingen op verdere doorgifte

97. Het EDPB verwelkomt de inspanningen van de Japanse autoriteiten en de Europese Commissie om het niveau van bescherming bij verdere doorgifte te verhogen in Aanvullende Regel (4), waarin wordt uitgesloten dat vanuit de EU doorgegeven persoonsgegevens verder worden doorgegeven naar een derde land op basis van de grensoverschrijdende privacyregels van de economische samenwerking Azië-Stille Oceaan (APEC). Daarnaast erkent het EDPB dat de Europese Commissie zich in de overwegingen 177 en 184 van haar nieuwe ontwerp van het adequaatheidsbesluit ertoe heeft verbonden het adequaatheidsbesluit op te schorten wanneer bij verdere doorgifte de bescherming niet langer is gewaarborgd. Het EDPB wil echter twee punten aan de orde stellen met betrekking tot deze doorgiften van persoonsgegevens uit de EU vanuit Japan naar derde landen.
98. **Het gebruik, in het Japanse rechtsstelsel, van toestemming als basis voor de doorgifte van gegevens vanuit Japan naar een derde land geeft aanleiding tot bezorgdheid, aangezien het EDPB van mening is dat de informatie die vóór het verkrijgen van toestemming aan de betrokkene uit de EU wordt verstrekt te beperkt lijkt te zijn.**
99. In artikel 24 van de WBP is bepaald dat het verboden is persoonsgegevens aan een derde buiten het grondgebied van Japan door te geven zonder voorafgaande toestemming van de betrokkene. In Aanvullende Regel (4) is bepaald dat een betrokkene uit de EU informatie over de omstandigheden van de doorgifte moet krijgen die hij nodig heeft om een besluit over zijn toestemming te kunnen nemen.
100. De Europese Commissie concludeert in haar ontwerpadequaatheidsbesluit dat Aanvullende Regel (4) een bijzondere goed geïnformeerde toestemming van de betrokkene uit de EU garandeert⁴⁴, aangezien hij op de hoogte zal worden gesteld van het feit dat de gegevens naar het buitenland zullen worden doorgegeven en van het specifieke land van bestemming. Dat zou de betrokkene in staat stellen het aan de doorgifte verbonden privacyrisico te beoordelen.
101. Op grond van het transparantiebeginsel in het adequaatheidsreferentiedocument moet bij het informeren van betrokkenen een zekere mate van billijkheid worden gewaarborgd. In de context van verdere doorgiften op basis van toestemming is het EDPB van mening dat om een dergelijke adequate mate van billijkheid te waarborgen de betrokkenen uitdrukkelijk moeten worden geïnformeerd over de mogelijke risico's van die doorgiften als gevolg van het ontbreken van adequate bescherming in het derde land en het ontbreken van passende waarborgen vóór de toestemming. Een dergelijke kennisgeving moet bijvoorbeeld informatie bevatten over het feit dat er in het derde land mogelijk geen toezichthoudende autoriteit is en/of geen beginselen voor gegevensverwerking en/of rechten van de betrokkene zijn vastgelegd⁴⁵. Voor het EDPB is de verstrekking van deze informatie van

⁴² Zie punt 2.1.4.

⁴³ Zie punt 2.1.6.

⁴⁴ Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, overweging 76.

⁴⁵ EDPB-richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 25 mei 2018, blz. 8.

essentieel belang om de betrokkene in staat te stellen toestemming te geven met volledige kennis van deze specifieke feiten van de doorgifte⁴⁶.

102. Geïnformeerde toestemming is ook belangrijk in verband met sectorale uitsluitingen. Het adequaatheidsbesluit heeft geen betrekking op bepaalde vormen van verwerking van persoonsgegevens voor academische doeleinden door bepaalde organen zoals universiteiten. De bezorgdheid van het EDPB heeft hier betrekking op het specifieke scenario waarin gegevens die in het kader van het adequaatheidsbesluit vanuit de EU worden doorgegeven – bijvoorbeeld de persoonsgegevens van Erasmus-studenten in Japan – vervolgens met toestemming van de betrokkene worden gebruikt voor een ander doel dat buiten het toepassingsgebied van het adequaatheidsbesluit valt (bv. onderzoeksdoeleinden), en derhalve niet langer onder de aanvullende bescherming van de aanvullende regels vallen.
103. De Europese Commissie stelt in overweging 38 van haar ontwerpadequaatheidsbesluit dat een dergelijk scenario onder verdere doorgifte valt en dat, wanneer dat gebeurt, de OPIB de betrokkene alle nodige informatie moet verstrekken alvorens zijn toestemming te verkrijgen, met inbegrip van het feit dat de persoonsgegevens niet onder de bescherming van de WBP-regels vallen.
104. Aanvullende Regel (4) vereist slechts dat de OPIB de toestemming van de betrokkene verkrijgt nadat de betrokkene informatie over de omstandigheden van de doorgifte heeft ontvangen die hij nodig heeft om een beslissing over zijn toestemming te kunnen nemen.
105. **Het EDPB verzoekt de Europese Commissie ervoor te zorgen dat de aan de betrokkenen te verstrekken informatie "over de omstandigheden van de doorgifte" informatie omvat over de mogelijke risico's van doorgifte als gevolg van het ontbreken van adequate bescherming in het derde land en het ontbreken van passende waarborgen of, in het geval van sectorale uitsluitingen, het ontbreken van bescherming van de aanvullende regels en van de WBP.**
106. **Persoonsgegevens kunnen verder worden doorgegeven naar derde landen die het voorwerp van een eventueel later Japans adequaatheidsbesluit worden.**
107. Onverminderd de afwijkingen die zijn uiteengezet in artikel 23, lid 1, van de WBP kunnen gegevens die aanvankelijk vanuit de EU naar Japan zijn doorgegeven, in twee gevallen zonder toestemming vanuit Japan naar een derde land worden doorgegeven:
 - Indien de OPIB en de ontvanger in het derde land samen maatregelen hebben genomen die een beschermingsniveau bieden dat gelijkwaardig is aan het beschermingsniveau dat wordt geboden door de WBP gelezen in combinatie met de aanvullende regels, door middel van een contract, andere vormen van bindende overeenkomsten of bindende overeenkomsten binnen een ondernemingsgroep⁴⁷.
 - Indien de CBP het derde land overeenkomstig artikel 24 van de WBP en artikel 11 van de CBP-regels⁴⁸ heeft erkend als een land dat een beschermingsniveau biedt dat gelijkwaardig is aan het in Japan gewaarborgde beschermingsniveau.

⁴⁶ EDPB-richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 25 mei 2018, blz. 7.

⁴⁷ Aanvullende Regel (4) (ii).

⁴⁸ Handhavingsregels voor de wet op de bescherming van persoonsgegevens, 30 mei 2017. De Europese Commissie heeft het EDPB een Engelse vertaling van het nieuwe artikel 11 verstrekt, maar dat artikel is nog niet gepubliceerd.

108. Het EDPB beoordeelt artikel 24 van de WBP als de meer specifieke regel, die een afwijking van de algemene regel op grond van artikel 23 van de WBP bevat. Daarom is het EDPB het niet eens met de beoordeling van de Europese Commissie in de nieuwe laatste zin van overweging 78 van het ontwerpadequaateitsbesluit, waarin staat dat zelfs in die gevallen de doorgifte aan de derde onderworpen blijft aan de verplichting om toestemming te verkrijgen overeenkomstig artikel 23, lid 1, van de WBP.
109. Overeenkomstig artikel 11, lid 1, van de CBP-regels vereist een adequaatheidsbesluit van de CBP inhoudelijke normen die gelijkwaardig zijn aan de WBP waarvan de toepassing in het derde land is gewaarborgd en waarop effectief toezicht wordt uitgeoefend door een onafhankelijke handhavingsinstantie. Bovendien kan de CBP de nodige voorwaarden opleggen om de rechten en belangen van betrokkenen in Japan te beschermen, overeenkomstig artikel 11, lid 2, van de CBP-regels.
110. In Aanvullende Regel (4) is bepaald dat persoonsgegevens uit de EU zonder verdere beperkingen kunnen worden doorgegeven naar een derde land dat het voorwerp is van een Japans adequaatheidsbesluit. In artikel 44 van de AVG is echter bepaald dat elke doorgifte van persoonsgegevens naar een derde land moet voldoen aan de voorwaarden van hoofdstuk V van de AVG, met inbegrip van verdere doorgiften vanuit het derde land naar een ander derde land. Het niveau van bescherming van natuurlijke personen wier gegevens worden doorgegeven mag niet door de verdere doorgifte worden ondermijnd⁴⁹. Hoewel deze interpretatie in beginsel ook door de Europese Commissie in haar ontwerpadequaateitsbesluit wordt gedeeld⁵⁰, lijkt zij niet volledig te worden gevolgd. De Europese Commissie heeft onderhandeld over het verbod op de doorgifte van gegevens uit de EU naar een derde land op basis van de grensoverschrijdende privacyregels van de economische samenwerking Azië-Stille Oceaan (APEC). In het licht van het in 2014 in het kader van de EU-richtlijn ontwikkelde instrument voor vergelijkingen tussen bindende bedrijfsvoorschriften en grensoverschrijdende privacyregels, dat de vereisten van beide systemen, hun overeenkomsten en hun verschillen laat zien (advies 02/2014 van de WP29), maakt het EDPB zich zorgen over het gebruik van grensoverschrijdende privacyregels als instrument voor de verdere doorgifte van persoonsgegevens uit de EU naar landen buiten Japan.
111. Daarentegen lijkt de Europese Commissie akkoord te gaan met de verdere doorgifte van persoonsgegevens die op basis van een Japans adequaatheidsbesluit vanuit de EU naar Japan zijn doorgegeven, zonder dat de CBP de mogelijkheid heeft om indien nodig de aanvullende regels op te leggen als voorwaarden voor de bescherming van de rechten en belangen van natuurlijke personen uit de EU. Het EDPB leidt uit artikel 44 van de AVG af dat de in de aanvullende regels voorziene betere bescherming van gegevens die vanuit de EU naar Japan zijn overgedragen, altijd moet worden geboden wanneer vanuit de EU naar Japan doorgegeven persoonsgegevens verder worden doorgegeven naar een derde land indien het gegevensbeschermingskader in dat land niet wordt erkend als in wezen gelijkwaardig aan de AVG.
112. **Daarom verzoekt het EDPB de Europese Commissie om haar controlerende rol te vervullen en ervoor te zorgen dat het niveau van bescherming van gegevens uit de EU wordt gehandhaafd of om de opschorting van dit adequaatheidsbesluit te overwegen indien vanuit de EU naar Japan doorgegeven persoonsgegevens verder worden doorgegeven naar derde landen die het voorwerp van een**

⁴⁹ WP254, blz. 5.

⁵⁰ Uitvoeringsbesluit van de Commissie van XXXX, overeenkomstig Verordening 2016/679 van het Europees Parlement en de Raad betreffende de adequate bescherming van persoonsgegevens door Japan, zoals op 13 november 2018 aan het EDPB toegezonden, overweging 75.

eventueel later Japans adequaatheidsbesluit worden, indien die derde landen niet het voorwerp zijn geweest van een eerdere beoordeling of vaststelling van adequaatheid door de EU.

3.1.5 Direct marketing

113. Volgens Aanvullende Regel (3) is het een OPIB verboden de gegevens met het oog op direct marketing te verwerken indien de gegevens voor een ander doel vanuit de Europese Unie zijn doorgegeven en de betrokkene uit de EU geen toestemming heeft gegeven voor de wijziging van het gebruiksdoel.
114. Volgens het adequaatheidsreferentiedocument moet de betrokkene, indien gegevens met het oog op direct marketing worden verwerkt, te allen tijde zonder kosten bezwaar kunnen maken tegen de verwerking van zijn gegevens voor dergelijke doeleinden. Volgens artikel 16 van de WBP mag een OPIB alleen persoonsgegevens verwerken als de betrokkene daar toestemming voor heeft gegeven. De intrekking van de toestemming zou hetzelfde resultaat kunnen opleveren als het geprivilegieerde recht om bezwaar te maken tegen direct marketing.
115. Het Japanse kader voor gegevensbescherming voorziet niet in een geprivilegieerd recht van bezwaar en zoals hierboven in het deel over toestemming uiteengezet, is de intrekking van de toestemming overeenkomstig de richtsnoeren van de CBP slechts wenselijk en voorwaardelijk en kan ze daarom niet worden gelijkgesteld met een recht om te allen tijde bezwaar te maken, zoals gevraagd in het adequaatheidsreferentiedocument. **Het EDPB verzoekt de Europese Commissie om garanties te geven over het recht op intrekking van de toestemming en om toezicht te houden op gevallen van direct marketing.**

3.1.6 Geautomatiseerde besluitvorming en profilering

116. Volgens het adequaatheidsreferentiedocument kunnen besluiten die uitsluitend op geautomatiseerde verwerking (geautomatiseerde individuele besluitvorming) zijn gebaseerd, met inbegrip van profilering, en die rechtsgevolgen of aanzienlijke gevolgen hebben voor de betrokkene, alleen plaatsvinden onder bepaalde voorwaarden die in het rechtskader van het derde land zijn vastgesteld. Telkens wanneer onder de bovengenoemde omstandigheden geautomatiseerde besluitvorming en profilering wordt uitgevoerd, moet daar een rechtsgrond voor zijn.
117. In het Europese kader omvatten de voorwaarden voor geautomatiseerde besluitvorming bijvoorbeeld de noodzaak om de uitdrukkelijke toestemming⁵¹ van de betrokkene te verkrijgen of de noodzaak van een dergelijk besluit voor het sluiten van een contract. Indien het besluit niet voldoet aan de voorwaarden die in het rechtskader van het derde land zijn vastgelegd, moet de betrokkene het recht hebben om niet aan het besluit te worden onderworpen. Voorts moet het recht van het derde land in elk geval de nodige waarborgen bieden, waaronder het recht om te worden geïnformeerd over de specifieke redenen die aan het besluit ten grondslag liggen en over de procedure om onjuiste of onvolledige informatie te corrigeren en het besluit aan te vechten indien het op basis van onjuiste feiten is genomen.
118. Het besluit van de Commissie heeft alleen betrekking op de banksector, waar sectorale regels⁵² betreffende geautomatiseerde besluiten van toepassing zouden zijn. In de in overweging 93 van het ontwerpadequaatheidsbesluit genoemde uitvoerige richtsnoeren voor toezicht op grote banken is

⁵¹ Voor kritische opmerkingen over het begrip "toestemming" in het Japanse rechtskader voor gegevensbescherming wordt verwezen naar: 2.1. Algemeen en [2.2.8. Direct marketing](#).

⁵² Deze sectorale regels zijn niet aan het EDPB verstrekt.

aangegeven dat de betrokkene specifieke uitleg moet krijgen over de redenen voor de afwijzing van een verzoek om een leningovereenkomst te sluiten.

119. In de argumenten van de Europese Commissie met betrekking tot het ontwerpadequaateitsbesluit (overweging 94), volgens welke het onwaarschijnlijk is dat het ontbreken van specifieke regels voor geautomatiseerde besluitvorming in de WBP van invloed zal zijn op het beschermingsniveau, lijkt (bijvoorbeeld) geen rekening te zijn gehouden met het geval waarin vanuit de EU doorgegeven persoonsgegevens vervolgens door een andere Japanse verwerkingsverantwoordelijke dan de oorspronkelijke Japanse gegevensimporteur worden verwerkt.
120. Het lijkt er dus op dat in Japan geen algemene sectorale regels voor geautomatiseerde besluitvorming en profilering van toepassing zijn.
121. **Het EDPB verzoekt de Europese Commissie om toezicht te houden op zaken die verband houden met geautomatiseerde besluitvorming en profilering.**

3.2 Procedurele en handhavingsmechanismen

122. Op basis van de in het adequaatheidsreferentiedocument vastgestelde criteria heeft het EDPB een analyse gemaakt van de volgende aspecten van het Japanse gegevensbeschermings- en rechtskader die onder het ontwerpadequaateitsbesluit vallen: het bestaan en de effectieve werking van een onafhankelijke toezichthoudende autoriteit; het bestaan van een systeem dat een goede naleving waarborgt en een systeem van toegang tot passende verhaalsmogelijkheden die natuurlijke personen uit de EU de middelen verschaffen om hun rechten uit te oefenen en verhaal te halen zonder de hinderlijke belemmeringen die zich voordoen bij verhaal via een bestuursorgaan en bij gerechtelijk verhaal.
123. Voortbouwend op de parameters die door het HvJ in de zaak-Schrems⁵³ zijn vastgesteld en die welke in overweging 104 en artikel 45 van de AVG zijn uiteengezet, is het EDPB van oordeel dat, hoewel er in Japan een systeem bestaat dat in overeenstemming is met het Europese systeem, dit systeem in de praktijk soms moeilijk toegankelijk is voor natuurlijke personen uit de EU wier gegevens op grond van dit adequaatheidsbesluit zullen worden doorgegeven wegens het bestaan van taalbarrières en institutionele belemmeringen.
124. In de onderstaande delen worden de bovengenoemde aspecten van het Japanse kader onderzocht alvorens enkele aanbevelingen voor de Commissie te belichten.

3.2.1 Bevoegde onafhankelijke toezichthoudende autoriteit

125. De CBP is op 1 januari 2016 opgericht naar aanleiding van de wijzigingen van de WBP van 2015, ter vervanging van zijn voorganger – de Commissie voor de bescherming van specifieke persoonsgegevens (opgericht in 2013 krachtens de "wet mijn nummer"). De CBP is nog een jonge organisatie, maar heeft sinds haar oprichting al aanzienlijke inspanningen geleverd om de nodige infrastructuur op te bouwen teneinde de uitvoering van de gewijzigde WBP mogelijk te maken. Opvallend zijn onder meer de vaststelling van de CBP-regels, de richtsnoeren van de CBP om OPIB's te helpen bij de interpretatie van de WBP, de publicatie van een vraag-en antwoorddocument van de CBP⁵⁴, de oprichting van een hulplijn om ondernemers en burgers te adviseren over bepalingen inzake gegevensbescherming en de oprichting van een bemiddelingsdienst voor de behandeling van klachten.
126. De oprichting en werking van de CBP is geregeld in hoofdstuk V van de WBP. De CBP valt onder de bevoegdheid van de eerste minister, maar in artikel 62 van de WBP is bepaald dat de CBP haar functie

⁵³ Zaak 362/14 (2015) Maximilian Schrems/Data Protection Commissioner (punten 73 en 74).

⁵⁴ Dit document is door de Europese Commissie niet in het Engels aan het EDPB verstrekt.

onafhankelijk moet uitoefenen. Het EDPB verwelkomt de verduidelijking door de Europese Commissie in haar op 13 november 2018 verspreide gewijzigde ontwerp van het adequaatheidsbesluit, waarin nader is beschreven in welke mate de CBP vrij is van interne en externe invloeden.

3.2.2 Het systeem voor gegevensbescherming moet een goede naleving waarborgen

127. In het ontwerpadequaathheidsbesluit worden de bevoegdheden waarover de CBP krachtens de artikelen 40, 41 en 42 van de WBP beschikt uitgebreid onderzocht om het toezicht op en de handhaving van de wetgeving te waarborgen. Artikel 40 machtigt de CBP om OPIB's te verzoeken verslagen en documenten met betrekking tot verwerkingsactiviteiten in te dienen en om inspecties ter plaatse uit te voeren. Op grond van artikel 42 heeft de CBP de bevoegdheid om – wanneer zij erkent dat het noodzakelijk is om rechten van natuurlijke personen te beschermen of wanneer zij een inbreuk op de bepalingen van de wet vaststelt – aanbevelingen te doen aan OPIB's en, als deze niet worden opgevolgd, hen te gelasten de inbreuk te staken of de nodige maatregelen te nemen om de inbreuk ongedaan te maken.
128. In oktober 2018 heeft de CBP een van de eerste acties op grond van artikel 41 van de gewijzigde WBP ondernomen en een OPIB "richtsnoeren" gegeven. Hierbij werd de onderneming geadviseerd om haar beveiligingsmaatregelen aan te scherpen, effectief toezicht te houden op aanbieders van applicaties, de gebruikers in heldere en gemakkelijk te begrijpen bewoordingen uit te leggen hoe hun persoonsgegevens worden gebruikt, vooraf toestemming te verkrijgen wanneer de informatie met een derde wordt gedeeld en op correcte wijze gevolg te geven aan het verzoek van gebruikers om hun informatie te wissen. In de aan het EDPB verstrekte antwoorden⁵⁵ hebben de functionarissen van de CBP meegedeeld dat de onderneming heeft bekendgemaakt dat zij zal meewerken en dat de functionarissen van de CBP, ingeval die medewerking er niet komt, de onderneming een "aanbeveling" als bedoeld in artikel 42, lid 1, van de WBP zullen doen.
129. Het onderzoek van de CBP naar de bovengenoemde OPIB is een zeer positieve indicatie van de inspanningen van de Japanse toezichthoudende autoriteit om te zorgen voor een goede naleving in het land.
130. Hoewel er verbeteringen zijn aangebracht in het kader dat vóór de wijzigingen van 2015 bestond, merkt het EDPB op dat de CBP minder bevoegdheden heeft dan die welke de Europese gegevensbeschermingsautoriteiten op grond van de AVG hebben, met name op het gebied van **handhaving**. De administratieve geldboeten⁵⁶ zijn bijvoorbeeld vrij mild. In overweging 108 van het besluit van de Europese Commissie wordt benadrukt dat in gevallen van niet-naleving of bepaalde schendingen van de WBP strafrechtelijke sancties zijn bepaald en dat de voorzitter van de CBP zaken aan het Openbaar Ministerie kan overmaken. In het besluit van de Europese Commissie is echter geen rekening gehouden met het feit dat openbare vervolging in Japan discretionair is en soms onderworpen is aan langdurige evaluatieprocedures⁵⁷. Bovendien kan de gevangenisstraf (met of zonder dwangarbeid) die aan schendingen van de WBP is verbonden overeenkomstig de bepalingen

⁵⁵ Bijlage III.

⁵⁶ Deze zijn bepaald in hoofdstuk VII van de WBP. De maximale boete is bepaald in artikel 83 (verstrekken of heimelijk gebruiken van een database met persoonsgegevens voor eigen illegaal gewin of voor illegaal gewin van een derde) en staat gelijk aan hetzij een jaar gevangenisstraf met dwangarbeid, hetzij een boete van maximaal 500 000 yen (ongeveer 3 900 euro). Volgens de toelichting van de Commissie zijn de boetes cumulatief per inbreuk. Hoewel dat het geval kan zijn, merkt het EDPB op dat zelfs indien cumulatieve boetes worden toegepast, het totale bedrag waarschijnlijk nog steeds veel lager is dan bij toepassing van de Europese normen.

⁵⁷ Oda H., *Japanese Law*, Oxford University Press (III edition), 2009: 439 – 440.

van hoofdstuk VII moeilijk uitvoerbaar zijn omdat deze gericht is tegen natuurlijke personen en in ieder geval niet tegen een OPIB die als rechtspersoon zijn verantwoordingsverplichtingen niet nakomt.

131. **In het licht van het bovenstaande verzoekt het EDPB de Europese Commissie nauwlettend toe te zien op de doeltreffendheid van sancties en relevante rechtsmiddelen in het Japanse gegevensbeschermingsstelsel.**

3.2.3 Het gegevensbeschermingsstelsel moet individuele betrokkenen ondersteunen en helpen bij de uitoefening van hun rechten en passende verhaalsmogelijkheden.

132. De CBP biedt uitgebreide informatie en richtsnoeren op haar website om OPIB's bewust te maken van hun verplichtingen en verantwoordelijkheden krachtens het gegevensbeschermingskader, alsook een hulplijn voor het verstrekken van informatie en ondersteuning aan Japanse burgers over hun rechten als natuurlijke personen op grond van de WBP. De website heeft ook een deel, de "Kinderkamer" genoemd, dat expliciet op kinderen en jongeren is gericht. Het EDPB merkt op dat deze informatie – samen met de hulplijnondersteuning, richtsnoeren en vraag-en-antwoorddocumentatie – beschikbaar is in het Japans⁵⁸. Het EDPB is er dan ook sterk van overtuigd dat het nuttig zou zijn als de CBP op de Engelse versie van haar website een speciale pagina zou aanbieden om natuurlijke personen uit de EU wier gegevens op grond van het adequaatheidsbesluit van de Europese Commissie naar Japan worden doorgegeven, informatie te verstrekken over hun rechten als natuurlijk persoon op grond van het Japanse gegevensbeschermingskader en op grond van de aanvullende regels.

133. Het EDPB verwelkomt de door de Europese Commissie verstrekte verduidelijking – in overweging 104 van het op 13 november 2018 verspreide gewijzigde ontwerpadequaatheidsbesluit – betreffende de bemiddelingsdienst die door de CBP wordt beheerd overeenkomstig artikel 61, onder ii), van de WBP. Het EDPB wil in dit verband echter drie punten aan de orde stellen. Ten eerste is de bemiddelingsdienst niet gepubliceerd op de Engelse versie van de website van de CBP. Ten tweede is de dienst alleen telefonisch te bereiken en wordt er alleen Japans gesproken. Ten slotte is bemiddeling slechts een faciliterend proces dat niet leidt tot een bindende overeenkomst tussen de partijen, wat gevolgen heeft voor de doeltreffendheid van de verhaalsmogelijkheden waarover betrokkenen beschikken⁵⁹.

134. Ten slotte merkt het EDPB op dat het ontwerpadequaatheidsbesluit de nadruk legt op de rechtsmiddelen die via civiel- en strafrechtelijke procedures beschikbaar zijn, maar niet het bestaan erkent van **institutionele belemmeringen bij rechtszaken** in Japan, zoals juridische kosten (deze worden gelijk verdeeld tussen eiser en verweerder, ongeacht welke partij de procedure wint⁶⁰), het tekort aan advocaten in het land⁶¹, het feit dat buitenlandse advocaten niet in een op het Japanse recht gebaseerde rechtszaak mogen pleiten en de bewijslastvereiste krachtens het recht inzake onrechtmatige daad. Het EDPB vreest dat deze factoren in de praktijk de toegang van natuurlijke personen tot de rechter kunnen belemmeren en hun recht om snel en zonder prohibitieve kosten rechtsmiddelen aan te wenden in gevaar kunnen brengen.

135. **In het licht van het bovenstaande vreest het EDPB dat natuurlijke personen uit de EU moeilijkheden kunnen ondervinden bij de toegang tot verhaal via een bestuursorgaan en gerechtelijk verhaal.**

⁵⁸<https://www.ppc.go.jp/en/contactus/piinquiry/>.

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

⁶⁰ Wagatsuma (2012), 'Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure' in Reimann (ed.), *Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11*, blz. 195 tot 200.

⁶¹ Volgens de recentste cijfers zijn er in Japan 38 980 advocaten (ongeveer 290 advocaten per 1 miljoen inwoners [Japanse orde van advocaten] (2017), *White Paper on Attorneys*: blz. 8 en 9.

Daarom zou het EDPB het verwelkomen als de Europese Commissie met de CBP de mogelijkheid zou bespreken om een onlinedienst op te zetten, ten minste in het Engels, die **gericht is op het ondersteunen en behandelen van klachten⁶² van natuurlijke personen uit de EU**. Daarnaast zou het EDPB graag zien dat de gegevensbeschermingsautoriteiten van de EU kunnen optreden als tussenpersoon voor klachten van betrokkenen uit de EU bij organisaties die in Japan actief zijn en bij de CBP.

4 OVER DE INZAGE VAN OVERHEIDSINSTANTIES IN NAAR JAPAN DOORGEGEVEN GEGEVENS

136. Het is de bedoeling van de Commissie om door middel van het adequaatheidsbesluit te erkennen dat "Japan een adequaat beschermingsniveau waarborgt voor persoonsgegevens die vanuit de Europese Unie worden doorgegeven aan ondernemers die persoonlijke informatie behandelen in Japan", zoals in artikel 1 van het ontwerpadequaatheidsbesluit vermeld. Overeenkomstig artikel 45, lid 2, van de AVG heeft de Commissie ook een analyse gemaakt van de beperkingen en waarborgen met betrekking tot de inzage van overheidsinstanties in persoonsgegevens. Dit hoofdstuk is gericht op de beoordeling van de inzage in persoonsgegevens door rechtshandavingsinstanties en door andere overheidsinstanties ten behoeve van de nationale veiligheid. De analyse van het EDPB is gebaseerd op het ontwerpadequaatheidsbesluit, bijlage II bij dat besluit, waarin de Japanse overheid een overzicht van het relevante rechtskader geeft, en de Japanse wetteksten, voor zover deze door de Commissie zijn verstrekt. Daarom heeft het EDPB in de specifieke context van deze beoordeling rekening gehouden met elementen betreffende de Japanse wetgeving die geen deel uitmaken van de bevindingen van de Europese Commissie maar die relevant zijn voor de beoordeling van de voorwaarden en waarborgen waaronder Japanse overheidsinstanties inzage hebben in persoonsgegevens die vanuit de Europese Unie zijn doorgegeven.

4.1 Inzage van rechtshandavingsinstanties in gegevens

4.1.1 Procedures voor inzage in gegevens in strafrechtelijke context

137. In het ontwerpadequaatheidsbesluit zijn drie manieren beschreven waarop rechtshandavingsinstanties volgens de Japanse wetgeving inzage kunnen krijgen in gegevens in Japan:

4.1.1.1 Verzoeken om inzage met een gerechtelijk bevel

138. In het ontwerpadequaatheidsbesluit staat dat overheidsinstanties in Japan, en met name strafrechtelijke handavingsinstanties, die in het kader van een strafrechtelijk onderzoek om inzage in elektronisch bewijsmateriaal verzoeken, altijd een gerechtelijk bevel nodig hebben, tenzij zij de procedure voor vrijwillige informatieverstrekking volgen – zie hieronder.

4.1.1.1.1 Vereiste van "voldoende reden", noodzaak en evenredigheid van de gerechtelijke bevelen

139. Het EDPB erkent dat volgens de Japanse grondwet elke verzameling van persoonsgegevens met toepassing van dwangmiddelen op een gerechtelijk bevel moet zijn gebaseerd. Meer in het bijzonder wordt in het ontwerpadequaatheidsbesluit aangegeven dat in alle gevallen van "huiszoeken en inbeslagnemingen" gerechtelijke bevelen moeten zijn uitgevaardigd op grond van "voldoende reden", waarvan naar het oordeel van het Hooggerechtshof alleen sprake is als de betrokken persoon

⁶² Vergelijkbaar met de in bijlage II van dit adequaatheidsbesluit bedoelde dienst voor klachten van EU-ingezetenen over de inzage in hun gegevens door Japanse overheidsinstanties.

(verdachte of beklagde) wordt geacht een strafbaar feit te hebben gepleegd en de huiszoeking en inbeslagneming noodzakelijk zijn voor het strafrechtelijke onderzoek. De Commissie verwijst hier naar het arrest van het Hoogerechtshof van 18 maart 1969, zaak N. 100 (1968(Shi)). Het EDPB herinnert eraan dat volgens de jurisprudentie van het HvJ⁶³ alleen een rechtbank, en niet bijvoorbeeld een aanklager, toestemming kan geven voor het verzamelen van met name verkeers- en locatiegegevens.

140. Ook in het licht van de jurisprudentie van het HvJ, volgens welke de inzage in gegevens onderworpen kan zijn aan het verkrijgen van een gerechtelijk bevel, zoals in de zaak-Tele2, betreft het EDPB het dat er geen aanvullende informatie is verstrekt om te beoordelen hoe de criteria voor de beoordeling van de noodzaak van een gerechtelijk bevel – ernst van het strafbare feit en de wijze waarop het is gepleegd; de waarde en het belang van het als bewijs in beslag genomen materiaal; de waarschijnlijkheid van achterhouding of vernietiging van in beslag genomen materiaal; de omvang van de nadelen van een inbeslagneming; andere daarmee samenhangende voorwaarden – en het uit de Grondwet voortkomende begrip "voldoende reden" in de praktijk worden toegepast. Daarom verzoekt het EDPB de Commissie om te monitoren of de uitvoering van gerechtelijke bevelen in de praktijk voldoet aan de door het HvJ vastgestelde criteria.

4.1.1.1.2 Soorten misdrijven waarvoor gerechtelijke bevelen kunnen worden uitgevaardigd

141. De procedure inzake het gerechtelijk bevel is alleen van toepassing wanneer een "onderzoek met toepassing van dwangmiddelen" wordt uitgevoerd. Deze gerechtelijke bevelen kunnen in principe alleen worden uitgevaardigd indien een wet is overtreden. In dat verband neemt het EDPB nota van de onlangs aangenomen "Wet inzake de bestraffing van georganiseerde misdaad en de controle op opbrengsten van misdrijven" van 15 juni 2017 in het kader van de toetreding van Japan tot het Verdrag van de Verenigde Naties tegen grensoverschrijdende georganiseerde misdaad (UNTOC)⁶⁴. Bij gebrek aan een Engelstalige versie van deze wetgeving en gezien de vereiste in de EU-wetgeving dat sommige gegevens alleen in het kader van een onderzoek, opsporing of vervolging van ernstige misdrijven worden verzameld⁶⁵, alsook gezien de bezorgdheid van verscheidene commentatoren, onder wie de speciale VN-rapporteur Joseph Cannataci⁶⁶, over het brede toepassingsgebied dat is gebaseerd op een definitie van "georganiseerde criminele groep" die naar verluidt vaag en te ruim is, kan het EDPB niet concluderen dat de inzage in elektronisch bewijsmateriaal krachtens de relevante Japanse wetgeving beperkt is tot de in EU-recht bepaalde drempels.
142. Ook moet worden opgemerkt dat voor sommige soorten strafbare feiten de prefecturale politie bevoegd is en dat zij haar specifieke politieverordeningen heeft. De interne regels die van toepassing zijn op de prefecturale politie waren niet beschikbaar voor het EDPB.
143. Volgens het ontwerpadequaateheidsbesluit valt het verzamelen van elektronische informatie in de context van strafrechtelijke handhaving onder de verantwoordelijkheid van de prefecturale politie.

4.1.1.2 Gerechtelijke aftapbevelen

144. In bijlage II bij het ontwerpadequaateheidsbesluit is aangegeven dat de wet inzake aftappen voor strafrechtelijk onderzoek voorziet in bijzonderheden voor het aftappen van communicatie. Deze wetgeving is pas zeer laat ingediend, waardoor een grondige analyse niet mogelijk was. Hoewel er binnen dit rechtskader veel waarborgen lijken te worden geboden, is het EDPB dus niet in staat om te beoordelen of de voorwaarden in deze wetgeving worden ondersteund door waarborgen die in wezen

⁶³ Zie de zaken 203/15 en C 293/12 en C 594/12 van het HvJ.

⁶⁴ Zie: <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>.

⁶⁵ Zie de gevoegde zaken C 293/12 en C 594/12 en zaak C 203/15.

⁶⁶ Speciaal VN-rapporteur voor het recht op privacy en Graham Greenleaf, juridisch onderzoeker aan de University of New South Wales (UNSW).

gelijkwaardig zijn aan die welke in de EU worden vereist door zowel het Handvest van de grondrechten van de Europese Unie zoals uitgelegd door het Hof van Justitie van de Europese Unie als het Europees Verdrag voor de rechten van de mens (EVRM) zoals uitgelegd door het Europees Hof voor de Rechten van de Mens (EHRM).

4.1.1.3 De procedure voor "vrijwillige informatieverstrekking" op basis van een inlichtingenblad

145. Deze vorm van medewerking zonder toepassing van dwangmiddelen stelt overheidsinstanties in staat om verwerkingsverantwoordelijken (met uitzondering van telecombedrijven) te vragen hen informatie te verstrekken waarover zij beschikken. De inwilliging van het verzoek kan niet worden afgedwongen. Het blijft onduidelijk welke instanties dit soort procedure kunnen gebruiken, maar ze lijkt zich te beperken tot instanties die misdrijven onderzoeken.

4.1.1.3.1 Voorwaarden voor de afgifte van "inlichtingenbladen"

146. Het EDPB erkent dat het Japanse Hooggerechtshof, onder verwijzing naar de grondwet, beperkingen heeft gesteld aan het gebruik van "vrijwillige informatieverstrekking"⁶⁷. Uit het ontwerpadequaatebesluit blijkt dat de bevoegde autoriteiten alleen door middel van de afgifte van een "inlichtingenblad" concreet om "vrijwillige informatieverstrekking" kunnen verzoeken. De verzending van dat "inlichtingenblad" zou alleen in het kader van een strafrechtelijk onderzoek toegestaan zijn, wat dus altijd een concreet vermoeden van een reeds gepleegd misdrijf vooronderstelt. Dergelijke onderzoeken worden over het algemeen door de prefecturale politie gevoerd. Hierbij gelden de beperkingen op grond van artikel 2, lid 2, van de politiewet, wat betekent dat het onderzoek relevant moet zijn voor de politieactiviteiten. Het EDPB wenst echter meer duidelijkheid over de concrete contouren van de criteria op grond waarvan een inlichtingenblad kan worden verstuurd (zoals jurisprudentie die de toepassing van deze criteria illustreert) en over het verband tussen de procedure voor vrijwillige informatieverstrekking en de inbeslagneming van gegevens op basis van een gerechtelijk bevel. Het lijkt er immers op dat zelfs indien gegevens niet via de procedure voor vrijwillige informatieverstrekking konden worden verkregen, deze nog steeds kunnen worden verkregen met een gerechtelijk bevel indien dat voor de onderzoeksautoriteiten onontbeerlijk is⁶⁸.

4.1.1.3.2 Beschikbare jurisprudentie over de beperkingen op het gebruik van de procedure voor vrijwillige informatieverstrekking

147. De in het ontwerpadequaatebesluit aangehaalde gevallen⁶⁹ ter illustratie van de beperkingen op het gebruik van de procedure voor vrijwillige informatieverstrekking hebben betrekking op gevallen waarin de beklagde rechtstreeks door de politie in een openbare ruimte is gefotografeerd of gefilmd en geven derhalve beperkte aanwijzingen voor situaties waarin de bevoegde autoriteiten een verwerkingsverantwoordelijke kunnen vragen om gegevens te verstrekken, met name met betrekking tot het in bijlage II genoemde criterium "geschiktheid van methoden", dat betrekking lijkt te hebben op de beoordeling van de vraag of een vrijwillig onderzoek "passend" of redelijk is om het doel van het onderzoek te bereiken. Hetzelfde kan worden gezegd over het algemene criterium "of het volgens sociaal aanvaarde conventies als redelijk kan worden beschouwd" om de wettigheid van vrijwillige onderzoeken te beoordelen. Bovendien heeft de nationale politie, zijnde de federale autoriteit die belast is met alle aangelegenheden betreffende de gerechtelijke politie, de prefecturale politie instructies gegeven over de "juiste werkwijze bij schriftelijke verzoeken om informatie in onderzoekszaken". Zo moet bijvoorbeeld de hoofdonderzoeker een interne goedkeuring krijgen van

⁶⁷ Zie bijlage II, bladzijde 8.

⁶⁸ Zie bijlage II, bladzijde 7.

⁶⁹ Zie bijlage II, blz. 8 – twee uitspraken van het Hooggerechtshof van 24 december 1969 (1965 (A) nr. 1187) en 15 april 2008 (2007 (A) nr. 839).

een hoge ambtenaar. Het EDPB heeft geen informatie over het al dan niet bindend zijn van deze instructies. Het EDPB stelt evenwel dat het gebruik van deze procedure evenredig of noodzakelijk moet zijn.

4.1.1.3.3 Rechten en verplichtingen van verwerkingsverantwoordelijken in de context van vrijwillige informatieverstrekking

148. Daarnaast is het aan de verwerkingsverantwoordelijken om in te stemmen met het verstrekken van gegevens (zij lijken echter niet verplicht te zijn om de toestemming van betrokkenen te vragen of om hen te informeren) voor zover deze verzoeken niet in strijd zijn met andere wettelijke verplichtingen (zoals geheimhoudingsverplichtingen). Het door de Commissie verstrekte verslag lijkt aan te geven dat verwerkingsverantwoordelijken na een hoge mate van inwilliging van deze verzoeken rekening zijn gaan houden met de bescherming van de gegevens van hun klanten en dus minder vaak op deze verzoeken zijn gaan antwoorden.
149. Het blijft ook onduidelijk of er voor verwerkingsverantwoordelijken een stimulans is om aan de verzoeken te voldoen (bijvoorbeeld of zij bij het inwilligen van een verzoek een voordeel hebben, worden vrijgesteld van vervolging enz.). Er wordt met name geen melding gemaakt van een beginsel zoals het "recht om niet tegen zichzelf te getuigen".
150. Het EDPB zou graag aanvullende informatie ontvangen, indien deze beschikbaar is, over het aantal en de soorten verzoeken, alsook over de antwoorden die door de verwerkingsverantwoordelijken zijn verstrekt. Bij gebrek aan jurisprudentie en cijfers verzoekt het EDPB de Commissie toe te zien op de efficiëntie en concrete toepassing van deze procedure in de praktijk.
151. Het ontbreekt het EDPB echter aan jurisprudentie en cijfers over deze procedure om deze elementen vast te stellen. Bijgevolg is het EDPB niet in staat een beoordeling te geven van de efficiëntie en concrete toepassing van deze procedure zonder verdere elementen met betrekking tot de praktijk.

4.1.1.4 Conclusie over procedures voor inzage in gegevens voor rechtshandavingsdoeleinden

152. Concluderend erkent het EDPB dat het beginsel volgens hetwelk de verplichting om bevoegde autoriteiten inzage te geven in persoonsgegevens alleen geldt indien die inzage noodzakelijk is en in verhouding staat tot het doel en, indien gebaseerd op een gerechtelijk bevel, in overeenstemming is met de belangrijkste essentiële waarborgen waarin het EU-recht en het EVRM voorzien. Naar aanleiding van bovenstaande bevindingen verzoekt het EDPB de Commissie om de reikwijdte van deze maatregelen, de reikwijdte van de procedure voor vrijwillige informatieverstrekking en de toepassing van dit beginsel door de prefecturale politie en door rechtbanken in de relevante jurisprudentie te monitoren, en ook om te monitoren of het Japanse rechtskader de essentiële waarborgen biedt die het HvJ heeft vastgesteld op basis van het Handvest en het EVRM op basis van het Verdrag.

4.1.2 Toezicht op strafrechtelijk gebied

153. Het ontwerpadequaateitsbesluit en bijlage II bevatten vier soorten toezicht op de politie, ministeries en overheidsinstanties.

4.1.2.1 Gerechtig toezicht

4.1.2.1.1 In gevallen waarin elektronische informatie met toepassing van dwangmiddelen (huiszoeking en inbeslagneming) wordt verzameld

154. Volgens het ontwerpadequaateitsbesluit moet de politie in alle gevallen waarin elektronische informatie met toepassing van dwangmiddelen (huiszoeking en inbeslagneming) wordt verzameld, vooraf een gerechtelijk bevel verkrijgen. Er is echter een uitzondering op die regel⁷⁰. Krachtens artikel

⁷⁰ Zie bijlage II.

220, lid 1, van het Wetboek van Strafvordering is het een openbaar aanklager, zijn assistent of een agent van de gerechtelijke politie bij het arresteren van een verdachte toegestaan elektronische informatie op de plaats van de arrestatie te doorzoeken of in beslag te nemen. In deze situatie bestaat de mogelijkheid dat die informatie door een rechter als bewijs wordt uitgesloten.

155. Het EDPB is zich ervan bewust dat soortgelijke uitzonderingen ook in het EU-recht bestaan. Het EDPB merkt op dat er niet altijd een gerechtelijke controle is in gevallen waarin elektronische informatie met toepassing van dwangmiddelen wordt verzameld, zoals in het ontwerpadequaateheidsbesluit bepaald. In dit verband herinnert het EDPB aan de jurisprudentie van het EHRM inzake gerechtelijke controles achteraf.⁷¹

4.1.2.1.2 In het geval van verzoeken om vrijwillige informatieverstrekking

156. Volgens het ontwerpadequaateheidsbesluit is er in het geval van verzoeken om vrijwillige informatieverstrekking geen sprake van controle vooraf door een rechter. In dat geval opereert de prefecturale politie onder toezicht van het Openbaar Ministerie. In het ontwerpadequaateheidsbesluit worden de artikelen 192, lid 1, en 246 betreffende de onderlinge samenwerking en coördinatie van de openbaar aanklagers, de prefecturale commissie openbare veiligheid en agenten van de gerechtelijke politie en betreffende de uitwisseling van informatie tussen hen vermeld. In het ontwerpadequaateheidsbesluit wordt ook verwezen naar artikel 193, lid 1, volgens hetwelk het Openbaar Ministerie de nodige instructies kan geven aan de gerechtelijke politie en normen voor een eerlijk onderzoek kan vaststellen. Ten slotte wordt in het ontwerpadequaateheidsbesluit melding gemaakt van artikel 194 over de disciplinaire maatregelen door de nationale of prefecturale commissie openbare veiligheid tegen de gerechtelijke politie wegens niet-eerbiediging van de openbare aanklagers.

157. Het EDPB erkent de vaststelling van de eerdere maatregelen en het toezicht van de nationale en prefecturale commissie openbare veiligheid op de gerechtelijke politie (zie hieronder).

4.1.2.2 Toezicht door de commissies openbare veiligheid op de politie

158. Volgens bijlage II van het ontwerpadequaateheidsbesluit oefenen twee soorten commissies toezicht uit op de politie. Beide zijn gericht op het waarborgen van het democratische beheer en de politieke neutraliteit van het politiebureau.

4.1.2.2.1 Toezicht uitgeoefend door de nationale commissie openbare veiligheid

159. In bijlage II bij het ontwerpadequaateheidsbesluit wordt melding gemaakt van het toezicht dat de nationale commissie openbare veiligheid uitoefent op de nationale politie. De politiewet bevat een lijst van de taken van deze commissie waaruit haar toezichtsbevoegdheden voortvloeien (zie artikel 5).

160. Volgens artikel 4 van de politiewet is de nationale commissie openbare veiligheid opgericht onder de jurisdictie van de eerste minister en bestaat zij uit een voorzitter en vijf leden. In artikel 7 zijn enkele beperkingen met betrekking tot de benoeming van de leden van deze commissie vastgesteld. De leden van deze commissie worden benoemd voor een periode van vijf jaar die slechts eenmaal kan worden verlengd, zoals voorgeschreven in artikel 8. Bovendien lijkt het Japanse parlement veel macht te hebben over de benoeming en het ontslag van de leden van de nationale commissie openbare veiligheid, wat haar onafhankelijkheid waarborgt.

161. Dergelijke wettelijke bepalingen versterken de politieke neutraliteit van deze commissie.

⁷¹ EHRM, Modestou/Griekenland, nr. 51693/13.

4.1.2.2.2 Toezicht uitgeoefend door de prefecturale commissies openbare veiligheid

162. De prefecturale politie staat onder toezicht van de in elke prefectuur opgerichte prefecturale commissie openbare veiligheid. Volgens de artikelen 2 en 36, lid 2, van de politiewet zijn de prefecturale commissies openbare veiligheid verantwoordelijk voor "de bescherming van de rechten en vrijheden van natuurlijke personen". In de artikelen 38 en 42 van de politiewet zijn de taken van deze commissies opgesomd. Deze commissies hebben ook tot doel het democratische beheer en de politieke neutraliteit van het politiebesteding te waarborgen, zoals bepaald in artikel 43, lid 2, door individuele zaken aan de prefecturale politie toe te wijzen wanneer zij dit nodig achten in het kader van een onderzoek naar de activiteiten van de prefecturale politie of naar wangedrag van haar personeel.
163. Het is echter onduidelijk of deze commissies andere bevoegdheden hebben dan het onderzoek van het gedrag van de politie. Het EDPB vraagt zich af of de term "wangedrag" ook onrechtmatige inzage in gegevens omvat en, zo ja, of die commissies de wissing van gegevens kunnen gelasten of niet.
164. Wat de neutraliteit en de onafhankelijkheid van deze commissies betreft, zijn de prefecturale commissies openbare veiligheid, zoals in het ontwerpadequaateitsbesluit vermeld⁷², opgericht onder de jurisdictie van de gouverneur van de desbetreffende prefectuur, die de leden van de commissie benoemt met instemming van het prefecturale parlement. De leden van de prefecturale commissie openbare veiligheid worden benoemd voor een periode van drie jaar en kunnen tot twee keer worden herbenoemd. In artikel 39 van de politiewet zijn beperkingen met betrekking tot de benoeming van de leden vastgesteld. In het ontwerpadequaateitsbesluit wordt ook melding gemaakt van het toezicht op de prefecturale politie door het lokale parlement, met verwijzing naar artikel 100 van de wet op de lokale autonomie. Deze wet is echter niet aan het EDPB verstrekt⁷³.
165. Voorts is in artikel 42, leden 2 en 3, van de politiewet het volgende bepaald: "Geen enkel lid van de commissie mag tegelijkertijd parlamentslid zijn of voltijds in dienst zijn van een lokale overheidsinstantie of deeltijds werkzaam zijn zoals bepaald in artikel 28, lid 5, punt 1, van de wet op de lokale openbare dienstverlening.
166. Volgens de hierboven genoemde elementen en rekening houdend met de samenwerking tussen de prefecturale commissies openbare veiligheid en de nationale commissie openbare veiligheid, is het EDPB het eens met het ontwerpadequaateitsbesluit en verwelkomt het de neutraliteit en onafhankelijkheid van de leden van de prefecturale commissies openbare veiligheid. Het EDPB heeft begrepen dat de prefecturale commissies openbare veiligheid alleen bevoegd zijn om het gedrag van de politie te onderzoeken en dat ze geen andere toezichtsbevoegdheden hebben, wat betekent dat ze ook niet bevoegd zijn voor het wisselen van gegevens die door de prefecturale politie zijn verzameld. Daarom lijkt het erop dat verdere verduidelijking nodig is over de vraag of het toezicht door de prefecturale commissies openbare veiligheid voldoende is volgens de in EU-recht vastgestelde normen.

4.1.2.2.3 Toezicht uitgeoefend door het Japanse parlement

167. Het ontwerpadequaateitsbesluit⁷⁴ en bijlage II⁷⁵ verschaffen enige informatie over het toezicht van het Japanse parlement op de overheid, onder meer met betrekking tot de rechtmatigheid van de gegevensverzameling door de politie. In beide wordt namelijk verwezen naar artikel 62 van de grondwet, volgens hetwelk het Japanse parlement kan verzoeken om overlegging van documenten en

⁷² Zie het ontwerpadequaateitsbesluit, blz. 31.

⁷³ Zie het ontwerpadequaateitsbesluit, blz. 33.

⁷⁴ Zie het ontwerpadequaateitsbesluit, blz. 30.

⁷⁵ Zie bijlage II, blz. 12.

om getuigenverklaringen. Beide bevatten ook wettelijke bepalingen uit de parlementswet, met name artikel 104 betreffende de bevoegdheden van het Japanse parlement alsmede artikel 74 betreffende de indiening van schriftelijke verzoeken om informatie, die binnen zeven dagen schriftelijk door de regering moeten worden beantwoord zoals in artikel 75 voorgeschreven. In het ontwerpadequaateitsbesluit is ook het volgende toegevoegd: "De rol van het Japanse parlement bij het toezicht op de uitvoerende macht wordt ondersteund door rapportageverplichtingen, bijvoorbeeld krachtens artikel 29 van de aftapwet".

168. Het EDPB erkent de betrokkenheid van het Japanse parlement bij het toezicht op de overheid en de politie met betrekking tot de rechtmatigheid van gegevensverzameling.

4.1.2.2.4 Toezicht uitgeoefend door de uitvoerende macht

169. Volgens bijlage II bij het ontwerpadequaateitsbesluit is enerzijds de minister of het hoofd van elk ministerie of agentschap bevoegd voor toezicht en handhaving op basis van de Japanse wet op de bescherming van persoonsgegevens waarover bestuursorganen beschikken (hierna: "WBPBB")⁷⁶. Anderzijds heeft de minister van Binnenlandse Zaken en Communicatie (MIC) onderzoeksbevoegdheid met betrekking tot de handhaving van de WBPBB door alle andere ministeries, met inbegrip van het ministerie van Justitie voor de politie, zoals in het ontwerpadequaateitsbesluit vermeld⁷⁷.
170. De minister kan het hoofd van een bestuursorgaan verzoeken om op grond van artikel 50 van de WBPBB materiaal en uitleg te verstrekken over de behandeling van persoonsgegevens door het betrokken bestuursorgaan. De minister kan verzoeken om maatregelen te herzien als het vermoeden bestaat dat de wet is overtreden of niet naar behoren is toegepast alsmede om adviezen uit te brengen over de behandeling van persoonsgegevens door het betrokken bestuursorgaan overeenkomstig de artikelen 50 en 51 van de WBPBB.
171. In het ontwerpadequaateitsbesluit en bijlage II wordt ook melding gemaakt van de oprichting van 51 uitgebreide informatiecentra die "zorgen voor de vlotte uitvoering van deze wet" overeenkomstig artikel 47 van de WBPBB. Het EDPB merkt op dat de WBPBB de rol en de bevoegdheden van deze informatiecentra niet nader toelicht, maar dat het ontwerpadequaateitsbesluit enkele preciseringen bevat.
172. Daarom verwelkomt het EDPB het feit dat de minister van Binnenlandse Zaken en Communicatie toezicht houdt op de naleving van de WBPBB op ministeries en bestuursorganen.
173. Concluderend kan worden gesteld dat de EU-wetgeving en het EVRM in de jurisprudentie van hun respectieve rechtbanken normen en waarborgen vaststellen volgens welke het toezicht volledig, neutraal en onafhankelijk moet zijn. Het EDPB merkt op dat de CBP geen toezichtsbevoegdheden heeft op het gebied van rechtshandhaving. Als het toezicht uitgeoefend door het Japanse parlement en door zowel de nationale als prefecturale commissies openbare veiligheid neutraal en onafhankelijk lijkt te zijn, moeten de toezichtsbevoegdheden van de prefecturale commissies openbare veiligheid verder worden verduidelijkt.

4.1.3 Verhaal in strafrechtelijke context

174. In het ontwerpadequaateitsbesluit, aangevuld met bijlage II, zijn verschillende kanalen vermeld via welke natuurlijke personen klachten kunnen indienen bij onafhankelijke autoriteiten en bij rechters.
175. Deze kanalen en de kernelementen van deze procedures die uit de beschikbare documentatie voortkomen, worden hierna geschetst, na een kort overzicht van de beschikbare rechten om te

⁷⁶ Zie bijlage II, blz. 10.

⁷⁷ Zie bijlage II, blz. 11.

verduidelijken wat betrokkenen van overheidsinstanties kunnen verwachten wat betreft de verwerking van gegevens in het kader van strafrechtelijke procedures.

4.1.3.1 Beschikbare rechten van betrokkenen in het kader van strafrechtelijke procedures

176. Om verhaal te halen, moeten betrokkenen wettelijke rechten hebben om te kunnen beweren dat die rechten niet zijn geëerbiedigd. Daarom heeft het EDPB ook de in het ontwerpadequaateitsbesluit geschetste beschikbare rechten in het kader van strafrechtelijke procedures beoordeeld.

4.1.3.1.1 Algemene beperkingen van de rechten van betrokkenen op grond van de WBPBB

177. In haar ontwerpadequaateitsbesluit verwijst de Commissie naar en gaat zij uit van algemene beginselen inzake gegevensbescherming die overheidsinstanties in acht moeten nemen zodra zij persoonsgegevens hebben verzameld. Deze beginselen zijn ook nader uiteengezet in bijlage II, zodat het EDPB heeft besloten om ook met betrekking tot deze beginselen opmerkingen te maken.

178. Wat de beschikbare rechten betreft, merkt het EDPB op dat volgens bijlage II van het ontwerpadequaateitsbesluit sommige van de algemene rechten die betrokkenen genieten wanneer hun gegevens door bestuursorganen worden verwerkt, ook beschikbaar blijven in het kader van strafrechtelijke onderzoeken. Uit de WBPBB zelf vloeien echter ook bijkomende beperkingen voort met betrekking tot het verzamelen en verder verwerken van persoonsgegevens in deze context.

179. Deze beperkingen, die ook van toepassing lijken te zijn in de context van gegevens die zijn verzameld op basis van een gerechtelijk bevel of op basis van een inlichtingenblad in de context van vrijwillige informatieverstrekking, roepen vragen op over verschillende aspecten.

180. Wat het beginsel van doelbinding betreft, kunnen bestuursorganen, hoewel zij in beginsel verplicht zijn het doel waarvoor zij persoonsgegevens bewaren te specificeren en zij de persoonsgegevens niet langer mogen bewaren dan noodzakelijk is om het gespecificeerde gebruiksdoel te bereiken, het doel wijzigen indien het nieuwe doel "redelijkerwijs als voldoende relevant voor het oorspronkelijke doel kan worden beschouwd".

181. In de WBPBB is ook het beginsel van niet-openbaarmaking opgenomen, volgens hetwelk een werknemer de verkregen persoonsgegevens niet zonder gerechtvaardigde grond aan een andere persoon mag verstrekken en niet voor een ongerechtvaardigd doel mag gebruiken. Er wordt echter geen aanvullende informatie verstrekt over de interpretatie van wat onder "gerechtvaardigde grond" of "ongerechtvaardigd doel" zou kunnen vallen, zodat verdere verduidelijking nodig is voor de beoordeling.

182. In artikel 8, lid 1, van de WBPBB is ook het verbod neergelegd om gegevens te gebruiken of aan derden te verstrekken "tenzij in wet- en regelgeving anders is bepaald". Hoewel deze bepaling in beginsel niet in strijd is met het door het EU-recht geboden beschermingsniveau, ontbreekt het het EDPB aan aanvullende gegevens over de mate waarin toezicht of controle wordt uitgeoefend wanneer de verstrekking van persoonsgegevens op grond van wet- of regelgeving verplicht is. Bovendien gelden krachtens artikel 8, lid 2, aanvullende uitzonderingen op deze regel indien "het niet waarschijnlijk is dat een dergelijke uitzonderlijke gegevensverstrekking ongerechtvaardigde schade zal toebrengen aan de rechten en belangen van de betrokkene of van een derde". Zonder verdere elementen over dit punt behoeft deze uitzondering, die gebaseerd is op het onduidelijke begrip "ongerechtvaardigde" schade, verdere verduidelijking, indien het beperkt genoeg is.

183. Ten slotte voorziet artikel 9 van de WBPBB in aanvullende beperkingen van het gebruiksdoel of de gebruikwijze of andere noodzakelijke beperkingen die door het hoofd van een bestuursorgaan moeten worden opgelegd indien bewaarde persoonsgegevens aan een andere persoon worden

verstrekt. Aangezien de begrippen "andere noodzakelijke beperkingen" en "aan een andere persoon worden verstrekt" zeer ruim zijn, geven deze aanvullende beperkingen van de rechten van betrokkenen aanleiding tot bezorgdheid zonder nadere verduidelijking over de werkingssfeer van deze bepaling.

184. Hoewel het EDPB zich er ten volle van bewust is dat inzagerechten en andere gegevensbeschermingsbeginselen ook in strafrechtelijke procedures onder het EU-recht beperkt zijn, worden aanvullende waarborgen geboden wanneer in dergelijke beperkingen is voorzien, onder meer op het gebied van toezicht, controle en verhaalsmogelijkheden. Bij gebrek aan voldoende jurisprudentie over deze beperkingen of aanvullende elementen om de werkingssfeer van deze bepalingen te verduidelijken, kan het EDPB niet beoordelen of deze beperkingen van de rechten van betrokkenen beperkt zijn tot wat in het EU-recht strikt noodzakelijk en evenredig wordt geacht, en of deze rechten dus in wezen gelijkwaardig zouden zijn aan de rechten die betrokkenen uit de EU genieten.

4.1.3.1.2 Aanvullende beperkingen van de rechten van de WBPBB die voortvloeien uit het wetboek van strafvordering en de verordeningen van de prefecturale politie

185. Het EDPB merkt op dat, hoewel de WBPBB van toepassing lijkt te zijn op alle verwerkingen door bestuursorganen in Japan, enkele belangrijke beperkingen van de rechten van betrokkenen voortvloeien uit specifieke wetgeving. Met name in artikel 53, lid 2, van het wetboek van strafvordering⁷⁸ is bepaald dat "persoonsgegevens die zijn opgenomen in documenten die verband houden met gerechtelijke onderzoeken en in beslag genomen voorwerpen" zijn uitgesloten van het toepassingsgebied van de rechten van natuurlijke personen in hoofdstuk IV van de WBPBB. Het EDPB heeft derhalve begrepen dat betrokkenen in het kader van strafrechtelijke procedures niet beschikken over het recht op informatie, inzage, rectificatie of wissing met betrekking tot persoonsgegevens die zijn opgenomen in documenten die verband houden met gerechtelijke onderzoeken en in beslag genomen voorwerpen.
186. Het EDPB heeft begrepen dat deze beperkingen van toepassing zijn in de context van gegevens die op basis van een gerechtelijk bevel zijn verzameld alsook in de context van gegevens die zijn verzameld in het kader van de procedure voor vrijwillige informatieverstrekking via inlichtingenbladen (zie hieronder). Aangezien de rechtsgrond van de twee procedures voor inzage in gegevens (via een gerechtelijk bevel en via een inlichtingenblad) in het wetboek van strafvordering zijn bepaald, lijkt artikel 53-2 van dat wetboek van toepassing te zijn op beide soorten gegevensverzameling. Aangezien in artikel 53-2 wordt verwezen naar "in beslag genomen" voorwerpen, zou echter kunnen worden verduidelijkt of de beperkingen van de rechten waarin deze bepaling voorziet ook van toepassing zijn in de context van vrijwillige informatieverstrekking.
187. Het EDPB betreurt het dat het de verordeningen van de prefecturale politie, die naar verluidt persoonsgegevens beschermen alsook rechten en verplichtingen die gelijkwaardig zijn aan die welke in de WBPBB zijn opgenomen, niet heeft ontvangen. Gezien de onduidelijkheid over de interpretatie van de WBPBB en omdat het EDPB niet over de verordeningen van de prefecturale politie beschikt, vraagt het EDPB zich af of de in deze context aan natuurlijke personen toegekende rechten en de aanvullende toezichts- en/of verhaalmechanismen voldoende zijn om de afwezigheid van rechten te compenseren.

⁷⁸ Beschikbaar op <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02> en geciteerd in bijlage II bij het ontwerpadequaathheidsbesluit, voetnoot 25.

4.1.3.2 Verhaal via onafhankelijke instanties

4.1.3.2.1 Verhaal via een bestuursorgaan

188. Het EDPB merkt op dat de bestuursorganen die gegevens verzamelen, zoals de prefecturale politie, bevoegd zijn om verzoeken in behandeling te nemen die afkomstig zijn van natuurlijke personen en betrekking hebben op hun – beperkte – rechten met betrekking tot hun in het kader van een strafrechtelijk onderzoek verzamelde gegevens (zie hierboven voor de beschikbare rechten), die zowel het verzamelen van gegevens op basis van een gerechtelijk bevel als het verzamelen van informatie via een inlichtingenblad lijken te omvatten. Concreet lijken deze rechten beperkt te zijn tot algemene beginselen, zoals de noodzaak van gegevensbewaring, in verband met het doel (zie artikel 3, lid 1, WBPBB), het doelbindingsbeginsel (artikel 4) of de juistheid van de gegevens (artikel 5), terwijl rechten van natuurlijke personen zoals het recht op informatie, inzage, rectificatie of wissing zijn uitgesloten voor persoonsgegevens die zijn opgenomen in documenten die verband houden met gerechtelijke onderzoeken en in beslag genomen voorwerpen⁷⁹. Hoewel deze organen niet als onafhankelijk kunnen worden beschouwd en dus niet als organen die de mogelijkheid van verhaal of toezicht via een onafhankelijke instantie bieden, verwelkomt het EDPB deze weg. Het EDPB benadrukt echter dat de in deze context ingediende klachten beperkt blijven tot zeer weinig rechten van de betrokkenen, gezien de beperkingen van rechten waarin de WBPBB voorziet.
189. Aangezien "persoonsgegevens die zijn opgenomen in documenten die verband houden met gerechtelijke onderzoeken en in beslag genomen voorwerpen" zijn uitgesloten van het toepassingsgebied van de rechten van natuurlijke personen in hoofdstuk IV van de WBPBB op grond van artikel 53-2 van het wetboek van strafvordering, zijn de mogelijkheden om te verzoeken om inzage in persoonsgegevens ook beperkt tot de procedures waarin andere bepalingen van dit wetboek van strafvordering voorzien. Het lijkt erop dat alleen slachtoffers, verdachten of beklaagden in deze context kunnen optreden, afhankelijk van de fase van de strafrechtelijke procedure. Het EDPB maakt zich er dan ook zorgen over dat de betrokkenen krachtens het Japanse recht in het kader van een strafrechtelijke procedure geen algemeen recht op inzage in en/of rectificatie of wissing van gegevens hebben en dat alle beschikbare verhaalsmogelijkheden impliceren dat zij ofwel een slachtoffer zijn (in welk geval de betrokkene waarschijnlijk zou weten dat zijn gegevens zijn verzameld) ofwel een verdachte of beklagde, of dat zij kunnen aantonen dat zij schade hebben geleden, terwijl betrokkenen ook het recht moeten hebben op inzage in hun gegevens en eventueel het recht om hun gegevens te laten rectificeren of wissen indien zij (mogelijk) geen schade hebben geleden en/of indien zij geen slachtoffer, verdachte of beklagde maar bijvoorbeeld een getuige zijn.

4.1.3.2.2 Verhaal via een bestuursorgaan: de prefecturale commissies openbare veiligheid

190. Daarnaast lijken de prefecturale commissies openbare veiligheid bevoegd te zijn voor de behandeling van klachten. Op grond van artikel 79 van de politiewet waarnaar in het ontwerpadequaateheidsbesluit wordt verwezen, kunnen natuurlijke personen een klacht indienen tegen onwettig of ongepast gedrag van een agent bij de uitvoering van zijn taken.
191. Het EDPB verzoekt om verduidelijking over de vraag of een "illegale" verwerking van persoonsgegevens kan worden beschouwd als "illegaal of ongepast gedrag van een agent" en over het aantonen van een nadeel zoals dat van de betrokkene lijkt te worden verlangd. De mededeling van de nationale politie aan de politie en prefecturale commissies openbare veiligheid met betrekking tot de juiste behandeling van klachten over de uitvoering van taken door politieambtenaren beperkt de klachten tot concrete klachten over "het corrigeren van een specifiek nadeel dat is geleden als gevolg

⁷⁹ Zie hierboven voor de beperkingen van de WBPBB en zie in het bijzonder artikel 53-2 van het wetboek van strafvordering (niet verstrekt maar geciteerd in bijlage II bij het ontwerpadequaateheidsbesluit, voetnoot 25).

van onwettig of ongepast gedrag of het niet nemen van de nodige maatregelen door een politieambtenaar bij de uitvoering van zijn taken" en de mogelijkheid om "een klacht in te dienen op basis van ongenoegen/ontevredenheid over de ongepaste wijze waarop een politieambtenaar zijn taken uitvoert". Er wordt uitdrukkelijk verduidelijkt dat "klachten over wanprestaties door een politieambtenaar in verband met een aangelegenheid die niet tot de taak van een politieambtenaar wordt gerekend, en ook klachten waarin een algemene mening of een voorstel wordt geformuleerd die/dat niet rechtstreeks betrekking heeft op de klagende partij zelf, worden uitgesloten".

192. Wat de procedurele vereisten voor het indienen van een klacht betreft, merkt het EDPB op dat klachten weliswaar schriftelijk moeten worden ingediend, maar dat in deze context krachtens het Japanse recht hulp bij het opstellen van de klacht wordt verleend, ook aan buitenlanders. Bovendien lijkt de Japanse overheid de CBP ook te hebben belast met de taak om betrokkenen uit de EU bij te staan bij de indiening en afhandeling van klachten op dit gebied, hetgeen het EDPB toejuicht. Het EDPB benadrukt dat het heeft begrepen dat de CBP in dit verband alleen zal fungeren als contactpunt tussen de betrokkenen uit de EU en de bevoegde autoriteiten in Japan.
193. De resultaten van de prefecturale commissie openbare veiligheid na een klacht worden niet ter kennis gebracht in de gevallen genoemd in artikel 79-2 van de politiewet, waaronder het geval waarin de huidige "verblijfplaats van de klager onbekend is". Het EDPB erkent dat de verwijzing naar de verblijfplaats niet impliceert dat betrokkenen uit de EU in alle gevallen zouden worden uitgesloten van de kennisgeving van de resultaten van hun klachten op grond van het feit dat zij niet in Japan verblijven.

4.1.3.2.3 Ad-hocmechanisme waarbij de CBP wordt betrokken

194. In het licht van de hierboven beschreven bevindingen verwelkomt het EDPB dat de Japanse overheid en de Europese Commissie overeenstemming hebben bereikt over een aanvullend verhaalmechanisme dat natuurlijke personen uit de EU een extra verhaalsmogelijkheid in Japan biedt, via welke natuurlijke personen ook verhaal kunnen halen tegen onrechtmatige of ongepaste onderzoeken door overheidsinstanties. Het EDPB merkt ook op en verwelkomt dat de verzoeken bij de CBP kunnen worden ingediend in plaats van bij een andere overheidsinstantie, waardoor de bevoegdheid van de CBP wordt uitgebreid tot het gebied van rechtshandhaving en nationale veiligheid.
195. Het EDPB heeft zich bij de analyse van het nieuwe mechanisme vooral gericht op een beter begrip van de bevoegdheden van de CBP in deze context.
196. Hoewel de taal niet helemaal duidelijk is, heeft het EDPB begrepen dat het aanvullende verhaalmechanisme niet vereist dat de verzoeker aantoont dat zijn persoonsgegevens waarschijnlijk aan toezicht door een Japanse autoriteit zijn onderworpen. Het EDPB wenst nog steeds bevestiging van de Commissie te vragen.
197. In overeenstemming met zijn beoordeling van het in het kader van het privacyschild ingestelde ombudsmanmechanisme benadrukt het EDPB de noodzaak van effectieve bevoegdheden van de adressaat van het verzoek, in dit geval de CBP, om het verhaalmechanisme als in wezen gelijkwaardig te kunnen beschouwen aan een doeltreffende voorziening in rechte in de zin van artikel 47 van het Handvest van de grondrechten.
198. Bij het uitleggen van het verhaalmechanisme verwijst de Japanse overheid naar de artikelen 6, 61, onder ii), en 80 van de WBP en zet zij deze bevoegdheden uiteen in bijlage II. Het EDPB heeft begrepen dat de procedure zoals beschreven in bijlage II de bevoegdheden van de CBP specificeert of uitbreidt, aangezien de bewoordingen in de artikelen 6, 61, onder ii), en 80 van de WBP nogal vaag en algemeen zijn. Voor zover bijlage II de bevoegdheden van de CBP specificeert of uitbreidt, zou het EDPB graag

antwoord krijgen op de vraag of de andere agentschappen van de Japanse overheid erdoor gebonden zijn.

199. Op basis van de procedure in bijlage II merkt het EDPB op dat de bevoegde overheidsinstanties in Japan verplicht zijn met de CBP samen te werken, "onder meer door hen de nodige informatie en relevant materiaal te verstrekken, zodat de CBP kan beoordelen of de verzameling of het latere gebruik van persoonsgegevens in overeenstemming met de toepasselijke regels heeft plaatsgevonden". Voor de beoordeling van de doeltreffendheid van het systeem is het dus belangrijk om opnieuw te verwijzen naar de bevoegdheden van deze bevoegde autoriteiten waarmee de CBP samenwerkt. Het EDPB heeft begrepen dat deze bevoegdheden niet zouden worden uitgebreid door de in bijlage II opgenomen garanties.
200. Het EDPB merkt ook op dat, indien een overtreding van de regels is vastgesteld, "de samenwerking van de betrokken overheidsinstanties met de CBP de verplichting omvat om de overtreding ongedaan te maken", hetgeen uitdrukkelijk het wissen van de in strijd met de toepasselijke regels verzamelde gegevens omvat. Het EDPB heeft begrepen dat de verplichtingen van de bevoegde autoriteit voortvloeien uit de "samenwerking met de CBP" en niet uit een besluit van de CBP.
201. Ten slotte zal de CBP de verzoeker in kennis stellen van het "resultaat van de beoordeling, met inbegrip van de genomen corrigerende maatregelen, in voorkomend geval". Daarnaast zal de CBP de verzoeker informeren over de "mogelijkheid om de bevoegde overheidsinstantie te vragen het resultaat te bevestigen en over de instantie waaraan een dergelijk verzoek om bevestiging dient te worden gericht".
202. Daarnaast heeft de CBP zich ertoe verbonden de verzoeker bij te staan bij het ondernemen van verdere actie krachtens het Japanse recht indien de verzoeker ontevreden is over het resultaat van de procedure.
203. In het licht van de behoefte aan een doeltreffend verhaalmechanisme dat in wezen gelijkwaardig is aan de EU-normen, vraagt het EDPB zich niettemin af of de CBP over andere specifieke bevoegdheden beschikt dan het beoordelen of de verzameling of het latere gebruik van persoonsgegevens in overeenstemming met de toepasselijke regels heeft plaatsgevonden en het oproepen van de bevoegde autoriteiten om gebruik te maken van hun respectieve bevoegdheden en de door de CBP aan hen doorgezonden klachten te behandelen. Indien de CBP alleen als contactpunt voor natuurlijke personen uit de EU zou fungeren, zou het EDPB dat als onvoldoende beschouwen om te voorzien in een doeltreffend verhaalmechanisme dat in wezen gelijkwaardig is aan de EU-normen. Het EDPB verzoekt de Commissie derhalve de in dit subhoofdstuk genoemde punten te verduidelijken, met name of en hoe het mechanisme de verplichtingen van bevoegde autoriteiten uitbreidt, hoe zij eraan gebonden zijn en hoe de CBP de naleving doeltreffend kan waarborgen en niet alleen als contactpunt voor natuurlijke personen uit de EU kan optreden.

4.1.3.3 Gerechtig verhaal

4.1.3.3.1 Quasi-klachtenmechanisme

204. De zogenaamde "quasi-klachtenprocedure" maakt het mogelijk om op basis van een gerechtelijk bevel tot intrekking of wijziging van een illegale inbeslagneming op te treden tegen het met toepassing van dwangmiddelen verzamelen van informatie.
205. Deze mogelijkheid impliceert dat de betrokkene op de hoogte is van de inbeslagneming van de gegevens. Het EDPB heeft echter begrepen dat de procedure voor het verzamelen van gegevens op basis van een gerechtelijk bevel niet aan de betrokkene wordt meegedeeld. Evenzo heeft het EDPB begrepen dat vrijwillige verstrekking niet betekent dat de ondernemingen die een verzoek ontvangen

verplicht zijn de betrokkenen te informeren over ontvangen en ingewilligde verzoeken. Hoewel in bijlage II wordt benadrukt dat "een dergelijke betwisting mogelijk is zonder dat de betrokkene hoeft te wachten op de afronding van de zaak", lijkt deze mogelijkheid in de praktijk, afgezien van gerechtelijke aftapbevelen waarvoor is aangegeven dat de wet in een kennisgevingsplicht voorziet⁸⁰, pas daadwerkelijk beschikbaar te zijn wanneer de betrokkene via een tegen hem aangespannen zaak kennis heeft gekregen van de gegevensverzameling.

4.1.3.3.2 Dwangmiddel tot rechtsherstel

206. Daarnaast kunnen natuurlijke personen ook een civiele vordering bij de rechter instellen om gegevens die via een strafrechtelijke procedure zijn verzameld te laten wissen (het zogenaamde "dwangmiddel tot rechtsherstel") of om een schadevergoeding te verkrijgen.
207. Wat de schadevergoeding betreft, merkt het EDPB op dat de procedure beperkt lijkt te zijn tot situaties waarin een overheidsfunctionaris in de uitoefening van zijn functie onrechtmatig en met schuld (opzettelijk of uit onachtzaamheid) de betrokkene schade heeft berokkend. Volgens het EDPB lijkt de schade ook morele schade te omvatten. Er wordt echter niet nader uiteengezet wat de betrokkene moet aantonen om te bewijzen dat hij schade heeft geleden. Het EDPB was niet in staat om de jurisprudentie betreffende de toekenning van schadevergoedingen te beoordelen en kan derhalve niet beoordelen of deze mogelijkheid in geval van schade een doeltreffende voorziening in rechte vormt.
208. Wat het "dwangmiddel tot rechtsherstel" betreft, merkt het EDPB ook op dat om een verzoek in te dienen de betrokkene zich er eerst van bewust moet zijn dat zijn gegevens zijn verzameld en nog steeds worden bewaard. Gezien de beperkte rechten van natuurlijke personen op informatie en op inzage in het kader van strafrechtelijke onderzoeken en procedures lijkt de doeltreffendheid van de procedure dan ook vrij beperkt.

4.1.3.4 Algemene beoordeling van de verhaalsmogelijkheden

209. Na de beoordeling van alle verhaalsmogelijkheden voor natuurlijke personen krachtens het Japanse recht alsmede voor betrokkenen uit de EU vóór de CBP, verwelkomt het EDPB het ad-hocmechanisme voor geschillenbeslechting, waarbij de CBP betrokken is. Dat mechanisme is een meerwaarde voor betrokkenen uit de EU, met name omdat het hen in staat stelt te begrijpen welke mogelijkheden zij hebben om verhaal te halen en/of een schadevergoeding te krijgen en om hun verzoeken in te dienen overeenkomstig de toepasselijke procedurele vereisten van het Japanse recht. Verdere verduidelijkingen zijn echter noodzakelijk, met name over de vraag of en hoe het mechanisme de verplichtingen van bevoegde autoriteiten uitbreidt, hoe zij eraan gebonden zijn en hoe de CBP de naleving ervan effectief kan waarborgen om ervoor te zorgen dat dit nieuwe mechanisme in doeltreffende verhaalsmogelijkheden voorziet.
210. Uit deze beoordeling blijkt dat geen enkel verhaalmechanisme in het Japanse recht lijkt te voorzien in de mogelijkheid van inzage in, rectificatie van of wissing van gegevens van betrokkenen die geen slachtoffer, verdachte of beklaagde zijn in het kader van een strafprocedure, bijvoorbeeld om een einde te maken aan het onrechtmatig verzamelen of bewaren van hun gegevens. Ook blijkt uit deze beoordeling dat alle verhaal- en schadevergoedingsmechanismen en -procedures die volgens het Japanse recht beschikbaar zijn voor slachtoffers, verdachten of beklaagden impliceren dat zij op de hoogte zijn van de verzameling van gegevens, wat in de praktijk niet altijd het geval lijkt te zijn gezien het beperkte recht van inzage en recht op informatie waarover zij beschikken. Daarnaast lijkt verdere verduidelijking nodig over het aantonen van illegaal gedrag van de autoriteiten, in het bijzonder over

⁸⁰ Artikel 23 van de aftapwet is vermeld op bladzijde 33 van het ontwerpadequaateheidsbesluit, maar het EDPB heeft deze tekst niet ontvangen en kan derhalve niet beoordelen in welke mate deze kennisgevingsplicht van toepassing is en in welke gevallen deze beperkt kan zijn.

de vraag of dit gedrag de onrechtmatige verwerking van persoonsgegevens omvat, en over het aantonen van door de betrokkene geleden schade.

211. Zonder verdere documentatie en elementen maakt het EDPB zich dan ook zorgen over de vraag of de verhaalsmogelijkheden op grond van het Japanse recht en het ontwerpadequaateheidsbesluit voldoende doeltreffend zijn in vergelijking met de normen in het EU-recht.

4.2 Inzage ten behoeve van de nationale veiligheid

4.2.1 Reikwijdte van het toezicht

212. In het ontwerpadequaateheidsbesluit is het hoofdstuk over "inzage en gebruik door Japanse overheidsinstanties ten behoeve van de nationale veiligheid" ingevoegd door middel van een algemene verklaring, in overeenstemming met de garantie van de Japanse overheid in bijlage II, volgens welke geen enkele Japanse wet zou voorzien in de mogelijkheid van, of toestemming zou geven voor, "verzoeken om informatie met toepassing van dwangmiddelen" of "administratief aftappen" buiten een strafrechtelijk onderzoek". Concluderend wordt gesteld dat "het verkrijgen van informatie ten behoeve van de nationale veiligheid alleen mogelijk is uit een informatiebron die vrij toegankelijk is voor iedereen of op basis van vrijwillige informatieverstrekking. Dat sluit alle geheime toezichtsactiviteiten op dit gebied uit. Ondernemers die een verzoek om vrijwillige medewerking (in de vorm van de verstrekking van elektronische informatie) ontvangen, zijn niet wettelijk verplicht deze informatie te verstrekken".⁸¹
213. Binnen deze beperkingen zijn vier overheidsentiteiten vermeld die bevoegd zijn om elektronische informatie die in het bezit is van Japanse ondernemers te verzamelen om redenen van nationale veiligheid. Wat het ministerie van Defensie betreft, dat een van die vier entiteiten is, wordt gezegd dat het "alleen bevoegd is om (elektronische) informatie te verzamelen op basis van vrijwillige informatieverstrekking".⁸²
214. Voor zijn beoordeling van de algemene opzet van de gegevensverzameling ten behoeve van de nationale veiligheid wenst het EDPB te herinneren aan de eerste van de vier zogenaamde "essentiële waarborgen", volgens welke "de verwerking op duidelijke, precieze en toegankelijke regels moet zijn gebaseerd"⁸³. Het Europees Hof voor de Rechten van de Mens heeft heel duidelijk gesteld dat toezichtsprogramma's alleen "in overeenstemming met de wet" zijn als de toezichtsmaatregelen "een grondslag in het nationale recht" hebben. De rechtbank heeft verduidelijkt dat de verenigbaarheid met de beginselen van de rechtsstaat vereist dat de wet die de maatregel toestaat toegankelijk is en dat de gevolgen ervan voorzienbaar moeten zijn. Verwijzend naar het risico van willekeur heeft de rechtbank "duidelijke, gedetailleerde regels inzake geheime toezichtsmaatregelen" geëist die "voldoende duidelijk zijn om de burgers een adequate indicatie te geven van de omstandigheden waarin en de voorwaarden waaronder overheidsinstanties bevoegd zijn hun toevlucht te nemen tot een dergelijke maatregel".⁸⁴
215. Wat de toepassing van deze essentiële waarborgen op het rechtssysteem van Japan betreft, is het EDPB zich niet alleen bewust van het feit dat staten op het gebied van nationale veiligheid een ruime beoordelingsmarge hebben, die door het Europees Hof voor de Rechten van de Mens wordt erkend. Ook de bevoegdheden op het gebied van nationale veiligheid weerspiegelen de historische ervaringen

⁸¹ Adequaateheidsbesluit, punt 151.

⁸² Adequaateheidsbesluit, punt 153.

⁸³ WP29, WP 237: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

⁸⁴ Zie bijvoorbeeld Big Brother Watch e.a. tegen het Verenigd Koninkrijk, punt 305.

van de naties. Het EDPB is zich er dus van bewust dat, zoals de Japanse regering benadrukt, de Japanse nationale inlichtingendiensten na de Tweede Wereldoorlog beperktere bevoegdheden hebben gekregen dan de nationale inlichtingendiensten van andere staten.

216. Het EDPB heeft begrepen dat in het ontwerpadequaateitsbesluit, in overeenstemming met de garantie van de Japanse overheid, wordt gesuggereerd dat Japanse overheidsinstanties geen programma's uitvoeren die (internet)communicatie strategisch monitoren of er algemeen toezicht op houden. Zoals hierboven vermeld, heeft de Japanse overheid in een door de minister van Justitie ondertekende brief de verzekering gegeven dat "het verkrijgen van informatie ten behoeve van de nationale veiligheid alleen mogelijk is uit een informatiebron die vrij toegankelijk is voor iedereen of op basis van vrijwillige informatieverstrekking".
217. Wat de rechtsgrond van het ministerie van Defensie betreft, merkt het EDPB op dat het ontwerpadequaateitsbesluit algemene informatie over de bevoegdheden van dat ministerie bevat alsook een citaat van zijn missie: "het verrichten van zaken die verband houden met de rechtsgrond teneinde de nationale vrede en onafhankelijkheid, en de veiligheid van de natie te waarborgen". Het EDPB heeft echter geen Engelse vertaling van de rechtsgrond ontvangen.
218. Tegelijkertijd is het EDPB op de hoogte van rapporten die in verschillende media zijn gepubliceerd waarin wordt gesuggereerd dat het directoraat Inlichtingen uit berichtenverkeer van het Japanse ministerie van Defensie toezichtsprogramma's heeft lopen⁸⁵. In een van die rapporten wordt ook beweerd dat het Japanse ministerie van Defensie, hoewel het weigert om bijzonderheden van het rapport te bespreken, "heeft erkend dat Japan "in het hele land kantoren" heeft die communicatie onderscheppen" en dat die "gericht zouden zijn op militaire activiteiten en "cyberbedreigingen" en "geen informatie over het grote publiek verzamelen". Deze laatste bewering (dat het ministerie van Defensie geen informatie over het grote publiek verzamelt) wordt door de Japanse overheid herhaald.
219. In dat rapport staat dat de Japanse overheid in een door de minister van Justitie ondertekende brief heeft herhaald dat het ministerie van Defensie geen informatie over het grote publiek verzamelt.
220. Het overstijgt de taak van het EDPB om een algemene beoordeling te maken van de mogelijke toezichtcapaciteiten van de Japanse overheid. Deze activiteiten zijn alleen van belang voor zijn beoordeling als ze relevant zijn voor de doorgifte van persoonsgegevens tussen de EU en Japan. In dat verband wenst het EDPB zijn aanpak te bevestigen die reeds door zijn voorganger werd gevolgd toen deze werd gevraagd zijn mening te geven over het EU-VS-privacyschild. Bij het uitbrengen van een advies over dat privacyschild heeft de WP29 in zijn analyse melding gemaakt van de bevoegdheden en beperkingen van de VS om toezicht te houden op gegevens die "onderweg" zijn naar de VS⁸⁶. Bij toepassing van dezelfde norm voor het adequaateitsbesluit op Japan is het EDPB van mening dat informatie over de bevoegdheden van de Japanse autoriteiten om toezicht te houden op gegevens die "onderweg" zijn naar Japan relevant is. Indien deze toezichtbevoegdheden bestaan, lijkt ook de

⁸⁵ In mei 2018 publiceerde het onlinetijdschrift "The Intercept" een rapport getiteld "The untold story of Japan's secret spy agency".

⁸⁶ Zie WP255, EU-U.S. Privacy Shield – First annual joint review, goedgekeurd op 28 november 2017, blz. 16: "WP29 is van mening dat de analyse van de wetgeving van het derde land waarvoor een adequaateitsbesluit wordt overwogen, niet beperkt mag blijven tot de wetgeving en de praktijk die toezicht binnen de fysieke grenzen van dat land mogelijk maken, maar ook een analyse moet omvatten van de rechtsgronden in de wetgeving van dat derde land op grond waarvan het land buiten zijn grondgebied toezicht kan uitoefenen voor zover het EU-gegevens betreft. Zoals reeds in zijn vorige advies onderstreept, "moet het duidelijk zijn dat de beginselen van het privacyschild van toepassing zullen zijn vanaf het moment dat de doorgifte van gegevens plaatsvindt; dit omvat dus ook gegevens die "onderweg" zijn naar dat land".

uitspraak van het EHRM in de zaak-Big Brother Watch te suggereren dat dergelijke bevoegdheden moeten worden geregeld in overeenstemming met de door het EHRM vastgestelde normen.

221. Indien het aftappen beperkt zou blijven tot "ondersteuning van militaire actie", zou het dus kunnen dat dit niet relevant is voor de beoordeling van het adequaatheidsbesluit. Het EDPB krijgt derhalve graag verduidelijking over de toezichtsmaatregelen van Japanse overheidsinstanties. In dat verband zou die verduidelijking welkom zijn om te bepalen of gegevens die in dit adequaatheidskader worden doorgegeven, door de Japanse bevoegde autoriteiten op dat gebied om redenen van nationale veiligheid zouden kunnen worden ingezien.

4.2.2 Vrijwillige informatieverstrekking in geval van nationale veiligheid

222. In het ontwerpadequaateitsbesluit staat dat de vier overheidsentiteiten alleen de bevoegdheid hebben om vrijwillig verstrekte (elektronische) informatie te verzamelen. Volgens het ontwerpbesluit en bijlage II zijn er enkele beperkingen inzake wettelijke gronden, wat betekent dat het verzamelen van gegevens beperkt is tot wat noodzakelijk is voor de uitvoering van de taken door de entiteiten.
223. In strafrechtelijke context is vrijwillige informatieverstrekking alleen toegestaan in het kader van een strafrechtelijk onderzoek, wat een concreet vermoeden van een reeds gepleegde misdaad vooronderstelt, zoals in het deel over rechtshandhaving vermeld. Onderzoeken op het gebied van nationale veiligheid verschillen van onderzoeken op het gebied van rechtshandhaving. Het EDPB erkent dat, volgens bijlage II, de centrale beginselen "noodzaak van het onderzoek" en "geschiktheid van de methode" eveneens van toepassing zijn op het gebied van de nationale veiligheid en dat zij moeten worden geëerbiedigd, rekening houdend met de specifieke omstandigheden van elk geval⁸⁷. Het EDPB betreurt dat de toepassing niet verder wordt verduidelijkt, onder meer door een verdere verwijzing naar de jurisprudentie. Het EDPB stelt evenwel dat het gebruik van deze procedure evenredig of noodzakelijk moet zijn.
224. Volgens het ontwerpbesluit wordt, indien persoonsgegevens zijn verzameld ("verkregen"), de behandeling ervan geregeld door de WBPBB, tenzij de persoonsgegevens door de prefecturale politie worden behandeld⁸⁸. In bijlage II staat dat de behandeling van persoonsgegevens door de prefecturale politie wordt geregeld bij prefecturale verordeningen waarin beginselen voor de bescherming van persoonsgegevens, rechten en verplichtingen zijn vastgelegd die gelijkwaardig zijn aan die van de WBPBB⁸⁹. Omdat er voor deze verordeningen geen Engelse vertalingen beschikbaar zijn, kan het EDPB niet beoordelen of de beginselen gelijkwaardig zijn aan die van de WBPBB.
225. Voor de overige opmerkingen over vrijwillige informatieverstrekking wordt verwezen naar het deel over rechtshandhaving.

4.2.3 Toezicht

4.2.3.1 Algemene punten

226. De vier overheidsentiteiten die bevoegd zijn om elektronische informatie die in het bezit is van Japanse ondernemers te verzamelen om redenen van nationale veiligheid, zijn: (i) de inlichtingen- en onderzoeksdienst van de regering; ii) het ministerie van Defensie; iii) de politie (zowel de nationale als de prefecturale politie⁹⁰); en iv) de inlichtingendienst voor de openbare veiligheid.

⁸⁷ Zie bijlage II, blz. 23.

⁸⁸ Adequaateitsbesluit, punten 118 en 157.

⁸⁹ Zie bijlage II, blz. 3.

⁹⁰ Volgens de ontvangen informatie is de belangrijkste taak van de nationale politie echter het coördineren van de onderzoeken van de verschillende diensten van de prefecturale politie en zijn de activiteiten van de nationale

227. Volgens het ontwerpadequaateitsbesluit zijn deze overheidsentiteiten onderworpen aan verschillende lagen van toezicht door drie takken van de overheid⁹¹. Het EDPB merkt op dat er een toezichtsmechanisme bestaat binnen de wetgevende tak (Japans parlement) en de uitvoerende tak (Bureau van de inspecteur-generaal voor naleving van de wet, de prefecturale commissies openbare veiligheid en de Onderzoekscommissie openbare veiligheid). Het EDPB benadrukt dat de Commissie het gerechtelijk toezicht (ambtshalve/garantie C van de WP237; voor verhaal is er een apart hoofdstuk in het ontwerpbesluit en een extra waarborg in de WP237) door de bovengenoemde overheidsinstanties moet verduidelijken, aangezien het onduidelijk is of er sprake is van een dergelijk gerechtelijk toezicht op het zonder toepassing van dwangmiddelen verzamelen van persoonsgegevens ten behoeve van de nationale veiligheid.

4.2.3.2 Toezicht door het Japanse parlement

228. Het EDPB merkt op dat het Japanse parlement een onderzoek met betrekking tot de activiteiten van overheidsinstanties kan instellen, dus ook voor alle bovengenoemde overheidsentiteiten. Bovendien kan het Japanse parlement ook de overlegging van documenten en getuigenverklaringen verlangen (*artikel 62 van de Japanse grondwet, artikel 104 van de Japanse parlements wet*). Het EDPB merkt ook op dat parlementsleden volgens de *artikelen 74 en 75 van de Japanse parlements wet* schriftelijke vragen kunnen stellen aan de regering, die door de regering kunnen worden beantwoord (*artikel 75 van de Japanse parlements wet*). Ten slotte wordt ook opgemerkt dat er specifieke rapportageverplichtingen zijn voor bijvoorbeeld de inlichtingendienst voor de openbare veiligheid (*artikel 36 van de Wet ter voorkoming van subversieve activiteiten/artikel 31 van de Wet op de controle van organisaties die zich schuldig hebben gemaakt aan willekeurige massamoord*), door middel van een jaarlijks verslag aan het Japanse parlement. Het EDPB heeft geen dergelijk verslag ontvangen.

4.2.3.3 Toezicht door het Bureau van de inspecteur-generaal voor naleving van de wet

229. Het EDPB merkt op dat er een toezichtsorgaan voor het Japanse ministerie van Defensie is, namelijk het Bureau van de inspecteur-generaal voor naleving van de wet. Het EDPB heeft geen exemplaar van de Wet tot oprichting van het ministerie van Defensie ontvangen, maar alleen van de verklaringen in bijlage II bij het ontwerpbesluit. Overeenkomstig bijlage II is het Bureau van de inspecteur-generaal voor naleving van de wet een onafhankelijk bureau binnen het ministerie van Defensie dat volgens artikel 29 van de Wet tot oprichting van het ministerie van Defensie onder rechtstreeks toezicht van de minister van Defensie staat. Het Bureau van de inspecteur-generaal voor naleving van de wet is bevoegd om binnen het hele ministerie van Defensie, inclusief de Zelfverdedigingstroepen, inspecties uit te voeren op de naleving van wet- en regelgeving door ambtenaren van het ministerie van Defensie ("defensie-inspecties").

230. Overeenkomstig bijlage II verricht het Bureau van de inspecteur-generaal voor naleving van de wet zijn taken onafhankelijk van de operationele diensten van het ministerie van Defensie. Het EDPB merkt op dat het Bureau van de inspecteur-generaal voor naleving van de wet een *intern* toezichtsorgaan is.

231. Inspecties leiden tot bevindingen en, met het oog op het waarborgen van de naleving, tot maatregelen waarover rechtstreeks aan de minister van Defensie verslag wordt uitgebracht. Op basis van het rapport van het Bureau van de inspecteur-generaal voor naleving van de wet kan de minister van Defensie bevelen uitvaardigen om de nodige maatregelen te treffen teneinde het probleem te verhelpen. De plaatsvervangende viceminister van Defensie is verantwoordelijk voor de uitvoering van

politie op het gebied van het verzamelen van informatie beperkt tot uitwisselingen met buitenlandse autoriteiten.

⁹¹ Zie bijlage II, blz. 39.

deze maatregelen en moet aan de minister van Defensie verslag uitbrengen over de status van de uitvoering.

232. Op basis van een analyse van bijlage II en zonder de wettelijke bepalingen (Wet tot oprichting van het ministerie van Defensie) voor deze overwegingen te hebben ontvangen, verwelkomt het EDPB de mogelijkheid om de nodige nalevingsmaatregelen te gelasten teneinde het probleem te verhelpen. Het EDPB heeft echter twijfels over de onafhankelijkheid van het Bureau van de inspecteur-generaal voor naleving van de wet, aangezien het een bureau binnen het ministerie van Defensie is en onder rechtstreeks toezicht staat van de minister van Defensie overeenkomstig bijlage II (volgens de WP 237 "volstaat een dergelijke functionele onafhankelijkheid als zodanig niet om die toezichthoudende autoriteit voor elke beïnvloeding van buitenaf te behoeden").
233. In overeenstemming met de jurisprudentie van het EHRM, respectievelijk de WP 237 kan de inspecteur-generaal volgens de overwegingen in bijlage II het betrokken bureau om verslagen (documenten, locaties, toelichtingen) verzoeken. Verduidelijking of de betrokken bureaus verplicht zijn deze verzoeken al dan niet in te willigen en of de gevraagde documenten vertrouwelijke informatie bevatten, zoals de WP 237 vermeldt, lijkt het EDPB noodzakelijk.
234. Hoewel het EDPB verwelkomt dat zeer hooggeplaatste juristen (voormalig procureur-generaal) aan het hoofd van het Bureau van de inspecteur-generaal voor naleving van de wet staan, lijkt verduidelijking van de wijze waarop de leden van dit toezichthoudende orgaan worden benoemd noodzakelijk.

4.2.3.4 Toezicht door de Onderzoekscommissie openbare veiligheid

235. Volgens bijlage II (blz. 25) voert de inlichtingendienst voor de openbare veiligheid regelmatige en speciale inspecties uit van de activiteiten van zijn afzonderlijke bureaus en diensten (inlichtingendiensten voor de openbare veiligheid, onderafdelingen daarvan enz.). Voor de regelmatige inspecties worden een adjunct-directeur-generaal en/of een directeur als inspecteur aangewezen. Dergelijke inspecties moeten ook betrekking hebben op het beheer van persoonsgegevens.
236. Overeenkomstig overweging 163 van het ontwerpbesluit treedt de *Onderzoekscommissie openbare veiligheid* voor de inlichtingendienst voor de openbare veiligheid op als een onafhankelijk orgaan voor voorafgaand toezicht met betrekking tot zaken die verband houden met de Wet op de controle van organisaties die zich schuldig hebben gemaakt aan willekeurige massamoord⁹² en de Wet ter voorkoming van subversieve activiteiten⁹³. Het EDPB verwelkomt dat.
237. Hoewel de website van het Japanse ministerie van Justitie enige informatie bevat⁹⁴, is het EDPB niet in staat om de onafhankelijkheid van de Onderzoekscommissie openbare veiligheid zorgvuldig te beoordelen, aangezien die onafhankelijkheid niet was voorzien in de Wet tot oprichting van de

⁹² Wet op de controle van organisaties die zich schuldig hebben gemaakt aan willekeurige massamoord (Wet nr. 147 van 7 december 1999).

⁹³ Wet ter voorkoming van subversieve activiteiten (Wet nr. 240 van 21 juli 1952).

⁹⁴ Zie <http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html> (september 2018): *het extra-ministeriële orgaan "bestaat uit een voorzitter en zes leden. Zij worden geselecteerd uit personen van goed gedrag die in staat zijn een eerlijk oordeel te vellen over de controle van organisaties en personen van goed gedrag die veel kennis en ervaring hebben op het gebied van zowel het recht als de maatschappij. Zij worden door de premier benoemd en moeten door beide kamers van het Japanse parlement worden goedgekeurd. Wat betreft de toepassing van de eerder genoemde wetten (Wet ter voorkoming van subversieve activiteiten/ Wet op de controle van organisaties die zich schuldig hebben gemaakt aan willekeurige massamoord), oefenen de leden hun taken vrij onafhankelijk uit, zonder enige leiding of enig toezicht van de premier of de minister van Justitie".*

Onderzoekscommissie openbare veiligheid⁹⁵ en het Reglement van de Onderzoekscommissie openbare veiligheid⁹⁶.

4.2.3.5 Toezicht door de Nationale commissie openbare veiligheid, de prefecturale commissies openbare veiligheid en de WBPBB (uitvoerend)

238. Zie 3.1.2.2.1 (Nationale commissie openbare veiligheid), 3.1.2.2.2. (prefecturale commissies openbare veiligheid) en 3.1.2.2.4. (uitvoerend).

4.2.3.6 Toezicht door de CBP

239. Het EDPB verzoekt de Commissie om ofwel in overweging 164 te vermelden dat de CBP geen toezichtsorgaan is voor de bovengenoemde overheidsentiteiten en dat zij alleen bevoegd is voor het verhaal van natuurlijke personen, ofwel de passage in overweging 164 over de CBP te verplaatsen naar het deel "verhaal van natuurlijke personen".

4.2.4 Verhaalmechanisme

240. Voor de analyse van het nieuwe verhaalmechanisme waarover onderhandeld is, wordt verwezen naar het deel over rechtshandhaving.

241. Daarnaast is het vermeldenswaardig dat de Japanse wet voorziet in een specifieke individuele verhaalsmogelijkheid op het gebied van nationale veiligheid. Het EDPB heeft begrepen dat alle personen, met inbegrip van natuurlijke personen uit de EU, de bestuursorganen algemeen kunnen verzoeken om verstrekking, rectificatie, wissing of opschorting van het gebruik van persoonsgegevens, ook als deze om redenen van nationale veiligheid worden verwerkt. Indien een dergelijk verzoek "wordt afgewezen op grond van het feit dat de betrokken informatie wordt beschouwd als informatie die niet openbaar kan worden gemaakt", kan beroep worden ingesteld en moet de "Raad voor de beoordeling van de openbaarmaking van informatie en de bescherming van persoonsgegevens" worden geraadpleegd. Deze raad is samengesteld uit leden die door de premier met instemming van beide kamers van het parlement zijn benoemd, heeft onderzoeksbevoegdheden en sluit het beroep af met een schriftelijk verslag voor de betrokkene dat niet wettelijk bindend is maar bijna altijd wordt gevolgd⁹⁷. Volgens bijlage II zijn er slechts 2 van de 2 000 gevallen waarin een bestuursorgaan een besluit heeft genomen dat afweek van de conclusie van deze raad.⁹⁸

242. Uit de verschaftte toelichting lijkt te volgen dat de beroepsmogelijkheid niet beschikbaar is als de informatie "openbaar kan worden gemaakt" maar de betrokkene ontevreden is over de uitkomst. Het EDPB erkent deze verhaalsmogelijkheid maar wil graag meer duidelijkheid over dit laatste aspect, dat de beroepsmogelijkheid aanzienlijk zou beperken.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

⁹⁵ http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (september 2018).

⁹⁶ Artikel 28 van de Wet op de controle van organisaties die zich schuldig hebben gemaakt aan willekeurige massamoord.

⁹⁷ Bijlage II, blz. 25 en 26. Wet tot oprichting van de Raad voor de beoordeling van de openbaarmaking van informatie en de bescherming van persoonsgegevens, artikelen 4, 9 en 11.

⁹⁸ Bijlage II, voetnoot 35.