Advies 32/2021 over het ontwerpuitvoeringsbesluit van de Europese Commissie overeenkomstig Verordening (EU) 2016/679 betreffende de passende bescherming van persoonsgegevens in de Republiek Korea

Versie 1.0

Goedgekeurd op 24 september 2021

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

INHOUDSOPGAVE

Het Europees Comité voor gegevensbescherming,

gezien artikel 70, lid 1, punt 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 (**AVG**),

gezien de Overeenkomst betreffende de Europese Economische Ruimte (**EER**) en met name bijlage XI en protocol 37 daarbij, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

gezien de artikelen 12 en 22 van zijn reglement van orde,

BRENGT HET VOLGENDE ADVIES UIT:

1. SAMENVATTING

1. De Europese Commissie heeft op 16 juni 2021 op grond van de AVG de formele procedure ingeleid voor de vaststelling van een ontwerpuitvoeringsbesluit (hierna: "**ontwerpbesluit**") betreffende de passende bescherming van persoonsgegevens in de Republiek Korea overeenkomstig de wet op de bescherming van persoonsgegevens van dat land (**WBP**)[2].

2. Op dezelfde datum heeft de Europese Commissie het Europees Comité voor gegevensbescherming (**EDPB**) om advies gevraagd[3]. Het EDPB heeft de vraag of in de Republiek Korea een passend beschermingsniveau wordt geboden, beoordeeld op basis van een analyse van het ontwerpbesluit zelf en van de door de Europese Commissie ter beschikking gestelde documentatie[4].

3. Het EDPB heeft zich gericht op de beoordeling van zowel de algemene, AVG-gerelateerde aspecten van het ontwerpbesluit als de toegang van overheidsinstanties tot persoonsgegevens die vanuit de EER worden doorgegeven voor doeleinden in verband met rechtshandhaving en nationale veiligheid, met inbegrip van de voorzieningen in rechte die personen uit de EER ter beschikking staan. Het EDPB heeft ook beoordeeld of de waarborgen die het Zuid-Koreaanse rechtskader biedt, daadwerkelijk voorhanden en doeltreffend zijn.

4. Bij het opstellen van dit advies heeft het EDPB ter referentie in de eerste plaats gebruikgemaakt van de **Adequaatheidsreferentie**[5], vastgesteld in februari 2018, en van de Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen[6].

1.1. Punten van overeenstemming

5. Het hoofddoel van dit advies bestaat erin de Europese Commissie het standpunt van het EDPB mee te delen omtrent de vraag of er passende bescherming wordt geboden aan personen van wie

[1] Waar in dit advies "**lidstaten**" staat, moet "EER-lidstaten" worden gelezen.
[2] Zie persbericht: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibid.
[4] De analyse van de documentatie is gebaseerd op officiële vertalingen van de Zuid-Koreaanse regering.
[5] WP 254, Adequaatheidsreferentie, 6 februari 2018 (goedgekeurd door het EDPB, zie https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, vastgesteld op 10 november 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

persoonsgegevens worden doorgegeven aan de Republiek Korea. Het is belangrijk in te zien dat het EDPB niet verwacht dat het Zuid-Koreaanse kader voor gegevensbescherming de Europese wetgeving inzake gegevensbescherming kopieert.

6. Het EDPB herinnert er echter aan dat de wetgeving van het derde land krachtens artikel 45 AVG en volgens de rechtspraak van het Hof van Justitie van de Europese Unie (**HvJ**) in lijn moet zijn met de essentie van de fundamentele beginselen die in de AVG zijn verankerd om te kunnen worden geacht een passend beschermingsniveau te bieden. In dit verband kan worden geconcludeerd dat het Zuid-Koreaanse kader voor gegevensbescherming veel gelijkenissen vertoont met het Europese: één hoofdwet, die zowel de publieke als de private sector bestrijkt, is aangevuld met sectorspecifieke wetgevingshandelingen.

7. Inhoudelijk gesproken merkt het EDPB op dat het AVG-kader en het Zuid-Koreaanse kader voor gegevensbescherming op verschillende sleutelterreinen met elkaar in lijn zijn. Het gaat dan met name om bepaalde kernbepalingen, bijvoorbeeld inzake begrippen als “persoonsgegevens”, “verwerking” en “betrokkene” en inzake de gronden voor rechtmatige en behoorlijke verwerking voor gerechtvaardigde doeleinden, doelbinding, kwaliteit van gegevens en evenredigheid, gegevensbewaring, beveiliging en vertrouwelijkheid, transparantie en bijzondere categorieën van gegevens.

8. Daarnaast verwelkomt het EDPB de inspanningen van de Europese Commissie en de Zuid-Koreaanse autoriteiten om door middel van kennisgevingen van de Zuid-Koreaanse toezichthoudende autoriteit hiaten in het Zuid-Koreaanse gegevensbeschermingskader te dichten, zodat dit in overeenstemming wordt gebracht met de AVG en de Republiek Korea een passend beschermingsniveau biedt dat gelijkwaardig is aan het AVG-niveau (bedoelde kennisgevingen zijn overigens niet alleen van toepassing op persoonsgegevens die vanuit de EER aan de Republiek Korea worden doorgegeven). In dit verband onderstreept het EDPB het belang van deze kennisgevingen voor de beoordeling van de vraag of het beschermingsniveau in de Republiek Korea passend is. Zo bevatten zij relevante toelichtingen over enkele belangrijke waarborgen, bijvoorbeeld wat betreft het toepassingsgebied van de vrijstellingen die in de WBP zijn opgenomen voor de verwerking van gepseudonimiseerde persoonsgegevens voor wetenschappelijke, onderzoeksgerelateerde en statistische doeleinden, alsook wat betreft de voorschriften voor verdere doorgiften en de regels die van toepassing zijn in de context van de toegang van overheidsinstellingen tot persoonsgegevens.

1.2. Uitdagingen

9. Hoewel het Zuid-Koreaanse kader voor gegevensbescherming op vele punten in wezen gelijkwaardig is aan het Europese, heeft het EDPB ook moeten vaststellen dat bepaalde aspecten mogelijk nader bekeken en verduidelijkt moeten worden. Het is meer in het bijzonder van mening dat op onderstaande gebieden nader onderzoek vereist is om er zeker van te zijn dat aan de voorwaarde van een wezenlijk gelijkwaardig beschermingsniveau is voldaan, en dat de Europese Commissie de ontwikkelingen ter zake nauwgezet moet volgen.

1.2.1. Algemeen

10. Het EDPB neemt er nota van dat Kennisgeving nr. 2021-1 *de status heeft van een bestuursrechtelijk voorschrift dat rechtens bindend is voor de verwerkingsverantwoordelijke voor persoonsgegevens, in de zin dat elke schending van de kennisgeving kan worden beschouwd als een schending van de betreffende bepalingen van de WBP*[7]. De kennisgeving bevat feitelijk echter geen aanvullende regels maar licht eerder toe hoe de tekst van de WBP moet worden uitgelegd met het oog op de toepassing ervan. Daarom, en in het licht van het algemene belang van die wet (met name de pseudonimiseringsbepalingen, die – zo begrijpt het EDPB – het voorwerp van lopende rechtszaken

[7] Zie hoofdstuk I van bijlage I bij het ontwerpbesluit.

vormen), verzoekt het EDPB de Europese Commissie om aanvullende informatie over het bindende karakter, de afdwingbaarheid en de geldigheid van Kennisgeving nr. 2021-1 en doet het de aanbeveling om de naleving van deze kennisgeving in de praktijk zorgvuldig te monitoren. De Europese Commissie wordt verzocht daarbij met name te letten op de manier waarop niet alleen de Zuid-Koreaanse toezichthoudende autoriteit maar ook de rechter de kennisgeving toepast, vooral in gevallen waarin de aanname dat het Zuid-Koreaanse rechtskader een gelijkwaardig beschermingsniveau biedt is gebaseerd op de toelichtingen in die kennisgeving zelf.

1.2.2. Algemene aspecten van gegevensbescherming

11. Wat het toepassingsgebied van het adequaatheidsbesluit betreft, merkt het EDPB op dat daartoe ook doorgiften vanuit het EER-rechtskader aan zowel publieke als private "verwerkingsverantwoordelijken voor persoonsgegevens" (hierna: "PG-verwerkingsverantwoordelijken") zullen behoren die onder de reikwijdte van de WBP vallen. Het EDPB begrijpt dat onder de term "verwerkingsverantwoordelijke" ook entiteiten worden begrepen die optreden als verwerker in de zin van de AVG. Om misverstanden te voorkomen verzoekt het EDPB de Europese Commissie duidelijker aan te geven dat het adequaatheidsbesluit ook betrekking zal hebben op doorgiften aan verwerkers in de Republiek Korea.

12. Een belangrijk punt dat het EDPB onder de aandacht wil brengen betreft het begrip "gepseudonimiseerde gegevens" zoals gebezigd in het Zuid-Koreaanse kader voor gegevensbescherming. Krachtens Zuid-Koreaans recht is de verwerking van gepseudonimiseerde persoonsgegevens vrijgesteld van een aantal belangrijke voorschriften, onder meer op het gebied van de individuele rechten van betrokkenen en gegevensbewaring. Volgens de Europese Commissie gelden deze vrijstellingen alleen wanneer de gepseudonimiseerde gegevens worden verwerkt voor statistische doeleinden of met het oog op wetenschappelijk onderzoek of archivering in het algemeen belang. Deze aanname is echter hoofdzakelijk gebaseerd op Kennisgeving nr. 2021-1, wat de reeds vermelde noodzaak van aanvullende informatie over en monitoring van het bindende karakter, de afdwingbaarheid en de geldigheid van deze kennisgeving ook in dit verband zeer relevant maakt. Daarnaast wordt de Europese Commissie verzocht om nader onderzoek te doen naar de gevolgen die pseudonimisering naar Zuid-Koreaans recht heeft en, wat het EDPB nog belangrijker lijkt, de mogelijke gevolgen van pseudonimisering voor de grondrechten en fundamentele vrijheden van betrokkenen van wie persoonsgegevens op basis van het adequaatheidsbesluit aan de Republiek Korea worden doorgegeven. Het EDPB verzoekt de Europese Commissie in het bijzonder om nader onderzoek te doen naar de afwijkingen vervat in artikel 28, lid 7, WBP en artikel 40, lid 3, van de wet op het gebruik en de bescherming van kredietinformatie, en zorgvuldig de toepassing van deze bepalingen te monitoren en de relevante rechtspraak te volgen om er zeker van te zijn dat de rechten van betrokkenen niet onnodig worden beperkt wanneer op basis van het adequaatheidsbesluit doorgegeven persoonsgegevens voor de voornoemde doeleinden worden verwerkt.

13. Het EDPB merkt verder op dat het recht om toestemming voor gegevensverwerking in te trekken volgens de Zuid-Koreaanse wetgeving alleen bestaat in specifieke omstandigheden. Het verzoekt de Europese Commissie derhalve om nader onderzoek te doen naar de gevolgen van het ontbreken van een algemeen recht op het intrekken van toestemming, en om aanvullende garanties te geven dat er steeds een minimumniveau aan gegevensbescherming wordt gewaarborgd. Daartoe zou ook, voor zover nodig, duidelijkheid moeten worden verschaft over de rol die het recht op opschorting in de WBP speelt bij gebrek aan een algemeen recht om toestemming in te trekken.

14. Wat verdere doorgifte betreft, erkent het EDPB dat gegevens doorgaans door een in de Republiek Korea gevestigde PG-verwerkingsverantwoordelijke worden doorgegeven aan een in een derde land gevestigde ontvanger op basis van de geïnformeerde toestemming van de betrokkene en dat Kennisgeving nr. 2021-1 erin voorziet dat personen in kennis worden gesteld van het derde land waaraan hun gegevens worden verstrekt. Evenwel verzoekt het EDPB de Europese Commissie om ervoor te zorgen dat de informatie die aan de betrokkene wordt verstrekt, ook inlichtingen bevat over

de risico's die gepaard kunnen gaan met doorgiften naar het derde land wegens het ontbreken van adequate bescherming in dat land en het gebrek aan passende waarborgen. Voorts zou het EDPB graag zien dat er in het adequaatheidsbesluit wordt verzekerd dat persoonsgegevens niet door een in de Republiek Korea gevestigde PG-verwerkingsverantwoordelijke aan een derde land worden doorgegeven wanneer er volgens de AVG geen geldige toestemming zou kunnen worden verleend, bijvoorbeeld wegens machtsongelijkheid.

15. De formele procedure voor de benoeming van de leden van de Zuid-Koreaanse toezichthoudende autoriteit is in overeenstemming met de AVG en voldoet derhalve aan het criterium van gelijkwaardigheid met het EER-rechtskader. Toch zou het EPDB het toejuichen wanneer de Europese Commissie eventuele ontwikkelingen die de onafhankelijkheid van de toezichthoudende autoriteit kunnen aantasten, nauwgezet zou volgen.

16. Wat de begroting betreft, worden – opnieuw uitgaande van de informatie die door de Europese Commissie is verstrekt – geen specifieke details gegeven met betrekking tot de personele en financiële middelen die aan de Zuid-Koreaanse toezichthoudende autoriteit, de commissie voor de bescherming van persoonsgegevens, zijn toegewezen. Het EDPB zou aanvullende informatie over deze twee belangrijke punten in het ontwerpbesluit dan ook verwelkomen.

1.2.3. Toegang van overheidsinstanties tot gegevens die aan de Republiek Korea worden doorgegeven

17. Het EDPB heeft het Zuid-Koreaanse rechtskader tevens geanalyseerd vanuit het oogpunt van de toegang van de overheid tot persoonsgegevens die vanuit de EER aan de Republiek Korea worden doorgegeven ten behoeve van rechtshandhaving en nationale veiligheid. Ondanks de verklaringen en waarborgen die door de Zuid-Koreaanse regering zijn gegeven, zoals weergegeven in bijlage II bij het ontwerpbesluit, zijn er een aantal aspecten die verduidelijkt moeten worden of reden tot bezorgdheid geven.

18. Het EDPB merkt op dat de WBP onbeperkt van toepassing is op het gebied van rechtshandhaving, maar dat gegevensverwerking ten behoeve van de nationale veiligheid krachtens die wet aan minder voorschriften onderhevig is.

19. Wat de vrijwillige verstrekking van persoonsgegevens door telecomaanbieders aan nationale veiligheidsdiensten betreft, is het EDPB bezorgd over de onduidelijke relatie tussen enerzijds hoofdstuk III van bijlage I bij het ontwerpbesluit, waarin wordt aangegeven dat telecomaanbieders de betrokkene er in beginsel van in kennis moeten stellen wanneer zij vrijwillig aan een informatieverzoek voldoen, en anderzijds artikel 58, lid 1, punt 2, WBP, dat voorziet in een gedeeltelijke vrijstelling van de kennisgevingsplicht in geval van informatieverzoeken voor nationaleveiligheidsdoeleinden. Dit zou van informatievereisten een dode letter maken en het voor betrokkenen een stuk moeilijker maken om hun gegevensbeschermingsrechten te doen gelden en met name om in beroep te gaan bij de rechter.

20. Hoewel dit niet expliciet in het ontwerpbesluit staat vermeld, maakt het EDPB uit de uitleg van de Europese Commissie op dat volgens het Zuid-Koreaanse recht het in bulk onderscheppen van telecomgegevens niet is toegestaan. De recente rechtspraak van het Europees Hof voor de Rechten van de Mens (**EHRM**) inzake regelingen voor onderschepping in bulk is daarom niet rechtstreeks van belang voor het beoordelen van het gegevensbeschermingsniveau in de Republiek Korea.

21. Het ontwerpbesluit bevat geen enkele informatie over het Zuid-Koreaanse rechtskader voor verdere doorgiften voor nationaleveiligheidsdoeleinden. Hoewel het EDPB begrijpt dat verdere doorgiften voor nationaleveiligheidsdoeleinden naar de opvatting van de Europese Commissie afdoende geregeld worden door de algemene waarborgen en beginselen die voortvloeien uit het grondwettelijk kader en de WBP, vraagt het zich af of hiermee wel wordt voldaan aan het vereiste van

nauwkeurigheid en duidelijkheid van de wet en of daarin doeltreffende en afdwingbare waarborgen zijn verankerd. De waarborgen waarnaar de Europese Commissie verwijst, zijn heel algemeen en zien niet – in het kader van een rechtsgrond – op de specifieke omstandigheden en voorwaarden waaronder verdere doorgifte voor nationaleveiligheidsdoeleinden mag plaatsvinden. In dit verband merkt het EDPB ook op dat de Europese Commissie niet is nagegaan of de Republiek Korea wellicht overeenkomsten met derde landen of internationale organisaties heeft gesloten die voorzien in specifieke voorschriften voor de internationale doorgifte van persoonsgegevens door rechtshandhavingsautoriteiten en/of inlichtingendiensten aan derde landen. Het EDPB meent dat het sluiten van bilaterale of multilaterale overeenkomsten met derde landen ten behoeve van samenwerking op het gebied van rechtshandhaving en inlichtingenactiviteiten gevolgen kan hebben voor het beschermingsniveau dat door het beoordeelde Zuid-Koreaanse rechtskader voor gegevensbescherming wordt geboden.

22. Het EDPB neemt er nota van dat het toezicht op zowel instanties belast met strafrechtelijke handhaving als nationale veiligheidsdiensten wordt gewaarborgd door een combinatie van verschillende interne en externe organen, met name de Zuid-Koreaanse toezichthoudende autoriteit, die beschikt over voldoende uitvoeringsbevoegdheden.

23. Voorzieningen in rechte en verhaalsmogelijkheden zijn alleen doeltreffend als betrokkenen zich kunnen wenden tot een bevoegde instantie die voldoet aan de vereisten van artikel 47 van het Handvest van de grondrechten van de Europese Unie (hierna: "**Handvest**"), d.w.z. een instantie die bevoegd is om te bepalen dat gegevensverwerking plaatsvindt en te beoordelen of deze rechtmatig is, en die beschikt over afdwingbare corrigerende bevoegdheden ingeval de verwerking onrechtmatig blijkt. Tegen deze achtergrond verzoekt het EDPB de Europese Commissie om duidelijk te maken of voor het indienen van een klacht bij de Zuid-Koreaanse toezichthoudende autoriteit of het instellen van een rechtsvordering inhoudelijke en/of procedurele eisen gelden, bijvoorbeeld met betrekking tot bewijslast, en of personen uit de EER aan dergelijke eisen kunnen voldoen.

1.3. Conclusie

24. Het EDPB is van mening dat dit adequaatheidsbesluit van het allergrootste belang is, ook gezien het feit dat – behoudens de uitzonderingen waarop in dit advies wordt gewezen – het op doorgiften in zowel de publieke als de private sector betrekking heeft.

25. Het EDPB verwelkomt de inspanningen van de Europese Commissie en de Zuid-Koreaanse autoriteiten om het Zuid-Koreaanse rechtskader in overeenstemming te brengen met het Europese. De verbeteringen die de Zuid-Koreaanse toezichthoudende autoriteit door middel van Kennisgeving nr. 2021-1 heeft doorgevoerd om enkele van de verschillen tussen de twee kaders te overbruggen, zijn zeer belangrijk en zijn goed onthaald. Het EDPB merkt echter op dat er nog steeds een aantal punten van zorg bestaan, onder meer met betrekking tot Kennisgeving nr. 2021-1, en dat andere aspecten nadere toelichting behoeven. De Europese Commissie wordt aanbevolen om die bezorgdheid weg te nemen en de gevraagde toelichting te verschaffen, alsook om aanvullende informatie en uitleg te geven met betrekking tot de punten die in dit advies worden aangekaart.

2. INLEIDING

2.1. Zuid-Koreaans kader voor gegevensbescherming

26. De wetgeving inzake gegevensbescherming van de Republiek Korea (hierna ook: "**Zuid-Korea**") bestaat in de eerste plaats uit de wet op de bescherming van persoonsgegevens (wet nr. 10465 van 29 maart 2011, zoals laatstelijk gewijzigd bij wet nr. 16930 van 4 februari 2020 – hierna: "**WBP**"). Deze wet is aangevuld met een uitvoeringsbesluit (presidentieel besluit nr. 23169 van 29 september 2011,

zoals laatstelijk gewijzigd bij presidentieel besluit nr. 30892 van 4 augustus 2020 – hierna: "**WBP-uitvoeringsbesluit**"), dat rechtens bindend en afdwingbaar is.

27. Naast de WBP bevat het Zuid-Koreaanse gegevensbeschermingskader ook kennisgevingen van de Zuid-Koreaanse toezichthoudende autoriteit, de commissie voor de bescherming van persoonsgegevens (hierna: "**toezichthouder**"), waarin aanvullende regels worden gegeven voor de interpretatie en toepassing van de WBP. De toezichthouder heeft onlangs Kennisgeving nr. 2021-1 van 21 januari 2021 vastgesteld tot wijziging van Kennisgeving nr. 2020-10 van 1 september 2020 (hierna: "**Kennisgeving nr. 2021-1**") betreffende de interpretatie, toepassing en handhaving van bepaalde bepalingen van de WBP. De kennisgeving is het resultaat van adequaatheidsbesprekingen tussen de Zuid-Koreaanse autoriteiten en de Europese Commissie. In dit document wordt toegelicht hoe specifieke bepalingen van de WBP moeten worden toegepast, onder meer wat betreft de verwerking van persoonsgegevens die op basis van het beoogde adequaatheidsbesluit naar Zuid-Korea worden doorgegeven[8]. Het *heeft de status van een bestuursrechtelijk voorschrift dat rechtens bindend is voor de PG-verwerkingsverantwoordelijke, in de zin dat elke schending van de kennisgeving kan worden beschouwd als een schending van de betreffende bepalingen van de WBP*.[9] Het EDPB merkt in dit verband op dat in het ontwerpbesluit weliswaar wordt gesproken over "aanvullende regels", maar dat de kennisgeving feitelijk geen aanvullende regels bevat. Er wordt eerder in toegelicht hoe de tekst van de WBP moet worden uitgelegd met het oog op de toepassing ervan, in het bijzonder met betrekking tot persoonsgegevens die vanuit de EER worden doorgegeven. Tegen deze achtergrond doet het EDBP de aanbeveling om de naleving van Kennisgeving nr. 2021-1 in de praktijk zorgvuldig te monitoren en daarbij met name te letten op de manier waarop niet alleen de toezichthouder maar ook de rechter de kennisgeving toepast, vooral in gevallen waarin de aanname dat het Zuid-Koreaanse rechtskader een gelijkwaardig beschermingsniveau biedt is gebaseerd op de toelichtingen in die kennisgeving zelf.

28. Andere relevante wetgeving in het Zuid-Koreaanse rechtskader regelt de verwerking van persoonsgegevens in specifieke bedrijfstakken. Het gaat bijvoorbeeld om:

    - de wet op het gebruik en de bescherming van kredietinformatie (hierna: "**kredietinformatiewet**") en het bijbehorende uitvoeringsbesluit (hierna: "**uitvoeringsbesluit bij de kredietinformatiewet**"), die specifieke voorschriften bevatten voor handelsondernemingen en gespecialiseerde entiteiten (zoals kredietbeoordelingsbureaus en financiële instellingen) inzake het verwerken van gegevens betreffende persoonlijke kredieten die noodzakelijk zijn om de kredietwaardigheid van partijen bij financiële of commerciële transacties te kunnen bepalen;

    - de wet op bevordering van het gebruik van informatie- en communicatienetwerken en gegevensbescherming (hierna: "**netwerkwet**"), en

    - de wet op bescherming van de privacy van communicatie (hierna: "**privacywet**").

29. Op het gebied van overheidstoegang heeft het EDPB naast de relevante bepalingen van de WBP en de privacywet ook nog enkele andere wetgevingsstukken in zijn beoordeling meegenomen, namelijk de wet op de strafvordering (hierna: "**strafvorderingswet**"), de wet op het telecombedrijf (hierna: "**telecomwet**"), de wet op het melden en gebruiken van gespecificeerde informatie over financiële transacties (hierna: "**wet financiële transacties**") en de **wet op de nationale inlichtingendienst**.

[8] Zie hoofdstuk I van bijlage I bij het ontwerpbesluit.
[9] Ibid.

2.2. Reikwijdte van de beoordeling van het EDPB

30. Het ontwerpbesluit van de Europese Commissie is het resultaat van een beoordeling van het Zuid-Koreaanse kader voor gegevensbescherming en daaropvolgende besprekingen met de Zuid-Koreaanse regering. Overeenkomstig artikel 70, lid 1, punt s), AVG wordt 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 voorstellen doet om die tekortkomingen aan te pakken.

31. Teneinde onnodige herhaling te voorkomen en te helpen bij de beoordeling van het Zuid-Koreaanse rechtskader heeft het EDPB ervoor gekozen om zijn analyse en advies te richten op enkele specifieke punten die in het ontwerpbesluit aan de orde komen. Wanneer er geen reden bestond om aan te nemen dat de Zuid-Koreaanse wetgeving niet in wezen gelijkwaardig is aan de wetgeving in de EER, zijn de feitelijke bevindingen en vaststellingen van de Commissie over het algemeen niet weergegeven. Daarnaast, en in lijn met de rechtspraak van het HvJ, heeft een zeer belangrijk deel van de analyse betrekking op de wettelijke voorschriften voor de toegang van het nationale veiligheidsapparaat tot aan de Republiek Korea doorgegeven persoonsgegevens en de wijze waarop een en ander in de praktijk verloopt.

32. Bij zijn beoordeling heeft het EDPB rekening gehouden met het toepasselijke Europese kader voor gegevensbescherming, waaronder de artikelen 7, 8 en 47 van het Handvest, die respectievelijk het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, het recht op bescherming van persoonsgegevens en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht waarborgen, en artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM), dat het recht op eerbiediging van het privéleven en van het familie- en gezinsleven beschermt. Daarnaast heeft het EDPB zowel naar de vereisten van de AVG als naar de relevante rechtspraak gekeken.

33. Deze analyse moet leiden tot een advies aan de Europese Commissie ter beoordeling van de vraag of het in de Republiek Korea geboden beschermingsniveau passend is. Het begrip “passend beschermingsniveau”, dat reeds bestond in Richtlijn 95/46/EG, is door het HvJ verder uitgewerkt. Het is belangrijk om te herinneren aan de norm die het HvJ in het arrest Schrems I heeft gesteld, namelijk dat het “niveau van bescherming” in het derde land weliswaar “in grote lijnen overeenkomt met” het in de EU gewaarborgde niveau, maar dat “*de middelen waarmee dat derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders [kunnen] zijn dan die welke binnen de Unie worden ingezet*”[10]. Het doel is dus niet om de Europese wetgeving punt voor punt te weerspiegelen, maar om de essentiële en kernvereisten van de onderzochte wetgeving vast te stellen. Een passend beschermingsniveau kan worden bereikt door een combinatie van rechten voor de betrokkenen, verplichtingen voor gegevensverwerkers of verwerkingsverantwoordelijken en toezicht door onafhankelijke instanties. Regels voor gegevensbescherming zijn echter alleen doeltreffend als zij afdwingbaar zijn en in de praktijk worden nageleefd. Daarom moet niet alleen worden gekeken naar de inhoud van de regels die van toepassing zijn op de doorgifte van persoonsgegevens aan een derde land of internationale organisatie, maar ook naar het systeem waarmee de doeltreffendheid van die regels wordt gewaarborgd. Voor de doeltreffendheid van gegevensbeschermingsregels zijn efficiënte handhavingsmechanismen van eminent belang[11].

[10] Arrest van het Hof van Justitie van 6 oktober 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, punten 73 en 74.
[11] WP 254, blz. 2.

2.3. Algemene opmerkingen en punten van zorg

2.3.1. Internationale verbintenissen die de Republiek Korea is aangegaan

34. Overeenkomstig artikel 45, lid 2, punt c), AVG en de adequaatheidsreferentie[12] moet de Europese Commissie bij de beoordeling van de passendheid 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.

35. Zuid-Korea is partij bij meerdere internationale overeenkomsten die het recht op privacy waarborgen, zoals het Internationaal Verdrag inzake burgerrechten en politieke rechten (artikel 17), het Verdrag inzake de rechten van personen met een handicap (artikel 22) en het Verdrag inzake de rechten van het kind (artikel 16). Bovendien houdt Zuid-Korea zich als lid van de OESO aan het privacykader van die organisatie, in het bijzonder de Richtsnoeren inzake de bescherming van de privacy en het grensoverschrijdende verkeer van persoonsgegevens.

36. Het EDPB heeft ook nota genomen van de deelname van Zuid-Korea als waarnemer aan de werkzaamheden van het Raadgevend Comité voor Verdrag 108(+) van de Raad van Europa, hoewel het land nog niet heeft besloten om al dan niet toe te treden.

2.3.2. Toepassingsgebied van het adequaatheidsbesluit

37. Overeenkomstig overweging 5 van het ontwerpbesluit concludeert de Europese Commissie dat de Republiek Korea een passend beschermingsniveau waarborgt voor persoonsgegevens die door een in de Unie gevestigde verwerkingsverantwoordelijke of verwerker worden doorgegeven aan PG-verwerkingsverantwoordelijken (bijv. natuurlijke of rechtspersonen, organisaties, overheidsinstellingen) die onder het toepassingsgebied van de WBP vallen, behalve wat betreft de verwerking van persoonsgegevens voor zendingswerk van religieuze organisaties en voor kandidaatstellingen door politieke partijen[13] en de verwerking van informatie over persoonlijke kredieten overeenkomstig de kredietinformatiewet door verwerkingsverantwoordelijken die onder toezicht van de commissie Financiële Diensten staan.

38. Het EDPB merkt op dat het adequaatheidsbesluit betrekking zal hebben op doorgiften vanuit het EER-rechtskader aan zowel publieke als private “PG-verwerkingsverantwoordelijken” die onder het toepassingsgebied van de WBP vallen. Het EDPB begrijpt dat onder de term “PG-verwerkingsverantwoordelijke” ook entiteiten vallen die optreden als verwerker in de zin van de AVG, aangezien de WBP evenzeer op hen van toepassing zal zijn, en dat er specifieke verplichtingen gelden wanneer een PG-verwerkingsverantwoordelijke (de “uitbesteder”) voor de verwerking van persoonsgegevens een derde partij (de “dienstverlener”) contracteert. Om misverstanden te voorkomen verzoekt het EDPB de Europese Commissie evenwel duidelijker aan te geven dat het adequaatheidsbesluit ook betrekking zal hebben op doorgiften aan verwerkers in Zuid-Korea, en dat ook in die gevallen het beschermingsniveau voor uit de EER doorgegeven persoonsgegevens niet in het gedrang zal komen.

39. Het feit dat het adequaatheidsbesluit ook betrekking zal hebben op doorgiften van persoonsgegevens tussen overheidsinstanties, betekent bovendien dat het ook zal gelden voor doorgiften tussen toezichthoudende autoriteiten voor gegevensbescherming. Het EDBP verzoekt de Europese Commissie ter verduidelijking hierop specifiek in te gaan.

[12] WP 254, blz. 2.

[13] Voor meer context zie afdeling 3.1.2 van dit advies.

40. Wat betreft de entiteiten die van het toepassingsgebied van het adequaatheidsbesluit zijn uitgesloten, wijst het EDPB erop dat het de duidelijkheid van het besluit ten goede zou komen als duidelijker wordt aangegeven welke "commerciële organisaties" onder toezicht van de toezichthouder staan (artikel 45, lid 3, van de kredietinformatiewet). In de EER gevestigde verwerkingsverantwoordelijken en verwerkers kunnen dan eenvoudig vaststellen of een ontvanger onder het adequaatheidsbesluit valt voordat zij persoonsgegevens doorgeven aan entiteiten waarop de kredietinformatiewet van toepassing is, of zij worden er tenminste op gewezen dat ze dit moeten nagaan.

41. Het EDPB maakt uit de aanvullende toelichtingen van de Europese Commissie op dat de financiële-inlichtingeneenheid van Zuid-Korea (**KOFIU**), die ressorteert onder de commissie Financiële Diensten en overeenkomstig de wet financiële transacties toezicht houdt op de bestrijding van witwassen en terrorismefinanciering[14], eveneens van het toepassingsgebied van het adequaatheidsbesluit is uitgesloten, omdat deze eenheid alleen rechtsbevoegdheid heeft ten aanzien van financiële instellingen die daar zelf buiten vallen. In artikel 1, lid 2, punt c), van het ontwerpbesluit worden echter alleen PG-verwerkingsverantwoordelijken van het toepassingsgebied ervan uitgesloten die onder toezicht van de commissie Financiële Diensten staan en informatie over persoonlijke kredieten verwerken overeenkomstig de kredietinformatiewet. In het licht daarvan verzoekt het EDPB de Europese Commissie om te verduidelijken of de KOFIU en de gegevensverwerkingsactiviteiten die door deze eenheid zelf worden verricht, al dan niet onder het adequaatheidsbesluit vallen.

3. ALGEMENE ASPECTEN VAN GEGEVENSBESCHERMING

3.1. Inhoudelijke beginselen

42. Hoofdstuk 3 van de adequaatheidsreferentie is gewijd aan "inhoudelijke beginselen". Het systeem van een derde land of internationale organisatie kan alleen dan worden geacht een beschermingsniveau te bieden dat in wezen gelijkwaardig is aan het door de EU-wetgeving gewaarborgde niveau, als het deze beginselen bevat.

43. Hoewel het recht op bescherming van persoonsgegevens niet uitdrukkelijk in de Zuid-Koreaanse grondwet is verankerd, wordt het erkend als een basisrecht dat voortvloeit uit het grondwettelijke recht op menselijke waardigheid en het nastreven van geluk (artikel 10), op een privéleven (artikel 17) en op communicatieprivacy (artikel 18). Dit is zowel door het hooggerechtshof als door het grondwettelijk hof bevestigd. In het ontwerpbesluit van de Europese Commissie wordt verwezen naar de betreffende arresten[15]. Het EDPB neemt nota van deze erkenning en leidt hieruit af dat gegevensbescherming als basisrecht ingevolge artikel 37 van de Zuid-Koreaanse grondwet "*alleen bij wet kan worden beperkt en uitsluitend wanneer dit noodzakelijk is voor de nationale veiligheid, het handhaven van recht en orde of het maatschappelijk welzijn*" en dat "*zelfs wanneer een dergelijke beperking wordt opgelegd, deze niet de essentie van de vrijheid of het recht mag aantasten*".

44. Volgens de Europese Commissie[16] heeft het grondwettelijk hof beslist dat basisrechten ook voor vreemdelingen gelden. Volgens officiële verklaringen van de Zuid-Koreaanse regering[17] is weliswaar nog geen zaak voor de rechter gebracht die specifiek betrekking heeft op het recht op privacy van vreemdelingen, maar wordt door rechtsgeleerden algemeen aanvaard dat in de artikelen 12 tot en met 22 van de grondwet "rechten van mensen" zijn vastgelegd. Bovendien heeft de Republiek Korea een reeks wetten op het gebied van gegevensbescherming vastgesteld die waarborgen bieden voor alle personen, ongeacht hun nationaliteit, zoals de WBP. In dit opzicht neemt het EDPB nota van het

[14] Zie bijlage II, afdeling 2.2.3.1.
[15] Zie overweging 8 van het ontwerpbesluit en de relevante rechtspraak in voetnoot 10 ervan. Van deze rechtspraak zijn alleen samenvattingen in het Engels beschikbaar.
[16] Zie overweging 9 van het ontwerpbesluit.
[17] Afdeling 1.1 van bijlage II bij het ontwerpbesluit.

feit dat artikel 6, lid 2, van de grondwet bepaalt dat vreemdelingen de bij internationaal recht en internationale verdragen voorgeschreven status hebben en dat een "buitenlander" volgens de in het ontwerpbesluit genoemde rechtspraak de houder van "basisrechten" kan zijn. Gezien het belang van de erkenning van het recht op gegevensbescherming voor vreemdelingen, wijst het EDPB de Europese Commissie erop dat de rechtspraak verder moet worden gevolgd om er zeker van te zijn dat gegevensbescherming niet alleen voor Zuid-Koreaanse burgers maar voor alle betrokkenen als basisrecht wordt erkend, zodat het beschermingsniveau dat door de AVG voor natuurlijke personen wordt gewaarborgd, niet wordt ondergraven wanneer op basis van het adequaatheidsbesluit persoonsgegevens naar Zuid-Korea worden doorgeven.

3.1.1. Begrippen

45. Op basis van de adequaatheidsreferentie moeten in het rechtskader van het derde land bepaalde basisbegrippen en/of beginselen inzake gegevensbescherming zijn opgenomen. Hoewel deze geen kopie hoeven te zijn van de terminologie die in de AVG wordt gehanteerd, moeten zij wel een afspiegeling vormen van de begrippen in de Europese wetgeving wel weerspiegelen inzake gegevensbescherming en daarmee consistent zijn. In de AVG zijn bijvoorbeeld de volgende belangrijke begrippen opgenomen: "persoonsgegevens", "verwerking van persoonsgegevens", "verwerkingsverantwoordelijke", "verwerker", "ontvanger" en "gevoelige gegevens".[18]

46. De WBP bevat een aantal definities die grote gelijkenissen vertonen met definities in de AVG, bijvoorbeeld van "persoonsgegevens", "verwerking" en "betrokkene".

3.1.1.1. Het begrip "gepseudonimiseerde gegevens"

47. In de WBP wordt onder meer in artikel 2, lid 1, het begrip "persoonsgegevens" gedefinieerd als informatie over een levende persoon a) aan de hand waarvan die persoon kan worden geïdentificeerd: volledige naam, registratienummer als ingezetene, afbeeldingen enz., of b) die misschien op zichzelf niet volstaat om een bepaalde persoon te identificeren maar gemakkelijk met andere informatie kan worden gecombineerd waardoor dat wel mogelijk wordt. Het antwoord op de vraag of informatie zich gemakkelijk met andere informatie laat combineren, is afhankelijk van de tijd, kosten, technologie enz. die redelijkerwijs nodig zijn voor het identificeren van een persoon en van de waarschijnlijkheid dat die andere informatie kan worden verkregen.

48. Ingevolge artikel 2, lid 1, punt c), WBP worden ook "gepseudonimiseerde gegevens" als persoonsgegevens beschouwd. "Gepseudonimiseerde gegevens" worden gedefinieerd als informatie zoals bedoeld onder a) of b) hierboven die is gepseudonimiseerd overeenkomstig de leden 1 en 2 en daardoor niet meer kan worden gebruikt voor het identificeren van een bepaalde persoon zonder dat eerst met behulp van andere informatie de originele staat ervan wordt hersteld. Volledig geanonimiseerde gegevens, daarentegen, vallen buiten het toepassingsgebied van de WBP. Ingevolge artikel 58, lid 2, WBP is de wet niet van toepassing op gegevens waarmee een bepaalde persoon redelijkerwijs niet langer kan worden geïdentificeerd, ook al worden zij gecombineerd met andere informatie, rekening houdend met factoren als tijd, kosten, technologie enz.

49. De Europese Commissie stelt in overweging 17 van het ontwerpbesluit dat dit overeenkomt met het materiële toepassingsgebied van de AVG en met de begrippen "persoonsgegevens", "pseudonimisering" en "anonieme gegevens" zoals gebruikt in die verordening.

50. Ingevolge artikel 28, lid 7, WBP gelden de artikelen 20, 21 en 27, artikel 34, lid 1, de artikelen 35, 36 en 37, en artikel 39, leden 3, 4, 6, 7 en 8, echter niet voor gepseudonimiseerde persoonsgegevens.

[18] WP 254, blz. 4.

51. In het ontwerpbesluit stelt de Europese Commissie dat artikel 28, lid 7, WBP alleen geldt voor gepseudonimiseerde persoonsgegevens die worden verwerkt voor statistische doeleinden of met het oog op wetenschappelijk onderzoek of archivering in het algemeen belang.[19] Dit volgt echter niet uit de letterlijke tekst van de wet maar uit de toelichtingen in Kennisgeving nr. 2021-1.[20] Het EDPB erkent dat uit de opbouw en ratio van de WBP zou kunnen worden afgeleid dat artikel 28, lid 2, logischerwijs zo moet worden uitgelegd dat het ook van toepassing is op artikel 28, lid 7. Niettemin verzoekt het de Europese Commissie – gezien het belang van Kennisgeving nr. 2021-1 voor haar beoordeling van de vraag of persoonsgegevens in de Republiek Korea op passende wijze worden beschermd, en om elke twijfel weg te nemen – aanvullende informatie te verstrekken over het bindende karakter, de afdwingbaarheid en de geldigheid van Kennisgeving nr. 2021-1 en te monitoren hoe deze kennisgeving in deze specifieke context wordt toegepast.

52. Het EDPB brengt in dit verband in herinnering dat pseudonimisering in het kader van de AVG wordt gezien als een aanbevolen veiligheidsmaatregel. Met andere woorden: in het kader van de AVG gelden ook gepseudonimiseerde persoonsgegevens als persoonsgegevens waarop de AVG volledig van toepassing is. Op basis van het voorgaande maakt het EDPB zich zorgen dat het beschermingsniveau voor gepseudonimiseerde persoonsgegevens mogelijk wordt ondergraven wanneer deze gegevens aan Zuid-Korea worden doorgegeven. Het verzoekt de Europese Commissie derhalve om nader onderzoek te doen naar de gevolgen die pseudonimisering volgens de WBP heeft, en, wat het EDPS nog belangrijker lijkt, naar de mogelijke gevolgen van pseudonimisering voor de grondrechten en fundamentele vrijheden van betrokkenen van wie persoonsgegevens op basis van het adequaatheidsbesluit aan de Republiek Korea worden doorgegeven. Bijgevolg roept het EDPB de Europese Commissie ertoe op te verzekeren dat het beschermingsniveau voor persoonsgegevens van betrokkenen in de EER na doorgifte aan de Republiek Korea niet wordt verlaagd, zelfs niet wanneer de doorgegeven persoonsgegevens zijn gepseudonimiseerd.

3.1.1.2. *Het begrip "PG-verwerkingsverantwoordelijke"*

53. Volgens artikel 2, lid 5, WBP wordt onder "PG-verwerkingsverantwoordelijke" het volgende verstaan: een overheidsinstelling, rechtspersoon, organisatie, persoon enz. die "*als onderdeel van zijn/haar activiteiten*" direct of indirect persoonsgegevens verwerkt voor het beheer van bestanden met persoonsgegevens. In de aanvullende waarborgen die in Kennisgeving nr. 2021-1 zijn omschreven, wordt het begrip "PG-verwerkingsverantwoordelijke" echter gedefinieerd als een overheidsinstelling, rechtspersoon, organisatie, persoon enz. die "*voor bedrijfsdoeleinden*" direct of indirect persoonsgegevens verwerkt voor het beheer van bestanden met persoonsgegevens. In voetnoot 272 van het ontwerpbesluit staat daarentegen de volgende toelichting bij het begrip "PG-verwerkingsverantwoordelijke": "*Zoals gedefinieerd in artikel 2 WBP, dat wil zeggen: een overheidsinstelling, rechtspersoon, organisatie, persoon enz. die 'voor officiële of bedrijfsdoeleinden' direct of indirect persoonsgegevens verwerkt voor het beheer van bestanden met persoonsgegevens.*"

54. Het EDPB erkent dat deze inconsistenties mogelijk te wijten zijn aan de vertalingen van de originele teksten die door de Zuid-Koreaanse autoriteiten zijn verstrekt, en verzoekt de Europese Commissie om regelmatig de kwaliteit en juistheid van de vertalingen te verifiëren. Om te kunnen beoordelen of het beschermingsniveau dat door het Zuid-Koreaanse rechtskader wordt geboden in wezen gelijkwaardig is aan het Europese, moeten de verwerkingsdoeleinden die onder het materiële toepassingsgebied van de WBP vallen echter duidelijk worden omschreven. Het EDPB merkt in dit verband verder op dat de WBP met betrekking tot de begrippen "verwerkingsverantwoordelijke" en "verwerker" andere terminologie gebruikt dan de AVG en verzoekt de Europese Commissie om

[19] Zie onder andere overweging 82 van het ontwerpbesluit.
[20] Hoofdstuk 4 van bijlage I bij het ontwerpbesluit.

duidelijk te maken wat de juiste definitie en reikwijdte van het begrip "PG-verwerkingsverantwoordelijke" is, en specifiek aan te geven of hieronder ook verwerkers in de zin van de AVG vallen, aangezien dit rechtstreekse gevolgen heeft voor het toepassingsgebied van het adequaatheidsbesluit.[21]

3.1.2. Gedeeltelijke vrijstellingen krachtens de WBP

55. Ingevolge artikel 58, lid 1, WBP geldt een deel van die wet (namelijk de artikelen 15 tot en met 57) niet voor de vier hieronder beschreven categorieën van verwerking van persoonsgegevens. Meer in het bijzonder hebben de vrijstellingen betrekking op de bepalingen van de WBP die zien op specifieke verwerkingsgronden, bepaalde verplichtingen inzake gegevensbescherming, de gedetailleerde voorschriften voor de uitoefening van individuele rechten en de regels voor geschillenbeslechting. Het EDPB neemt echter nota van het feit dat sommige algemene bepalingen van de WBP van toch toepassing blijven, bijvoorbeeld met betrekking tot de beginselen van gegevensbescherming (artikel 3) en individuele rechten (artikel 4). Daarnaast zijn in artikel 58, lid 4, WBP specifieke verplichtingen voor de voornoemde vier verwerkingscategorieën vastgelegd.

56. Ten eerste geldt een gedeeltelijke vrijstelling voor persoonsgegevens die op grond van de wet op de statistiek worden verzameld voor verwerking door overheidsinstellingen. De Europese Commissie stelt in overweging 27 van het ontwerpbesluit dat, volgens toelichtingen van de Zuid-Koreaanse regering, op deze grond verwerkte persoonsgegevens normaal gesproken betrekking hebben op Zuid-Koreaanse onderdanen. Het gaat slechts bij uitzondering om vreemdelingen, namelijk in geval van statistieken over binnenkomst in en vertrek uit het grondgebied of statistieken over buitenlandse investeringen. Maar zelfs in die gevallen worden dergelijke gegevens volgens het ontwerpbesluit normaal gesproken niet doorgegeven door verwerkingsverantwoordelijken/verwerkers in de EER, maar rechtstreeks door overheidsinstanties in Zuid-Korea verzameld.

57. Het EDPB begrijpt de gedachtegang van de Europese Commissie aangaande het uitzonderlijke karakter van de toepassing van de wet op de statistiek op de verwerking van persoonsgegevens die op basis van het adequaatheidsbesluit worden doorgegeven. Niettemin zou het aanvullende informatie en bevestiging verwelkomen omtrent de specifieke waarborgen die gelden voor gevallen waarin persoonsgegevens die vanuit de EER zijn doorgegeven, vervolgens worden verzameld op grond van de wet op de statistiek voor verwerking door overheidsinstellingen, in het bijzonder wat betreft de uitoefening van individuele rechten door betrokkenen overeenkomstig artikel 89, lid 2, AVG, voor zover het onwaarschijnlijk is dat die rechten de verwezenlijking van de specifieke doeleinden onmogelijk maken of ernstig belemmeren en de bedoelde afwijkingen niet noodzakelijk zijn om die doeleinden te bereiken.

58. Vanuit dit perspectief lijkt het feit dat artikel 4 WBP ook voor deze categorie verwerking geldt, enige zekerheid te bieden. Het EDPB zou evenwel graag zien dat in het adequaatheidsbesluit aanvullende informatie wordt opgenomen en een en ander wordt verduidelijkt over de specifieke verplichtingen die overeenkomstig artikel 58, lid 4, WBP met betrekking tot dergelijke verwerking gelden, te weten: minimale gegevensverwerking, beperkte gegevensbewaring, beveiligingsmaatregelen en de behandeling van klachten.

59. Ten tweede geldt een gedeeltelijke vrijstelling voor persoonsgegevens die worden verzameld of opgevraagd voor de analyse van informatie betreffende de nationale veiligheid. Het EDPB is zich ervan bewust dat het EHRM staten in kwesties van nationale veiligheid een ruime beoordelingsmarge geeft, maar merkt ook op dat ingevolge artikel 37, lid 2, van de Zuid-Koreaanse grondwet de beperking van een vrijheid of recht (bijvoorbeeld wanneer dit noodzakelijk is voor het beschermen van de nationale veiligheid) nooit de essentie van die vrijheid of dat recht mag aantasten. Het EDPB neemt daarnaast nota van de waarborgen in hoofdstuk 6 van Kennisgeving nr. 2021-1 betreffende de verwerking van

[21] Zie ook punt 38.

persoonsgegevens voor nationaleveiligheidsdoeleinden, waaronder het onderzoeken van inbreuken en handhaving. Het verzoekt de Europese Commissie echter om de reikwijdte van de vrijstellingen verder te verduidelijken. Het vraagt zich namelijk of alle in artikel 58, lid 1, punt 2, WBP (hoofdstukken III tot en met VII) neergelegde vrijstellingen relevant zijn voor het werk van inlichtingendiensten en of de beginselen van noodzakelijkheid en evenredigheid hierbij zijn gewaarborgd. Meer in het bijzonder verzoekt het EDPB de Europese Commissie meer duidelijkheid te verschaffen over de omstandigheden waaronder een inlichtingendienst zich op de vrijstellingen kan beroepen. Het EDBP acht het noodzakelijk dat nauwgezet wordt gemonitord welke gevolgen deze beperkingen in de praktijk zullen hebben, met name voor de doeltreffende uitoefening en handhaving van de rechten van betrokkenen.

60. Ten derde geldt een gedeeltelijke vrijstelling voor "*persoonsgegevens die tijdelijk verwerkt worden wanneer dit dringend noodzakelijk is voor de openbare veiligheid, de volksgezondheid enz.*" Volgens overweging 29 van het ontwerpbesluit van de Europese Commissie wordt deze categorie strikt uitgelegd door de toezichthouder en geldt de vrijstelling alleen voor noodsituaties waarin dringend actie moet worden genomen, bijvoorbeeld voor het opsporen van ziekteverwekkers of het redden en helpen van slachtoffers van natuurrampen.

61. Het EDPB benadrukt dat afwijkingen van het beschermingsniveau voor persoonsgegevens strikt moeten worden uitgelegd. Tegelijkertijd merkt het op dat de betreffende bepaling niet strikt is verwoord en geen uitputtende lijst bevat van situaties waarin de verwerking van persoonsgegevens "*dringend noodzakelijk*" kan worden geacht. Het EDPB is bijvoorbeeld bezorgd dat internationale doorgiften van gezondheidsgegevens tijdens de heersende COVID-19-pandemie ook onder de genoemde vrijstelling zouden vallen. In het licht van het bovenstaande verzoekt het EDPB de Europese Commissie om nader te verduidelijken wat de reikwijdte van deze vrijstelling is en te monitoren hoe en in welke situaties deze in de praktijk wordt toegepast, om er zeker van te zijn dat de vrijstelling niet tot gevolg heeft dat het beschermingsniveau voor persoonsgegevens afkomstig uit de EER wordt verlaagd nadat zij op basis van het adequaatheidsbesluit aan Zuid-Korea zijn doorgegeven.

62. Tot slot geldt een gedeeltelijke vrijstelling voor persoonsgegevens die worden verzameld of gebruikt voor persverslaggeving, zendingswerk van religieuze organisaties en kandidaatstellingen door politieke partijen.[22] Wat de verwerking van persoonsgegevens door de pers voor journalistieke activiteiten betreft, stelt de Europese Commissie in overweging 31 van het ontwerpbesluit dat de wet inzake arbitrage en voorzieningen in rechte enz. voor schade door persberichten (hierna: "**perswet**") voorziet in een evenwicht tussen de vrijheid van meningsuiting en andere rechten, waaronder het recht op privacy. In diezelfde overweging worden ook specifieke waarborgen genoemd die voortvloeien uit deze wet. Het EDPB verzoekt de Europese Commissie evenwel de toepassing van deze vrijstelling en de relevante rechtspraak nauwgezet te monitoren, om er zeker van te zijn dat het Zuid-Koreaanse rechtskader ook in de praktijk een gelijkwaardig niveau van gegevensbescherming waarborgt.

3.1.3. Gronden voor een rechtmatige en behoorlijke verwerking voor gerechtvaardigde doeleinden

63. Volgens de adequaatheidsreferentie moeten persoonsgegevens overeenkomstig de AVG op een rechtmatige, behoorlijke en gerechtvaardigde wijze worden verwerkt. De rechtsgrond op basis waarvan persoonsgegevens op een rechtmatige, behoorlijke en gerechtvaardigde wijze kunnen worden verwerkt, moet voldoende duidelijk zijn uiteengezet. In het Europese kader worden verschillende gerechtvaardigde gronden erkend, waaronder bepalingen in de nationale wetgeving, de

[22] Bijgevolg valt ook de verwerking van persoonsgegevens door religieuze organisaties ten behoeve van zendingswerk en door politieke partijen in de context van kandidaatstellingen buiten het toepassingsgebied van het adequaatheidsbesluit. Zie tevens punt 37 (afdeling 2.3.2).

toestemming van de betrokkene, de uitvoering van een overeenkomst of de behartiging van gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, zolang die niet zwaarder wegen dan de belangen van de betrokkene.

64. De WBP heeft een vergelijkbare opbouw als de AVG: eerst worden de beginselen van rechtmatigheid, behoorlijkheid en transparantie geïntroduceerd (artikel 3, leden 1 en 2) en verderop volgen de specifieke voorschriften voor de toepassing van deze beginselen (artikelen 15 tot en met 19). Meer in het bijzonder bevat artikel 15 een opsomming van de rechtsgronden die PG-verwerkingsverantwoordelijken kunnen aanvoeren voor het verzamelen en gebruiken van persoonsgegevens in overeenstemming met het doel waarvoor de gegevens zijn verzameld. Deze rechtsgronden zijn: 1) geïnformeerde toestemming van de betrokkene, 2) wettelijke machtiging of noodzaak voor het naleven van een wettelijke verplichting, 3) noodzaak voor het uitoefenen van een overheidstaak, 4) noodzaak voor het uitvoeren van een overeenkomst met de betrokkene, 5) noodzaak voor de bescherming van het leven, het lichaam of een vermogensrechtelijk belang van de betrokkene of een derde tegen onmiddellijk dreigend gevaar (wanneer geen voorafgaande toestemming kan worden verkregen), en 6) een gerechtvaardigd belang van de PG-verwerkingsverantwoordelijke dat zwaarder weegt dan de belangen van de betrokkene.

65. Daarnaast bevat artikel 17 WBP de rechtsgronden voor het delen van persoonsgegevens met een derde partij, namelijk onder meer: 1) geïnformeerde toestemming van de betrokkene, 2) wettelijke machtiging of noodzaak voor het naleven van een wettelijke verplichting, 3) noodzaak voor het uitoefenen van een overheidstaak, en 4) noodzaak voor de bescherming van het leven, het lichaam of een vermogensrechtelijk belang van de betrokkene of een derde tegen onmiddellijk dreigend gevaar (wanneer geen voorafgaande toestemming kan worden verkregen). Zelfs zonder toestemming van de betrokkene is het delen van persoonsgegevens toegestaan wanneer dit redelijk verband houdt met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (artikel 17, lid 4, WBP).

66. Artikel 18 WBP bevat specifieke voorschriften voor het gebruiken en delen van persoonsgegevens, wanneer dit gebeurt buiten het oorspronkelijke doel van de verzameling of verstrekking om. Ook hier wordt onder meer de toestemming van de betrokkene als voorwaarde genoemd.

67. Hoewel het Zuid-Koreaanse recht en de AVG wat betreft het rechtmatigheidsbeginsel en het bestaan van een algemeen recht op opschorting (artikel 37 WBP), waarop ook een beroep kan worden gedaan wanneer persoonsgegevens op basis van toestemming zijn verwerkt, in wezen gelijkwaardig zijn, wijst het EDPB op het ontbreken van een algemeen recht op het intrekken van toestemming in de WBP[23]. Gezien het belang van toestemming als rechtsgrond in alle hierboven beschreven scenario's en aangezien individuele rechten in een rechtsstelsel voor gegevensbescherming belangrijk zijn voor het waarborgen van de grondrechten en fundamentele vrijheden van betrokkenen, verzoekt het EDPB de Europese Commissie om nader onderzoek te doen naar de gevolgen die het ontbreken van een algemeen recht op het intrekken van toestemming in de Zuid-Koreaanse wetgeving heeft en om aanvullende garanties te geven dat steeds een niveau van gegevensbescherming wordt gewaarborgd

[23] Wel kunnen betrokkenen in bepaalde omstandigheden besluiten om geen toestemming te geven. Zie bijvoorbeeld artikel 18, lid 3, punt 5, WBP. Het recht op het intrekken van toestemming lijkt slechts in specifieke gevallen te bestaan Ingevolge artikel 27, lid 1, punt 2, WBP hebben betrokkenen het recht hun toestemming in te trekken wanneer zij niet willen dat hun persoonsgegevens aan een derde partij worden doorgegeven als gevolg van de gehele of gedeeltelijke overdracht van het bedrijf van de PG-verwerkingsverantwoordelijke, een fusie enz. Uit hoofde van artikel 39, lid 7, WBP kunnen gebruikers hun toestemming voor de verzameling, het gebruik en de verstrekking van persoonsgegevens op elk moment intrekken bij een aanbieder van informatie- en communicatiediensten enz., en ingevolge artikel 37 van de kredietinformatiewet kan een persoon op wie kredietgegevens betrekking hebben, de toestemming intrekken die aan de aanbieder/gebruiker van de kredietgegevens was verstrekt.

dat gelijkwaardig is aan de AVG. Daartoe dient ook, voor zover nodig, verduidelijkt te worden wat de functie van het recht op opschorting in deze specifieke context is.

3.1.4. Beginsel van doelbinding

68. In lijn met de AVG schrijft de adequaatheidsreferentie voor dat persoonsgegevens verwerkt moeten worden voor een specifiek doel en vervolgens uitsluitend gebruikt mogen worden voor zover dit niet onverenigbaar is met dat doel.

69. Ingevolge artikel 3, leden 1 en 2, WBP moeten PG-verwerkingsverantwoordelijken expliciet aangeven voor welke doeleinden gegevens worden verwerkt en ervoor zorgen dat de verwerking verenigbaar daar verenigbaar mee is. Hoewel dit beginsel in andere bepalingen van de WBP wordt bevestigd (namelijk in artikel 15, lid 1, artikel 18, lid 1, en artikel 19, lid 1), is verwerking in bepaalde omstandigheden ook toegestaan voor doeleinden die "redelijk verband houden" met de aangegeven doeleinden (zie artikel 17, lid 4, WBP)[24], evenals gebruik en verstrekking voor geheel andere doeleinden (zie de artikelen 18 en 19 WBP)[25].

70. Het EDPB begrijpt dat, in het geval van doorgiften van persoonsgegevens uit de EER naar de Republiek Korea op basis van het adequaatheidsbesluit, het doel van de gegevensverzameling zoals aangegeven door de in de EER gevestigde verwerkingsverantwoordelijke wordt geacht het doel te zijn waarvoor de gegevens worden doorgegeven en waarvoor de in Zuid-Korea gevestigde PG-verwerkingsverantwoordelijke die de gegevens ontvangt, deze verwerkt. Wijziging van het doel door de in Zuid-Korea gevestigde verwerkingsverantwoordelijke is uitsluitend toegestaan in de gevallen die worden genoemd in artikel 18, lid 2, punten 1, 2 en 3, WBP, "*tenzij hiermee wellicht een onredelijk inbreuk wordt gemaakt op de belangen van een betrokkene of een derde partij*"[26]. Het EDPB erkent dat de Europese Commissie in overweging 55 van het ontwerpbesluit verklaart dat, wanneer veranderingen van doel bij wet worden toegestaan, in de betreffende wet rekening moet worden gehouden met het grondrecht op privacy en gegevensbescherming. Er is echter geen specifieke informatie verstrekt ter onderbouwing van deze verklaring, bijvoorbeeld via een verwijzing naar artikel 37 van de Zuid-Koreaanse grondwet. Het EDPB verzoekt de Europese Commissie derhalve in het ontwerpbesluit aanvullende garanties en waarborgen op te nemen die ertoe strekken dat in wetten die voorzien in de mogelijkheid om het verwerkingsdoel te veranderen, rekening wordt gehouden met de grondrechten en fundamentele vrijheden van betrokkenen met betrekking tot privacy en gegevensbescherming.

3.1.5. Beginselen van gegevenskwaliteit en evenredigheid

71. In de adequaatheidsreferentie wordt aangegeven dat gegevens nauwkeurig moeten zijn en zo nodig moeten worden bijgewerkt. Zij moeten toereikend, ter zake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden verwerkt.

72. Ingevolge de WBP moet de PG-verwerkingsverantwoordelijke ervoor zorgen dat persoonsgegevens juist, volledig en actueel zijn voor zover noodzakelijk voor de doeleinden waarvoor die gegevens worden verwerkt (artikel 3, lid 3, WBP). De PG-verwerkingsverantwoordelijke mag slechts persoonsgegevens verzamelen die nodig zijn voor het bereiken van een bepaald doel, en draagt hiervoor zelf de bewijslast (artikel 16, lid 1, WBP).

73. Tegen deze achtergrond deelt het EDPB het oordeel van de Europese Commissie dat het beschermingsniveau waarin de WBP en de AVG voorzien, in dit opzicht in wezen gelijkwaardig zijn.

[24] Daarbij moet vooraf worden nagegaan of de doeleinden verenigbaar zijn, op basis van de criteria van artikel 14-2 van het WBP-uitvoeringsbesluit.
[25] Zie ook punt 66.
[26] Artikel 18, lid 2, WBP.

3.1.6. Beginsel van gegevensbewaring

74. Volgens de adequaatheidsreferentie mogen persoonsgegevens in de regel niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Uit hoofde van artikel 21, lid 1, WBP bestaat dit beginsel ook in het Zuid-Koreaanse recht. Ingevolge de WBP moet de PG-verwerkingsverantwoordelijke persoonsgegevens die niet langer noodzakelijk zijn, onverwijld vernietigen zodra de bewaartermijn verstrijkt of het doel van de verwerking is bereikt, tenzij er wettelijke bewaartermijnen gelden.

75. Het EDPB vindt het niettemin zorgwekkend dat artikel 21, lid 1, WBP niet geldt voor gepseudonimiseerde persoonsgegevens. Het EDPB neemt nota van de volgende toelichting in hoofdstuk 4, iii), van Kennisgeving nr. 2021-1: "*Wanneer een PG-verwerkingsverantwoordelijke gepseudonimiseerde gegevens verwerkt voor het opstellen van statistieken, wetenschappelijk onderzoek, het bewaren van openbare stukken enz., en de gepseudonimiseerde gegevens niet moeten worden vernietigd zodra het specifieke verwerkingsdoel is bereikt, overeenkomstig artikel 37 van de grondwet en artikel 3 ("Beginselen voor de bescherming van persoonsgegevens") van de wet, dan anonimiseert de verwerkingsverantwoordelijke de betreffende gegevens zodat daarmee redelijkerwijs niet langer een specifieke persoon geïdentificeerd kan worden, ook niet in combinatie met andere informatie, rekening houdend met factoren als tijd, kosten, technologie enz., overeenkomstig artikel 58, lid 2, WBP.*" Gezien het belang, ook op dit gebied, van Kennisgeving nr. 2021-1, en met het oog op rechtszekerheid omtrent de gelijkwaardigheid van het beschermingsniveau voor persoonsgegevens die op basis van het adequaatheidsbesluit aan de Republiek Korea worden doorgegeven, doet het EDPB opnieuw een oproep aan de Europese Commissie om aanvullende informatie te verstrekken over de wijze waarop Kennisgeving nr. 2021-1 bindend wordt gemaakt en ervoor wordt gezorgd dat deze afdwingbaar en geldig is[27].

3.1.7. Beginsel van beveiliging en vertrouwelijkheid

76. Zoals beschreven in de adequaatheidsreferentie vereist het beginsel van beveiliging en vertrouwelijkheid dat verwerkers ervoor zorgen dat persoonsgegevens door het nemen van passende technische of organisatorische maatregelen op een zodanige manier worden verwerkt dat een passende beveiliging van de gegevens wordt gewaarborgd en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, onopzettelijke vernietiging of onopzettelijke beschadiging. Bij het beveiligingsniveau dient rekening te worden gehouden met de stand van de techniek en de bijbehorende kosten.

77. De Europese Commissie heeft vastgesteld dat in de WBP wordt uitgegaan van een vergelijkbaar beginsel van gegevensbeveiliging, dat is neergelegd in artikel 3, lid 4, met een nadere omschrijving in artikel 29. Daarnaast zijn er bepalingen inzake gegevensbeveiliging die specifiek van toepassing zijn op situaties waarin de PG-verwerkingsverantwoordelijke een dienstverlener in de arm neemt. De beveiliging van de verwerking moet zowel technisch als beheersmatig worden gewaarborgd, zoals vastgelegd in een bindende gegevensverwerkingsovereenkomst (artikel 26 WBP en artikel 28 van het WBP-uitvoeringsbesluit). Verder gelden krachtens de WBP specifieke verplichtingen bij een gegevenslek. Zo moeten de betrokkenen die daarvan het slachtoffer zijn geworden en de toezichthouder van het lek in kennis worden gesteld wanneer het aantal slachtoffers een bepaalde grens overschrijdt (artikel 34 WBP, in samenhang met artikel 39 van het WBP-uitvoeringsbesluit). Deze verplichting geldt niet voor gegevens die gepseudonimiseerd zijn en die worden verwerkt voor statistische doeleinden, wetenschappelijk onderzoek of archivering in het algemeen belang

[27] Zie tevens punt 51 (afdeling 3.1.1.1) alsook punt 52 van dit advies voor de algemene punten van zorg van het EDPB over de gevolgen die pseudonimisering naar Zuid-Koreaans recht heeft.

(artikel 28, lid 7, WBP). Ook hieromtrent[28] maakt het EDPB zich zorgen over de ruime vrijstellingen voor gepseudonimiseerde gegevens en verzoekt het de Europese Commissie opnieuw om dit aspect nader te onderzoeken om er zeker van te zijn dat het Zuid-Koreaanse recht een in wezen gelijkwaardig beschermingsniveau biedt[29].

78. Niettemin is het EDPB over het algemeen tevreden met de beoordeling van de Europese Commissie en haar conclusie dat het Zuid-Koreaanse recht, wat het beginsel van beveiliging en vertrouwelijkheid betreft, in wezen gelijkwaardig is.

3.1.8. Transparantiebeginsel

79. Ingevolge artikel 5, lid 1, punt a), AVG is transparantie een fundamenteel beginsel van het EU-stelsel voor gegevensbescherming. In overweging 39 van de AVG wordt aangegeven wat de cruciale functie van dit beginsel is: "*Voor natuurlijke personen dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt. […] Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot deze verwerking kunnen uitoefenen.*"

80. In de adequaatheidsreferentie wordt "transparantie" uitdrukkelijk genoemd als een van de inhoudelijke beginselen die in aanmerking moeten worden genomen bij de beoordeling van de vraag of het door een derde land geboden beschermingsniveau in wezen gelijkwaardig is. Meer in het bijzonder staat daarin dat "*[i]edere betrokkene […] in een duidelijke, gemakkelijk toegankelijke, beknopte, transparante en begrijpelijke vorm [moet] worden geïnformeerd over alle belangrijke elementen van de verwerking van zijn/haar persoonsgegevens. Deze informatie moet het doel van de verwerking omvatten, de identiteit van de verwerkingsverantwoordelijke, de rechten die hem/haar ter beschikking staan en andere informatie, voor zover noodzakelijk om een behoorlijke verwerking te waarborgen. Onder bepaalde voorwaarden kunnen uitzonderingen op dit informatierecht worden gemaakt, bijvoorbeeld om onderzoeken naar strafbare feiten veilig te stellen, om redenen van nationale veiligheid of de onafhankelijkheid van de rechter en gerechtelijke procedures te beschermen of om andere gewichtige redenen van openbaar belang, zoals bedoeld in artikel 23 van de AVG.*"

81. Net als de AVG kent de WBP een algemeen transparantiebeginsel op basis waarvan PG-verwerkingsverantwoordelijken hun privacybeleid en andere kwesties in verband met de verwerking van persoonsgegevens openbaar moeten maken (artikel 3, lid 5, WBP). Er gelden specifieke informatieverplichtingen wanneer de PG-verwerkingsverantwoordelijke van betrokkenen toestemming probeert te verkrijgen voor het verzamelen en verwerken van persoonsgegevens (artikel 15, lid 2, WBP), voor het delen van persoonsgegevens met een derde partij (artikel 17, lid 2, WBP) en voor het verwerken van de gegevens voor een ander dan het oorspronkelijke doel (artikel 18, lid 3, WBP). Het verdient opmerking dat deze informatieverplichtingen mutatis mutandis ook gelden voor eventuele dienstverleners (artikel 26, lid 7, WBP).

82. Het EDPB verwelkomt de aanvullende waarborgen in hoofdstuk 3, i) en ii), van Kennisgeving nr. 2021-1[30] op grond waarvan de betrokkenen op de hoogte moeten worden gebracht als hun gegevens worden doorgegeven door een in de EER gevestigde entiteit. Wanneer persoonsgegevens afkomstig zijn van een andere bron dan de betrokkene, wordt deze uit hoofde van artikel 20, lid 1, WBP namelijk alleen op verzoek geïnformeerd. Een algemeen recht op informatie bestaat ingevolge artikel 20, lid 2,

[28] Het EDPS heeft zijn bezorgdheid hierover al kenbaar gemaakt in de punten 51 en 52 en afdeling 3.1.1.1 van dit advies.
[29] Zie tevens de afdelingen 3.1.6 en 3.1.10 van dit advies.
[30] Bijlage I bij het ontwerpbesluit.

WBP alleen wanneer bepaalde verwerkingsactiviteiten een in het WBP-uitvoeringsbesluit (artikel 15, lid 2) neergelegde drempel overschrijden.

83. Alles bij elkaar genomen is het EDPB ervan overtuigd dat het Zuid-Koreaanse recht wat het transparantiebeginsel betreft in een beschermingsniveau voorziet dat in wezen gelijkwaardig is aan het niveau waarin de AVG voorziet.

3.1.9. Bijzondere categorieën van persoonsgegevens

84. Het systeem voor gegevensbescherming van een derde land wordt alleen geacht in een beschermingsniveau voor persoonsgegevens te voorzien dat in wezen gelijkwaardig is aan dat van de AVG, als er sprake is van specifieke waarborgen voor bijzondere categorieën van persoonsgegevens in de zin van de artikelen 9 en 10 AVG.

85. De WBP bevat specifieke bepalingen voor de verwerking van "gevoelige gegevens", waartoe onder meer informatie wordt gerekend waaruit de ideologie, de levensovertuiging, de toetreding tot of uittreding uit een vakbond of politieke partij, de gezondheidstoestand of het seksuele gedrag van een betrokkene blijkt, evenals andere persoonsgegevens waarvan de verwerking waarschijnlijk een aanmerkelijk privacyrisico voor betrokkenen oplevert. Onder verwijzing naar het WBP-uitvoeringsbesluit omvat dit begrip tevens uit genetisch onderzoek verkregen DNA-informatie, gegevens over gepleegde strafbare feiten, informatie die het resultaat is van een specifieke technische verwerking van gegevens betreffende fysieke, fysiologische of gedragsmatige kenmerken met het oog op de unieke identificatie van een persoon, en persoonsgegevens waaruit ras of etnische afkomst blijkt.

86. Net als de AVG bevat ook het Zuid-Koreaanse gegevensbeschermingsrecht een verbod op de verwerking van gevoelige gegevens, tenzij er specifieke vrijstellingen gelden: 1) de betrokkene wordt geïnformeerd en geeft specifiek toestemming voor de verwerking, en 2) de verwerking is toegestaan op grond van een wettelijke bepaling (artikel 23, lid 2, WBP).

87. Op basis hiervan is het EDPB het in beginsel eens met de Europese Commissie dat het Zuid-Koreaanse recht wat de verwerking van bijzondere categorieën van persoonsgegevens betreft, in wezen gelijkwaardig is. Het heeft het handboek voor de interpretatie van de WBP echter niet ontvangen, noch de toelichtingen van de toezichthouder met betrekking tot de term "seksueel gedrag" waaruit zou blijken dat daaronder ook iemands seksuele geaardheid en seksuele voorkeuren vallen. Deze toelichtingen zijn niet opgenomen in Kennisgeving nr. 2021-1. Het EDPB verzoekt de Europese Commissie derhalve om deze informatie te verstrekken, zodat het zich hierover een zelfstandig oordeel kan vormen. Verder verzoekt het EDPB de Europese Commissie om specifiek de bronnen te vermelden van de informatie waarnaar in verband met dit thema wordt verwezen.

3.1.10. Recht van inzage, rectificatie, wissing en bezwaar

88. In het Zuid-Koreaanse rechtskader worden de rechten van betrokkenen erkend in artikel 3, lid 5, WBP. Op grond daarvan moet de PG-verwerkingsverantwoordelijke de rechten van betrokkenen respecteren die worden vermeld in artikel 4 WBP en nader worden omschreven in de artikelen 35, 36, 37, 39 en 39-2 WBP en, wat "informatie over persoonlijke kredieten" betreft (d.w.z. "informatie die noodzakelijk is voor het bepalen van de kredietwaardigheid van partijen bij financiële of handelstransacties"; zie overweging 3 van het ontwerpbesluit), in de artikelen 37, 38 en 38-3 van de kredietinformatiewet.

89. Het EDPB merkt op dat het recht van inzage (evenals het recht op rectificatie en wissing, dat kan worden uitgeoefend door een "*betrokkene die krachtens artikel 35 [WBP] hem of haar betreffende persoonsgegevens heeft ingezien*") kan worden beperkt of ontzegd, "*wanneer inzage bij wet is verboden of beperkt*", "*wanneer door inzage mogelijk een levensbedreigende situatie of kans op letsel*

ontstaat voor een derde, dan wel kan leiden tot een ongerechtvaardigde inbreuk op de eigendom of andere belangen van enige andere persoon", en daarnaast, met betrekking tot overheidsinstellingen, wanneer toestemming tot inzage het uitvoeren van bepaalde taken, die nader worden omschreven in artikel 35, lid 4, WBP, "*in ernstige mate zou bemoeilijken*".[31] Soortgelijke bepalingen zijn ook te vinden in artikel 37 WBP inzake het recht op opschorting van de verwerking van persoonsgegevens.

90. Artikel 23 AVG voorziet in de mogelijkheid individuele rechten bij Unie- of lidstaatrecht te beperken "op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van [onder andere] de bescherming van de betrokkene of van de rechten en vrijheden van anderen" of "*een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a) tot en met e) en punt g) [van hetzelfde artikel] bedoelde gevallen*".

91. Tegen deze achtergrond zou het EDPB het toejuichen dat in het ontwerpbesluit in het algemeen de zekerheid wordt geboden dat eventuele wetten waarbij de rechten van betrokkenen aan banden worden gelegd, voldoen aan het in de Zuid-Koreaanse grondwet vastgelegde vereiste dat een grondrecht slechts wordt beperkt wanneer dit noodzakelijk is voor de nationale veiligheid, het handhaven van recht en orde of het maatschappelijk welzijn, en dat de beperking de essentie van de betreffende vrijheid of het betreffende recht niet aantast (artikel 37, lid 2, van de Zuid-Koreaanse grondwet).

92. Wat betreft de uitzondering in verband met een "*ongerechtvaardigde inbreuk op de eigendom of andere belangen van enige andere persoon*", erkent het EDPB dat dit "*impliceert dat gezocht moet worden naar een evenwicht tussen de grondwettelijk beschermde rechten en vrijheden van de betrokkene en die van andere personen*"[32]. Het EDPB verzoekt de Europese Commissie echter om de toepassing van deze uitzondering en de relevante rechtspraak nauwgezet te monitoren om er zeker van te zijn dat het Zuid-Koreaanse rechtskader ook in de praktijk een gelijkwaardig niveau van bescherming van de rechten van betrokkenen waarborgt.

93. Het EDPB zou het evenzeer toejuichen dat de toepassing van de uitzondering voor overheidsinstellingen nauwgezet wordt gemonitord, in het bijzonder wat betreft gevallen waarin het geven van toestemming tot inzage het uitvoeren van hun taken "*ernstig zou bemoeilijken*". Deze omschrijving lijkt namelijk ruimer dan de bewoordingen in andere bepalingen van de WBP, bijvoorbeeld artikel 18, lid 2, punt 5[33], en moet restrictief worden opgevat om te voorkomen dat de rechten van betrokkenen onnodig worden beperkt.

94. Daarnaast vraagt het EDPB zich af of de uitzonderingen waardoor de bepalingen inzake "transparantie op verzoek" (artikel 20 WBP) en individuele rechten (artikelen 35, 36 en 37 WBP) – alsook vergelijkbare bepalingen inzake de vereisten voor aanbieders van informatie- en communicatiediensten (artikel 39, leden 2, 6, 7 en 8, WBP) en de bepalingen in de kredietinformatiewet (zie de uitzonderingen van artikel 40, lid 3, van de kredietinformatiewet) – niet gelden voor gepseudonimiseerde gegevens, wanneer die worden verwerkt voor statistische doeleinden of met het oog op wetenschappelijk onderzoek of archivering in het algemeen belang

[31] De voorwaarden voor en uitzonderingen op het recht van inzage en het recht op rectificatie waarin de WBP voorziet, gelden ook met betrekking tot het recht van inzage en het recht op rectificatie zoals neergelegd in de kredietinformatiewet met betrekking tot informatie over persoonlijke kredieten (voetnoot 135 van het ontwerpbesluit).

[32] Overweging 76 van het ontwerpbesluit.

[33] Wat betreft de uitzonderingen op de beperking van het gebruik en de verstrekking van persoonsgegevens voor een ander dan het oorspronkelijke doel, wordt in artikel 18, lid 2, punt 5, WBP verwezen naar situaties waarin het voor overheidsinstellingen "*onmogelijk is*" om hun taken uit te voeren.

(artikel 28, lid 7, WBP), in overeenstemming zijn met de waarborgen waarin het Europese rechtskader voorziet.

95. Deze bepalingen lijken een algemene afwijking in het leven te roepen voor de verwerking van gepseudonimiseerde gegevens. In de AVG wordt weliswaar bepaald dat, wanneer persoonsgegevens (inclusief gepseudonimiseerde persoonsgegevens) met het oog op wetenschappelijk of historisch onderzoek of voor statistische doeleinden worden verwerkt, in het Unie- of lidstaatrecht kan worden voorzien in afwijkingen van de rechten van betrokkenen, maar dat kan uitsluitend "*voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken*". Daarbij is pseudonimisering slechts een van de technische en organisatorische maatregelen die getroffen moeten worden om inachtneming van het beginsel van minimale gegevensverwerking te garanderen (artikel 89, lid 1, AVG).

96. De Europese Commissie acht de afwijking neergelegd in artikel 28, lid 7, WBP ook gerechtvaardigd in het licht van artikel 28, lid 5, WBP, dat de PG-verwerkingsverantwoordelijke uitdrukkelijk verbiedt om gepseudonimiseerde gegevens te verwerken voor het identificeren van specifieke personen. Zij verwijst daarbij naar de benadering in artikel 11, lid 2, AVG (in samenhang met overweging 57 AVG) voor verwerking waarvoor identificatie niet vereist is.[34]

97. Ingevolge artikel 11 AVG is een verwerkingsverantwoordelijke niet verplicht om, uitsluitend om aan de AVG te voldoen, "*aanvullende gegevens ter identificatie van de betrokkene bij te houden, te verkrijgen of te verwerken*", indien de doeleinden waarvoor de verwerkingsverantwoordelijke persoonsgegevens verwerkt, niet of niet meer vereisen dat een betrokkene wordt geïdentificeerd. Wanneer de verwerkingsverantwoordelijke in een dergelijk geval kan aantonen de betrokkene niet te kunnen identificeren, zijn de rechten van de betrokkene niet van toepassing. De Europese Commissie erkent in het ontwerpbesluit[35] dat de AVG in een dergelijk geval vereist dat er sprake is van een "praktische" onmogelijkheid voor de verwerkingsverantwoordelijke en dat er, overeenkomstig het beginsel van minimale gegevensverwerking, geen aanvullende gegevens verwerkt hoeven te worden "vanwege" de AVG.

98. Volgens het EDPB verschilt deze situatie echter van het geval waarin een verwerkingsverantwoordelijke praktisch in de positie verkeert om een betrokkene te identificeren, maar dit krachtens een wettelijke bepaling, zoals artikel 28, lid 5, WBP, niet is toegestaan. In dit opzicht is het EDPB ingenomen met de verduidelijkingen die de toezichthouder in Kennisgeving nr. 2021-1 geeft[36], waarbij deze bevestigt dat afdeling 3 van de WBP (waartoe ook artikel 28, lid 7, behoort) en de uitzondering in artikel 40, lid 3, van de kredietinformatiewet slechts van toepassing zijn wanneer gepseudonimiseerde gegevens worden verwerkt voor wetenschappelijk onderzoek, statistische doeleinden of archivering in het algemeen belang. Niettemin – en bovenop de reeds vermelde twijfels omtrent het daadwerkelijk bindende karakter van Kennisgeving nr. 2021-1[37] – vraagt het EDPB zich af of de afwijkingen in artikel 28, lid 7, WBP en artikel 40, lid 3, van de kredietinformatiewet kunnen worden beschouwd als "in een democratische samenleving noodzakelijke en evenredige maatregelen". Deze afwijkingen beperken de rechten van betrokkenen

[34] Deze redenering kan als zodanig niet gebruikt worden ter rechtvaardiging van de uitzondering in artikel 40, lid 3, van de kredietinformatiewet voor de verwerking van gepseudonimiseerde kredietgegevens, aangezien artikel 40, lid 2, punt 6, van diezelfde wet bepaalt dat "*[e]en kredietinformatiemaatschappij enz. […] gepseudonimiseerde kredietgegevens niet op een zodanige wijze [mag] verwerken dat een specifieke persoon kan worden geïdentificeerd uit enig winstoogmerk of voor oneerlijke doeleinden*" en bijgevolg de mogelijkheid openlaat van heridentificatie voor eerlijke doeleinden, bijvoorbeeld om te voldoen aan het verzoek van een betrokkene.

[35] Overweging 82 van het ontwerpbesluit.

[36] Hoofdstuk 4 van bijlage I bij het ontwerpbesluit.

[37] Zie afdeling 3.1.1.1.

immers consequent wanneer gepseudonimiseerde gegevens voor die doeleinden worden verwerkt, dus zelfs wanneer de PG-verwerkingsverantwoordelijke praktisch in een positie verkeert om de betrokkene te identificeren en het onwaarschijnlijk is dat de betreffende rechten de verwezenlijking van de specifieke doeleinden onmogelijk maken of ernstig belemmeren.

99. Het EDPB heeft in het bijzonder twijfels over de gerechtvaardigdheid van deze afwijkingen en meent dat deze nader moeten worden onderzocht, met name wanneer zij worden toegepast door een PG-verwerkingsverantwoordelijke die gegevens pseudonimiseert "*voor statistische doeleinden, wetenschappelijk onderzoek, archivering in het algemeen belang enz.*" en dat, overeenkomstig artikel 28, lid 2, WBP, "*zonder de toestemming van de betrokkenen*" doet (en ook zonder kennisgeving hieromtrent krachtens artikel 20 WBP)[38], voor zover deze verwerkingsverantwoordelijke de informatie bewaart waardoor heridentificatie mogelijk is. Uit hoofde van de AVG moeten personen in staat worden gesteld hun rechten uit te oefenen met betrekking tot alle gegevens op basis waarvan zij kunnen worden geïdentificeerd of onderscheiden, ook als die gegevens worden geacht te zijn "gepseudonimiseerd", tenzij het reeds genoemde artikel 11 AVG van toepassing is. In dit opzicht merkt het EDPB op dat informatie op basis waarvan een bepaalde persoon geïdentificeerd kan worden enkel achterwege wordt gelaten wanneer de gegevensverstrekking aan een derde partij plaatsvindt voor dezelfde doeleinden inzake statistiek, wetenschappelijk onderzoek of archivering als waarvoor de gegevens oorspronkelijk zijn verwerkt. Bijgevolg verkeert alleen een PG-verwerkingsverantwoordelijke waaraan gepseudonimiseerde gegevens worden verstrekt overeenkomstig artikel 28-2, lid 2, WBP waarschijnlijk "praktisch" niet in de positie om de betrokkene zonder aanvullende informatie te identificeren.

100. Samengevat: overwegende dat, zoals de Europese Commissie erkent, "*pseudonimisering in de WBP niet wordt gebruikt als eventuele waarborg, maar als een basisvoorwaarde voor het uitvoeren van bepaalde verwerkingsactiviteiten voor statistische doeleinden, wetenschappelijk onderzoek en archivering in het algemeen belang (zodat de gegevens verwerkt kunnen worden zonder toestemming van de betrokkene of om verschillende datareeksen te kunnen combineren)*"[39] en die wet met betrekking tot dergelijke verwerking verregaande beperkingen stelt aan de rechten van betrokkenen, verzoekt het EDPB de Europese Commissie om de afwijkingen vervat in artikel 28, lid 7, WBP en artikel 40, lid 3, van de kredietinformatiewet nader te onderzoeken en om de toepassing ervan en relevante rechtspraak[40] nauwgezet te monitoren, om te verzekeren dat de rechten van betrokkenen niet onnodig worden beperkt wanneer op basis van het adequaatheidsbesluit doorgegeven persoonsgegevens voor de genoemde doeleinden worden verwerkt, rekening houdend met het feit dat deze rechten in veel gevallen ook de verwerkingsverantwoordelijke helpen om de kwaliteit van de verwerkte gegevens te waarborgen.

3.1.11. Beperkingen op verdere doorgifte

101. De adequaatheidsreferentie maakt duidelijk dat het beschermingsniveau voor natuurlijke personen van wie de persoonsgegevens op basis van een adequaatheidsbesluit worden doorgegeven, niet mag worden ondermijnd door verdere doorgifte en dat dit bijgevolg "*alleen [mag] worden toegestaan wanneer a) de latere ontvanger – dat wil zeggen de ontvanger van de verdere doorgifte – eveneens is onderworpen aan voorschriften (met inbegrip van contractuele bepalingen) die een passend*

[38] Zie artikel 28, lid 7, WBP, zoals uitgelegd in Kennisgeving nr. 2021-1, op grond waarvan bepaalde waarborgen in de WBP (d.w.z. "*[d]e artikelen 20, 21 en 27, artikel 34, lid 1, de artikelen 35, 36 en 37, en artikel 39, leden 3, 4, 6, 7 en 8*") niet van toepassing zijn op gepseudonimiseerde gegevens die worden verwerkt ten behoeve van het samenstellen van statistieken, wetenschappelijk onderzoek, bewaren van openbare stukken enz.

[39] Overweging 42 van het ontwerpbesluit.

[40] Zie bijvoorbeeld de beroepen van Open Net wegens ongrondwettelijkheid (informatie op https://opennet.or.kr/19909, uitsluitend in het Koreaans).

beschermingsniveau opleveren en b) deze ontvanger de relevante instructies opvolgt wanneer hij/zij namens de verwerkingsverantwoordelijke gegevens verwerkt".

102. Wat de verdere doorgifte aan in andere derde landen gevestigde dienstverleners (d.w.z. "verwerkers") betreft, neemt het EDPB nota van het feit dat het Zuid-Koreaanse rechtskader hiervoor geen bijzondere voorschriften kent en dat, zoals de Europese Commissie bij haar beoordeling in overweging heeft genomen[41], een Zuid-Koreaanse PG-verwerkingsverantwoordelijke door middel van een rechtens bindend instrument moet waarborgen dat de dienstverlener de bepalingen van de WBP inzake uitbesteding (artikel 26 WBP) naleeft en verantwoordelijk blijft voor de persoonsgegevens die door de dienstverlener worden verwerkt (artikel 26 WBP).

103. Wat betreft de verdere doorgifte aan derde partijen (d.w.z. andere PG-verwerkingsverantwoordelijken), schrijft artikel 17, lid 3, WBP voor dat een Zuid-Koreaanse PG-verwerkingsverantwoordelijke de betrokkenen in voorkomend geval moet informeren over overzeese doorgiften en hun toestemming hiervoor moet verkrijgen, en dat die verwerkingsverantwoordelijke "*geen overeenkomst aangaat voor een grensoverschrijdende doorgifte van persoonsgegevens die in strijd is met de WBP*". Het EDPB merkt op dat laatstgenoemde bepaling waarborgt – zoals de Europese Commissie bij haar beoordeling in overweging heeft genomen[42] – dat een overeenkomst voor grensoverschrijdende doorgifte geen voorwaarden kan bevatten die in strijd zijn met de vereisten voor PG-verwerkingsverantwoordelijken zoals vastgelegd in de WBP en bijgevolg als een waarborg kan worden beschouwd. De WBP bevat echter geen enkele verplichting tot het bieden van waarborgen die ertoe strekken dat de ontvanger hetzelfde beschermingsniveau verleent als de WBP. Het EDPB erkent dan ook dat doorgiften van een in Zuid-Korea gevestigde PG-verwerkingsverantwoordelijke aan een in een derde land gevestigde ontvanger in de regel op basis van geïnformeerde toestemming van de betrokkene zullen gebeuren.

104. In dit opzicht verwelkomt het EDPS de aanvullende verduidelijkingen die de toezichthouder in Kennisgeving nr. 2021-1 geeft met betrekking tot de verplichting om personen te informeren over het derde land waaraan hen betreffende persoonsgegevens worden verstrekt[43], aangezien dit – zoals de Europese Commissie onderstreept[44] – betrokkenen in de EER zal helpen een geïnformeerde beslissing te nemen als zij worden gevraagd toestemming te geven voor overzeese verstrekking.

105. Benadrukt moet echter worden dat – zoals ook is overwogen in Advies 28/2018 over het ontwerpuitvoeringsbesluit van de Europese Commissie betreffende de adequate bescherming van persoonsgegevens in Japan – betrokkenen, voordat zij toestemming verlenen, krachtens de AVG uitdrukkelijk moeten worden geïnformeerd over de mogelijke risico's van doorgiften naar een derde land als gevolg van het ontbreken van adequate bescherming in dat land en het ontbreken van passende waarborgen. Een dergelijke kennisgeving moet bijvoorbeeld de informatie bevatten dat het derde land misschien niet over een toezichthoudende autoriteit en/of beginselen inzake gegevensverwerking beschikt en/of dat betrokkenen geen rechten hebben in dit derde land.[45] Voor het EDPB is de verstrekking van deze informatie absoluut noodzakelijk om de betrokkene in staat te stellen toestemming te geven met volledige kennis van deze specifieke feiten inzake de doorgifte.[46] Het EDPB heeft daarom twijfels over de bevindingen van de Europese Commissie met betrekking tot dit specifieke soort doorgiften. Betrokkenen zijn doorgaans niet goed geïnformeerd over het gegevensbeschermingskader in derde landen. Er kan dan ook niet worden geconcludeerd dat het voor

[41] Overweging 87 van het ontwerpbesluit.
[42] Overweging 88 van het ontwerpbesluit.
[43] Ibid.
[44] Ibid.
[45] Richtsnoeren 2/2018 van het EDPB inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 25 mei 2018, blz. 8.
[46] Richtsnoeren 2/2018 van het EDPB inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 25 mei 2018, blz. 7.

een betrokkene voldoende is om het land van bestemming te kennen om het risico van een doorgifte te kunnen beoordelen. Integendeel, voordat de betrokkene toestemming kan geven, moet er duidelijke informatie worden verschaft over de specifieke risico's van een doorgifte van persoonsgegevens naar een land buiten de Republiek Korea.

106. Bijgevolg verzoekt het EDPB de Europese Commissie om te waarborgen dat de informatie die aan de betrokkene wordt verstrekt "*over de omstandigheden van de doorgifte*" ook informatie bevat over eventuele risico's van de doorgifte wegens het ontbreken van adequate bescherming in het derde land en het gebrek aan passende waarborgen. Dit is belangrijk om te kunnen beoordelen of de toestemmingsvereisten in wezen gelijkwaardig zijn aan die van de AVG.

107. Aangezien toestemming vrijelijk moet worden gegeven en specifiek, geïnformeerd en ondubbelzinnig moet zijn, zou het EDPB graag zien dat er in het adequaatheidsbesluit wordt verzekerd dat persoonsgegevens niet door een in de Republiek Korea gevestigde PG-verwerkingsverantwoordelijke aan een derde partij in een derde land worden doorgegeven wanneer er volgens de AVG geen geldige toestemming zou kunnen worden verleend, bijvoorbeeld wegens machtsongelijkheid.

108. Wat betreft gevallen waarin de PG-verwerkingsverantwoordelijke persoonsgegevens aan een overzeese derde partij kan verstrekken zonder dat daarvoor de toestemming van de betrokkene nodig is – d.w.z. wanneer 1) het doel van de gegevensverstrekking redelijk verband houdt met het oorspronkelijke doel van de gegevensverzameling (artikel 17, lid 4, WBP), of 2) het een van de in artikel 18, lid 2, WBP genoemde uitzonderingsgevallen betreft – neemt het EDPB nota van de verduidelijkingen die de toezichthouder in hoofdstuk 2 van Kennisgeving nr. 2021-1 geeft (en is het verheugd over het voornemen om aan de in Zuid-Korea gevestigde verwerkingsverantwoordelijke en de overzeese ontvanger de verplichting op te leggen om door middel van een rechtens bindend instrument, zoals een overeenkomst, een beschermingsniveau te waarborgen dat gelijkwaardig is aan dat van de WBP, onder andere met betrekking tot de rechten van betrokkenen).

3.1.12. Direct marketing

109. Ingevolge artikel 21, leden 2 en 3, AVG en de adequaatheidsreferentie moet de betrokkene te allen tijde kosteloos bezwaar kunnen maken tegen gegevensverwerking voor profileringsdoeleinden of ten behoeve van direct marketing.

110. Wat het recht op opschorting in artikel 37 WBP betreft, erkent het EDPB dat de Europese Commissie dit recht ook van toepassing acht wanneer gegevens ten behoeve van direct marketing worden gebruikt[47]. Het EDPB zou het toejuichen dat in het adequaatheidsbesluit aanvullende informatie en verduidelijkingen worden opgenomen met betrekking tot deze beoordeling en met name over de praktische toepassing van het opschortingsrecht in de context van direct marketing (verwijzingen naar relevante rechtspraak enz.). Het EDPB onderstreept in dit verband ook dat het recht om een aanbieder/gebruiker van kredietgegevens te vragen geen contact meer op te nemen voor het aanprijzen of aanbieden van goederen of diensten, uitdrukkelijk is vastgelegd in de kredietinformatiewet (artikel 37, lid 2).

111. Voorts is voor een dergelijke verwerking, zoals de Europese Commissie erkent[48], volgens het Zuid-Koreaanse recht in de regel de specifieke (aanvullende) toestemming van de betrokkene vereist (artikel 15, lid 1, punt 1, en artikel 17, lid 2, punt 1, WBP).

112. Aangezien niet kan worden uitgesloten dat vanuit de EER doorgegeven persoonsgegevens in Zuid-Korea voor dergelijke doeleinden worden verwerkt, zou het EDPB het ook toejuichen als in het

[47] Overweging 79 van het ontwerpbesluit.
[48] Ibid.

adequaatheidsbesluit werd verduidelijkt of betrokkenen het recht hebben om hun toestemming in te trekken[49] alsook om hen betreffende persoonsgegevens te doen wissen en niet verder te laten verwerken wanneer de verwerking op toestemming is gebaseerd (zoals het geval is bij verwerking voor marketingdoeleinden) en de betrokkenen hun toestemming hebben ingetrokken.

3.1.13. Geautomatiseerde besluitvorming en profilering

113. Zoals de Europese Commissie in het ontwerpbesluit erkent[50], bevatten de WBP en het WBP-uitvoeringsbesluit geen algemene bepalingen die zien op besluiten die gevolgen hebben voor de betrokkene en die uitsluitend op de geautomatiseerde verwerking van persoonsgegevens zijn gebaseerd. Toch kent het Zuid-Koreaanse rechtssysteem dergelijke voorschriften wel. Artikel 36, lid 2, van de kredietinformatiewet bevat regels betreffende geautomatiseerde besluiten, hoewel de toepassing daarvan buiten het toezicht van de toezichthouder lijkt te vallen (en als zodanig ook buiten het toepassingsgebied van het adequaatheidsbesluit – zie afdeling 2.3.2 ("Toepassingsgebied van het adequaatheidsbesluit")).

114. Zoals reeds is overwogen door de Groep gegevensbescherming artikel 29[51] in haar Advies 1/2016 betreffende het EU-VS-privacyschild, en door het EDPB in zijn eerdere advies over het adequaatheidsbesluit betreffende Japan[52], duiden het groeiende belang van geautomatiseerde besluitvorming, profilering en kunstmatige intelligentie (KI) erop dat in dit opzicht wellicht een meer beschermende benadering moet worden gevolgd. In tegenstelling tot het argument van de Europese Commissie[53] dat het onwaarschijnlijk is dat het ontbreken van specifieke voorschriften inzake geautomatiseerde besluitvorming in de WBP gevolgen zal hebben voor het beschermingsniveau voor persoonsgegevens die in de Unie zijn verzameld (aangezien eventuele besluiten op basis van geautomatiseerde verwerking in de regel worden genomen door een verwerkingsverantwoordelijke in de Unie die een rechtstreekse relatie met de betrokkene heeft), meent het EDPB dat het niet uitgesloten kan worden dat een in Zuid-Korea gevestigde PG-verwerkingsverantwoordelijke op basis van het adequaatheidsbesluit doorgegeven persoonsgegevens gebruikt voor geautomatiseerde besluitvorming (bijvoorbeeld in de context van tewerkstelling, voor het beoordelen van werkprestaties, betrouwbaarheid, gedrag enz.).

115. De ontwikkeling van nieuwe technologieën maakt het voor bedrijven gemakkelijker om geautomatiseerde besluitvormingssystemen in te voeren, of de invoering daarvan te overwegen, wat de positie van natuurlijke personen kan verzwakken. Wanneer besluiten die uitsluitend door deze geautomatiseerde systemen zijn genomen, rechtsgevolgen hebben voor natuurlijke personen of hen anderszins in aanmerkelijke mate treffen (bijvoorbeeld doordat zij op een zwarte lijst worden gezet en daardoor van hun rechten worden beroofd), is het van wezenlijk belang dat voldoende waarborgen bestaan, waaronder het recht om te worden geïnformeerd over de specifieke redenen die ten grondslag liggen aan het besluit en de onderliggende logica, om onjuiste of onvolledige informatie te

[49] Zie tevens punt 67; hoewel artikel 37, lid 1, van de kredietinformatiewet duidelijk voorziet in de mogelijkheid om toestemming in te trekken, wordt dit recht in de WBP maar twee keer genoemd en dan alleen in het kader van specifieke omstandigheden, namelijk in artikel 27, lid 1, punt 2, en artikel 39, lid 7.

[50] Zie overweging 81 van het ontwerpbesluit.

[51] Deze werkgroep werd opgericht op grond van artikel 29 van Richtlijn 95/46/EG, en was een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en privacy. De taken van de werkgroep zijn omschreven in artikel 30 van Richtlijn 95/46/EG en artikel 15 van Richtlijn 2002/58/EG. De Groep gegevensbescherming artikel 29 is inmiddels het EDPB geworden.

[52] Advies 28/2018 over het ontwerpuitvoeringsbesluit van de Europese Commissie betreffende de adequate bescherming van persoonsgegevens in Japan, goedgekeurd op 5 december 2018.

[53] Overweging 81 van het ontwerpbesluit.

corrigeren en om het besluit aan te vechten wanneer het is goedgekeurd op basis van onjuiste gegevens[54].

116. Het EDPB vindt het ontbreken van bepalingen in de WBP die zien op geautomatiseerde besluitvorming onrustbarend en verzoekt de Europese Commissie hier werk van te maken en de ontwikkeling van het Zuid-Koreaanse rechtskader op dit punt te blijven volgen.

3.1.14. Verantwoordingsplicht

117. Het Zuid-Koreaanse rechtskader bevat meerdere voorschriften op grond waarvan PG-verwerkingsverantwoordelijken passende technische en organisatorische maatregelen moeten treffen om te waarborgen en aan te kunnen tonen, onder andere aan de toezichthouder, dat zij daadwerkelijk aan hun verplichtingen inzake gegevensbescherming voldoen. Het EDPB is met name verheugd dat er een intern beheerplan moet worden vastgesteld (artikel 29 WBP), dat een zogenoemde privacyeffectbeoordeling (**PEB**) moet worden verricht voor verwerkingen met een buitengewoon risico van inbreuken op de privacy (artikel 33, lid 1, WBP en artikel 35 van het WBP-uitvoeringsbesluit), dat er regels bestaan betreffende de opleiding van en het toezicht op personeel (artikel 28 WBP) en dat er een privacyfunctionaris moet worden aangesteld (artikel 31 WBP in samenhang met artikel 32 van het WBP-uitvoeringsbesluit).

118. Het EDPB deelt de opvatting van de Europese Commissie dat deze voorschriften in wezen een gelijkwaardig beschermingsniveau waarborgen, zelfs waar zij enigszins afwijken van de AVG. Zo is er bijvoorbeeld geen bepaling die expliciet de onafhankelijkheid van de privacyfunctionaris waarborgt, maar is wel duidelijk vastgelegd dat die functionaris moet rapporteren aan de leidinggevende van de PG-verwerkingsverantwoordelijke (artikel 31, lid 4, WBP) en als gevolg van zijn werkzaamheden geen ongerechtvaardigde nadelen mag ondervinden (artikel 31, lid 5, WBP). Het EDPB stelt de Europese Commissie voor om bij de herziening van het adequaatheidsbesluit de daadwerkelijke toepassing van deze voorschriften te monitoren om te kunnen beoordelen of ze doeltreffend ten uitvoer worden gelegd.

3.2. Procedurele en handhavingsmechanismen

119. Op basis van de in de adequaatheidsreferentie vastgestelde criteria heeft het EDPB een analyse gemaakt van de volgende aspecten van het Zuid-Koreaanse gegevensbeschermingskader die onder het ontwerpbesluit vallen: het bestaan en de doeltreffende werking van een onafhankelijke toezichthoudende autoriteit, het bestaan van een systeem dat goede naleving waarborgt, en het bestaan van een systeem dat toegang biedt tot passende verhaalsmogelijkheden waarmee natuurlijke personen uit de EER hun rechten kunnen uitoefenen en verhaal kunnen nemen, zonder dat zij bij administratief beroep en beroep in rechte op hinderlijke belemmeringen stuiten.

120. Overeenkomstig hoofdstuk VI van de AVG en hoofdstuk 3 van de adequaatheidsreferentie moeten er in het derde land één of meer onafhankelijke toezichthoudende autoriteiten bestaan, die tot taak hebben de naleving van de gegevensbeschermings- en privacybepalingen te controleren, te waarborgen en te handhaven om een aan de EER gelijkwaardig beschermingsniveau te waarborgen.

121. De toezichthoudende autoriteit van het derde land moet haar taken en bevoegdheden volledig onafhankelijk en onpartijdig uitoefenen, zonder daarbij instructies te krijgen of te aanvaarden. Daarnaast moet de toezichthoudende autoriteit beschikken over alle noodzakelijke en beschikbare bevoegdheden en missies om toe te zien op de naleving van de gegevensbeschermingsrechten en het bewustzijn hieromtrent te bevorderen. De personeelsbezetting en de begroting van de

[54] WP 254, blz. 7.

toezichthoudende autoriteit verdienen eveneens aandacht. De toezichthoudende autoriteit moet ook op eigen initiatief onderzoek kunnen doen.

3.2.1. Bevoegde onafhankelijke toezichthoudende autoriteit

122. De onafhankelijke autoriteit die in de Republiek Korea is belast met het toezicht op en handhaving van de WBP, is de commissie voor de bescherming van persoonsgegevens (de toezichthouder). Die commissie bestaat uit een voorzitter, een vicevoorzitter en zeven commissieleden. De voorzitter en de vicevoorzitter worden benoemd door de president van de Republiek, op voordracht van de minister-president. Van de commissieleden worden er twee benoemd op voordracht van de voorzitter, twee op voordracht van vertegenwoordigers van de politieke partij waartoe de president van de Republiek behoort, en de overige drie op voordracht van vertegenwoordigers van andere politieke partijen (artikel 7, lid 2, punt 2, WBP). De toezichthouder wordt bijgestaan door een secretariaat (artikel 7, lid 13, WBP) en kan subcommissies instellen (bestaande uit drie commissieleden) voor het behandelen van lichte schendingen en terugkerende kwesties (artikel 7, lid 12, WBP).
123. Het EDPB erkent dat de toezichthouder ondanks de recente herstructurering, waarbij zijn status en bevoegdheden ingrijpend zijn gewijzigd, aanzienlijke inspanningen heeft verricht om de noodzakelijke infrastructuur uit te bouwen voor het uitvoeren van de WBP en de meest recente wijzigingen daarvan. De toezichthouder heeft bijvoorbeeld zijn reglement van orde vastgesteld, richtsnoeren voor de interpretatie van de WBP uitgewerkt, een hulp- en advieslijn opgezet voor ondernemers en natuurlijke personen die vragen hebben over gegevensbeschermingsvoorschriften, en een dienst voor klachtenbehandeling via bemiddeling in het leven geroepen. De belangrijkste taken van de toezichthouder bestaan met name in het geven van adviezen over wet- en regelgeving betreffende gegevensbescherming, het ontwikkelen van beleid en richtsnoeren inzake gegevensbescherming, het onderzoeken van inbreuken op individuele rechten, het behandelen van klachten en het bemiddelen in geschillen, het handhaven van de WBP, het bevorderen van onderwijs en promotie op het gebied van gegevensbescherming en het bevorderen van uitwisselingen en samenwerking met gegevensbeschermingsautoriteiten van derde landen.[55]

124. De benoemingen voor en samenstelling van de toezichthouder zijn geregeld in artikel 7, lid 2, WBP. Hoewel de toezichthouder onder de minister-president ressorteert (en de voorzitter en vicevoorzitter worden benoemd door de president van de Republiek op voordracht van de minister-president), schrijft de wet voor dat de leden van de toezichthouder hun taken onafhankelijk uitoefenen en daarbij volgens de wet en naar eer en geweten handelen. Het EDPB erkent dat in de WBP – en in het bijzonder in artikel 7, leden 4 tot en met 7 – institutionele en procedurele waarborgen zijn vastgelegd. Niettemin zou het EDPB het toejuichen, wanneer de Europese Commissie eventuele ontwikkelingen die de onafhankelijkheid van leden van de toezichthouder kunnen aantasten, nauwgezet zou volgen.

125. Voorts bevat het ontwerpbesluit nog geen analyse van de begroting van de toezichthouder, en evenmin van de financieringsbronnen en de doorzichtigheid van de begroting. Het EDPB is van mening dat terdege rekening moet worden gehouden met dit aspect, dat zowel wordt genoemd in artikel 56, lid 1, AVG als in de beginselen en mechanismen voor de procedures/handhaving met betrekking tot gegevensbescherming die volgens de adequaatheidsreferentie moeten worden meegenomen bij de beoordeling van een systeem van een land of internationale organisatie, omdat het een indicator vormt van de economische en personele middelen waarover de toezichthouder beschikt voor het onafhankelijk uitvoeren van zijn wettelijke verplichtingen en taken met betrekking tot gegevensbescherming. Het EDPB adviseert de Europese Commissie derhalve om hier in het adequaatheidsbesluit uitgebreider aandacht aan te besteden.

[55] De taken en bevoegdheden van de toezichthouder zijn hoofdzakelijk neergelegd in artikel 7, leden 8 en 9, en de artikelen 61 tot en met 66 WBP.

3.2.2. Bestaan van een gegevensbeschermingssysteem dat goede naleving waarborgt

126. Wat handhaving betreft, erkent het EDPB dat de toezichthouder een reeks handhavingsbevoegdheden en sanctiemiddelen tot zijn beschikking heeft, zoals vastgelegd in de WBP en de kredietinformatiewet. Het neemt nota van de verduidelijkingen in Kennisgeving nr. 2021-1 waaruit blijkt dat de voorwaarden genoemd in artikel 64, lid 1, WBP en artikel 45, lid 4, van de kredietinformatiewet[56] altijd van toepassing zijn ingeval één of meer van de beginselen, rechten of verplichtingen die in de wet zijn opgenomen voor het beschermen van persoonsgegevens niet in acht worden genomen. Het EDPB doet de Europese Commissie evenwel de aanbeveling om nauwgezet te monitoren hoe de toezichthouder in de praktijk gebruikmaakt van zijn bevoegdheid om overtreders te gelasten de in artikel 64, lid 1, WBP of artikel 45, lid 4, van de kredietinformatiewet genoemde maatregelen te treffen die hij passend acht.

127. Wat betreft de corrigerende maatregelen waarin artikel 64, lid 1, WBP voorziet, is de toezichthouder bevoegd om in geval van niet-naleving daarvan een geldboete op te leggen van maximaal 50 miljoen Zuid-Koreaanse won (36 564 EUR) (artikel 75, lid 2, punt 13, WBP). Het EDPB vreest dat dit te laag is om, zoals de wet beoogt, potentiële overtreders af te schrikken en de handhaving van gegevensbeschermingsvoorschriften te waarborgen. De geldboete lijkt niet hoog genoeg om te kunnen overtuigen, zeker in het geval van grote organisaties of ondernemingen met aanzienlijke financiële middelen.

128. De toezichthouder kan eisen dat het hoofd van een centrale bestuursinstelling onderzoek doet naar een PG-verwerkingsverantwoordelijke of samen met de toezichthouder overtredingen van de WBP onderzoekt, en zelfs dat de instelling corrigerende maatregelen treft ten aanzien van PG-verwerkingsverantwoordelijken die onder haar ressorteren (artikel 63, leden 4 en 5, WBP). In dat verband merkt het EDPB op dat, ondanks de informatie die in overweging 122 van het ontwerpbesluit wordt verstrekt, het karakter van deze instellingen en hun rechtsverhouding met de toezichthouder in het algemeen vrij onduidelijk zijn. Daar komt nog bij dat in artikel 68, lid 1, WBP veel entiteiten worden genoemd waaraan de bevoegdheden van de toezichthouder gedelegeerd kunnen worden. Hoewel deze bepaling schijnbaar alleen is toegepast met betrekking tot het Zuid-Koreaanse agentschap voor internet- en beveiligingsaangelegenheden[57], zou het EDPB graag meer duidelijkheid krijgen over het karakter van de mogelijke interacties tussen de voornoemde entiteiten en zien dat deze bepaling nauwgezet wordt gemonitord om zeker te zijn van de onafhankelijkheid van de entiteiten die met de toepassing van de gegevensbeschermingsvoorschriften zijn belast.

129. In het Zuid-Koreaanse sanctiesysteem lijken verschillende soorten sancties te kunnen worden gecombineerd, van corrigerende maatregelen en administratieve boetes tot strafrechtelijke sancties, die vermoedelijk behoorlijk afschrikwekkend werken. De Zuid-Koreaanse autoriteiten hebben meerdere voorbeelden aangevoerd van geldboetes die recentelijk door de toezichthouder zijn opgelegd. Zo werd een onderneming in december 2020 beboet ten belope van 6,7 miljard Zuid-Koreaanse won voor het overtreden van verschillende WBP-bepalingen, en kreeg een andere onderneming, die zich bezighoudt met KI-technologie, op 28 april 2021 een boete van 103,3 miljoen Zuid-Koreaanse won voor het overtreden van voorschriften op het gebied van de rechtmatigheid van verwerkingen, met name het toestemmingsvereiste, en de verwerking van gepseudonimiseerde gegevens.

130. Hoewel bovengenoemde bedragen een afschrikwekkend effect kunnen hebben, zou het EDPB ingenomen zijn met aanvullende informatie over de wijze waarop de toezichthouder administratieve boetes berekent, bijvoorbeeld in geval van niet-naleving van een corrigerende maatregel die is

[56] Namelijk "*een overtreding van de wet wordt geacht vermoedelijk inbreuk te maken op individuele rechten en vrijheden met betrekking tot persoonsgegevens en het niet nemen van maatregelen veroorzaakt waarschijnlijk schade die moeilijk ongedaan kan worden gemaakt*".

[57] Zie overweging 117 van het ontwerpbesluit en artikel 62 van het WBP-uitvoeringsbesluit.

opgelegd op grond van artikel 64, lid 1, WBP (zie artikel 75, lid 2, punt 13, WBP). Dit is met name relevant voor strafrechtelijke sancties en de toepassing van de (Zuid-Koreaanse) strafwet.

3.2.3. Het gegevensbeschermingssysteem moet betrokkenen ondersteunen en bijstaan bij het uitoefenen van hun rechten en het benutten van passende verhaalsmogelijkheden

131. Wat verhaalsmogelijkheden betreft, biedt het Zuid-Koreaanse systeem verschillende mechanismen om een passende bescherming te waarborgen. Het biedt in het bijzonder effectieve mechanismen voor het handhaven van individuele rechten door het instellen van administratief beroep of beroep in rechte, waarbij ook schadevergoeding kan worden gevorderd.

132. Behalve de mogelijkheid om naar de bestuursrechter of gewone rechter te stappen, kent het Zuid-Koreaanse systeem ook alternatieve mechanismen waarvan natuurlijke personen gebruik kunnen maken om verhaal te nemen, zoals uitgelegd in de overwegingen 132 en 133 van het ontwerpbesluit, die respectievelijk betrekking hebben op het privacycallcenter en de commissie voor geschillenbeslechting via bemiddeling. Aangezien dit aanvullende verhaalsmogelijkheden zijn, zou het EDBP graag meer weten over hun aanvullende waarde voor betrokkenen van wie persoonsgegevens aan Zuid-Korea worden doorgegeven, ten opzichte van de beroepswegen via de toezichthouder of de rechter.

4. TOEGANG TOT EN GEBRUIK VAN PERSOONSGEGEVENS DIE VANUIT DE EU ZIJN DOORGEGEVEN DOOR OVERHEIDSINSTANTIES IN ZUID-KOREA

133. Wat de beoordeling van het gegevensbeschermingsniveau op de gebieden rechtshandhaving en nationale veiligheid betreft, geeft de Europese Commissie in het ontwerpbesluit en de beschikbare bijlagen daarbij uitgebreide informatie. De meeste feitelijke bevindingen en vaststellingen van de Europese Commissie worden daarom niet opnieuw weergegeven in dit advies.

134. De Europese Commissie concludeert voor bovengenoemde gebieden dat het beschermingsniveau overeenkomt met de eisen die zijn neergelegd in de rechtspraak van het HvJ, en bijgevolg in wezen gelijkwaardig kan worden geacht aan dat van de Europese Unie.

135. Het EDPB zou er in het algemeen op willen wijzen dat zelfs wanneer het erop lijkt – of de Europese Commissie beweert – dat vanuit de EU naar Zuid-Korea doorgegeven gegevens waarschijnlijk buiten het toepassingsgebied van de relevante Zuid-Koreaanse wetgeving vallen, het nog steeds aangewezen is om te beoordelen of het beschermingsniveau in Zuid-Korea passend is. De relevantie van dergelijke gevallen blijkt ook uit feit dat de Europese Commissie deze in het ontwerpbesluit heeft behandeld.

4.1. Algemeen kader voor gegevensbescherming in de context van overheidstoegang

136. Voor een beoordeling van de toegang van overheidsinstanties tot persoonsgegevens en de bescherming van het recht op privacy en gegevensbescherming in dergelijke gevallen, moet worden gekeken naar verschillende Zuid-Koreaanse wetten. Het EDPB merkt om te beginnen op dat de WBP, als een van de belangrijkste wetten inzake gegevensbescherming, wordt geacht een breed toepassingsgebied te hebben. Hoewel de WBP volledig geldt voor gegevensverwerking ten behoeve van rechtshandhaving, is de wet echter beperkt van toepassing wanneer het gaat om nationale veiligheid. Ingevolge artikel 58, lid 1, punt 2, WBP zijn de hoofdstukken III tot en met VII niet van toepassing op de verwerking van persoonsgegevens voor nationaleveiligheidsdoeleinden. De hoofdstukken I, II, IX en X daarentegen zijn dat wel. Bijgevolg gelden de kernbeginselen van de WBP,

alsook de fundamentele waarborgen voor de rechten van betrokkenen en de bepalingen die zien op toezicht, handhaving en voorzieningen in rechte, ook voor de toegang tot en het gebruik van persoonsgegevens door nationale veiligheidsdiensten.

137. Ook in de Zuid-Koreaanse grondwet zijn essentiële beginselen van gegevensbescherming vastgelegd, namelijk rechtmatigheid, noodzakelijkheid en evenredigheid. Deze beginselen zijn tevens van toepassing op de toegang tot persoonsgegevens door Zuid-Koreaanse overheidsinstellingen op het gebied van rechtshandhaving en nationale veiligheid.[58]

138. Op het gebied van rechtshandhaving kunnen de politie, aanklagers, rechtbanken en andere overheidsinstellingen persoonsgegevens verzamelen op grond van specifieke wetgeving, te weten de **strafvorderingswet**, de **privacywet**, de **telecomwet** en de **wet financiële transacties**, die ziet op de vervolging en preventie van witwassen en terrorismefinanciering. In deze specifieke wetten zijn aanvullende beperkingen, waarborgen en uitzonderingen neergelegd.

139. Op het gebied van nationale veiligheid kan de **nationale inlichtingendienst** persoonsgegevens verzamelen en communicatie onderscheppen op basis van de **wet op de nationale inlichtingendienst** en aanvullende "nationale veiligheidswetten"[59]. Het EDPB begrijpt dat de nationale veiligheidsdienst bij de uitoefening van zijn bevoegdheden zowel voornoemde wettelijke bepalingen als de WBP in acht moet nemen.

140. Het EDPB vraagt de Europese Commissie om duidelijk te maken of er naast de nationale inlichtingendienst in Zuid-Korea nog andere instanties bestaan die taken op het gebied van nationale veiligheid uitoefenen, omdat in bijlage I, hoofdstuk 6, van het ontwerpbesluit de indruk wordt gewekt dat de nationale inlichtingendienst louter als voorbeeld wordt genoemd en niet de enige nationale veiligheidsdienst is.

4.2. Bescherming en waarborgen ten aanzien van communicatiebevestigingsgegevens in de context van overheidstoegang voor rechtshandhavingsdoeleinden

141. Op basis van de toepasselijke wet, de privacywet, kunnen rechtshandhavingsinstanties twee soorten maatregelen nemen om toegang te krijgen tot communicatiegegevens. De privacywet maakt onderscheid tussen communicatiebeperkende maatregelen, waaronder zowel het verzamelen van de inhoud van gewone post en het rechtstreeks onderscheppen van de inhoud van telecommunicatie[60] als het verzamelen van communicatiebevestigingsgegevens valt. Onder "communicatiebevestigingsgegevens" vallen onder meer de datum van telecommunicatie, de begin- en eindtijd ervan, het aantal in- en uitgaande gesprekken, alsook het abonneenummer van de tegenpartij, de gebruiksfrequentie, logbestanden over het gebruik van telecomdiensten en locatiegegevens.[61]

142. Het EDPB merkt op dat ten aanzien van communicatiebevestigingsgegevens niet dezelfde waarborgen lijken te gelden als voor gegevens die door middel van communicatiebeperkende maatregelen zijn verzameld, d.w.z. gegevens over de inhoud. Sterker nog, het valt het EDPB op dat ten aanzien van het verzamelen van inhoud meer waarborgen gelden dan ten aanzien van het verzamelen van communicatiegegevens voor rechtshandhavingsdoeleinden. Ten eerste is het verzamelen van bevestigingsgegevens, in tegenstelling tot inhoudelijke gegevens, niet alleen toegestaan voor onderzoek naar bepaalde ernstige misdrijven maar ook wanneer dit noodzakelijk wordt geacht voor

[58] Overweging 145 van het ontwerpbesluit.
[59] Bijvoorbeeld de privacywet, de wet op terrorismebestrijding voor de bescherming van burgers en de openbare veiligheid en de telecomwet.
[60] Artikel 2, leden 6 en 7, en artikel 3, lid 2, van de privacywet.
[61] Artikel 2, lid 11, van de privacywet.

"eender welk onderzoek of de tenuitvoerlegging van een straf" (artikel 13, lid 1, van de privacywet). Ten tweede heeft het verzamelen van bevestigingsgegevens in beginsel niet de vorm van een maatregel die alleen in laatste instantie is toegestaan, wanneer het voorkomen van een misdrijf, de arrestatie van een misdadiger of het verzamelen van bewijsmateriaal via een andere maatregel niet goed mogelijk is.[62] Integendeel, wanneer een aanklager of ambtenaar van de gerechtelijke politie dit "noodzakelijk acht" voor het onderzoeken van een misdrijf of ten uitvoer leggen van een straf, mogen er altijd communicatiebevestigingsgegevens worden verzameld. Wel geldt in dit verband een uitzondering voor traceringsgegevens in real time en communicatiebevestigingsgegevens die betrekking hebben op een specifiek grondstation (artikel 13, lid 2, van de privacywet). Ten derde moeten rechtshandhavingsinstanties die inhoudelijke communicatiegegevens verzamelen, daar onmiddellijk mee stoppen wanneer toegang niet langer nodig wordt geacht.[63] Met betrekking tot communicatiebevestigingsgegevens is dit op zijn minst niet uitdrukkelijk in de wet of het bijbehorende uitvoeringsbesluit bepaald.

143. Het EDPB neemt nota van het feit dat het verzamelen van communicatiebevestigingsgegevens slechts kan plaatsvinden op basis van een gerechtelijk bevel. Bovendien schrijft de privacywet voor dat gedetailleerde informatie moet worden verstrekt in zowel het verzoekschrift tot uitvaardiging van het bevel als in het bevel zelf.[64] Het vereiste van een voorafgaande gerechtelijke machtiging beperkt de beoordelingsvrijheid van rechtshandhavingsinstanties bij het toepassen van de wet en zorgt ervoor dat per geval wordt getoetst of er voldoende gronden voor het verzamelen van communicatiebevestigingsgegevens bestaan. Het EDPB erkent ook dat de Zuid-Koreaanse wetgeving niet lijkt te voorzien in een algemene en willekeurige bewaring van dergelijke gegevens. Bijgevolg heeft de toegang van overheidsinstellingen tot die gegevens altijd betrekking op gegevens die nog bewaard worden voor factureringsdoeleinden en voor het verstrekken van de communicatiediensten zelf.

144. Het EDPB wijst er echter op dat het HvJ betwijfelt dat verkeersgegevens minder gevoelig zijn dan andere gegevens, in het bijzonder gegevens over de inhoud.[65] Aangezien voor communicatiebevestigingsgegevens in verschillende opzichten minder bescherming wordt geboden dan voor inhoudelijke gegevens, verzoekt het EDPB de Europese Commissie om nauwgezet te monitoren of de waarborgen die de Zuid-Koreaanse wetgeving ten aanzien van deze categorie persoonsgegevens biedt, een beschermingsniveau opleveren dat in wezen gelijkwaardig is aan het in de EU gewaarborgde niveau, in het bijzonder wat de evenredigheid en voorzienbaarheid van de wetgeving betreft.

[62] Dit is volgens artikel 3, lid 2, en artikel 5, lid 1, van de privacywet wel het geval ten aanzien van inhoudelijke gegevens.

[63] Artikel 2 van het uitvoeringsbesluit bij de privacywet.

[64] Overweging 156 van het ontwerpbesluit.

[65] Arrest van het Hof van Justitie van 6 oktober 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, punt 71: "*De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 27 en 37, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 99 en 100).*"

4.3. Toegang tot communicatiegegevens door overheidsinstellingen in de Republiek Korea voor nationaleveiligheidsdoeleinden

145. Wat betreft het rechtskader voor de toegang van nationale veiligheidsdiensten tot vanuit de EER naar Zuid-Korea doorgegeven communicatiegegevens, heeft het EDPB twee zorgpunten vastgesteld, die allebei betrekking hebben op de regeling voor de toegang tot communicatie tussen personen zonder de Zuid-Koreaanse nationaliteit die tot een specifieke reeks van gebruiksgevallen behoort (zie punt 29). Bepaalde waarborgen die anders wel gelden, met betrekking tot zowel communicatiebevestigingsgegevens als gegevens over inhoud, gelden in die gevallen niet. Met andere woorden: in die specifieke gevallen gelden ten aanzien van deze gegevens niet dezelfde waarborgen als wanneer zij deel uitmaken van communicatie tussen personen van wie er ten minste één de Zuid-Koreaanse nationaliteit heeft.

4.3.1. Geen verplichting om personen in kennis te stellen van overheidstoegang voor communicatie tussen vreemdelingen

146. In de hierboven beschreven situatie, namelijk communicatie waarbij geen van de deelnemers de Zuid-Koreaanse nationaliteit heeft, zijn de nationale veiligheidsdiensten niet verplicht personen ervan op de hoogte te stellen dat hun gegevens worden verzameld en verwerkt. Het EDPB erkent dat deze kwestie alleen gevolgen heeft voor bepaalde gevallen. Ten eerste gelden, zoals reeds is opgemerkt, wanneer ten minste één persoon met de Zuid-Koreaanse nationaliteit betrokken is bij de communicatie, de kennisgevingsvereisten van de privacywet voor alle deelnemers, ongeacht hun nationaliteit.[66] Ten tweede is het verzamelen van persoonsgegevens uit communicatie tussen personen die allemaal een buitenlandse nationaliteit hebben, beperkt tot een specifieke reeks gebruiksgevallen. Meer in het bijzonder strekt het recht van toegang zich in die gevallen uit tot communicatie a) uit landen die vijandig staan tegenover de Republiek Korea, b) tussen buitenlandse instellingen, groepen of onderdanen die verdacht worden van anti-Zuid-Koreaanse activiteiten[67], of c) tussen leden van groepen die actief zijn op het Koreaanse schiereiland maar feitelijk buiten de rechtsmacht van de Republiek Korea vallen, alsmede in het buitenland gevestigde overkoepelende organisaties van die groepen. Berichten tussen personen uit de EU die worden doorgegeven vanuit de EU naar Zuid-Korea kunnen zodoende alleen voor nationaleveiligheidsdoeleinden worden verzameld als zij in een van de drie voornoemde categorieën vallen.[68] Verder begrijpt het EDPB uit de aanvullende toelichtingen van de Europese Commissie dat het toepasselijke rechtskader niet voorziet in het onderscheppen van gegevensverkeer buiten Zuid-Korea.

147. Vandaar dat de praktische gevolgen van het ontbreken van een kennisgevingsvereiste wellicht kunnen worden geacht beperkt te zijn. Het EDPB onderstreept echter het belang van de (latere) kennisgeving van overheidstoegang, in het bijzonder met het oog op doeltreffende voorzieningen in rechte. Volgens het HvJ is kennisgeving aan de betrokken personen "*noodzakelijk om die personen in staat te stellen hun uit de artikelen 7 en 8 van het Handvest voortvloeiende rechten uit te oefenen, inzage te vragen in de persoonsgegevens die in real time zijn opgevraagd, en in voorkomend geval rectificatie of vernietiging van die gegevens te verlangen, alsook overeenkomstig artikel 47, eerste alinea, van het Handvest een doeltreffende voorziening in rechte in te stellen*".[69] Overheidstoegang ten behoeve van de nationale veiligheid omvat vaak geheime surveillancemaatregelen, waarbij de personen die daar

[66] Overweging 192 van het ontwerpbesluit.
[67] Zie bijlage II, voetnoot 244, ingevolge waarvan het begrip "anti-Zuid-Koreaanse activiteiten" verwijst naar activiteiten die een bedreiging vormen voor het bestaan en de veiligheid van het land, de democratische orde of de overleving en vrijheid van het volk.
[68] Overweging 187 van het ontwerpbesluit.
[69] Arrest van het Hof van Justitie van 6 oktober 2020, La Quadrature du Net e.a., gevoegde zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, punt 190.

het voorwerp van zijn, de betrokkenen, niet weten dat hun gegevens worden verwerkt. Er is dan ook "*in beginsel weinig ruimte voor een gang naar de rechter door de betrokken persoon, tenzij laatstgenoemde in kennis is gesteld van de maatregelen die zonder zijn of haar medeweten zijn getroffen en dus in staat is om de wettigheid ervan met terugwerkende kracht te betwisten of, in het andere geval, tenzij een persoon die vermoedt dat zijn of haar communicatie is of wordt onderschept de tussenkomst van de rechter kan inroepen, zodat de bevoegdheid van de rechter niet afhankelijk is van een kennisgeving aan de betrokkene dat zijn of haar communicatie is onderschept*"[70]. In dit verband, en in overeenstemming hiermee, heeft het EDBP tal van keren zijn bezorgdheid geuit over het ontbreken van doeltreffende voorzieningen in rechte bij surveillancezaken. Het EDPB benadrukt dat het geheimhouden van overheidsmaatregelen niet tot gevolg mag hebben dat dergelijke maatregelen feitelijk niet aangevochten kunnen worden. Tegen deze achtergrond dient de vraag of het ontbreken van een kennisgevingsvereiste voor communicatie tussen personen met een buitenlandse nationaliteit gevolgen heeft voor het in het ontwerpbesluit beoordeelde beschermingsniveau, te worden beantwoord als onderdeel van een algemene beoordeling, waarbij met name gekeken wordt naar de toezichtsmechanismen en verhaalsmogelijkheden waarin het Zuid-Koreaanse recht voorziet (zie de afdelingen 4.7 en 4.8).

148. Daarnaast merkt het EDPB in dit verband op dat in de wetgeving tamelijk vage termen worden gebruikt, zoals "anti-Zuid-Koreaanse activiteiten" of "antinationale activiteiten"[71], en dat niet duidelijk is hoe deze volgens het Zuid-Koreaanse recht moeten worden uitgelegd. Het EDPB verzoekt de Europese Commissie om te monitoren hoe deze termen in het Zuid-Koreaanse recht worden uitgewerkt en of de praktische toepassing ervan voldoet aan de eisen van evenredigheid die uit het EU-recht voortvloeien.

4.3.2. Geen voorafgaande onafhankelijke toestemming voor het verzamelen van gegevens uit communicatie tussen vreemdelingen

149. Het verzamelen van EER-persoonsgegevens uit communicatie tussen personen zonder de Zuid-Koreaanse nationaliteit (in een van de bovengenoemde gebruiksgevallen), met het oog op verwerking in Zuid-Korea voor nationaleveiligheidsdoeleinden, is niet onderworpen aan de voorafgaande goedkeuring van een onafhankelijke instantie (zoals wel het geval is voor communicatie waarbij ten minste één deelnemer de Zuid-Koreaanse nationaliteit heeft).[72]

150. Vooral in het licht van de recente uitspraken van het EHRM in de zaken Big Brother Watch e.a. tegen Verenigd Koninkrijk en Centrum för Rättvisa tegen Zweden, acht het EDPB het noodzakelijk om te onderzoeken of dit een kritieke tekortkoming in het Zuid-Koreaanse kader voor gegevensbescherming vormt. Het EDPB brengt in dit verband in herinnering dat, zoals ook wordt benadrukt in de bijgewerkte aanbevelingen over de Europese essentiële garanties voor surveillancemaatregelen[73], in artikel 6, lid 3, van het Verdrag betreffende de Europese Unie wordt bepaald dat de grondrechten die in het EVRM zijn verankerd, als algemene beginselen deel uitmaken van het recht van de EU, ofschoon het EVRM, zoals het HvJ in zijn rechtspraak in herinnering brengt, zolang de Europese Unie er geen partij

[70] Arresten van het EHRM van 25 mei 2021, Big Brother Watch e.a. tegen Verenigd Koninkrijk, ECLI:CE:ECHR:2021:0525JUD005817013, § 337, en 4 december 2015, Roman Zakharov tegen Rusland, ECLI:CE:ECHR:2015:1204JUD004714306, § 234.

[71] De Europese Commissie heeft uitgelegd dat hiermee volgens een toelichting van de Zuid-Koreaanse regering activiteiten worden bedoeld "die een bedreiging vormen voor het bestaan en de veiligheid van het land, de democratische orde of de overleving en vrijheid van het volk". Zie tevens voetnoot 319 van het ontwerpbesluit.

[72] Zie overweging 190 van het ontwerpbesluit.

[73] Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, punten 10 en 11.

bij is, geen formeel in de rechtsorde van de Unie opgenomen rechtsinstrument is[74]. Derhalve moet het in artikel 45 AVG vereiste beschermingsniveau van de grondrechten worden gemeten op basis van de bepalingen van die verordening, gelezen in het licht van de in het Handvest verankerde grondrechten. Dat gezegd zijnde, moeten ingevolge artikel 52, lid 3, van het Handvest de daarin vervatte rechten die corresponderen met in het EVRM gewaarborgde rechten, dezelfde inhoud en reikwijdte hebben als in het EVRM. Bijgevolg moet de rechtspraak van het EHRM met betrekking tot rechten die ook zijn neergelegd in het Handvest, in acht worden genomen als een minimumbeschermingsniveau voor de uitlegging van de corresponderende rechten in het Handvest, tenzij het Handvest, zoals uitgelegd door het HvJ, een hoger beschermingsniveau biedt.[75]

151. Het EDPB merkt op dat voorafgaande (onafhankelijke) goedkeuring van surveillancemaatregelen weliswaar wordt geacht een belangrijke waarborg tegen willekeur te zijn, maar dat uit de rechtspraak van het HvJ niet kan worden afgeleid dat voorafgaande goedkeuring uit het oogpunt van evenredigheid absoluut vereist is. Het EHRM heeft nu echter uitdrukkelijk vastgesteld dat voor onderschepping in bulk een voorafgaande, onafhankelijke goedkeuring vereist is.[76] Hoewel dit niet uitdrukkelijk in het ontwerpbesluit staat vermeld, begrijpt het EDPB dat het rechtskader van de Republiek Korea niet voorziet in onderschepping in bulk, alleen in de gerichte onderschepping van telecommunicatie.[77] De Europese Commissie heeft dit bevestigd.

152. Niettemin blijkt uit bovengenoemde uitspraken van het EHRM, die in lijn zijn met de rechtspraak van het HvJ[78] en eerdere rechtspraak van het EHRM zelf[79], eens te meer het belang van uitgebreid toezicht door onafhankelijke toezichthoudende autoriteiten. Het EDPB benadrukt dat onafhankelijk toezicht in alle fasen van het proces waarbij de overheid zich voor rechtshandhavings- of nationaleveiligheidsdoeleinden toegang tot persoonsgegevens verschaft, een belangrijke waarborg vormt tegen willekeurige surveillancemaatregelen en dus van belang is voor de beoordeling of een passend beschermingsniveau wordt geboden. De garantie van onafhankelijkheid van de toezichthoudende autoriteiten in de zin van artikel 8, lid 3, van het Handvest moet waarborgen dat effectief en betrouwbaar toezicht wordt gehouden op de naleving van de voorschriften voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Dat geldt in het bijzonder wanneer de betrokkene, wegens het karakter van geheime surveillance, niet in staat wordt gesteld de maatregel te laten toetsen of rechtstreeks deel te nemen aan een toetsingsprocedure vóór of tijdens de tenuitvoerlegging ervan.

153. Het ontbreken van voorafgaande, onafhankelijke goedkeuring kan op zichzelf niet beschouwd worden als een aanzienlijke tekortkoming in het Zuid-Koreaanse recht ten aanzien van de vraag of het beschermingsniveau voor persoonsgegevens in wezen gelijkwaardig is. Nogmaals, bij die beoordeling

[74] Arrest van het Hof van Justitie van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, ECLI:EU:C:2020:559 (hierna: "Schrems II"), punt 98.

[75] Arrest van het Hof van Justitie van 6 oktober 2020, La Quadrature du Net e.a., gevoegde zaken C-511/18, C-512/18 en C-520/18, punt 124.

[76] Arrest van het EHRM van 25 mei 2021, Big Brother Watch e.a. tegen Verenigd Koninkrijk, ECLI:CE:ECHR:2021:0525JUD005817013, § 351: "voor onderschepping in bulk [moet] vooraf toestemming [...] worden gegeven door een onafhankelijk orgaan", "voor onderschepping in bulk [is] toestemming nodig van een onafhankelijk orgaan, d.w.z. een orgaan dat onafhankelijk is van de uitvoerende macht".

[77] Alleen bijlage II, afdeling 3.2, bevat een uitdrukkelijke verklaring over nationaleveiligheidsdoeleinden, wanneer wordt aangegeven dat de beperkingen en waarborgen "*ervoor zorgen dat het verzamelen en verwerken niet verder gaat dan wat strikt noodzakelijk is voor het bereiken van een gerechtvaardigd doel. Dit sluit elke vorm van massaal en ongericht verzamelen van persoonsgegevens voor nationaleveiligheidsdoeleinden uit.*"

[78] Zie bijvoorbeeld het arrest van het Hof van Justitie van 21 december 2016, Tele2 Sverige en Watson e.a., gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970.

[79] Zie bijvoorbeeld het arrest van het EHRM van 4 december 2015, Roman Zakharov tegen Rusland, ECLI:CE:ECHR:2015:1204JUD004714306.

moet worden gekeken naar alle omstandigheden van het geval, in het bijzonder de doeltreffendheid van het toezicht achteraf en de beroepsmogelijkheden waarin het Zuid-Koreaanse rechtskader voorziet (zie hieronder de afdelingen 4.7 en 4.8).

4.4. Vrijwillige verstrekking van gegevens

154. Ingevolge artikel 83, lid 3, van de telecomwet kunnen aanbieders van telecommunicatiediensten op vrijwillige basis zogenoemde "abonneegegevens"[80] verstrekken op verzoek van nationale veiligheidsdiensten en rechtshandhavingsinstanties. Hoewel het EDPB erkent dat het maar zelden zal voorkomen dat deze vrijwillige verstrekking van abonneegegevens persoonsgegeven betreft die vanuit de EER naar Zuid-Korea zijn doorgegeven, moeten – zoals hierboven reeds vermeld – ook deze gevallen meegenomen in de beoordeling van het gegevensbeschermingsniveau.

155. Het EDPB begrijpt dat in deze gevallen de gegevensbeschermingswaarborgen van de WBP van toepassing zijn. Zowel overheidsinstanties als telecomaanbieders moeten zich daaraan houden[81] en beide kunnen bij een inbreuk op de rechten en vrijheden van betrokkenen aansprakelijk worden gesteld[82]. Verder begrijpt het EDPB dat telecomaanbieders niet verplicht zijn aan dergelijke verzoeken gevolg te geven.

156. Wat betreft de mogelijkheid voor nationale autoriteiten om voor rechtshandhavings- en in het bijzonder nationaleveiligheidsdoeleinden toegang te krijgen tot abonneegegevens door middel van "vrijwillige verstrekking" door telecomaanbieders, bestaat desalniettemin bezorgdheid dat dit een verhoogd risico meebrengt op een inbreuk op de rechten en vrijheid van betrokkenen, vooral het recht te worden geïnformeerd.

157. Ingevolge artikel 58, lid 1, punt 2, WBP zijn de bepalingen van hoofdstuk III tot en met VII niet van toepassing op persoonsgegevens die op verzoek worden verstrekt voor nationaleveiligheidsdoeleinden. De bepalingen van bijvoorbeeld artikel 18 ("Beperking van gebruik en verstrekking van persoonsgegevens voor een ander dan het oorspronkelijke doel") en artikel 20 ("Kennisgeving van bronnen enz. van persoonsgegevens die door derden zijn verstrekt") van de WBP zijn bijgevolg niet op dergelijke verzoeken van toepassing. Wanneer een nationale veiligheidsdienst een verzoek indient, doet zich derhalve enerzijds de vraag voor of artikel 58, lid 1, punt 2, ook de toepassing van de WBP op telecomaanbieders uitsluit en anderzijds of de uitsluiting van de toepassing van artikel 20 zich in dat geval uitstrekt tot de bijbehorende bepaling in hoofdstuk 3 van bijlage I ("Kennisgeving ingeval persoonsgegevens niet zijn verkregen van de betrokkene (artikel 20)"). Als dat het geval is en artikel 58, lid 1, punt 2, ook betrekking heeft op telecomaanbieders, bestaat op basis van de beschikbare informatie het risico dat er geen wettelijke verplichting bestaat om de betrokkene op de hoogte te brengen van de vrijwillige verstrekking.

158. Het EDPB is bijgevolg bezorgd dat hierdoor van informatievereisten een dode letter wordt gemaakt en het voor betrokkenen een stuk moeilijker wordt om hun gegevensbeschermingsrechten te doen gelden en met name om in beroep te gaan bij de rechter. Het EDPB verzoekt de Europese Commissie om de reikwijdte van de relevante bepalingen te verduidelijken.

[80] Er kan naar de volgende datasets worden gevraagd: namen, registratienummers voor ingezetenen, adressen en telefoonnummers van gebruikers, data waarop gebruikers een abonnement hebben genomen/opgezegd en identificatiecodes (voor het identificeren van de rechtmatige gebruiker van computersystemen of communicatienetwerken).
[81] Zie de overwegingen 164 en 194 van het ontwerpbesluit.
[82] Zie overweging 166 van het ontwerpbesluit.

4.5. Aanvullend gebruik van informatie

159. Het beginsel van doelbinding is een kernvereiste in de wetgeving inzake gegevensbescherming. Volgens dit beginsel mogen persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Overheidsinstanties mogen volgens het EU-recht wel persoonsgegevens verwerken met het oog op het voorkomen, onderzoeken en vervolgen van strafbare feiten, zelfs wanneer die gegevens oorspronkelijk voor een ander doel zijn verkregen, indien de toepasselijke wetgeving in een rechtsgrond voor die verwerking voorziet en de verdere verwerking niet onevenredig is[83].

160. Het EDPB merkt hieromtrent op dat het Zuid-Koreaanse kader voor gegevensbescherming ten aanzien van het verdere gebruik van gegevens voor rechtshandhavings- en nationaleveiligheidsdoeleinden in vergelijkbare waarborgen en beperkingen als het EU-recht voorziet (bijv. artikel 3, leden 1 en 2, WBP, waarin het beginsel van doelbinding is vastgelegd).

4.6. Verdere doorgifte en het delen van inlichtingen

161. Artikel 44 AVG bepaalt dat de doorgifte en verdere doorgifte van persoonsgegevens alleen mag plaatsvinden indien het door de AVG gewaarborgde beschermingsniveau niet wordt ondermijnd. Derhalve mag het beschermingsniveau voor persoonsgegevens die vanuit de EER naar Zuid-Korea worden doorgeven, niet worden ondermijnd door de verdere doorgifte aan ontvangers in een derde land. Met andere woorden: verdere doorgifte mag alleen worden toegestaan wanneer er wordt gewaarborgd dat de door het EU-recht geboden bescherming in wezen behouden blijft. Bij het beoordelen van de vraag of een derde land een passend beschermingsniveau waarborgt, moet bijgevolg het rechtskader van dat land voor verdere doorgifte in aanmerking worden genomen. Dit is onomstreden en in overeenstemming met de opvatting van zowel de Europese Commissie[84] als het EDPB.

162. Het EDPB neemt in deze context nota van het feit dat het EHRM in zijn recente arresten in de zaken Big Brother Watch e.a. tegen Verenigd Koninkrijk en Centrum för Rättvisa tegen Zweden richtsnoeren heeft uiteengezet[85] aangaande de voorzorgsmaatregelen die in de verdragsluitende staten met betrekking tot gegevensbescherming in acht moeten worden genomen wanneer in bulk verzamelde persoonsgegevens voor rechtshandhavings- en nationaleveiligheidsdoeleinden aan andere partijen worden doorgegeven: "*Ten eerste moeten de omstandigheden waaronder een dergelijke doorgifte kan plaatsvinden, duidelijk in de nationale wetgeving zijn omschreven. Ten tweede moet de staat die de gegevens doorgeeft zich ervan verzekeren dat de ontvangende staat waarborgen heeft ingevoerd die misbruik en onevenredige inmenging bij het verwerken van die gegevens voorkomen. De ontvangende staat moet in het bijzonder de veilige opslag van het materiaal waarborgen en de verdere verstrekking ervan beperken. […] Ten derde moeten er strengere waarborgen worden geboden*

[83] Zie artikel 4, lid 2, van richtlijn (EU) 2016/680.
[84] Zie de overwegingen 84 e.v. van het ontwerpbesluit.
[85] De genoemde elementen zijn vastgesteld in de zaken Big Brother Watch e.a. tegen Verenigd Koninkrijk en Centrum för Rättvisa tegen Zweden, die betrekking hadden op voorschriften voor onderschepping in bulk. Het vereiste dat er voorzorgsmaatregelen worden getroffen wanneer materiaal aan andere partijen wordt doorgegeven, maakte al deel uit van de criteria die door het EHRM in de context van gerichte onderschepping waren ontwikkeld, maar was niet nader door dat Hof uitgewerkt (zie Big Brother Watch e.a. tegen Verenigd Koninkrijk, §§ 335 en 362).

wanneer de doorgifte duidelijk materiaal betreft dat bijzondere geheimhouding vereist, zoals vertrouwelijk journalistiek materiaal."[86]

163. Op basis van deze richtsnoeren kwam het EHRM in de zaak Centrum för Rättvisa tegen Zweden tot de vaststelling dat het feit dat het in een regeling voor onderschepping ontbreekt aan enig uitdrukkelijk wettelijk vereiste om de noodzakelijkheid en evenredigheid van het delen van inlichtingen te beoordelen met het oog op de mogelijke gevolgen ervan voor het recht op privacy, een schending van artikel 8 EVRM vormt. Het EHRM sprak zich kritisch uit over de omstandigheid dat vanwege de algemene bewoordingen waarin de wet was gesteld, onderschept materiaal in beginsel altijd naar het buitenland kon worden verstuurd wanneer dit in het nationaal belang werd geacht, ongeacht of de buitenlandse ontvanger een aanvaardbaar minimumniveau aan waarborgen bood.[87]

164. Het EDPB erkent dat volgens het Zuid-Koreaanse recht onderschepping in bulk niet is toegestaan. In het licht van de implicaties van bovenstaande rechtspraak van het EHRM moeten evenwel in de beoordeling van de vraag of het rechtskader voor verdere doorgifte naar een derde land voorziet in passende regels voor gegevensbescherming, naast de vereisten die voortvloeien uit het EU-recht, zoals uitgelegd door het HvJ, ook de argumenten van het EHRM worden meegenomen.

4.6.1. Toepasselijk rechtskader voor verdere doorgifte door rechtshandhavingsinstanties

165. Het EDPB begrijpt uit de toelichtingen van de Europese Commissie dat hoofdstuk 2 van bijlage I bij het ontwerpbesluit, dat ziet op de beperking van verdere doorgifte, van toepassing is op verdere doorgifte door de bevoegde autoriteiten voor rechtshandhavingsdoeleinden, ook wanneer de doorgifte op basis van een andere wet dan de WBP plaatsvindt. De regel in kwestie luidt als volgt: "*Wanneer persoonsgegevens worden verstrekt aan een overzeese derde partij, bestaat door de verschillen in gegevensbeschermingssystemen tussen landen de mogelijkheid dat niet het beschermingsniveau wordt geboden dat door de [WBP] wordt gewaarborgd. Dergelijke situaties worden dienovereenkomstig aangemerkt als 'gevallen waarin de betrokkene nadelen kan ondervinden', zoals bedoeld in artikel 17, lid 4, WBP, of 'gevallen waarin een onredelijke inbreuk wordt gemaakt op de belangen van de betrokkene of een derde', zoals bedoeld in artikel 18, lid 2, en artikel 14, lid 2, van het uitvoeringsbesluit bij die wet. Om te voldoen aan de vereisten van deze bepalingen, moeten de PG-verwerkingsverantwoordelijke en de derde partij derhalve uitdrukkelijk garanderen dat een aan de WBP gelijkwaardig beschermingsniveau wordt geboden. Dit omvat eveneens de garantie, vastgelegd in een rechtens bindend document zoals een overeenkomst, dat de rechten van de betrokkene ook worden geëerbiedigd nadat de persoonsgegevens naar het derde land zijn doorgegeven."*[88]

166. Het EDPB is blij met deze regel, die – ervan uitgaande dat het niveau van gegevensbescherming in Zuid-Korea passend is – waarborgt dat het beschermingsniveau voor verdere doorgifte in wezen hetzelfde blijft als onder het EU-recht. Volgens de Europese Commissie is hoofdstuk 2 van bijlage I inderdaad van toepassing op alle verdere doorgiften door de bevoegde autoriteiten voor rechtshandhavingsdoeleinden. Het EDPB onderstreept echter dat gewaarborgd moet worden dat deze regel ook in de praktijk voor een gelijkblijvend beschermingsniveau zorgt, aangezien er onzekerheid kan bestaan over de vraag welke contractuele waarborgen of verplichtingen of andere soortgelijke instrumenten daartoe gebruikt kunnen worden wanneer het gaat om verwerking voor rechtshandhavingsdoeleinden. In dit verband moet bijvoorbeeld ook worden vermeld dat

[86] Arrest van het EHRM van 25 mei 2021, Big Brother Watch e.a. tegen Verenigd Koninkrijk, ECLI:CE:ECHR:2021:0525JUD005817013, § 362.
[87] Arrest van het EHRM van 25 mei 2021, Centrum för Rättvisa tegen Zweden, ECLI:CE:ECHR:2021:0525JUD003525208, § 326.
[88] Ontwerpbesluit, bijlage I, blz. 7.

persoonsgegevens alleen met de relevante bevoegde autoriteiten van het derde land mogen worden gedeeld.

167. Behoudens de hierboven gevraagde verduidelijking of de KOFIU onder het adequaatheidsbesluit valt, merkt het EDPB op dat in de officiële verklaring over overheidstoegang[89] wordt uitgelegd dat de commissaris van de KOFIU buitenlandse financiële-inlichtingendiensten op grond van artikel 8, lid 1, van de wet financiële transacties gespecificeerde informatie over financiële transacties mag verstrekken indien dat noodzakelijk wordt geacht voor het bereiken van de doelstellingen van die wet[90]. Genoemd artikel 8 zelf bevat geen verplichting om vast te stellen of, en erop toe te zien dat, het vreemde land passende waarborgen voor gegevensbescherming biedt. In bijlage II wordt in dit opzicht niet verwezen naar het nieuwe hoofdstuk van bijlage I. Het EDPB verzoekt de Europese Commissie derhalve om te verduidelijken hoe het hoofdstuk van bijlage I dat ziet op de beperking van verdere doorgifte en de rechtsgrond voor verdere doorgifte overeenkomstig de wet financiële transacties zich tot elkaar verhouden.

4.6.2. Toepasselijk rechtskader voor verdere doorgifte voor nationaleveiligheidsdoeleinden

168. Het ontwerpbesluit bevat geen enkele informatie over het rechtskader voor verdere doorgifte voor nationaleveiligheidsdoeleinden. Het EDPB maakt hieruit op dat hoofdstuk 2 van bijlage I wel van toepassing is op verdere doorgifte voor rechtshandhavingsdoeleinden, maar niet voor verdere doorgifte voor nationaleveiligheidsdoeleinden. De artikelen 17 en 18 WBP, die opgenomen zijn in het betreffende hoofdstuk, maken deel uit van hoofdstuk III van de WBP, dat op zijn beurt niet van toepassing is op de verwerking van persoonsgegevens voor nationaleveiligheidsdoeleinden (artikel 58, lid 1, WBP).

169. Het EDPB gaat er echter van uit dat het doorgeven van persoonsgegevens aan buitenlandse inlichtingendiensten voor nationaleveiligheidsdoeleinden voor Zuid-Korea een noodzaak is en dat het land dat ook doet, bijvoorbeeld in het kader van samenwerking bij het bestrijden van grensoverschrijdende bedreigingen voor de nationale veiligheid, namelijk om buitenlandse regeringen te waarschuwen voor of om hulp te vragen bij het opsporen van dergelijke dreigingen.

170. Het EDPB begrijpt dat verdere doorgifte naar de opvatting van de Europese Commissie afdoende geregeld is in Zuid-Koreaans recht door de waarborgen die voortvloeien uit het overkoepelend grondwettelijk kader, in het bijzonder de beginselen van noodzakelijkheid en evenredigheid, alsook door de kernbeginselen van gegevensbescherming die in de WBP zijn neergelegd, zoals de rechtmatigheid en behoorlijkheid van verwerkingen, doelbinding, minimale gegevensverwerking, beveiliging en de algemene verplichting tot het voorkomen van misbruik en oneigenlijk gebruik van persoonsgegevens.

171. Het EDPB erkent de algemene toepasselijkheid van deze kernbeginselen (van gegevensbescherming), maar uit zijn bezorgdheid over het feit dat de waarborgen heel algemeen zijn en niet – in het kader van een rechtsgrond – specifiek verwijzen naar of zien op de specifieke omstandigheden en voorwaarden waaronder verdere doorgifte van gegevens uit de EER voor nationaleveiligheidsdoeleinden plaatsvindt. Hoewel deze algemene en overkoepelende beginselen ruime toepassing vinden, betwijfelt het EDPB of hiermee wordt voldaan aan het vereiste van duidelijke

[89] Zie ontwerpbesluit, bijlage II.

[90] Zie ontwerpbesluit, bijlage II, afdeling 2.2.3.2. Hoewel bedoelde uitwisselingen slechts kunnen plaatsvinden onder de voorwaarde dat de buitenlandse dienst de informatie niet voor een ander doel gebruikt dan het oorspronkelijke doel waarvoor deze is verstrekt, in het bijzonder niet voor een strafrechtelijk onderzoek of proces (artikel 8, lid 2, van de wet financiële transacties), kan de commissaris van de KOFIU op verzoek van een vreemd land en met voorafgaande toestemming van de minister van Justitie, wel toestemming geven voor het gebruik van de bedoelde informatie voor een strafrechtelijk onderzoek of proces (artikel 8, lid 3, van de wet financiële transacties).

en nauwkeurige voorschriften en of daarin voldoende doeltreffende en afdwingbare waarborgen zijn verankerd. Zeker wanneer de toegang tot en verwerking van persoonsgegevens door de overheid in het geheim plaatsvindt en er uit de gegevens ernstige gevolgtrekkingen kunnen worden gemaakt, is het van wezenlijk belang dat er duidelijke en gedetailleerde voorschriften bestaan. In de wet moet duidelijk genoeg zijn aangegeven hoeveel beoordelingsvrijheid de bevoegde autoriteiten hebben en hoe zij die vrijheid kunnen uitoefenen, zodat betrokkenen passende bescherming wordt geboden. In het arrest in de zaak Schrems II brengt het HvJ in herinnering dat "een wettelijke grondslag op grond waarvan inmenging in de grondrechten mogelijk is, om te voldoen aan het [noodzakelijkheids- en het] evenredigheidsbeginsel, zelf de omvang van de beperking van de uitoefening van het betrokken recht moet bepalen en duidelijke en nauwkeurige regels moet bevatten die de reikwijdte en de toepassing van de betrokken maatregel bepalen en minimale eisen opleggen"[91]. Het EDPB is derhalve bezorgd dat het niet voldoende is dat dergelijke waarborgen algemeen zijn verankerd in wetten van een hogere orde, maar bijvoorbeeld het evenredigheidsbeginsel niet specifiek in de betreffende rechtsgrond zelf is opgenomen.

172. Deze bezorgdheid vindt steun in bovengenoemd arrest van het EHRM, waarin tot de vaststelling wordt gekomen dat een algemeen voorschrift zonder uitdrukkelijk vereiste om inmenging aan criteria inzake noodzakelijkheid en evenredigheid te toetsen of om privacyoverwegingen in aanmerking te nemen, niet verenigbaar is met het recht op privacy van artikel 8 EVRM. Het EDPB merkt in dit verband op dat er in de wet die in de betreffende zaak in het geding was, (net als in het Zuid-Koreaanse recht) wel sprake was van overkoepelende (grondwettelijk gewaarborgde) beginselen van noodzakelijkheid en evenredigheid, bijvoorbeeld via het Handvest en het EVRM.

173. Het EDPB verzoekt de Europese Commissie om duidelijkheid te verschaffen over de rechtsgrond op basis waarvan, de wijze waarop, de mate waarin en de specifieke omstandigheden waaronder inlichtingendiensten voorafgaand aan het verstrekken van persoonsgegevens voor nationaleveiligheidsdoeleinden aan buitenlandse partners, rekening moeten houden met privacyoverwegingen en gegevensbeschermingseisen. Indien een dergelijke verplichting rechtstreeks voortvloeit uit grondwettelijke beginselen, dient de Europese Commissie vervolgens vast te stellen of de toepasselijke wetgeving aan de eisen van nauwkeurigheid en duidelijkheid voldoet en te bevestigen dat de algemene grondwettelijke beginselen en de algemene beginselen van gegevensbescherming naar behoren worden toegepast.

4.6.3. Internationale overeenkomsten

174. Het EDPB merkt op dat de Europese Commissie, als onderdeel van de adequaatheidsbeoordeling, niet heeft gekeken of Zuid-Korea wellicht overeenkomsten met derde landen of internationale organisaties heeft gesloten die voorzien in specifieke bepalingen voor de internationale doorgifte van persoonsgegevens door rechtshandhavingsautoriteiten en/of inlichtingendiensten aan derde landen. Het EDPB meent dat het sluiten van bilaterale of multilaterale overeenkomsten met derde landen ten behoeve van samenwerking op het gebied van rechtshandhaving en inlichtingenactiviteiten gevolgen kan hebben voor het beschermingsniveau dat door het beoordeelde Zuid-Koreaanse rechtskader voor gegevensbescherming wordt geboden.

175. Het EDPB verzoekt de Europese Commissie derhalve om na te gaan of dergelijke overeenkomsten bestaan en onder welke voorwaarden zij kunnen worden gesloten, alsook om te bepalen of voorschriften in internationale overeenkomsten gevolgen kunnen hebben voor het beschermingsniveau dat voor vanuit de EER naar Zuid-Korea doorgegeven persoonsgegevens wordt geboden door het wetgevingskader en de werkwijzen inzake overzeese verstrekking voor rechtshandhavings- en nationaleveiligheidsdoeleinden.

[91] Zie het arrest Schrems II, punten 175 en 180.

4.7. Toezicht

176. Het EDPB neemt er nota van dat het toezicht op zowel instanties belast met strafrechtelijke handhaving als nationale veiligheidsdiensten wordt gewaarborgd door een combinatie van verschillende interne en externe organen.

177. Het HvJ heeft in dat opzicht al herhaaldelijk gewezen op de noodzaak van onafhankelijk toezicht als essentieel onderdeel van de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Het begrip "onafhankelijkheid" omvat institutionele autonomie, werken zonder instructies en materiële onafhankelijkheid. Om het gegevensbeschermingsrecht consequent te kunnen monitoren en handhaven moeten toezichthoudende autoriteiten beschikken over effectieve bevoegdheden, onder meer om corrigerende en herstellende maatregelen te nemen.

178. Het EDPB is het eens met de conclusie van de Europese Commissie dat Zuid-Korea, alles bij elkaar genomen, kan worden geacht een onafhankelijk en doeltreffend toezichtssysteem te hebben, ook al voldoen verscheidene organen in dat systeem op zichzelf beschouwd niet aan bovenstaande eisen. Het merendeel heeft bijvoorbeeld geen uitvoerende bevoegdheid en kan alleen aanbevelingen geven, bijvoorbeeld de nationale commissie voor de mensenrechten en de controle- en inspectieraad. Verder houden de meeste van die overheidsorganen zich niet uitsluitend bezig met gegevensbescherming maar hebben zij doorgaans ook andere taken op het gebied van grondrechtenbescherming.

179. Volgens de toelichtingen van de Europese Commissie wordt het toezicht op rechtshandhavingsinstanties niettemin volledig en zonder uitzondering gewaarborgd door de toezichthouder. Vandaar dat de toezichthouder op grond van de WBP en andere gegevensbeschermingswetten (bijv. de privacywet) beschikt over onderzoeks-, herstel- en handhavingsbevoegdheden voor al wat de toegang tot persoonsgegevens door rechtshandhavingsinstanties en nationale veiligheidsdiensten betreft.

180. Het EDPB onderstreept in dit verband opnieuw dat toezichthoudende autoriteiten hun taken en bevoegdheden alleen kunnen uitoefenen als zij over voldoende personele, technische en financiële middelen beschikken. Helaas is er geen enkele informatie beschikbaar over de middelen waarover de aangewezen toezichthoudende organen en met name de toezichthouder beschikken. Het EDPB vraagt de Europese Commissie derhalve opnieuw om hierover aanvullende informatie te verstrekken.

181. Het valt het EDPB in het algemeen op dat in het ontwerpbesluit nauwelijks verklaringen, voorbeelden of cijfers staan betreffende toezichthoudende activiteiten en de handhaving van de gegevensbeschermingswetgeving door de toezichthoudende organen op het gebied van rechtshandhaving en nationale veiligheid. Die zouden nochtans nuttig zijn om de doeltreffendheid van die organen te beoordelen.

4.8. Voorzieningen in rechte en verhaalsmogelijkheden

182. Het EDPB brengt in herinnering dat het voor een passend beschermingsniveau voor persoonsgegevens van wezenlijk belang is dat betrokkenen toegang hebben tot uitgebreide voorzieningen in rechte en verhaalsmogelijkheden tegen ongeoorloofde toegang of verwerking van gegevens. Deze voorzieningen in rechte moeten de betrokkenen in staat stellen inzage te krijgen in de gegevens die van hen worden bewaard en deze te laten rectificeren of wissen.

183. In het licht van de arresten Schrems I en Schrems II is het duidelijk dat behalve het recht om zich tot de bevoegde autoriteiten te wenden, ook een doeltreffende rechterlijke bescherming in de zin van artikel 47, lid 1, van het Handvest van wezenlijk belang is om ervan uit te kunnen gaan dat het recht van een derde land een passend beschermingsniveau biedt.

184. Het EDPB erkent dat Zuid-Korea krachtens de WBP verscheidene mechanismen heeft ingevoerd waarmee natuurlijke personen hun rechten van inzage, bewaring, wissing en opschorting kunnen

uitoefenen. Deze rechten kunnen rechtstreeks worden ingeroepen ten overstaan van de verwerkingsverantwoordelijke of via een klacht bij de toezichthouder of een ander toezichthoudend orgaan, zoals de nationale commissie voor de mensenrechten. Voorts erkent het EDPB dat betrokkenen de mogelijkheid hebben om op grond van de wet op bestuursrechtelijke geschillen een besluit van een verwerkingsverantwoordelijke of een overheidsinstelling op een verzoek aan te vechten.

185. Daarnaast begrijpt het EDPB uit de toelichtingen van de Europese Commissie dat natuurlijke personen op grond van de wet op bestuursrechtelijke geschillen en de wet op het grondwettelijk hof bij de rechter in beroep kunnen gaan tegen handelingen van rechtshandhavingsinstanties en nationale veiligheidsdiensten en krachtens de wet op overheidscompensatie een vergoeding voor geleden schade kunnen krijgen.[92]

186. In deze context is het EDPB echter bezorgd over het gebrek aan doeltreffende verhaalsmogelijkheden voor personen uit de EU in situaties van nationale veiligheid waarbij geen Zuid-Koreaanse staatsburgers zijn betrokken. Zoals opgemerkt in de punten 33 e.v., zijn nationale veiligheidsdiensten er niet toe verplicht betrokkenen op de hoogte te stellen van de verzameling en verwerking van hen betreffende persoonsgegevens. Omdat het in die gevallen beduidend moeilijker is doeltreffende juridische bescherming te krijgen, zijn er naar de opvatting van het EDPB bepaalde juridische waarborgen nodig wanneer daarmee vanuit de EER doorgegeven persoonsgegevens zijn gemoeid. Die waarborgen moeten betrokkenen daadwerkelijk in staat stellen op een juridisch veilige manier stappen te ondernemen tegen onrechtmatige gegevensverwerking, zonder daarbij te worden belemmerd door buitensporig strenge procedurele eisen, waarvan bijvoorbeeld sprake zou zijn als de bewijsplicht bij de betrokkenen wordt gelegd. Zij kunnen daar immers niet aan voldoen als zij niet op de hoogte zijn van de verwerking. Verder moeten betrokkenen zich tot een bevoegde instantie kunnen wenden die voldoet aan de vereisten van artikel 47 van het Handvest, d.w.z. een instantie die bevoegd is om te bepalen dat gegevensverwerking plaatsvindt en te beoordelen of deze rechtmatig is, en die beschikt over afdwingbare corrigerende bevoegdheden ingeval de verwerking onrechtmatig blijkt. Tegen deze achtergrond is het recht om bijvoorbeeld een klacht in te dienen bij de nationale commissie voor de mensenrechten op zichzelf onvoldoende. Het EDPB verzoekt de Europese Commissie derhalve om nader toe te lichten hoe in procedurele en materiële zin aan deze vereisten wordt voldaan, bijvoorbeeld of de betrokkene zich tot de toezichthouder en de rechter kan wenden zonder bewijs te hoeven leveren van de gegevensverwerking in kwestie.

187. Daarnaast ziet het EDPB dat het ontwerpbesluit in een verwijsmechanisme voor klachten voorziet, d.w.z. dat personen in de EU via de nationale gegevensbeschermingsautoriteit of het EDPB een klacht bij de Zuid-Koreaanse toezichthouder kunnen indienen. Zodra het onderzoek is afgerond, stelt de toezichthouder de betreffende persoon langs dezelfde weg in kennis van de uitslag.[93] Het EDPB verwelkomt deze poging om betrokkenen gemakkelijker toegang te geven tot verhaalsmogelijkheden tegen de Zuid-Koreaanse veiligheidsdiensten, maar pleit ervoor dit verwijsmechanisme niet via het EDPB te laten lopen maar via de Europese nationale gegevensbeschermingsautoriteiten, aangezien deze bevoegd zijn en dichter bij de klager staan.

188. Verder meent het EDPB dat er sprake is van een mogelijke tegenstrijdigheid met betrekking tot vrijwillige verstrekking. Aan de ene kant vermeldt het ontwerpbesluit dat personen verhaal kunnen nemen ingeval hen betreffende persoonsgegevens onrechtmatig worden verstrekt op grond van een verzoek tot vrijwillige verstrekking, onder meer jegens de rechtshandhavingsinstantie die het verzoek heeft uitgevaardigd.[94] Aan de andere kant staat in het ontwerpbesluit dat het recht om handelingen

[92] Zie bijlage II, afdeling 3.2.4 in samenhang met afdeling 2.4.3.
[93] Zie overweging 205 van en bijlage I, blz. 19, bij het ontwerpbesluit.
[94] Zie overweging 166 van het ontwerpbesluit.

van overheidsinstanties aan te vechten afhankelijk is van de vraag of de betreffende handeling directe gevolgen voor de rechten van de persoon in kwestie heeft, waarbij (alleen) een bindend informatieverzoek als voorbeeld wordt genoemd van een geval waarin een bestuurlijke handeling wordt geacht het recht op privacy direct te beïnvloeden.[95] Het EDPB begrijpt uit de toelichtingen van de Europese Commissie dat er feitelijk geen beperkingen zijn op de mogelijkheid om tegen een verzoek tot vrijwillige informatieverstrekking beroep in te stellen, en verzoekt de Europese Commissie derhalve dit in het besluit duidelijker uiteen te zetten, zowel op het gebied van rechtshandhaving als op het gebied van nationale veiligheid (in tegenstelling tot het hoofdstuk over rechtshandhaving, bevat het hoofdstuk over vrijwillige verstrekking voor nationaleveiligheidsdoeleinden in dit verband geen uitdrukkelijke verklaring over verhaalsmogelijkheden).

[95] Zie overweging 181 (rechtshandhaving) en de overwegingen 208 en 181 (nationale veiligheid) van het ontwerpbesluit.