II

(Niet-wetgevingshandelingen)

BESLUITEN

UITVOERINGSBESLUIT (EU) 2022/254 VAN DE COMMISSIE

van 17 december 2021

overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door de Republiek Korea krachtens de Wet bescherming persoonsinformatie

(Kennisgeving geschied onder nummer C(2021) 9316)

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien 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 (algemene verordening gegevensbescherming) ([1]), en met name artikel 45, lid 3,

Overwegende hetgeen volgt:

1. INLEIDING

(1) Bij Verordening (EU) 2016/679 zijn de voorschriften vastgesteld voor de doorgifte van persoonsgegevens door verwerkingsverantwoordelijken of verwerkers in de Unie aan derde landen en internationale organisaties, voor zover die doorgiften onder het toepassingsgebied ervan vallen. De voorschriften inzake de internationale doorgifte van gegevens zijn vastgelegd in hoofdstuk V (artikelen 44 tot en met 50) van die verordening. Hoewel het verkeer van persoonsgegevens van en naar landen buiten de Europese Unie noodzakelijk is voor de ontwikkeling van het grensoverschrijdende handelsverkeer en de internationale samenwerking, mogen doorgiften aan derde landen niet ten koste gaan van het beschermingsniveau van de persoonsgegevens in de Unie ([2]).

(2) Op grond van artikel 45, lid 3, van Verordening (EU) 2016/679 kan de Commissie door middel van een uitvoeringshandeling besluiten dat een derde land, een gebied of één of meerdere nader bepaalde sectoren in een derde land, of een internationale organisatie een passend beschermingsniveau waarborgt. Onder deze voorwaarde kan de doorgifte van persoonsgegevens aan een derde land plaatsvinden zonder dat verdere toestemming noodzakelijk is, zoals bepaald in artikel 45, lid 1, en overweging 103 van Verordening (EU) 2016/679.

(3) Zoals bepaald in artikel 45, lid 2, van Verordening (EU) 2016/679 moet de vaststelling van een adequaatheidsbesluit berusten op een grondige analyse van de rechtsorde van het derde land, die zowel de voorschriften betreft die gelden voor de importeurs van gegevens als de beperkingen en waarborgen wat betreft de toegang van overheidsinstanties tot persoonsgegevens. Bij haar beoordeling moet de Commissie nagaan of het betrokken derde land een beschermingsniveau waarborgt dat "in feite overeenkomend" is met het niveau dat in de Europese Unie wordt verzekerd (overweging 104 van Verordening (EU) 2016/679). Of dit het geval is, moet worden beoordeeld aan de hand van de wetgeving van de Unie, met name Verordening (EU) 2016/679, alsook de rechtspraak van het Hof van Justitie van de Europese Unie ([3]).

([1]) PB L 119 van 4.5.2016, blz. 1.
([2]) Zie overweging 101 van Verordening (EU) 2016/679.
([3]) Zie de meest recente zaak, C-311/18 van 16 juli 2020, Facebook Ireland en Schrems (hierna *Schrems II* genoemd), ECLI:EU:C:2020:559.

(4) Zoals het Hof van Justitie van de Europese Unie heeft verklaard, is het hiervoor niet noodzakelijk dat hetzelfde beschermingsniveau wordt geboden ([4]). Met name mogen de middelen die het derde land in kwestie voor de bescherming van de persoonsgegevens tot zijn beschikking heeft, anders zijn dan de middelen die binnen de Unie worden ingezet, zolang zij in de praktijk doeltreffend genoeg blijken om een passend beschermingsniveau te bieden ([5]). De adequaatheidsnorm vereist daarom niet dat de voorschriften van de Unie integraal worden overgenomen. Het gaat er veeleer om of het betreffende buitenlandse systeem als geheel het vereiste beschermingsniveau biedt, door de invulling van het recht op privacy, de doeltreffende toepassing en afdwingbaarheid daarvan en het toezicht dat wordt uitgeoefend ([6]). De adequaatheidsreferentie van het Europees Comité voor gegevensbescherming, die deze norm verder beoogt te verduidelijken, biedt in dit verband ook een leidraad ([7]).

(5) De Commissie heeft het Koreaanse recht en de Koreaanse rechtspraktijk zorgvuldig geanalyseerd. Op basis van de bevindingen in de overwegingen 8 tot en met 208 concludeert de Commissie dat de Republiek Korea een passend beschermingsniveau waarborgt voor persoonsgegevens die door een verwerkingsverantwoordelijke of verwerker in de Unie ([8]) worden doorgegeven aan entiteiten (bv. natuurlijke personen of rechtspersonen, organisaties, overheidsinstellingen) in Korea die onder het toepassingsgebied van de Wet bescherming persoonsinformatie vallen (Wet nr. 10465 van 29 maart 2011, zoals laatstelijk gewijzigd bij Wet nr. 16930 van 4 februari 2020). Dit omvat zowel verwerkingsverantwoordelijken als verwerkers ("opdrachtnemers" genoemd ([9])) in de zin van Verordening (EU) 2016/679. Het adequaatheidsbesluit heeft geen betrekking de verwerking van persoonsgegevens voor het zendingswerk van religieuze organisaties en voor de voordracht van kandidaten door politieke partijen, of de verwerking van persoonlijke kredietinformatie uit hoofde van de Wet kredietinformatie door verwerkingsverantwoordelijken die onderworpen zijn aan het toezicht van de Commissie financiële diensten.

(6) Bij deze conclusie is rekening gehouden met de aanvullende waarborgen die in Kennisgeving nr. 2021-5 (bijlage I) zijn uiteengezet en met de officiële verklaringen, garanties en toezeggingen van de Koreaanse regering aan de Commissie (bijlage II).

(7) Dit besluit heeft tot gevolg dat doorgifte aan verwerkingsverantwoordelijken en verwerkers in de Republiek Korea zonder verdere toestemming kan plaatsvinden. Dit doet geen afbreuk aan de directe toepassing van Verordening (EU) 2016/679 op dergelijke entiteiten, voor zover is voldaan aan de voorwaarden betreffende het territoriale toepassingsgebied zoals vastgelegd in artikel 3 van die verordening.

2. VOORSCHRIFTEN DIE VAN TOEPASSING ZIJN OP DE VERWERKING VAN PERSOONSGEGEVENS

2.1. Het gegevensbeschermingskader in de Republiek Korea

(8) Het Koreaanse rechtsstelsel inzake privacy en gegevensbescherming heeft zijn wortels in de Koreaanse grondwet, die op 17 juli 1948 is afgekondigd. Hoewel het recht op bescherming van persoonsgegevens niet uitdrukkelijk in de grondwet is opgenomen, wordt het niettemin erkend als een grondrecht, afgeleid van de grondwettelijke rechten op de menselijke waardigheid en het nastreven van geluk (artikel 10), het recht op een privéleven (artikel 17) en het recht op communicatieprivacy (artikel 18). Dit is bevestigd door zowel het Hooggerechtshof ([10]) als het Grondwettelijk Hof ([11]). Beperkingen van de grondrechten en fundamentele vrijheden (met inbegrip van het recht op privacy) mogen alleen bij wet worden opgelegd wanneer dat noodzakelijk is voor de nationale veiligheid of de handhaving van de openbare orde met het oog op het openbaar welzijn, en zij moeten de wezenlijke inhoud van de vrijheid of het recht onverlet laten (artikel 37, lid 2).

([4]) Zaak C-362/14, Maximilian Schrems/Data Protection Commissioner (hierna *Schrems* genoemd), ECLI:EU:C:2015:650, punt 73.
([5]) Schrems, punt 74.
([6]) Zie de mededeling van de Commissie aan het Europees Parlement en de Raad "Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld" (COM(2017) 7 final van 10.1.2017, punt 3.1, blz. 6-7).
([7]) Europees Comité voor gegevensbescherming, Adequaatheidsreferentie, WP 254 rev. 01, beschikbaar op: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
([8]) Dit besluit geldt voor de EER. De Overeenkomst betreffende de Europese Economische Ruimte (EER-overeenkomst) voorziet in de uitbreiding van de interne markt van de Europese Unie met de drie EER-staten IJsland, Liechtenstein en Noorwegen. Het besluit van het Gemengd Comité van de EER waarbij Verordening (EU) 2016/679 in bijlage XI bij de EER-overeenkomst wordt opgenomen, is vastgesteld door het Gemengd Comité van de EER op 6 juli 2018 en in werking getreden op 20 juli 2018. De verordening valt derhalve onder die overeenkomst. In het kader van het besluit moeten verwijzingen naar de EU en de lidstaten van de EU derhalve worden begrepen als verwijzingen die ook betrekking hebben op de EER-staten.
([9]) Zie punt 2.2.3 van dit besluit.
([10]) Zie bijvoorbeeld Beslissing 2014Da77970 van het Hooggerechtshof van 15 oktober 2015 (Engelse samenvatting beschikbaar via de link "Lawmaker's disclosure of teachers' trade union members case" op https://www.privacy.go.kr/eng/enforcement_01.do) en de aldaar aangehaalde rechtspraak, waaronder Beslissing 2012Da49933 van 24 juli 2014.
([11]) Zie met name Beslissing 99Hun-ma513 van het Grondwettelijk Hof van 26 mei 2005 (Engelse samenvatting beschikbaar op http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) en Beslissing 2014JHun-ma449 2013 Hun-Ba68 (geconsolideerd) van 23 december 2015 (Engelse samenvatting beschikbaar via de link "Change of resident registration number case" op https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Hoewel de grondwet op verschillende plaatsen verwijst naar de rechten van Koreaanse staatsburgers, oordeelde het Grondwettelijk Hof dat de grondrechten ook voor buitenlandse onderdanen gelden ([12]). Met name oordeelde dit hof dat de bescherming van de waardigheid en de waarde van de mens, alsmede het recht om geluk na te streven, rechten zijn van ieder mens, niet alleen van de eigen staatsburgers ([13]). Volgens officiële verklaringen van de Koreaanse regering ([14]) wordt bovendien algemeen erkend dat in de artikelen 12 tot en met 22 van de grondwet (waarin het recht op privacy is opgenomen) wordt voorzien in fundamentele mensenrechten ([15]). Hoewel er tot dusver geen rechtspraak bestaat die specifiek op het recht op privacy van buitenlandse onderdanen betrekking heeft, wordt die conclusie ondersteund door het feit dat het recht op privacy voor buitenlandse onderdanen is gegrondvest in de bescherming van de menselijke waardigheid en het nastreven van geluk ([16]).

(10) Bovendien heeft Korea een reeks wetten op het gebied van gegevensbescherming uitgevaardigd waarin waarborgen zijn opgenomen voor alle natuurlijke personen, ongeacht hun nationaliteit ([17]). Voor de toepassing van dit besluit, zijn de relevante wetten:

— de Wet bescherming persoonsinformatie (Personal Information Protection Act — PIPA);

— de Wet inzake het gebruik en de bescherming van kredietinformatie ([18]);

— de Wet op de bescherming van de communicatieprivacy.

(11) De PIPA vormt het algemene rechtskader voor gegevensbescherming in de Republiek Korea. Deze wet wordt aangevuld door een uitvoeringsdecreet (Presidentieel Decreet nr. 23169 van 29 september 2011, laatstelijk gewijzigd bij Presidentieel Decreet nr. 30892 van 4 augustus 2020) (hierna het "PIPA-uitvoeringsdecreet" genoemd), dat net als de PIPA juridisch bindend en afdwingbaar is.

(12) Bovendien bevatten de "kennisgevingen" die door de Commissie bescherming persoonsinformatie (Personal Information Protection Commission — PIPC) zijn vastgesteld verdere voorschriften voor de interpretatie en toepassing van de PIPA. Op basis van artikel 5 (verplichtingen van de staat) en artikel 14 (internationale samenwerking) van de PIPA heeft de PIPC Kennisgeving nr. 2021-5 van 1 september 2020 (zoals gewijzigd bij Kennisgeving nr. 2021-1 van 21 januari 2021 en Kennisgeving nr. 2021-5 van 16 november 2021, hierna "Kennisgeving nr. 2021-5 genoemd) vastgesteld over de uitlegging, toepassing en handhaving van een aantal bepalingen van de PIPA. Deze kennisgeving bevat verduidelijkingen die van toepassing zijn op elke verwerking van persoonsgegevens in het kader van de PIPA, alsook aanvullende waarborgen voor persoonsgegevens die op basis van dit besluit aan Korea worden doorgegeven. De kennisgeving is juridisch bindend voor degenen die verantwoordelijk zijn voor de verwerking van persoonsinformatie en de opvolging ervan kan zowel door de PIPC als door de rechtbanken worden afgedwongen ([19]). Een schending van de voorschriften in de kennisgeving houdt een schending in van de relevante bepalingen van de PIPA die zij aanvullen. De inhoud van de aanvullende waarborgen wordt derhalve geanalyseerd als onderdeel van de beoordeling van de relevante PIPA-artikelen. Tot slot zijn verdere richtsnoeren over de PIPA en het uitvoeringsdecreet, dat informatie verschaft over de toepassing en handhaving van de gegevensbeschermingsvoorschriften door de PIPC, opgenomen in het PIPA-handboek en in de richtsnoeren van de PIPC ([20]).

([12]) Beslissing 93 Hun-MA120 van het Grondwettelijk Hof van 29 december 1994.
([13]) Beslissing 99HeonMa494 van het Grondwettelijk Hof van 29 november 2001.
([14]) Zie punt 1.1 van bijlage II.
([15]) Zie ook artikel 1 van de Wet bescherming persoonsinformatie, waarin uitdrukkelijk wordt verwezen naar de vrijheden en rechten van natuurlijke personen. Meer bepaald wordt gesteld dat deze wet is bedoeld om te voorzien in de verwerking en bescherming van persoonsinformatie met het oog op de bescherming van de vrijheid en de rechten van natuurlijke personen en de verdere verwezenlijking van de waardigheid en de waarde van het individu. Evenzo wordt in artikel 5, lid 1, van de Wet bescherming persoonsinformatie de verantwoordelijkheid van de staat vastgesteld om beleid te formuleren ter voorkoming van de schadelijke gevolgen van het verzamelen van persoonsinformatie voor andere dan de beoogde doeleinden, het misbruik en oneigenlijk gebruik ervan, willekeurige surveillance en tracering enz. en ter versterking van de menselijke waardigheid en de persoonlijke levenssfeer.
([16]) Bovendien bepaalt artikel 6, lid 2, van de grondwet dat de status van buitenlandse onderdanen wordt gewaarborgd, zoals voorgeschreven door het internationale recht en de internationale verdragen. Korea is partij bij verschillende 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).
([17]) Hieronder vallen voorschriften die relevant zijn voor de bescherming van persoonsgegevens, maar die niet van toepassing zijn in een situatie waarin persoonsgegevens in de Unie worden verzameld en op grond van Verordening (EU) 2016/679 worden doorgegeven aan Korea, bijvoorbeeld in de Wet bescherming, gebruik enz. van locatiegegevens.
([18]) Deze wet heeft tot doel een gezonde omgang met kredietinformatie te bevorderen, een efficiënt gebruik en systematisch beheer van kredietinformatie te promoten en de privacy te beschermen tegen misbruik en oneigenlijk gebruik van kredietinformatie (artikel 1 van de wet).
([19]) Zo hebben Koreaanse rechtbanken in een aantal gevallen een uitspraak gedaan over de naleving van regelgevende kennisgevingen in een aantal gevallen, waarbij zij onder meer Koreaanse verwerkingsverantwoordelijken aansprakelijk hebben gesteld voor schendingen van een kennisgeving (zie bv. Beslissing 2018Da219406 van het Hooggerechtshof van 25 oktober 2018, waarbij het Hof een verwerkingsverantwoordelijke veroordeelde tot het betalen van schadevergoeding aan personen wegens een schending van de "kennisgeving inzake de norm voor maatregelen om de veiligheid van persoonsinformatie te waarborgen"; zie ook Beslissing nr. 12018Da219352 van het Hooggerechtshof van 25 oktober 2018, Beslissing nr. 2011Da24555 van het Hooggerechtshof van 16 mei 2016, Beslissing 2014Gahap511956 van de centrale districtsrechtbank van Seoul van 13 oktober 2016 en Beslissing 2009Gahap43176 van de centrale districtsrechtbank van Seoul van 26 januari 2010.
([20]) Artikel 12, lid 1, PIPA.

(13) Daarnaast bevat de Wet inzake het gebruik en de bescherming van kredietinformatie (*Act on the Use and Protection of Credit Information* - CIA) specifieke regels die zowel gelden voor "gewone" marktdeelnemers als voor gespecialiseerde entiteiten binnen de financiële sector wanneer zij persoonlijke kredietinformatie verwerken, met andere woorden informatie die nodig is om de kredietwaardigheid van partijen bij financiële of commerciële transacties te bepalen. Dit omvat in het bijzonder de naam, contactgegevens, financiële transacties, kredietbeoordeling, verzekeringsstatus of het saldo van een lening wanneer dergelijke informatie wordt gebruikt om de kredietwaardigheid van een natuurlijke persoon te bepalen ([21]). Wanneer dergelijke informatie daarentegen voor andere doeleinden wordt gebruikt (zoals personeelszaken), is de PIPA in haar geheel van toepassing. Het toezicht op de naleving van de specifieke bepalingen over gegevensbescherming in de CIA wordt deels uitgeoefend door de PIPC (voor commerciële organisaties, zie artikel 45-3 CIA) en deels door de Commissie financiële diensten ([22]) (voor de financiële sector, met inbegrip van kredietbeoordelingsbureaus, banken, verzekeringsmaatschappijen, onderlinge spaarbanken, gespecialiseerde kredietverstrekkers, financiële beleggingsmaatschappijen, effectenfinancieringsmaatschappijen, kredietcoöperaties enz., zie artikel 45, lid 1, CIA juncto artikel 36-2 van het CIA- uitvoeringsdecreet en artikel 38 van de Wet inzake de Commissie financiële diensten). In dit verband is de werkingssfeer van dit besluit beperkt tot marktdeelnemers die onder het toezicht van de PIPC vallen ([23]). De specifieke regels van de CIA die in deze context van toepassing zijn (de algemene PIPA-regels zijn van toepassing wanneer er geen specifieke regels bestaan), worden beschreven in punt 2.3.11.

2.2. **Materieel en personeel toepassingsgebied van de PIPA**

(14) Tenzij in andere wetten uitdrukkelijk anders is bepaald, wordt de bescherming van persoonsgegevens geregeld door de PIPA (artikel 6). Het materiële en personele toepassingsgebied wordt bepaald door de gedefinieerde begrippen "persoonsinformatie", "verwerking" en "verantwoordelijke voor de verwerking van persoonsinformatie".

2.2.1. *Definitie van persoonsgegevens*

(15) In artikel 2, lid 1, PIPA wordt persoonsinformatie gedefinieerd als informatie betreffende een levende persoon waarmee die persoon direct kan worden geïdentificeerd, bijvoorbeeld aan de hand van zijn of haar naam, burgerregistratienummer of beeltenis, of indirect kan worden geïdentificeerd, namelijk wanneer informatie die op zich niet volstaat om een bepaalde natuurlijke persoon te identificeren, gemakkelijk met andere informatie kan worden gecombineerd. Of informatie "gemakkelijk" kan worden gecombineerd, hangt af van de vraag of een dergelijke combinatie redelijkerwijs waarschijnlijk is, rekening houdend met de mogelijkheid om andere informatie te verkrijgen en met de tijd, kosten en technologie die nodig zijn om een natuurlijke persoon te identificeren.

(16) Bovendien wordt pseudonieme informatie — d.w.z. informatie aan de hand waarvan een specifieke natuurlijke persoon niet kan worden geïdentificeerd zonder dat de informatie met aanvullende gegevens wordt gebruikt of gecombineerd om de pseudonieme informatie in haar oorspronkelijke staat te herstellen — beschouwd als persoonsgegevens in de zin van de PIPA (artikel 2, lid 1, punt c), PIPA). Omgekeerd is informatie die volledig is "geanonimiseerd", uitgesloten van het toepassingsgebied van de PIPA (artikel 58-2, PIPA). Dit is het geval voor informatie waarmee geen specifieke natuurlijke personen kunnen worden geïdentificeerd, zelfs niet in combinatie met andere informatie, rekening houdend met de tijd, kosten en technologie die redelijkerwijs nodig zijn voor identificatie.

(17) Dit komt overeen met het materiële toepassingsgebied van Verordening (EU) 2016/679 en de daarin vervatte begrippen "persoonsgegevens", "pseudonimisering" ([24]) en "geanonimiseerde informatie" ([25]).

([21]) Artikel 2, lid 1, CIA.

([22]) De Commissie financiële diensten is de toezichthoudende autoriteit van Korea voor de financiële sector en ziet in die hoedanigheid ook toe op de naleving van de CIA.

([23]) Indien dit in de toekomst zou veranderen, bijvoorbeeld door de bevoegdheid van de PIPC uit te breiden tot elke verwerking van persoonlijke kredietinformatie in het kader van de CIA, zou kunnen worden overwogen het adequaatheidsbesluit zodanig te wijzigen dat het ook betrekking heeft op de entiteiten die momenteel onder het toezicht van de Commissie financiële diensten staan.

([24]) In de PIPA wordt onder "pseudonieme verwerking" een verwerking verstaan door middel van methoden zoals het gedeeltelijk verwijderen van persoonsgegevens of het geheel of gedeeltelijk vervangen van persoonsgegevens op zodanige wijze dat zonder aanvullende gegevens geen specifieke natuurlijke personen kunnen worden herkend (artikel 2, leden 1-2, PIPA). Dit komt overeen met de definitie van pseudonimisering in artikel 4, lid 5, van Verordening (EU) 2016/679, waarin wordt verwezen naar "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare persoon worden gekoppeld".

([25]) Met name wordt in overweging 26 van Verordening (EU) 2016/679 verduidelijkt dat de verordening niet van toepassing is op geanonimiseerde gegevens, d.w.z. gegevens die geen verband houden met een geïdentificeerde of identificeerbare natuurlijke persoon. Dit hangt op zijn beurt af van alle middelen waarvan redelijkerwijs te verwachten valt dat zij door de verwerkingsverantwoordelijke of door een andere persoon zullen worden gebruikt om de natuurlijke persoon direct of indirect te identificeren. Om uit te maken of redelijkerwijs te verwachten valt dat dergelijke middelen zullen worden gebruikt, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten en de tijd die nodig zijn voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen.

2.2.2. *Definitie van verwerking*

(18) Het begrip "verwerking" wordt in de PIPA ruim gedefinieerd en omvat het verzamelen, genereren, koppelen, met elkaar in verband brengen, vastleggen, opslaan, bewaren, verwerken met toegevoegde waarde, bewerken, opvragen, uitvoeren, corrigeren, herstellen, gebruiken, verstrekken, bekendmaken en vernietigen van persoonsinformatie en andere soortgelijke activiteiten ([26]). Hoewel in sommige bepalingen van de PIPA alleen wordt verwezen naar specifieke soorten verwerking, zoals "gebruiken", "verstrekken" of "verzamelen" ([27]), wordt het begrip "gebruiken" zodanig geïnterpreteerd dat het elke andere soort verwerking behalve "verzamelen" of "verstrekken" (aan derden) omvat. Dankzij deze ruime interpretatie van het begrip "gebruiken" zijn er geen hiaten in de bescherming met betrekking tot specifieke verwerkingsactiviteiten. Het begrip "verwerking" komt derhalve overeen met hetzelfde begrip in Verordening (EU) 2016/679.

2.2.3. *Verantwoordelijke voor de verwerking van persoonsinformatie en "opdrachtnemer"*

(19) De PIPA is van toepassing op "verantwoordelijken voor de verwerking van persoonsinformatie" ("verwerkingsverantwoordelijke"). Net als in Verordening (EU) 2016/679 omvat dit elke overheidsinstelling, rechtspersoon, organisatie of natuurlijke persoon die direct of indirect, als onderdeel van zijn of haar activiteiten, persoonsgegevens verwerkt om bestanden met persoonsgegevens te beheren ([28]). In dit verband wordt met "bestand met persoonsinformatie" gedoeld op een of meerdere sets van persoonsinformatie die systematisch geordend of georganiseerd zijn op basis van bepaalde regels, zodat de persoonsinformatie gemakkelijk toegankelijk is (artikel 2, lid 4, PIPA) ([29]). De verwerkingsverantwoordelijke is verplicht om de personen die onder zijn leiding bij de verwerking betrokken zijn, zoals bedrijfsfunctionarissen of werknemers, intern op te leiden, en om passende controles en toezicht uit te oefenen (artikel 28, lid 1, PIPA).

(20) Er gelden specifieke verplichtingen wanneer een verwerkingsverantwoordelijke (de "opdrachtgever") de verwerking van persoonsgegevens uitbesteedt aan een derde (de "opdrachtnemer"). De uitbesteding moet met name worden geregeld in een juridisch bindende overeenkomst (doorgaans een contract) ([30]) waarin de omvang van de uitbestede taken, het doel van de verwerking, de toe te passen technische en beheerswaarborgen, het toezicht door de verwerkingsverantwoordelijke, de aansprakelijkheid (zoals voor schade ten gevolge van de niet-nakoming van contractuele verplichtingen) en de beperkingen op eventuele subverwerking zijn vastgelegd ([31]) (artikel 26, leden 1 en 2, PIPA juncto artikel 28, lid 1, van het uitvoeringsdecreet) ([32]).

(21) Bovendien moet de verwerkingsverantwoordelijke de details over de uitbestede taken en de identiteit van de opdrachtnemer bekendmaken en voortdurend bijwerken, of, voor zover de uitbestede verwerking direct-marketingactiviteiten betreft, natuurlijke personen rechtstreeks in kennis stellen van de desbetreffende informatie (artikel 26, leden 2 en 3, PIPA juncto artikel 28, leden 2 tot en met 5, van het uitvoeringsdecreet) ([33]).

(22) Voorts is de verwerkingsverantwoordelijke krachtens artikel 26, lid 4, PIPA juncto artikel 28, lid 6, van het uitvoeringsdecreet verplicht om de opdrachtnemer "op te leiden" ("to educate") over de nodige beveiligingsmaatregelen en erop toe te zien, onder meer door middel van inspecties, of de opdrachtnemer alle door de verwerkingsverantwoordelijke opgelegde verplichtingen uit hoofde van de PIPA ([34]) alsook uit hoofde van de uitbestedingsovereenkomst nakomt. Wanneer de opdrachtnemer schade veroorzaakt door een inbreuk op de PIPA, wordt zijn of haar actie of nalatigheid met het oog op de aansprakelijkheid toegeschreven aan de verwerkingsverantwoordelijke, zoals in het geval van een werknemer (artikel 26, lid 6, PIPA).

([26]) Artikel 2, lid 2, PIPA.

([27]) De artikelen 15 tot en met 19 PIPA hebben bijvoorbeeld alleen betrekking op het verzamelen, gebruiken en verstrekken van persoonsinformatie.

([28]) Artikel 2, lid 5, PIPA. Overheidsinstellingen in de zin van de PIPA zijn alle centrale overheidsafdelingen of -agentschappen en de daarmee verbonden organen, plaatselijke overheden, scholen en plaatselijke overheidsbedrijven, de administratieve organen van de Nationale Vergadering en de rechterlijke macht (met inbegrip van het Grondwettelijk Hof) (artikel 2, lid 6, PIPA juncto artikel 2 van het PIPA-uitvoeringsdecreet).

([29]) Dit komt overeen met het materiële toepassingsgebied van Verordening (EU) 2016/679. In artikel 2, lid 1, van Verordening (EU) 2016/679 is bepaald dat de verordening van toepassing is "op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen". Artikel 4, punt 6, van Verordening (EU) 2016/679 definieert "bestand" als "elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn". In het verlengde daarvan, wordt in overweging 15 uiteengezet dat de bescherming van natuurlijke personen dient te gelden bij "zowel geautomatiseerde verwerking van persoonsgegevens als handmatige verwerking daarvan indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Dossiers of een verzameling dossiers en de omslagen ervan, die niet volgens specifieke criteria zijn gestructureerd, mogen niet onder het toepassingsgebied van deze richtlijn [verordening] vallen."

([30]) Zie PIPA-handboek, hoofdstuk III, deel 2 over artikel 26 (blz. 203-212), waarin wordt uitgelegd dat artikel 26, lid 1, PIPA verwijst naar bindende regelingen, zoals contracten of soortgelijke regelingen.

([31]) Volgens artikel 26, lid 5, PIPA is het de verwerker verboden persoonsinformatie te gebruiken buiten het kader van de uitbestede taken, of persoonsinformatie aan derden te verstrekken. Niet-naleving van dit vereiste kan leiden tot een strafrechtelijke sanctie overeenkomstig artikel 71, punt 2, PIPA.

([32]) Niet-naleving van dit vereiste kan leiden tot het opleggen van een boete, zie artikel 75, lid 4, punt 4, PIPA.

([33]) Niet-naleving van dit vereiste kan leiden tot het opleggen van een boete, zie artikel 75, lid 2, punt 1, en lid 4, punt 5, PIPA.

([34]) Zie ook artikel 26, lid 7, PIPA, waarin is bepaald dat de artikelen 15 tot en met 25, 27 tot en met 31, 33 tot en met 38, en 50 mutatis mutandis van toepassing zijn op de verwerker.

(23) Hoewel in de PIPA dus geen verschillende begrippen voor "verwerkingsverantwoordelijken" en "verwerkers" worden gebruikt, zijn in de voorschriften inzake uitbesteding in wezen gelijkwaardige verplichtingen en waarborgen opgenomen als die welke de relatie tussen verwerkingsverantwoordelijken en verwerkers regelen in het kader van Verordening (EU) 2016/679.

2.2.4. *Bijzondere bepalingen voor aanbieders van informatie- en communicatiediensten*

(24) Hoewel de PIPA van toepassing is op de verwerking van persoonsgegevens door gelijk welke verwerkingsverantwoordelijke, bevatten sommige bepalingen specifieke regels (als *lex specialis*) voor de verwerking van persoonsgegevens van "gebruikers" door "aanbieders van informatie- en communicatiediensten" ([35]). Het begrip "gebruikers" omvat natuurlijke personen die gebruikmaken van informatie- en communicatiediensten (artikel 2, lid 1, punt 4, van de Wet ter bevordering van het gebruik van informatie- en communicatienetwerken en van gegevensbescherming, hierna de "Netwerkwet" genoemd). Dit vereist dat de betrokkene hetzij direct gebruikmaakt van telecommunicatiediensten die door een Koreaans telecommunicatiebedrijf worden verstrekt, hetzij gebruikmaakt van informatiediensten ([36]) die commercieel (d.w.z. met winstoogmerk) worden verstrekt door een entiteit die op haar beurt gebruikmaakt van de diensten van een telecommunicatiebedrijf dat in Korea een vergunning heeft verkregen/is geregistreerd ([37]). In beide gevallen is de entiteit die door de specifieke PIPA-bepalingen is gebonden, een entiteit die direct een onlinedienst aan een natuurlijke persoon (d.w.z. een gebruiker) aanbiedt.

(25) Omgekeerd heeft een vaststelling van adequaatheid uitsluitend betrekking op het beschermingsniveau dat wordt geboden voor persoonsgegevens die door een verwerkingsverantwoordelijke/verwerker in de Unie worden doorgegeven aan een entiteit in een derde land (in dit geval de Republiek Korea). In laatstgenoemd scenario zullen natuurlijke personen in de Unie doorgaans alleen een directe band hebben met de "gegevensexporteur" in de Unie en niet met de Koreaanse aanbieder van informatie- en communicatiediensten ([38]). Daarom zullen de specifieke bepalingen van de PIPA met betrekking tot persoonsgegevens van gebruikers van informatie- en communicatiediensten hoogstens in beperkte gevallen van toepassing zijn op persoonsgegevens die in het kader van dit besluit worden doorgegeven.

2.2.5 *Vrijstelling van sommige bepalingen van de PIPA*

(26) Artikel 58, lid 1, PIPA sluit de toepassing van een deel van de PIPA (d.w.z. de artikelen 15 tot en met 57) uit met betrekking tot vier categorieën van gegevensverwerking ([39]). Met name de delen van de PIPA die betrekking hebben op de specifieke gronden voor verwerking, bepaalde verplichtingen inzake gegevensbescherming, de nadere regels voor de uitoefening van individuele rechten en de regels betreffende geschillenbeslechting door het Comité voor geschillenbeslechting in verband met persoonsinformatie zijn niet van toepassing. Andere basisbepalingen van de PIPA blijven van toepassing, met name de algemene bepalingen inzake de beginselen van gegevensbescherming (artikel 3 PIPA) – bijvoorbeeld de beginselen van rechtmatigheid, doelspecificatie en doelbinding, minimale gegevensverwerking, nauwkeurigheid en beveiliging van de gegevens – evenals de individuele rechten (op toegang, rectificatie, verwijdering en opschorting, zie artikel 4 PIPA). Bovendien worden in artikel 58, lid 4, PIPA specifieke eisen gesteld aan deze verwerkingsactiviteiten, namelijk met betrekking tot de minimale gegevensverwerking, de beperkte bewaring van gegevens, beveiligingsmaatregelen en de behandeling van klachten ([40]). Bijgevolg kunnen natuurlijke personen nog steeds een klacht indienen bij de PIPC indien deze beginselen en eisen niet zouden zijn nageleefd en is de PIPC gemachtigd om handhavingsmaatregelen te nemen in geval van niet-naleving.

([35]) Zie met name artikel 18, lid 2, en hoofdstuk VI, PIPA.

([36]) Informatiediensten omvatten zowel de verstrekking van informatie als tussenhandelsdiensten voor de verstrekking van informatie.

([37]) Zie artikel 2, lid 1, punt 3 (juncto artikel 2, lid 1, punten 2 en 4) van de Netwerkwet en artikel 2, leden 6 en 8, van de Wet op het telecommunicatiebedrijf.

([38]) Voor zover Koreaanse aanbieders van informatie- en communicatiediensten een directe band zouden hebben met natuurlijke personen in de EU (door het aanbieden van onlinediensten), zou dit kunnen leiden tot de directe toepassing van Verordening (EU) 2016/679 op grond van artikel 3, lid 2, punt a).

([39]) In artikel 58, lid 2, PIPA is voorts bepaald dat de artikelen 15 en 22, artikel 27, leden 1 en 2, en de artikelen 34 en 37 niet van toepassing zijn op persoonsinformatie die wordt verwerkt door middel van visuele gegevensverwerkingsapparatuur die op openbare plaatsen is geïnstalleerd en wordt gebruikt. Aangezien deze bepaling betrekking heeft op het gebruik van videobewaking binnen Korea, d.w.z. het direct verzamelen van persoonsinformatie bij personen in Korea, is zij niet relevant voor het doel van dit besluit, dat betrekking heeft op de doorgifte van persoonsgegevens door verwerkingsverantwoordelijken/verwerkers in de EU aan entiteiten in Korea. Bovendien zijn, overeenkomstig artikel 58, lid 3, PIPA, artikel 15 (verzamelen en gebruiken van persoonsinformatie), artikel 30 (verplichting om een beleid inzake de bescherming van de privacy in te voeren) en artikel 31 (verplichting om een privacyfunctionaris aan te stellen) niet van toepassing op persoonsinformatie die wordt verwerkt om groepen of amateurverenigingen (bv. hobbyclubs) te beheren. Omdat dergelijke groepen als persoonlijk worden beschouwd en geen verband houden met een professionele of commerciële activiteit, is er geen specifieke rechtsgrondslag (zoals toestemming van de betrokken personen) vereist om hun informatie in deze context te verzamelen en te gebruiken. Alle andere bepalingen van de PIPA (bv. minimale gegevensverwerking, doelbinding, rechtmatigheid van de verwerking, beveiliging en individuele rechten) blijven echter van toepassing. Bovendien zou elke verwerking van de persoonsinformatie die verder gaat dan de oprichting van een sociale groep, niet onder de uitzondering vallen.

([40]) Meer in het bijzonder bepaalt artikel 58, lid 4, PIPA dat persoonsinformatie niet verder mag worden verwerkt dan strikt noodzakelijk is om het beoogde doel te bereiken, dat de informatie niet langer mag worden verwerkt dan strikt noodzakelijk is, en dat de nodige regelingen moeten worden getroffen om dergelijke persoonsinformatie veilig te beheren en op passende wijze te verwerken. Dit laatste omvat technische, fysieke en beheerswaarborgen, alsook maatregelen om een behoorlijke behandeling van individuele klachten te waarborgen.

(27) Ten eerste heeft de gedeeltelijke vrijstelling betrekking op persoonsgegevens die op grond van de Statistiekwet worden verzameld voor verwerking door overheidsinstellingen. Volgens verduidelijkingen van de Koreaanse regering hebben de in dit verband verwerkte persoonsgegevens normaliter betrekking op Koreaanse onderdanen en kunnen zij slechts in uitzonderlijke gevallen informatie over buitenlanders bevatten, namelijk in het geval van statistieken over het binnenkomen op en verlaten van het grondgebied, of over buitenlandse investeringen. Zelfs in deze situaties worden dergelijke gegevens echter normaal gesproken niet doorgegeven door verwerkingsverantwoordelijken/verwerkers in de Unie, maar worden ze direct verzameld door overheidsinstanties in Korea ([41]). Bovendien gelden, net zoals is bepaald in overweging 162 van Verordening (EU) 2016/679, voor de verwerking van gegevens uit hoofde van de Statistiekwet verscheidene voorwaarden en waarborgen. De statistiekwet legt met name specifieke verplichtingen op, zoals de verplichting tot het waarborgen van nauwkeurigheid, consistentie en onpartijdigheid; het garanderen van de privacy van natuurlijke personen; het beschermen van de informatie van degenen die reageren op statistische vragen, onder meer om te voorkomen dat dergelijke gegevens voor andere doeleinden worden gebruikt dan voor het opstellen van statistieken, en het opleggen van geheimhoudingsvereisten aan personeelsleden ([42]). Overheidsinstanties die statistieken verwerken, moeten onder meer ook voldoen aan de beginselen van minimale gegevensverwerking, doelbinding en beveiliging (artikel 3 en 58, lid 4, PIPA) en personen in staat stellen hun rechten (tot toegang, correctie, verwijdering en schorsing, zie artikel 4 PIPA) uit te oefenen. Ten slotte moeten de gegevens in geanonimiseerde of gepseudonimiseerde vorm worden verwerkt, indien dit de verwezenlijking van het doel van de verwerking mogelijk maakt (artikel 3, lid 7, PIPA).

(28) Ten tweede heeft artikel 58, lid 1, PIPA betrekking op persoonsgegevens die worden verzameld of gevraagd voor de analyse van informatie in verband met de nationale veiligheid. Het toepassingsgebied en de gevolgen van deze gedeeltelijke vrijstelling worden nader beschreven in overweging 149.

(29) Ten derde is de gedeeltelijke vrijstelling van toepassing op de tijdelijke verwerking van persoonsgegevens wanneer dit dringend noodzakelijk is om redenen van openbare veiligheid of beveiliging, met inbegrip van de volksgezondheid. Deze categorie wordt door de PIPC strikt geïnterpreteerd en is volgens de ontvangen informatie nooit gebruikt. Zij is alleen van toepassing in noodsituaties die een dringend optreden vereisen, bijvoorbeeld om ziekteverwekkers op te sporen of om slachtoffers van natuurrampen te redden en te helpen ([43]). Zelfs in die situaties heeft de gedeeltelijke vrijstelling slechts betrekking op de verwerking van persoonsgegevens gedurende de beperkte periode die nodig is om een dergelijke handeling uit te voeren. De situaties waarin dit van toepassing zou kunnen zijn op de onder dit besluit vallende doorgiften van gegevens zijn nog beperkter, aangezien het weinig waarschijnlijk is dat persoonsgegevens die door de Unie aan Koreaanse marktdeelnemers worden doorgegeven, van dien aard zijn dat de latere verwerking ervan "dringend noodzakelijk" zou zijn voor dergelijke noodsituaties.

(30) Tot slot is de gedeeltelijke vrijstelling van toepassing op persoonsgegevens die worden verzameld of gebruikt door de pers, voor het zendingswerk van religieuze organisaties of voor de voordracht van kandidaten door politieke partijen. De vrijstelling geldt alleen wanneer persoonsgegevens door de pers, religieuze organisaties of politieke partijen worden verwerkt voor die specifieke doeleinden (d.w.z. journalistieke activiteiten, missiewerk en de voordracht van politieke kandidaten). Wanneer deze entiteiten persoonsgegevens verwerken voor andere doeleinden, zoals personeelsbeheer of interne administratie, is de PIPA volledig van toepassing.

(31) Wat de verwerking van persoonsgegevens door de pers voor journalistieke activiteiten betreft, wordt het evenwicht tussen de vrijheid van meningsuiting en andere rechten (waaronder het recht op privacy) geregeld door de Wet betreffende arbitrage en rechtsmiddelen enz. voor schade veroorzaakt door persberichten (hierna de "Perswet" genoemd) ([44]). Met name artikel 5 van de Perswet bepaalt dat noch de pers (d.w.z. elke omroeporganisatie, krant,

([41]) In dit verband verplicht artikel 33 van de Statistiekwet overheidsinstellingen ertoe de gegevens van degenen die reageren op statistische enquêtes te beschermen, onder meer om te voorkomen dat die gegevens voor een ander doel worden gebruikt dan voor het opstellen van statistieken.

([42]) Artikel 2, leden 2 en 3, artikel 30, lid 2, en artikelen 33 en 34 van de Statistiekwet.

([43]) PIPA-handboek, hoofdstuk over artikel 58.

([44]) Zo bepaalt artikel 4 van de Perswet dat persberichten onpartijdig en objectief moeten zijn, in het algemeen belang moeten zijn, de menselijke waardigheid en waarde moeten eerbiedigen, en andere personen niet in diskrediet mogen brengen noch een inbreuk mogen vormen op hun rechten, de openbare zeden of de maatschappelijke ethiek.

tijdschrift of onlinekrant), noch gelijk welke onlinenieuwsdienst of multimedia-omroeporganisatie op het internet inbreuken mag maken op de privacy van natuurlijke personen. Indien zich toch een inbreuk op de privacy voordoet, moet deze onmiddellijk worden verholpen volgens specifieke procedures die in de wet zijn vastgesteld. In dit verband verleent de wet natuurlijke personen die schade lijden door een persbericht een aantal rechten, zoals het recht op de publicatie van een correctie in het geval van een onjuiste verklaring, een rectificatie door middel van een andersluidende verklaring of een aanvullend bericht (wanneer een persbericht betrekking heeft op aantijgingen van misdrijven waarvan de betrokkene later wordt vrijgesproken) ([45]). Vorderingen van natuurlijke personen kunnen direct door de persorganisaties worden afgehandeld (via een ombudsdienst) ([46]), via bemiddeling of arbitrage (voor een gespecialiseerde arbitragecommissie voor de pers) ([47]) of voor een rechtbank. Natuurlijke personen kunnen ook een schadevergoeding krijgen wanneer zij financiële schade, inbreuken op een persoonlijkheidsrecht of ander emotioneel leed hebben geleden als gevolg van een onwettige handeling van de pers (door opzet of nalatigheid) ([48]). De pers is vrijgesteld van aansprakelijkheid op grond van de wet voor zover een persbericht dat ingrijpt in iemands rechten niet in strijd is met de maatschappelijke waarden en wordt gepubliceerd hetzij met instemming van de persoon in kwestie, hetzij in het algemeen belang (en er voldoende redenen zijn om aan te nemen dat het bericht overeenstemt met de waarheid) ([49]).

(32) Terwijl de verwerking van persoonsgegevens door de pers met het oog op journalistieke activiteiten dus onderworpen is aan specifieke waarborgen uit hoofde van de Perswet, zijn er geen dergelijke aanvullende waarborgen die een kader scheppen voor de toepassing van uitzonderingen voor verwerkingsactiviteiten door religieuze organisaties en politieke partijen op een manier die vergelijkbaar is met de artikelen 85, 89 en 91 van Verordening (EU) 2016/679. De Commissie acht het derhalve passend om religieuze organisaties, voor zover zij persoonsgegevens verwerken in het kader van hun zendingswerk, en politieke partijen, voor zover zij persoonsgegevens verwerken in het kader van de voordracht van kandidaten, uit te sluiten van het toepassingsgebied van dit besluit.

2.3. **Waarborgen, rechten en verplichtingen**

2.3.1. *Rechtmatigheid en behoorlijkheid van de verwerking*

(33) Persoonsgegevens moeten op rechtmatige en behoorlijke wijze worden verwerkt.

(34) Dit beginsel is vastgesteld in artikel 3, leden 1 en 2, PIPA en wordt versterkt door artikel 59 PIPA, dat de verwerking van persoonsgegevens door middel van fraude, ongeoorloofde of ongerechtvaardigde middelen, zonder wettelijke bevoegdheid of buiten het gezag om verbiedt ([50]). Deze algemene beginselen van rechtmatige verwerking zijn nader uitgewerkt in de artikelen 15 tot en met 19 PIPA, waarin de verschillende rechtsgrondslagen voor verwerking (verzameling, gebruik en verstrekking aan derden) worden uiteengezet, met inbegrip van de omstandigheden waarin dit een wijziging van het doel kan inhouden (artikel 18 PIPA).

([45]) Artikelen 15 tot en met 17 van de Perswet.

([46]) Elke pers- of mediaorganisatie moet een eigen ombudsdienst hebben om mogelijke schade veroorzaakt door de pers te voorkomen en te verhelpen (bv. door correcties aan te bevelen van persberichten met verkeerde informatie of persberichten die de reputatie van anderen schaden), artikel 6 van de Perswet.

([47]) De arbitragecommissie bestaat uit 40 tot 90 arbitragecommissarissen, die door de minister van Cultuur, Sport en Toerisme worden gekozen onder personen die gekwalificeerd zijn als rechter, advocaat, personen die ten minste 10 jaar werkzaam zijn in de nieuwsgaring of verslaggeving, of andere personen met deskundigheid op het gebied van de pers. Arbitragecommissarissen kunnen niet tegelijkertijd ambtenaar, lid van een politieke partij of journalist zijn. Overeenkomstig artikel 8 van de Perswet moeten de arbitragecommissarissen hun taken in alle onafhankelijkheid vervullen en mogen zij in dat verband geen aanwijzingen of instructies ontvangen. Bovendien zijn er specifieke regels om belangenconflicten te voorkomen, bv. door specifieke commissarissen uit te sluiten van de behandeling van zaken waarbij hun partner of een familielid betrokken partij is (artikel 10 van de Perswet). De Commissie kan geschillen behandelen via bemiddeling of arbitrage, maar kan ook aanbevelingen doen om inbreuken te verhelpen (deel 5 van de Perswet).

([48]) Artikel 30 van de Perswet.

([49]) Artikel 5 van de Perswet.

([50]) Artikel 59 PIPA verbiedt eenieder die persoonsinformatie verwerkt of ooit heeft verwerkt om op frauduleuze, onrechtmatige of oneerlijke wijze persoonsinformatie te verkrijgen of toestemming te verkrijgen voor de verwerking van persoonsinformatie, in het kader van de bedrijfsuitoefening verkregen persoonsinformatie te verspreiden of deze zonder toestemming aan derden te verstrekken of persoonsinformatie van anderen te beschadigen, te vernietigen, te wijzigen, te vervalsen of te verspreiden zonder wettelijke bevoegdheid of met overschrijding van bevoegdheid. Een schending van dit verbod kan leiden tot strafrechtelijke sancties, zie artikel 71, leden 5 en 6, en artikel 72, lid 2, PIPA. Artikel 70, lid 2, PIPA maakt het voorts mogelijk een strafrechtelijke sanctie op te leggen voor het verkrijgen van door derden verwerkte persoonsinformatie door middel van fraude of andere oneerlijke middelen of methoden, of voor het verstrekken van die informatie aan een derde met winstoogmerk of voor oneerlijke doeleinden, evenals voor het aanzetten tot of organiseren van dergelijk gedrag.

(35) Volgens artikel 15, lid 1, PIPA mag een verwerkingsverantwoordelijke persoonsgegevens (binnen het toepassingsgebied van het doel van de verzameling) slechts op een beperkt aantal rechtsgronden verzamelen. Dit zijn 1) de toestemming van de betrokkene ([51]) (punt 1); 2) de noodzaak om een overeenkomst met de betrokkene uit te voeren (punt 4); 3) een speciale vergunning via de wet of de noodzaak om een wettelijke verplichting na te komen (punt 2); de noodzaak ([52]) voor een openbare instelling om de taken uit te voeren die binnen haar bevoegdheid vallen, zoals bij wet voorgeschreven; 4) de duidelijke noodzaak om het leven, de lichamelijke integriteit of de eigendomsbelangen van de betrokkene of van een derde tegen onmiddellijk gevaar te beschermen (alleen indien de betrokkene niet in staat is zijn of haar wil kenbaar te maken, of indien geen voorafgaande toestemming kan worden verkregen) (punt 5); 5) de noodzaak om het rechtmatige belang van de verwerkingsverantwoordelijke te verwezenlijken, indien dit duidelijk zwaarder doorweegt dan het belang van de betrokkene (en alleen wanneer de verwerking wezenlijk verband houdt met het gerechtvaardigd belang en niet verder gaat dan wat redelijk is) (punt 6) ([53]). Deze verwerkingsgronden zijn in wezen gelijkwaardig aan die van artikel 6 van Verordening (EU) 2016/679, met inbegrip van de grond rechtmatig belang ("justifiable interest") die gelijk is aan de grond "gerechtvaardigde belangen" ("legitimate interests") in artikel 6, lid 1, punt f), van Verordening (EU) 2016/679.

(36) Zodra ze zijn verzameld, mogen persoonsgegevens worden gebruikt binnen het toepassingsgebied van het doel waarvoor ze zijn verzameld (artikel 15, lid 1, PIPA), of binnen het toepassingsgebied dat redelijkerwijs verband houdt met het doel waarvoor ze zijn verzameld, rekening houdend met eventuele nadelen voor de betrokkene en op voorwaarde dat de nodige beveiligingsmaatregelen (bv. encryptie) zijn getroffen (artikel 15, lid 3, PIPA). Om te bepalen of het gebruiksdoel "redelijkerwijs verband houdt" met het oorspronkelijke verzameldoel, bevat het uitvoeringsdecreet specifieke criteria, die vergelijkbaar zijn met die van artikel 6, lid 4, van Verordening (EU) 2016/679. Met name moet er voldoende verband zijn met het oorspronkelijke doel; moet het extra gebruik voorspelbaar zijn (bijvoorbeeld in het licht van de omstandigheden waarin de informatie is verzameld), en moeten de gegevens, waar mogelijk, worden gepseudonimiseerd ([54]). De specifieke criteria die een verwerkingsverantwoordelijke bij deze beoordeling hanteert, moeten vooraf worden bekendgemaakt in het privacybeleid ([55]). Bovendien moet de privacyfunctionaris (zie overweging 94) specifiek nagaan of verder gebruik plaatsvindt binnen die parameters.

([51]) Toestemming moet vrijelijk worden gegeven, geïnformeerd en specifiek zijn, en worden uitgedrukt op een van de wettelijk vastgelegde wijzen. Toestemming mag in geen geval worden verkregen door middel van fraude, ongeoorloofde of anderszins onrechtvaardige middelen (artikel 59, lid 1, PIPA). Ten eerste hebben betrokkenen overeenkomstig artikel 4, punt 2, PIPA het recht al dan niet toestemming te geven en de reikwijdte van de toestemming te kiezen, en moeten zij daarover worden geïnformeerd (artikel 15, lid 2, artikel 16, leden 2 en 3, artikel 17, lid 2, en artikel 18, lid 3, PIPA). Artikel 22, lid 5, PIPA bevat een verdere waarborg die de verwerkingsverantwoordelijke verbiedt om de levering van goederen of diensten te weigeren wanneer dit de vrije keuze van de betrokkene om toestemming te verlenen, zou kunnen ondermijnen. Dit omvat situaties waarin alleen voor bepaalde vormen van verwerking toestemming is vereist (terwijl andere op een overeenkomst zijn gebaseerd) en heeft ook betrekking op de verdere verwerking van persoonsgegevens die zijn verzameld in het kader van de levering van goederen of diensten. Ten tweede moet de verwerkingsverantwoordelijke overeenkomstig artikel 15, lid 2, artikel 17, leden 2 en 3, en artikel 18, lid 3, PIPA de betrokkene bij het verzoek om toestemming in kennis stellen van de bijzonderheden van de persoonsgegevens in kwestie (bv. dat het om gevoelige gegevens gaat, zie artikel 17, lid 2, punt 2, a), van het PIPA-uitvoeringsdecreet), het doel van de verwerking, de bewaartermijn en de eventuele ontvanger van de gegevens. Een dergelijk verzoek moet op uitdrukkelijk herkenbare wijze worden gedaan, zodat zaken waarvoor toestemming is vereist, worden onderscheiden van andere zaken (artikel 22, leden 1 tot en met 4, PIPA). Ten derde zijn in artikel 17, lid 1, punt 1-6, van het PIPA-uitvoeringsdecreet de specifieke methoden bepaald waarmee een verwerkingsverantwoordelijke toestemming moet verkrijgen, zoals schriftelijke toestemming met de handtekening van de betrokkene, of toestemming per e-mail. Hoewel de PIPA personen niet specifiek een algemeen recht verleent om hun toestemming in te trekken, hebben zij in plaats daarvan het recht om opschorting van de verwerking van hen betreffende gegevens te verkrijgen, hetgeen, wanneer dit recht wordt uitgeoefend, zal leiden tot beëindiging van de verwerking en tot verwijdering van gegevens (zie overweging 78 inzake het recht op opschorting).

([52]) Volgens de van de PIPC ontvangen informatie kunnen overheidsinstellingen zich alleen op deze grond beroepen als de verwerking van persoonsinformatie onvermijdelijk is, d.w.z. dat het voor de instelling onmogelijk of onredelijk moeilijk is om haar taken uit te voeren zonder de gegevens te verwerken.

([53]) Artikel 39-3 PIPA legt aanbieders van informatie- en communicatiediensten specifieke (strengere) verplichtingen op met betrekking tot het verzamelen en gebruiken van persoonsinformatie van hun gebruikers. Met name wordt vereist dat de dienstverlener de toestemming van de gebruiker verkrijgt, na informatie te hebben verstrekt over het doel van de verzameling/het gebruik, de categorieën persoonsinformatie die zullen worden verzameld en de periode gedurende welke de gegevens zullen worden verwerkt (artikel 39-3, lid 1, PIPA). Hetzelfde geldt wanneer een van deze aspecten wijzigt. Op het niet verkrijgen van toestemming om informatie te verzamelen, staan strafrechtelijke sancties (artikel 71, leden 4 en 5, PIPA). In uitzonderlijke gevallen kan persoonsinformatie van gebruikers worden verzameld of gebruikt door aanbieders van informatie- en communicatiediensten zonder voorafgaande toestemming te verkrijgen. Dit is het geval 1) wanneer het om economische en technische redenen duidelijk moeilijk is om toestemming te verkrijgen voor de persoonsinformatie die vereist is voor de uitvoering van het contract betreffende de levering van informatie- en communicatiediensten (bv. wanneer bij de uitvoering van een contract onvermijdelijk persoonsgegevens worden gecreëerd, zoals factureringsgegevens, toegangsaanmeldingen en betalingsbewijzen); 2) wanneer dit noodzakelijk is voor kostenafrekeningen naar aanleiding van de levering van informatie- en communicatiediensten, of 3) indien toegestaan door andere wetgeving (zo bepaalt artikel 21, lid 1, punt 6, van de wet inzake consumentenbescherming bij elektronische handel bijvoorbeeld dat exploitanten van bedrijven persoonsinformatie van wettelijke voogden van een minderjarige mogen verzamelen om te bevestigen of namens de minderjarige geldige toestemming is verkregen) (artikel 39-3, lid 2, PIPA). In geen enkel geval mogen aanbieders van informatie- en communicatiediensten weigeren om diensten te verlenen alleen omdat de gebruiker niet meer persoonsinformatie verstrekt dan strikt noodzakelijk (d.w.z. de informatie die nodig is om de essentiële onderdelen van de dienst in kwestie te verrichten), zie artikel 39-3, lid 3, PIPA.

([54]) Zie artikel 14-2 van het PIPA-uitvoeringsdecreet.

([55]) Artikel 14-2, lid 2, van het PIPA-uitvoeringsdecreet.

(37) Soortgelijke (maar iets strengere) voorschriften gelden voor de verstrekking van gegevens aan een derde partij. Overeenkomstig artikel 17, lid 1, PIPA is de verstrekking van persoonsgegevens aan een derde partij toegestaan op basis van toestemming ([56]) of, binnen het doel van de verzameling, wanneer de informatie is verzameld op een van de rechtsgronden in artikel 15, lid 1, punten 2, 3, en 5, PIPA. Dit sluit met name elke openbaarmaking uit die is gebaseerd op het "rechtmatig belang" van de verwerkingsverantwoordelijke. Daarnaast wordt in artikel 17, lid 4, PIPA toegestaan dat gegevens aan derden worden verstrekt binnen het toepassingsgebied dat redelijkerwijs verband houdt met het doel waarvoor ze zijn verzameld, rekening houdend met eventuele nadelen voor de betrokkene en op voorwaarde dat de nodige beveiligingsmaatregelen (bv. encryptie) zijn getroffen. Dezelfde factoren als die welke in overweging 36 zijn beschreven, moeten in aanmerking worden genomen om te beoordelen of de verstrekking binnen het toepassingsgebied valt dat redelijkerwijs in verband staat met het doel van de verzameling, en dezelfde waarborgen (d.w.z. met betrekking tot transparantie door middel van het privacybeleid en de betrokkenheid van de privacyfunctionaris) zijn van toepassing.

(38) De ontvangst van persoonsgegevens uit de Unie door een Koreaanse verwerkingsverantwoordelijke wordt beschouwd als een "verzameling" in de zin van artikel 15 PIPA. In Kennisgeving nr. 2021-5 (deel I van bijlage I bij dit besluit) wordt verduidelijkt dat het doel waarvoor de gegevens door de betrokken EU-entiteit zijn doorgegeven, voor de Koreaanse verwerkingsverantwoordelijke het doel van de verzameling vormt. Bijgevolg zijn de Koreaanse verwerkingsverantwoordelijken die persoonsgegevens uit de Unie ontvangen, in beginsel verplicht die informatie te verwerken binnen het toepassingsgebied van het doel van de doorgifte, overeenkomstig artikel 17 PIPA.

(39) Er gelden bijzondere beperkingen indien de verwerkingsverantwoordelijke de persoonsgegevens wil gebruiken of aan een derde wil verstrekken voor een ander doel dan waarvoor ze werden verzameld ([57]). Overeenkomstig artikel 18, lid 2, PIPA kan een particuliere verwerkingsverantwoordelijke bij wijze van uitzondering ([58]) persoonsgegevens gebruiken of deze aan een derde verstrekken voor een ander doel: 1) op basis van de aanvullende (d.w.z. afzonderlijke) toestemming van de betrokkene; 2) wanneer bijzondere wettelijke bepalingen in deze mogelijkheid voorzien, of 3) wanneer dit duidelijk nodig is om het leven, de lichamelijke integriteit of de eigendomsbelangen van de betrokkene of van een derde tegen onmiddellijk gevaar te beschermen (alleen indien de betrokkene niet in staat is zijn of haar wil kenbaar te maken en geen voorafgaande toestemming kan worden verkregen) ([59]).

(40) Overheidsinstellingen kunnen in bepaalde situaties ook persoonsgegevens gebruiken of voor een ander doel aan een derde partij verstrekken. Het gaat dan om gevallen waarin het voor overheidsinstellingen anders onmogelijk zou zijn hun bij wet voorgeschreven taken uit te voeren, onder voorbehoud van toestemming van de PIPC. Daarnaast kunnen overheidsinstellingen persoonsgegevens aan een andere autoriteit of een rechtbank verstrekken, indien dit noodzakelijk is voor het onderzoeken en vervolgen van misdrijven of voor een tenlastelegging; voor een rechtbank om taken in verband met lopende gerechtelijke procedures uit te voeren, of voor de uitvoering van een strafrechtelijke sanctie, een terbeschikkingstelling of verzekerde bewaring ([60]). Zij kunnen ook persoonsgegevens verstrekken aan een buitenlandse overheid of internationale organisatie om te voldoen aan een wettelijke verplichting die voortvloeit uit een verdrag of internationale overeenkomst, in welk geval zij ook moeten voldoen aan de vereisten voor grensoverschrijdende doorgiften van gegevens (zie overweging 90).

(41) De beginselen van rechtmatigheid en behoorlijkheid van de verwerking worden derhalve in het Koreaanse rechtskader uitgevoerd op een manier die in wezen overeenkomt met Verordening (EU) 2016/679, doordat verwerking alleen is toegestaan op basis van gerechtvaardigde en duidelijk omschreven gronden. Bovendien is de verwerking in alle genoemde gevallen alleen toegestaan indien het onwaarschijnlijk is dat de belangen van de betrokkene of van een derde partij onredelijk worden geschaad, anders is een belangenafweging vereist. Bovendien schrijft artikel 18, lid 5, PIPA aanvullende waarborgen voor wanneer de verwerkingsverantwoordelijke de persoonsgegevens aan een derde partij verstrekt, waaronder een verzoek om het doel en de wijze van gebruik te beperken, of om specifieke beveiligingsmaatregelen te treffen. De derde partij is op haar beurt verplicht de gevraagde maatregelen uit te voeren.

([56]) Overtredingen van artikel 17, lid 1, punt 1, PIPA kunnen tot strafrechtelijke sancties leiden (artikel 71, lid 1, PIPA).

([57]) Het "beoogde doel" is het doel waarvoor de informatie werd verzameld. Wanneer de informatie bijvoorbeeld is verzameld op basis van de toestemming van de betrokkene, is het beoogde doel het doel dat overeenkomstig artikel 15, lid 2, PIPA aan de betrokkene is meegedeeld.

([58]) Zie artikel 18, lid 1, PIPA. Overtredingen van artikel 18, leden 1 en 2, kunnen tot strafrechtelijke sancties leiden (artikel 71, lid 2, PIPA).

([59]) Het gebruik van persoonsinformatie of de verstrekking ervan aan een derde partij door aanbieders van informatie- en communicatiediensten voor een ander dan het oorspronkelijke doel mag alleen plaatsvinden op grond van de in artikel 18, lid 2, punten 1 en 2, PIPA vermelde redenen (d.w.z. wanneer aanvullende toestemming is verkregen of wanneer er bijzondere wettelijke bepalingen gelden). Zie artikel 18, lid 2, PIPA.

([60]) Behalve wanneer de verwerking noodzakelijk is voor de opsporing van misdrijven, tenlastelegging en vervolging, moeten overheidsinstellingen die persoonsinformatie gebruiken of aan derden verstrekken voor een ander doel dan waarvoor ze zijn verzameld (bijvoorbeeld wanneer dit specifiek bij wet is toegestaan of noodzakelijk is om een verdrag uit te voeren), de rechtsgronden voor de verwerking, het doel en de reikwijdte ervan op hun website of in het staatsblad bekend maken en een register bijhouden (artikel 18, lid 4, PIPA juncto artikel 15 van het PIPA-uitvoeringsdecreet).

(42) Tot slot is in artikel 28-2 PIPA de (verdere) verwerking van gepseudonimiseerde informatie toegestaan zonder toestemming van de betrokkene met het oog op statistieken, wetenschappelijk onderzoek ([61]) en archivering in het algemeen belang, mits specifieke waarborgen worden geboden. Vergelijkbaar met Verordening (EU) 2016/679 ([62]), vergemakkelijkt de PIPA derhalve de (verdere) verwerking van persoonsgegevens voor dergelijke doeleinden binnen een kader dat voorziet in passende waarborgen om de rechten van natuurlijke personen te beschermen. In plaats van te vertrouwen op pseudonimisering als mogelijke waarborg, legt de PIPA dit op als voorwaarde om bepaalde verwerkingsactiviteiten te mogen uitvoeren met het oog op statistieken, wetenschappelijk onderzoek en archivering in het algemeen belang (bijvoorbeeld om de gegevens zonder toestemming te kunnen verwerken of om verschillende gegevensreeksen te combineren).

(43) Bovendien legt de PIPA een aantal specifieke waarborgen op, met name wat betreft de vereiste technische en organisatorische maatregelen, het bijhouden van registers, beperkingen op het delen van gegevens en de aanpak van mogelijke risico's van re-identificatie. De combinatie van de verschillende in de overwegingen 44 tot en met 48 beschreven waarborgen zorgt ervoor dat de verwerking van persoonsgegevens in deze context onderworpen is aan beschermingsmaatregelen die in wezen overeenkomen met die welke op grond van Verordening (EU) 2016/679 vereist zouden zijn.

(44) Eerst en vooral verbiedt artikel 28-5, lid 1, PIPA de verwerking van gepseudonimiseerde informatie met het oog op de identificatie van een bepaalde natuurlijke persoon. Indien bij de verwerking van gepseudonimiseerde informatie toch informatie wordt gegenereerd waarmee een natuurlijke persoon kan worden geïdentificeerd, moet de verwerkingsverantwoordelijke de verwerking onmiddellijk opschorten en de informatie vernietigen (artikel 28-5, lid 2, PIPA). Niet-naleving van deze bepalingen kan worden bestraft met administratieve boetes en vormt een strafbaar feit ([63]). Dit betekent dat, zelfs in situaties waarin het *praktisch* mogelijk zou zijn de betrokkene opnieuw te identificeren, een dergelijke re-identificatie *bij wet* verboden is.

(45) Ten tweede moet de verwerkingsverantwoordelijke bij (verdere) verwerking van gepseudonimiseerde informatie voor dergelijke doeleinden, specifieke technologische, fysieke en beheersmaatregelen treffen om de beveiliging van de informatie te waarborgen (waaronder het afzonderlijk opslaan en beheren van de informatie die nodig is om de gepseudonimiseerde informatie in haar oorspronkelijke staat te herstellen) ([64]). Bovendien moet een register worden bijgehouden van de verwerkte gepseudonimiseerde informatie, het doel van de verwerking, de gebruiksgeschiedenis en eventuele derde partijen die de informatie ontvangen (artikel 29-5, lid 2, van het PIPA-uitvoeringsdecreet).

(46) Ten derde en ten laatste voorziet de PIPA in specifieke waarborgen om de identificatie van natuurlijke personen door derden te voorkomen in het geval de informatie wordt gedeeld. In het bijzonder mogen verwerkingsverantwoordelijken, wanneer zij gepseudonimiseerde informatie aan derden verstrekken met het oog op statistieken, wetenschappelijk onderzoek of archivering in het algemeen belang, geen informatie opnemen die kan worden gebruikt om een specifieke natuurlijke persoon te identificeren (artikel 28-2, lid 2, PIPA) ([65]).

(47) Meer bepaald staat de PIPA weliswaar toe dat gepseudonimiseerde informatie (die door verschillende verwerkingsverantwoordelijken wordt verwerkt) wordt gecombineerd met het oog op statistieken, wetenschappelijk onderzoek of archivering in het algemeen belang, maar is die bevoegdheid voorbehouden aan gespecialiseerde instellingen die over specifieke beveiligingsvoorzieningen beschikken (artikel 28-3, lid 1, PIPA) ([66]). Wanneer een verwerkingsverantwoordelijke om een combinatie van gepseudonimiseerde gegevens verzoekt, moet hij of zij onder

([61]) Wetenschappelijk onderzoek wordt in artikel 2, lid 8, PIPA gedefinieerd als onderzoek waarbij wetenschappelijke methoden worden toegepast, zoals technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek. Deze categorieën komen overeen met die in overweging 159 van Verordening (EU) 2016/679.

([62]) Zie artikel 5, lid 1, punt b), artikel 89, leden 1 en 2, en overwegingen 50 en 157 van Verordening (EU) 2016/679.

([63]) Zie artikel 28-6, lid 1, artikel 71, lid 4-3, en artikel 75, lid 2, punt 4-4, PIPA.

([64]) Artikel 28-4 PIPA en artikel 29-5 van het PIPA-uitvoeringsdecreet. Niet-naleving van deze verplichting kan worden bestraft met administratieve en strafrechtelijke sancties, zie artikel 73, lid 1, en artikel 75, lid 2, punt 6, PIPA.

([65]) Schendingen van deze vereisten kunnen tot strafrechtelijke sancties leiden (artikel 71, lid 2, PIPA). De PIPC is onmiddellijk begonnen met de handhaving van deze nieuwe regels, bijvoorbeeld in haar besluit van 28 april 2021, waarin zij een boete en corrigerende maatregelen oplegde aan een onderneming die, naast andere schendingen van de PIPA, niet voldeed aan het vereiste van artikel 28-2, lid 2, PIPA, zie https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([66]) Om als een dergelijke gespecialiseerde instelling (een "gespecialiseerd agentschap voor gegevenscombinatie") te worden erkend, moet bij de PIPC een aanvraag worden ingediend, samen met ondersteunende documenten waarin onder meer de beschikbare faciliteiten en apparatuur worden beschreven om op veilige wijze gepseudonimiseerde gegevens te combineren, en waarin wordt bevestigd dat de aanvrager ten minste drie voltijdse personeelsleden in dienst heeft met kwalificaties of ervaring op het gebied van de bescherming van persoonsgegevens (artikel 29-2, leden 1 en 2, van het PIPA-uitvoeringsdecreet). Gedetailleerde vereisten, bijvoorbeeld met betrekking tot de kwalificaties van het personeel, de beschikbare faciliteiten, de beveiligingsmaatregelen, het interne beleid en de interne procedures, alsook de financiële vereisten, zijn opgenomen in Kennisgeving 2020-9 van de PIPC inzake het combineren en vrijgeven van gepseudonimiseerde informatie (bijlage I). De erkenning als gespecialiseerd agentschap voor gegevenscombinatie kan door de PIPC (na een hoorzitting) worden ingetrokken op bepaalde gronden, bv. indien het agentschap niet langer voldoet aan de voor erkenning vereiste beveiligingsnormen, of indien in de context van de gegevenscombinatie een gegevenslek heeft plaatsgevonden (artikel 29-2, leden 5 en 6, van het PIPA-uitvoeringsdecreet). De PIPC moet elke erkenning (of intrekking van een erkenning) van een gespecialiseerd agentschap voor gegevenscombinatie bekendmaken (artikel 29-2, lid 7, van het PIPA-uitvoeringsdecreet).

meer documentatie verstrekken over de te combineren gegevens, het doel van de combinatie, alsook de voorgestelde beveiligingsmaatregelen voor de verwerking van de gecombineerde gegevens ([67]). Om de combinatie mogelijk te maken, moet de verwerkingsverantwoordelijke de te combineren gegevens naar de gespecialiseerde instelling sturen en een "combinatiesleutel" (d.w.z. de informatie die voor pseudonimisering is gebruikt) aan het Koreaans Agentschap voor internet en veiligheid verstrekken ([68]). Dat agentschap genereert "koppelingsgegevens van combinatiesleutels" (die het mogelijk maken de combinatiesleutels van verschillende aanvragers te koppelen om de gegevensreeksen te combineren) en verstrekt deze aan de gespecialiseerde instelling ([69]).

(48) De verwerkingsverantwoordelijke die om de combinatie verzoekt, mag de gecombineerde informatie analyseren in de gebouwen van de gespecialiseerde instelling, in een ruimte waar specifieke technische, fysieke en administratieve beveiligingsmaatregelen worden toegepast (artikel 29-3 van het PIPA-uitvoeringsdecreet). Verwerkingsverantwoordelijken die een gegevensreeks voor een dergelijke combinatie bijdragen, mogen de gecombineerde gegevens alleen uit de gespecialiseerde instelling verwijderen na verdere pseudonimisering of anonimisering van de gecombineerde gegevens, en met de goedkeuring van die instelling (artikel 28-3, lid 2, PIPA) ([70]). Wanneer wordt nagegaan of al dan niet toestemming kan worden verleend, beoordeelt de instelling het verband tussen de gecombineerde gegevens en het doel van de verwerking, en gaat zij na of er een specifiek beveiligingsplan voor het gebruik van deze gegevens is opgesteld ([71]). Het uitvoeren van de gecombineerde informatie buiten de instelling is niet toegestaan indien de informatie gegevens bevat waarmee een natuurlijke persoon kan worden geïdentificeerd ([72]). Tot slot oefent de PIPC toezicht uit op het combineren en vrijgeven van gepseudonimiseerde gegevens door de gespecialiseerde instelling (artikel 29-4, lid 3, van het PIPA-uitvoeringsdecreet).

2.3.2. *Verwerking van bijzondere categorieën van persoonsgegevens*

(49) Wanneer "bijzondere categorieën" gegevens worden verwerkt, moet worden voorzien in bijzondere waarborgen.

(50) De PIPA bevat specifieke voorschriften met betrekking tot de verwerking van gevoelige gegevens ([73]), die worden gedefinieerd als persoonsgegevens waaruit informatie kan worden afgeleid over de levensbeschouwing, het geloof, de toetreding tot of uittreding uit een vakvereniging of politieke partij, de politieke opvattingen, de gezondheid en het seksleven van een persoon, alsook andere persoonsinformatie die de persoonlijke levenssfeer van de betrokkene "merkbaar" kan bedreigen en die bij presidentieel decreet ([74]) als gevoelige informatie is aangemerkt. Volgens verduidelijkingen die zijn ontvangen van de PIPC wordt onder seksleven ook de seksuele geaardheid of voorkeur van de persoon verstaan ([75]). Bovendien voegt artikel 18 van het uitvoeringsdecreet nog andere categorieën toe aan de reikwijdte van gevoelige gegevens, met name DNA-informatie die is verkregen door genetische tests en gegevens die een strafblad vormen. De recente wijziging van het PIPA-uitvoeringsdecreet heeft het begrip gevoelige gegevens verder verruimd, door ook persoonsgegevens op te nemen waaruit het ras of de etnische afkomst blijkt en biometrische informatie ([76]). Sinds die wijziging is het begrip "gevoelige gegevens" in het kader van de PIPA in wezen gelijkwaardig aan wat is opgenomen in artikel 9 van Verordening (EU) 2016/679.

(51) Volgens artikel 23, lid 1, PIPA en vergelijkbaar met wat is bepaald in artikel 9, lid 1, van Verordening (EU) 2016/679, is de verwerking van gevoelige gegevens in het algemeen verboden, tenzij een van de opgesomde uitzonderingen van toepassing is ([77]). Die beperken de verwerking tot gevallen waarin de verwerkingsverantwoordelijke de betrokkene informeert overeenkomstig de artikelen 15 en 17 PIPA en afzonderlijke toestemming

([67]) Artikel 8, leden 1 en 2, van Kennisgeving 2020-9 inzake het combineren en vrijgeven van gepseudonimiseerde informatie.
([68]) Artikel 2, leden 3 en 6, en artikel 9, lid 1, van Kennisgeving 2020-9 inzake het combineren en vrijgeven van gepseudonimiseerde informatie.
([69]) Artikel 2, lid 4, en artikel 9, leden 2 en 3, van Kennisgeving 2020-9 inzake het combineren en vrijgeven van gepseudonimiseerde informatie. De gespecialiseerde instelling moet de koppelingsgegevens van de combinatiesleutel na het combineren onmiddellijk vernietigen (artikel 9, lid 4, van de kennisgeving).
([70]) Inbreuken op de vereisten voor het combineren van gegevensreeksen kunnen tot strafrechtelijke sancties leiden (artikel 71, lid 4-2, PIPA). Zie ook artikel 29-2, lid 4, van het PIPA-uitvoeringsdecreet.
([71]) De goedkeuringsprocedure voor de vrijgave van gecombineerde gegevens is uiteengezet in artikel 11 van Kennisgeving 2020-9 inzake het combineren en vrijgeven van gepseudonimiseerde informatie. De gespecialiseerde instelling moet met name een toetsingscommissie voor vrijgave instellen, bestaande uit leden met een aanzienlijke kennis van en ervaring met gegevensbescherming.
([72]) Artikel 29-2, lid 4, van het PIPA-uitvoeringsdecreet en Kennisgeving nr. 2020-9, artikel 11.
([73]) De noodzaak om specifieke bescherming te bieden voor de verwerking van gevoelige gegevens, zoals gegevens over gezondheid of seksueel gedrag, is ook erkend door het Koreaans Grondwettelijk Hof, zie Beslissing HunMa 1139 van 31 mei 2007 van het Grondwettelijk Hof.
([74]) Artikel 23, lid 1, PIPA.
([75]) Zie ook het PIPA-handboek, hoofdstuk III, deel 2, artikel 23 (blz. 157-164).
([76]) Het gaat hierbij om persoonsinformatie die het resultaat is van een specifieke technische verwerking van gegevens over de fysieke, fysiologische of gedragskenmerken van een persoon met het oog op de unieke identificatie van die persoon.
([77]) Niet-naleving van deze vereisten kan leiden tot sancties uit hoofde van artikel 71, punt 3, PIPA.

verkrijgt (d.w.z. los van de toestemming voor de verwerking van andere persoonsgegevens), of waarin de verwerking bij wet verplicht of toegestaan is. Overheidsinstanties mogen ook biometrische informatie, DNA-informatie uit genetische tests, persoonsinformatie waaruit ras of etnische afkomst blijkt en gegevens die een strafblad vormen, verwerken op de gronden waarover uitsluitend zij beschikken (bijvoorbeeld wanneer dit noodzakelijk is voor het onderzoek naar misdrijven of voor de behandeling van een zaak door een rechtbank) ([78]). Als zodanig zijn de beschikbare rechtsgrondslagen voor de verwerking van gevoelige gegevens beperkter dan voor andere soorten persoonsgegevens, en in de Koreaanse wetgeving zelfs beperkender dan het bepaalde in artikel 9, lid 2, van Verordening (EU) 2016/679.

(52) Bovendien wordt in artikel 23, lid 2, PIPA — waarvan de niet-naleving kan leiden tot sancties ([79]) — het bijzondere belang benadrukt om te zorgen voor een passende beveiliging bij de behandeling van gevoelige gegevens, zodat deze niet verloren kunnen gaan of gestolen, openbaar gemaakt, vervalst, gewijzigd of beschadigd kunnen worden. Hoewel dit een algemeen vereiste is uit hoofde van artikel 29 PIPA, wordt in artikel 3, lid 4, duidelijk gesteld dat het beveiligingsniveau moet worden afgestemd op het soort persoonsgegevens dat wordt verwerkt, hetgeen betekent dat rekening moet worden gehouden met de bijzondere risico's die aan de verwerking van gevoelige gegevens zijn verbonden. Bovendien moet de verwerking van gegevens altijd op zodanige wijze plaatsvinden dat de mogelijkheid om inbreuken te plegen op de persoonlijke levenssfeer van de betrokkene zo gering mogelijk is, en indien mogelijk "in anonimiteit" (artikel 3, leden 6 en 7, PIPA). Deze vereisten zijn met name relevant wanneer de verwerking betrekking heeft op gevoelige gegevens.

2.3.3. *Doelbinding*

(53) Persoonsgegevens moeten worden verzameld voor een specifiek doel en op een manier die niet onverenigbaar is met het doel van de verwerking.

(54) Dit beginsel wordt gewaarborgd door artikel 3, leden 1 en 2, PIPA, waarin is bepaald dat de verwerkingsverantwoordelijke het doel van de verwerking vaststelt en duidelijk maakt, persoonsgegevens verwerkt op een passende wijze die noodzakelijk is voor dat doel, en deze gegevens niet voor andere dan dat doeleinde gebruikt. Het algemene beginsel van doelbinding wordt ook bevestigd in artikel 15, lid 1, artikel 18, lid 1, artikel 19 en — voor verwerkers (zogenoemde "opdrachtnemers") — in artikel 26, lid 1, punt 1, en leden 5 en 7, PIPA. Persoonsgegevens mogen met name in beginsel alleen worden gebruikt en aan derden worden verstrekt binnen de grenzen van het doel waarvoor zij zijn verzameld (artikel 15, lid 1, en artikel 17, lid 1, punt 2). Verwerking voor een verenigbaar doel, d.w.z. binnen het toepassingsgebied dat redelijkerwijs in verband staat met het oorspronkelijke doel van de verzameling, mag alleen plaatsvinden indien de betrokkenen daarvan geen nadelige gevolgen ondervinden en indien de nodige beveiligingsmaatregelen (zoals encryptie) worden getroffen (artikel 15, lid 3, en artikel 17, lid 4, PIPA). Om te bepalen of verdere verwerking een verenigbaar doel dient, somt het PIPA-uitvoeringsdecreet specifieke criteria op die vergelijkbaar zijn met die van artikel 6, lid 4, van Verordening (EU) 2016/679, zie overweging 36.

(55) Zoals in overweging 38 is uiteengezet, is het doel van de verzameling in het geval van Koreaanse verwerkingsverantwoordelijken die persoonsgegevens uit de Unie ontvangen, het doel waarvoor de gegevens worden doorgegeven. Een wijziging van het doel door de verwerkingsverantwoordelijke wordt slechts uitzonderlijk toegestaan, in specifieke (opgesomde) gevallen (artikel 18, lid 2, punt 1-3, PIPA, zie ook overweging 39). Voor zover een wijziging van het doel bij wet is toegestaan, moeten dergelijke wetten op hun beurt het fundamentele recht op privacy en gegevensbescherming eerbiedigen, evenals het noodzakelijkheid- en het evenredigheidssbeginsel, welke in de Koreaanse grondwet zijn neergelegd. Bovendien voorziet artikel 18, leden 2 en 5, PIPA in aanvullende waarborgen, met name de eis dat een dergelijke wijziging van het doel geen ongerechtvaardigde inbreuk mag vormen op het belang van een betrokkene, zodat altijd een belangenafweging moet worden gemaakt. Dit voorziet in een beschermingsniveau dat in wezen gelijkwaardig is aan dat van artikel 5, lid 1, punt b), en artikel 6, juncto overweging 50, van Verordening (EU) 2016/679.

2.3.4. *Juistheid van de gegevens en minimale gegevensverwerking*

(56) De persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd. Zij moeten ook toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

([78]) Artikel 18 van het PIPA-uitvoeringsdecreet bepaalt dat de daar genoemde gegevenscategorieën zijn uitgesloten van de bepaling van artikel 23, lid 1, van de wet wanneer zij worden verwerkt door een overheidsinstelling uit hoofde van artikel 18, lid 2, punt 5-9, PIPA.

([79]) Zie artikel 73, punt 1, en artikel 75, lid 2, punt 6, PIPA.

(57) Het beginsel van juistheid wordt ook erkend in artikel 3, lid 3, PIPA, waarin is bepaald dat persoonsgegevens juist, volledig en geactualiseerd moeten zijn, voor zover dat nodig is in verband met de doeleinden waarvoor de gegevens worden verwerkt. Het beginsel van minimale gegevensverwerking geldt op grond van artikel 3, leden 1 en 6, en artikel 16, lid 1, PIPA, waarin is bepaald dat de verwerkingsverantwoordelijke (slechts) persoonsgegevens verzamelt in de mate die minimaal noodzakelijk is voor het beoogde doel, en dat hij of zij in dit verband de bewijslast draagt. Indien het mogelijk is aan het doel van de verzameling te voldoen door informatie in geanonimiseerde vorm te verwerken, moeten de verwerkingsverantwoordelijken ernaar streven dit te doen (artikel 3, lid 7, PIPA).

2.3.5. *Opslagbeperking*

(58) Persoonsgegevens mogen in beginsel niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

(59) Het beginsel van opslagbeperking is eveneens vastgelegd in artikel 21, lid 1, PIPA ([80]), waarin is bepaald dat de verwerkingsverantwoordelijke ([81]) persoonsgegevens onverwijld moet vernietigen zodra het doel van de verwerking is bereikt of zodra de bewaringstermijn is verstreken (afhankelijk van wat er eerst komt), tenzij verdere bewaring bij wet is voorgeschreven ([82]). In dat laatste geval moeten de relevante persoonsgegevens gescheiden van andere persoonsinformatie worden opgeslagen en beheerd (artikel 21, lid 3, PIPA).

(60) Artikel 21, lid 1, PIPA is niet van toepassing wanneer gepseudonimiseerde gegevens worden verwerkt voor statistische doeleinden, wetenschappelijk onderzoek of archivering in het algemeen belang ([83]). Om ook in dit geval het beginsel van beperkte bewaring van gegevens te waarborgen, schrijft Kennisgeving 2021-5 voor dat de verwerkingsverantwoordelijken de informatie moeten anonimiseren overeenkomstig artikel 58-2 PIPA indien de gegevens niet zijn vernietigd nadat het specifieke doel van de verwerking is verwezenlijkt ([84]).

2.3.6. *Beveiliging van gegevens*

(61) Persoonsgegevens moeten op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daartoe moeten bedrijfsexploitanten passende technische of organisatorische maatregelen treffen om de persoonsgegevens te beschermen tegen mogelijke bedreigingen. Deze maatregelen moeten worden beoordeeld met inachtneming van de stand van de techniek, de daaraan verbonden kosten en de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede de risico's voor de rechten van natuurlijke personen.

(62) Een soortgelijk veiligheidsbeginsel is vastgesteld in artikel 3, lid 4, PIPA, dat verwerkingsverantwoordelijken verplicht de persoonsinformatie veilig te beheren, afhankelijk van de verwerkingsmethoden, soorten enz. van de persoonsinformatie, rekening houdend met de mogelijkheid van inbreuken op de rechten van de betrokkenen en de ernst van de desbetreffende risico's. Bovendien moet de verwerkingsverantwoordelijke de persoonsinformatie op zodanige wijze verwerken dat de mogelijkheid van inbreuken op de privacy van de betrokkene tot een minimum wordt beperkt, en er in dit verband naar streven om de persoonsgegevens zo mogelijk anoniem of in gepseudonimiseerde vorm te verwerken (artikel 3, leden 6 en 7, PIPA).

(63) Deze algemene vereisten worden verder uitgewerkt in artikel 29 PIPA, waarin is bepaald dat elke verwerkingsverantwoordelijke de technische, fysieke en beheersmaatregelen treft die nodig zijn om de bij presidentieel decreet voorgeschreven veiligheid te waarborgen, zoals de opstelling van een intern beheersplan en het bewaren van inloggegevens enz. zodat de persoonsinformatie niet verloren kan gaan of gestolen, openbaar gemaakt, vervalst,

([80]) Artikel 8 (juncto artikel 8-2, van het uitvoeringsdecreet), artikel 11 (juncto artikel 12, lid 2, van het uitvoeringsdecreet).
([81]) Zie artikel 16 van het PIPA-uitvoeringsdecreet over de methoden voor de vernietiging van persoonsinformatie. In artikel 21, lid 2, PIPA wordt verduidelijkt dat dit de nodige maatregelen omvat om het herstellen en opnieuw samenstellen te blokkeren.
([82]) Niet-naleving van deze vereisten kan leiden tot strafrechtelijke sancties (artikel 73, leden 1 en 2, PIPA). Artikel 39-6 PIPA legt aanbieders van informatie- en communicatiediensten de aanvullende verplichting op om persoonsinformatie van gebruikers die gedurende ten minste een jaar geen gebruik hebben gemaakt van de aangeboden informatie- en communicatiediensten te wissen (tenzij verdere bewaring bij wet is voorgeschreven of op verzoek van de betrokkene). Natuurlijke personen moeten dertig dagen voor het verstrijken van de termijn van één jaar in kennis worden gesteld van de voorgenomen verwijdering van hun informatie (artikel 39-6, lid 2, PIPA en artikel 48-5, lid 3, van het PIPA-uitvoeringsdecreet). Indien verdere bewaring wettelijk vereist is, moeten de bewaarde gegevens gescheiden van andere informatie van gebruikers worden opgeslagen en mogen zij alleen in overeenstemming met de desbetreffende wet worden gebruikt of bekendgemaakt (artikel 48-5, leden 1 en 2, van het PIPA-handhavingsdecreet).
([83]) Artikel 28-7 PIPA.
([84]) Kennisgeving 2021-5 (bijlage I), deel 4.

veranderd of beschadigd kan worden. In artikel 30, lid 1, van het PIPA-uitvoeringsdecreet worden deze maatregelen gespecificeerd door te verwijzen naar 1) de opstelling en uitvoering van een intern beheersplan voor de veilige verwerking van persoonsgegevens, 2) toegangscontroles en -beperkingen, 3) het gebruik van encryptietechnologie om persoonsgegevens veilig op te slaan en door te geven, 4) aanmeldingsregisters, 5) beveiligingsprogramma's, en 6) fysieke maatregelen zoals een veilig opslag- of vergrendelingssysteem ([85]).

(64) Bovendien gelden specifieke verplichtingen indien zich een inbreuk in verband met persoonsgegevens voordoet (artikel 34 PIPA juncto artikelen 39 en 40 van het PIPA-uitvoeringsdecreet) ([86]). De verwerkingsverantwoordelijke is met name verplicht de benadeelde betrokkenen onverwijld in kennis te stellen van de details van de inbreuk ([87]), met inbegrip van informatie over (verplichte) tegenmaatregelen die de verwerkingsverantwoordelijke heeft genomen en over eventuele acties die de betrokkenen kunnen ondernemen om het risico op schade zoveel mogelijk te beperken (artikel 34, leden 1 en 2, PIPA) ([88]). Indien het gegevenslek betrekking heeft op ten minste 1 000 betrokkenen, meldt de verwerkingsverantwoordelijke het gegevenslek en de getroffen tegenmaatregelen ook onverwijld aan de PIPC en het Koreaans Agentschap voor internet en veiligheid, die technische bijstand kunnen verlenen (artikel 34, lid 3, PIPA juncto artikel 39 van het PIPA-uitvoeringsdecreet). Verwerkingsverantwoordelijken zijn aansprakelijk voor schade als gevolg van gegevenslekken, overeenkomstig het burgerlijk wetboek inzake aansprakelijkheid uit onrechtmatige daad (zie ook punt 2.5 over verhaalsmogelijkheden) ([89]).

(65) In het kader van de naleving van de veiligheidsverplichtingen moet de verwerkingsverantwoordelijke worden bijgestaan door een privacyfunctionaris, die onder meer als taak heeft een intern controlesysteem op te zetten om de verspreiding, het misbruik en het oneigenlijke gebruik van persoonsinformatie te voorkomen (artikel 31, lid 2, punt 4, PIPA). Bovendien heeft de verwerkingsverantwoordelijke de plicht om passende controles en toezicht uit te oefenen op de personeelsleden die persoonsgegevens verwerken, ook wat het veilige beheer ervan betreft; dit omvat de noodzakelijke opleiding ("education") van werknemers (artikel 28, leden 1 en 2, PIPA). Tot slot moet de verwerkingsverantwoordelijke in geval van subverwerking eisen stellen aan de opdrachtnemer, onder meer met betrekking tot het veilige beheer van persoonsgegevens (technische en beheerswaarborgen), en moet hij of zij door middel van inspecties toezien op de wijze waarop deze eisen worden uitgevoerd (artikel 26, leden 1 en 4, PIPA juncto artikel 28, lid 1, punten 3 en 4, en lid 6, van het PIPA-uitvoeringsdecreet).

2.3.7. *Transparantie*

(66) Betrokkenen moeten worden ingelicht over de belangrijkste kenmerken van de verwerking van hun persoonsgegevens.

([85]) Wat de verwerking van persoonsgegevens door aanbieders van informatie- en communicatiediensten betreft, is in artikel 39-5 PIPA uitdrukkelijk bepaald dat het aantal personen dat persoonsinformatie van gebruikers behandelt, tot een minimum moet worden beperkt. Bovendien moeten de aanbieders van informatie- en communicatiediensten ervoor zorgen dat persoonsinformatie van gebruikers niet via het informatie- en communicatienetwerk aan het publiek wordt bekendgemaakt (artikel 39-10, lid 1, PIPA). Bekendgemaakte informatie moet op verzoek van de PIPC worden verwijderd of geblokkeerd (artikel 39-10, lid 2, PIPA). Meer in het algemeen gelden voor aanbieders van informatie- en communicatiediensten (en derden die persoonsgegevens van gebruikers ontvangen) aanvullende beveiligingsverplichtingen, die zijn gespecificeerd in artikel 48-2 van het PIPA-uitvoeringsdecreet, bv. de ontwikkeling en uitvoering van een intern beheersplan met betrekking tot beveiligingsmaatregelen, maatregelen om toegangscontrole te waarborgen, encryptie, het gebruik van software om kwaadaardige programma's op te sporen enz.

([86]) Bovendien geldt er een algemeen verbod om persoonsinformatie te beschadigen, te vernietigen, te wijzigen, te vervalsen of te lekken zonder wettelijke bevoegdheid, zie artikel 59, punt 3, PIPA.

([87]) De verplichting om de betrokkene in kennis te stellen, geldt niet wanneer zich een gegevenslek voordoet met gepseudonimiseerde informatie die wordt verwerkt voor statistische of wetenschappelijke doeleinden of voor archivering in het algemeen belang (artikel 28-7 PIPA, dat voorziet in een uitzondering op artikel 34, lid 1, en artikel 39-4 PIPA). Een individuele kennisgeving zou betekenen dat de betrokken verwerkingsverantwoordelijke de natuurlijke personen uit de gepseudonimiseerde gegevensreeks moet identificeren, hetgeen uitdrukkelijk is verboden krachtens artikel 28-5 PIPA. De algemene meldplicht voor gegevenslekken (aan de PIPC) blijft echter van toepassing.

([88]) De kennisgevingsvereisten, met inbegrip van het tijdschema en de mogelijkheid van een kennisgeving in fasen, worden nader gespecificeerd in artikel 40 van het PIPA-uitvoeringsdecreet. Er gelden strengere regels voor aanbieders van informatie- en communicatiediensten die verplicht zijn de betrokkene en de PIPC binnen 24 uur nadat zij kennis hebben gekregen van het verlies, de diefstal of het uitlekken van persoonsinformatie hiervan in kennis te stellen (artikel 39-4, lid 1, PIPA). Deze kennisgeving moet nadere gegevens bevatten over de persoonsinformatie die is gelekt, het tijdstip waarop dit is gebeurd, de maatregelen die de gebruiker kan nemen, de door de aanbieder genomen tegenmaatregelen en de contactgegevens van de afdeling waar de gebruiker met vragen terecht kan (artikel 39-4, lid 1, punt 1-5, PIPA). Indien er een gerechtvaardigde reden is, bv. de contactgegevens van de gebruiker zijn niet beschikbaar, kunnen andere middelen voor kennisgeving worden gebruikt, bv. door de informatie op een openbare website te plaatsen (artikel 39-4, lid 1, PIPA juncto artikel 48-4, lid 4, e.v. van het PIPA-uitvoeringsdecreet). In dat geval moet de PIPC van de redenen in kennis worden gesteld (artikel 34-4, lid 3, PIPA).

([89]) Zie bv. Beslissingen 2011Da59834, 2011Da59858 en 2011Da59841 van het Hooggerechtshof van 26 december 2012. Een Engelse samenvatting is hier beschikbaar: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm

(67) Dit wordt in het Koreaanse systeem op verschillende manieren gewaarborgd. Naast het recht op informatie uit hoofde van artikel 4, punt 1, (in het algemeen) en artikel 20, lid 1, PIPA (voor persoonsgegevens die van derden zijn verkregen), alsook het recht op toegang overeenkomstig artikel 35 PIPA, omvat de PIPA een algemeen transparantievereiste met betrekking tot het doel van de verwerking (artikel 3, lid 1, PIPA) en specifieke transparantievereisten in het geval van verwerking op basis van toestemming (artikel 15, lid 2, artikel 17, lid 2, en artikel 18, lid 3, PIPA) ([90]). Bovendien schrijft artikel 20, lid 2, PIPA voor dat bepaalde verwerkingsverantwoordelijken — voor wie de hoeveelheid verwerkte gegevens bepaalde drempels overschrijdt ([91]) — de betrokkene van wie zij via een derde partij persoonsgegevens hebben ontvangen, in kennis moeten stellen van de informatiebron, het doel van de verwerking en het recht van de betrokkene om een opschorting van de verwerking te eisen, tenzij een dergelijke kennisgeving onmogelijk blijkt door het ontbreken van contactgegevens. Uitzonderingen gelden voor bepaalde bestanden met persoonsgegevens die in het bezit zijn van overheidsinstanties, met name bestanden met gegevens die worden verwerkt met het oog op de nationale veiligheid, andere bijzonder belangrijke (gewichtige) nationale belangen of de strafrechtelijke rechtshandhaving, of wanneer kennisgeving het leven of de lichamelijke integriteit van een andere persoon kan schaden, of op oneerlijke wijze schade kan toebrengen aan de eigendoms- en andere belangen van een andere persoon, echter alleen wanneer de betrokken openbare of particuliere belangen duidelijk zwaarder doorwegen dan de rechten van de betrokkenen (artikel 20, lid 4, PIPA). Hiervoor is een afweging van de belangen noodzakelijk.

(68) Bovendien bepaalt artikel 3, lid 5, PIPA dat de verwerkingsverantwoordelijken hun privacybeleid (en andere zaken in verband met de verwerking van persoonsgegevens) openbaar moeten maken. Deze eis is nader uitgewerkt in artikel 30 PIPA juncto artikel 31 van het PIPA-uitvoeringsdecreet. Volgens die bepalingen moet het openbare privacybeleid onder meer het volgende omvatten: 1) de soorten persoonsgegevens die worden verwerkt, 2) het doel van de verwerking, 3) de bewaartermijn, 4) of persoonsgegevens aan een derde partij worden verstrekt ([92]), 5) eventuele subverwerking, 6) informatie over de rechten van de betrokkene en hoe deze kunnen worden uitgeoefend en 7) contactgegevens (waaronder de naam van de privacyfunctionaris of de interne afdeling die verantwoordelijk is voor het toezicht op de naleving van de gegevensbeschermingsvoorschriften en voor de behandeling van klachten). Het privacybeleid moet zodanig openbaar worden gemaakt dat de betrokkenen het gemakkelijk kunnen herkennen (artikel 30, lid 2, PIPA) ([93]) en het moet voortdurend worden bijgewerkt (artikel 31, lid 2, van het PIPA-uitvoeringsdecreet).

(69) Voor openbare instellingen geldt een aanvullende verplichting om met name de volgende informatie bij de PIPC te registreren: 1) de naam van de overheidsinstelling, 2) de gronden en doeleinden voor de verwerking van de bestanden met persoonsgegevens, 3) de bijzonderheden van de persoonsgegevens die worden geregistreerd, 4) de verwerkingsmethode, 5) de bewaartermijn, 6) het aantal betrokkenen van wie persoonsgegevens worden bewaard, 7) de afdeling die verzoeken van betrokkenen behandelt en 8) de ontvangers van persoonsgegevens wanneer gegevens routinematig of herhaaldelijk worden verstrekt (artikel 32, lid 1, PIPA) ([94]). Geregistreerde bestanden met persoonsgegevens worden door de PIPC openbaar gemaakt en moeten ook door openbare instellingen in hun privacybeleid worden vermeld (artikel 30, lid 1, en artikel 32, lid 4, PIPA).

(70) Om de transparantie te vergroten voor betrokkenen in de Unie van wie persoonsgegevens op basis van dit besluit worden doorgegeven aan Korea, worden in deel 3, punten i) en ii), van Kennisgeving 2021-5 (bijlage I) aanvullende transparantievereisten opgelegd. Ten eerste moeten Koreaanse verwerkingsverantwoordelijken, wanneer zij op grond van dit besluit persoonsgegevens uit de Unie ontvangen, de betrokkenen onverwijld (en in ieder geval niet later dan één maand na de doorgifte) in kennis stellen van de naam en de contactgegevens van de entiteiten

([90]) Met name wanneer persoonsinformatie met toestemming van een natuurlijke persoon wordt verwerkt, moet de verwerkingsverantwoordelijke de betrokkene in kennis stellen van het doel van de verwerking, details over de te verwerken informatie, de ontvanger van de informatie, de periode gedurende welke de persoonsinformatie wordt bewaard en gebruikt, alsook van het feit dat de betrokkene het recht heeft om de toestemming te weigeren (en van eventuele nadelen die daaruit kunnen voortvloeien).

([91]) Volgens artikel 15-2, lid 1, van het PIPA-uitvoeringsdecreet gaat het om verwerkingsverantwoordelijken die gevoelige informatie van ten minste 50 000 betrokkenen, of "normale" persoonsinformatie van ten minste 1 miljoen betrokkenen verwerken. In artikel 15-2, lid 2, van het PIPA-uitvoeringsdecreet zijn de wijze en het tijdstip van kennisgeving bepaald en in artikel 15-2, lid 3, de verplichting om bepaalde registers daarvan bij te houden. Bovendien gelden specifieke regels voor bepaalde categorieën aanbieders van informatie- en communicatiediensten (aanbieders die in het voorgaande jaar ten minste 10 miljard KRW aan verkoopopbrengsten hebben gegenereerd, of aanbieders die in de drie maanden voorafgaand aan het einde van het voorgaande jaar dagelijks gemiddeld de persoonsgegevens van ten minste één miljoen gebruikers opslaan/beheren); zij zijn verplicht de gebruikers regelmatig in kennis te stellen van de gebruiksgeschiedenis van hun persoonsinformatie, tenzij dit onmogelijk blijkt door het ontbreken van contactgegevens (artikel 39-8 PIPA en artikel 48-6 van het PIPA-uitvoeringsdecreet).

([92]) Volgens de van de Koreaanse regering ontvangen informatie houdt dit de verplichting in om de ontvanger(s) individueel te vermelden in het openbare privacybeleid.

([93]) Verdere modaliteiten zijn opgenomen in artikel 31, lid 3, van het PIPA-uitvoeringsdecreet.

([94]) De registratieplicht geldt niet voor bepaalde soorten bestanden met persoonsinformatie, bijvoorbeeld bestanden waarin zaken worden geregistreerd die verband houden met de nationale veiligheid, diplomatieke geheimen, strafrechtelijke onderzoeken, vervolging, bestraffing, onderzoeken naar belastingmisdrijven, of bestanden die uitsluitend betrekking hebben op interne arbeidsprestaties (artikel 32, lid 2, PIPA).

die de informatie doorgeven en ontvangen, de doorgegeven persoonsgegevens (of categorieën persoonsgegevens), het doel van de verzameling door de Koreaanse verwerkingsverantwoordelijke, de bewaartermijn en de rechten die op grond van de PIPA beschikbaar zijn. Ten tweede moeten betrokkenen, wanneer op grond van dit besluit persoonsgegevens die van de Unie zijn ontvangen aan derden worden verstrekt, onder meer worden ingelicht over de ontvanger, de persoonsgegevens of categorieën persoonsgegevens die worden verstrekt, het land waaraan de gegevens worden verstrekt (indien van toepassing), alsook over de rechten die op grond van de PIPA beschikbaar zijn ([95]). Op die manier zorgt de kennisgeving ervoor dat EU-burgers op de hoogte blijven van de specifieke verwerkingsverantwoordelijken die hun informatie verwerken en dat zij hun rechten ten aanzien van de betrokken entiteiten kunnen uitoefenen.

(71) Volgens deel 3, punt iii), van de kennisgeving (bijlage I) zijn bepaalde beperkte en gekwalificeerde uitzonderingen op deze aanvullende transparantieverplichtingen toegestaan, die in wezen gelijkwaardig zijn aan die waarin Verordening (EU) 2016/679 voorziet. In het bijzonder is kennisgeving aan betrokkenen in de Unie niet vereist 1) wanneer en zolang het noodzakelijk is de kennisgeving te beperken om bepaalde redenen van algemeen belang (bijvoorbeeld wanneer de informatie wordt verwerkt met het oog op de nationale veiligheid of lopende strafrechtelijke onderzoeken), voor zover deze doelstellingen van algemeen belang duidelijk zwaarder doorwegen dan de rechten van de betrokkene; 2) wanneer de betrokkene reeds over de informatie beschikt; 3) wanneer en zolang de kennisgeving het leven of de lichamelijke integriteit van de betrokkene of van een andere persoon kan schaden, dan wel op ongerechtvaardigde wijze inbreuk kan maken op de eigendomsbelangen van een andere persoon, wanneer deze rechten of belangen duidelijk zwaarder doorwegen dan de rechten van de betrokkene, of 4) wanneer er geen contactgegevens van de betrokkenen beschikbaar zijn, of wanneer het een onevenredige inspanning zou vergen om hen op de hoogte te brengen. Om te bepalen of het al dan niet mogelijk is om contact op te nemen met de betrokkene en of dit buitensporige inspanningen vergt, moet rekening worden gehouden met de mogelijkheid om samen te werken met de gegevensexporteur in de Unie.

(72) De voorschriften in overwegingen 67 tot en met 71 zorgen daarom voor een in wezen gelijkwaardig beschermingsniveau met betrekking tot transparantie als waarin wordt voorzien door Verordening (EU) 2016/679.

2.3.8. *Individuele rechten*

(73) Betrokkenen moeten bepaalde rechten hebben die kunnen worden afgedwongen ten opzichte van de verwerkingsverantwoordelijke of de verwerker, met name het recht op inzage van de gegevens, het recht op rectificatie, het recht om bezwaar te maken tegen de verwerking en het recht op wissing van de gegevens. Tegelijkertijd kunnen deze rechten aan beperkingen worden onderworpen, voor zover deze beperkingen noodzakelijk en evenredig zijn om belangrijke doelstellingen van algemeen openbaar belang te waarborgen.

(74) Overeenkomstig artikel 3, lid 5, PIPA waarborgt de verwerkingsverantwoordelijke de in artikel 4 PIPA genoemde en in de artikelen 35 tot en met 37, 39 en 39-2 PIPA nader omschreven rechten van de betrokkene.

(75) Ten eerste hebben natuurlijke personen recht op informatie en toegang. Wanneer de verwerkingsverantwoordelijke persoonsgegevens bij een derde heeft verzameld — wat altijd het geval zal zijn wanneer de gegevens vanuit de Unie worden doorgegeven — hebben betrokkenen in het algemeen het recht om informatie te ontvangen over 1) de "bron" van de verzamelde persoonsgegevens (d.w.z. de doorgever), 2) het doel van de verwerking en 3) het feit dat de betrokkene het recht heeft om opschorting van de verwerking te verzoeken (artikel 20, lid 1, PIPA). Er zijn beperkte uitzonderingen, namelijk wanneer een dergelijke kennisgeving schade kan toebrengen aan het leven of de lichamelijke integriteit van een andere persoon, of op oneerlijke wijze schade toebrengt aan de eigendoms- en andere belangen van een andere persoon, maar alleen wanneer deze belangen van derden duidelijk zwaarder doorwegen dan de rechten van de betrokkene (artikel 20, lid 4, punt 2, PIPA).

(76) Bovendien verleent artikel 35, leden 1 en 3, PIPA juncto artikel 41, lid 4, van het PIPA-uitvoeringsdecreet betrokkenen het recht op toegang tot hun persoonsinformatie ([96]). Het recht op toegang omvat een bevestiging van de verwerking, informatie over het soort verwerkte gegevens, het doel van de verwerking, de bewaartermijn,

([95]) Kennisgeving 2021-5, deel 3, punt ii) (bijlage I).

([96]) Overeenkomstig artikel 35, lid 3, PIPA juncto artikel 42, lid 2, van het PIPA-uitvoeringsdecreet, mag de verwerkingsverantwoordelijke de toegang om gegronde redenen uitstellen (d.w.z. op gerechtvaardigde gronden, bv. indien meer tijd nodig is om te beoordelen of toegang kan worden verleend), maar moet hij de betrokkene binnen tien dagen in kennis stellen van een dergelijke rechtvaardiging en deze laatste informatie verstrekken over de wijze waarop tegen dit besluit beroep kan worden aangetekend; zodra de reden voor het uitstel niet meer bestaat, moet toegang worden verleend.

alsmede eventuele verstrekking aan derden, en de verstrekking van een kopie van de verwerkte persoonsinformatie (artikel 4, punt 3, PIPA juncto artikel 41, lid 1, van het PIPA-uitvoeringsdecreet) ([97]). De toegang kan alleen worden beperkt (gedeeltelijke toegang) ([98]) of worden geweigerd wanneer de wet daarin voorziet ([99]), wanneer dit waarschijnlijk schade aan het leven of de lichamelijke integriteit van een derde zou toebrengen, of op ongerechtvaardigde wijze een inbreuk zou vormen op de eigendoms- en andere belangen van een andere persoon (artikel 35, lid 4, PIPA) ([100]). Dit laatste impliceert dat een evenwicht moet worden gevonden tussen de grondwettelijk beschermde rechten en vrijheden van het individu enerzijds en van andere personen anderzijds. Wanneer de toegang wordt beperkt of geweigerd, moet de verwerkingsverantwoordelijke de betrokkene in kennis stellen van de redenen daarvoor en van de wijze waarop tegen het besluit beroep kan worden aangetekend (artikel 41, lid 5, en artikel 42, lid 2, van het PIPA-uitvoeringsdecreet).

(77) Ten tweede hebben betrokkenen het recht op correctie of wissing ([101]) van hun persoonsgegevens, tenzij uitdrukkelijk anders bepaald door andere wetten (artikel 36, leden 1 en 2, PIPA) ([102]). Na ontvangst van een verzoek moet de verwerkingsverantwoordelijke de zaak onverwijld onderzoeken, de nodige maatregelen treffen ([103]) en de betrokkene daarvan binnen tien dagen in kennis stellen; wanneer het verzoek niet kan worden ingewilligd, omvat deze kennisgevingsverplichting de redenen voor de weigering en de wijze waarop beroep kan worden aangetekend (zie artikel 36, lid 4, PIPA juncto artikel 43, lid 3, van het PIPA-uitvoeringsdecreet) ([104]).

(78) Tot slot hebben betrokkenen het recht om de verwerking van hun persoonsgegevens onverwijld te laten opschorten ([105]), tenzij een van de opgesomde uitzonderingen van toepassing is (artikel 37, leden 1 en 2, PIPA) ([106]). De verwerkingsverantwoordelijke kan het verzoek weigeren 1) wanneer dit specifiek bij wet is toegestaan of noodzakelijk (onvermijdelijk) is om aan wettelijke verplichtingen te voldoen; 2) wanneer opschorting waarschijnlijk schade zou toebrengen aan het leven of de lichamelijke integriteit van een derde, of op ongerechtvaardigde wijze een inbreuk zou vormen op de eigendoms- en andere belangen van een andere persoon; 3) wanneer het voor een overheidsinstelling onmogelijk zou zijn haar bij wet voorgeschreven functie uit te oefenen zonder de informatie te verwerken, of 4) wanneer de betrokkene de onderliggende overeenkomst met de verwerkingsverantwoordelijke niet uitdrukkelijk beëindigt, ook al zou het onmogelijk zijn de overeenkomst zonder die gegevensverwerking uit te voeren. In dat geval moet de verwerkingsverantwoordelijke de betrokkene onverwijld in kennis stellen van de redenen voor de weigering en de wijze waarop beroep kan worden aangetekend (artikel 37, lid 2, PIPA juncto artikel 44, lid 2, van het PIPA-uitvoeringsdecreet). Overeenkomstig artikel 37, lid 4, PIPA moet de verwerkingsverantwoordelijke onverwijld de nodige maatregelen treffen, waaronder de vernietiging van de betrokken persoonsinformatie in het kader van de inwilliging van het verzoek om opschorting ([107]).

(79) Het recht op opschorting geldt ook wanneer persoonsgegevens worden gebruikt voor direct-marketingdoeleinden, d.w.z. om goederen of diensten aan te prijzen of om te verzoeken deze te kopen. Bovendien is voor een dergelijke verdere verwerking in het algemeen de specifieke (aanvullende) toestemming van de betrokkene vereist (zie artikel 15, lid 1, punt 1 en artikel 17, lid 2, punt 1, PIPA) ([108]). Wanneer om deze toestemming wordt gevraagd, moet de verwerkingsverantwoordelijke de betrokkene met name op uitdrukkelijk herkenbare wijze in kennis

([97]) Toegang tot persoonsinformatie die door een openbare instelling wordt verwerkt, kan direct bij de instelling worden verkregen of indirect door een verzoek in te dienen bij de PIPC, die het verzoek onverwijld doorstuurt (artikel 35, lid 2, PIPA en artikel 41, lid 3, van het PIPA-uitvoeringsdecreet).

([98]) Volgens artikel 42, lid 1, van het PIPA-uitvoeringsdecreet is de verwerkingsverantwoordelijke verplicht gedeeltelijke toegang te verlenen wanneer ten minste een deel van de informatie niet onder de weigeringsgronden valt.

([99]) Deze wetgeving moet op haar beurt het fundamentele recht op privacy en gegevensbescherming eerbiedigen, evenals het noodzakelijkheids- en het evenredigheidsbeginsel, welke in de Koreaanse grondwet zijn neergelegd.

([100]) Bovendien kunnen overheidsinstellingen toegang weigeren indien dit ernstige moeilijkheden zou veroorzaken voor de uitvoering van bepaalde taken, waaronder lopende controles of de heffing, inning of terugbetaling van belastingen (artikel 35, lid 4, PIPA).

([101]) In dit geval moet de verwerkingsverantwoordelijke maatregelen nemen om te voorkomen dat de persoonsinformatie kan worden hersteld, zie artikel 36, lid 3, PIPA.

([102]) Dergelijke wetten moeten voldoen aan de grondwettelijke vereisten dat een grondrecht alleen mag worden beperkt wanneer dat noodzakelijk is voor de nationale veiligheid of de handhaving van de openbare orde met het oog op het openbaar welzijn, en zij moeten de wezenlijke inhoud van de vrijheid of het recht onverlet laten (artikel 37, lid 2, van de grondwet).

([103]) Artikel 43, lid 2, van het PIPA-uitvoeringsdecreet voorziet in een speciale procedure voor het geval de verwerkingsverantwoordelijke bestanden met persoonsinformatie verwerkt die door een andere verwerkingsverantwoordelijke zijn verstrekt.

([104]) Het niet nemen van de nodige maatregelen om persoonsinformatie te corrigeren of te wissen en het aanhoudend gebruik of de verstrekking van die gegevens aan een derde partij kan leiden tot strafrechtelijke sancties (artikel 73, lid 2, PIPA).

([105]) Overeenkomstig artikel 44, lid 2, van het PIPA-uitvoeringsdecreet stelt de verwerkingsverantwoordelijke de betrokkene binnen tien dagen na ontvangst van het verzoek in kennis van het feit dat de verwerking naar behoren is opgeschort.

([106]) Wat overheidsinstellingen betreft, kan het recht op opschorting van de verwerking worden uitgeoefend voor gegevens in bestanden met persoonsinformatie die zijn geregistreerd (artikel 37 juncto artikel 32 PIPA). Een dergelijke registratie is niet vereist in een beperkt aantal situaties, bijvoorbeeld wanneer de bestanden met persoonsinformatie betrekking hebben op de nationale veiligheid, strafrechtelijke onderzoeken, diplomatieke betrekkingen enz. (artikel 32, lid 2, PIPA).

([107]) Het niet opschorten van de verwerking kan tot strafrechtelijke sancties leiden (artikel 73, lid 3, PIPA).

([108]) Het Comité voor geschillenbeslechting (zie overweging 133) heeft verschillende zaken behandeld waarin personen klaagden over het zonder toestemming gebruiken van hun gegevens voor direct-marketing. Sommige van deze zaken hebben geleid tot de betaling van een schadevergoeding en de verwijdering van persoonsgegevens door de betrokken verwerkingsverantwoordelijke (zie bv. Comité voor geschillenbeslechting 20R10-024(2020.11.18), 20R08-015(2020.8.28) en 20R07-031(2020.9.1)).

stellen van het voorgenomen gebruik van de gegevens voor direct-marketingdoeleinden — d.w.z. van het feit dat hij of zij kan worden benaderd om goederen of diensten aan te prijzen of om te verzoeken deze aan te kopen (artikel 22, leden 2 en 4, PIPA juncto artikel 17, lid 2, punt 1, van het PIPA-uitvoeringsdecreet).

(80) Om de uitoefening van individuele rechten te vergemakkelijken, moet de verwerkingsverantwoordelijke specifieke procedures vaststellen en deze openbaar maken (artikel 38, lid 4, PIPA) ([109]). Dit omvat procedures om bezwaar aan te tekenen tegen de afwijzing van een verzoek (artikel 38, lid 5, PIPA). De verwerkingsverantwoordelijke moet ervoor zorgen dat de procedure voor de uitoefening van rechten de betrokkene centraal stelt en niet moeilijker is dan de procedure voor de verzameling van de persoonsgegevens; dit omvat ook de verplichting om informatie over de procedure te verstrekken op zijn website (artikel 41, lid 2, artikel 43, lid 1, en artikel 44, lid 1, van het PIPA-uitvoeringsdecreet). ([110]) Natuurlijke personen kunnen een vertegenwoordiger machtigen om een dergelijk verzoek in te dienen (artikel 38, lid 1, PIPA juncto artikel 45 van het PIPA-uitvoeringsdecreet). Hoewel de verwerkingsverantwoordelijke het recht heeft een vergoeding op te leggen (alsook portkosten in het geval van een verzoek om kopieën van persoonsgegevens per post te verzenden), moet het bedrag worden vastgesteld binnen de grenzen van de werkelijke kosten die nodig zijn voor de verwerking van het verzoek; er mag geen vergoeding (noch portkosten) worden gevraagd wanneer de verwerkingsverantwoordelijke het verzoek heeft veroorzaakt (artikel 38, lid 3, PIPA juncto artikel 47 van het PIPA-uitvoeringsdecreet).

(81) De PIPA en het PIPA-uitvoeringsdecreet bevatten geen algemene voorzieningen die zijn gericht op de kwestie van besluiten die de betrokkene betreffen en die alleen zijn gebaseerd op de geautomatiseerde verwerking van persoonsgegevens. Wat betreft de persoonsgegevens die in de Europese Unie zijn verzameld, wordt echter elk besluit dat is gebaseerd op geautomatiseerde verwerking, doorgaans genomen door de verwerkingsverantwoordelijke in de Unie (die een directe relatie met de betrokkene heeft) en is daarom onderworpen aan Verordening (EU) 2016/679 ([111]). Dit omvat doorgiftescenario's waarin de verwerking wordt uitgevoerd door een buitenlandse (bijvoorbeeld Koreaanse) bedrijfsexploitant die handelt als verwerker namens de verwerkingsverantwoordelijke in de EU (of als subverwerker die handelt namens de verwerker in de EU, die de gegevens heeft ontvangen van een EU-verwerkingsverantwoordelijke die ze heeft verzameld) die op deze basis de beslissing neemt. Daarom is het onwaarschijnlijk dat het ontbreken van specifieke voorschriften voor geautomatiseerde besluitvorming in de PIPA een weerslag heeft op het beschermingsniveau van persoonsgegevens die in het kader van dit besluit worden doorgegeven.

(82) Bij wijze van uitzondering zijn de bepalingen inzake transparantie op verzoek (artikel 20) en individuele rechten (artikelen 35 tot en met 37), alsmede de individuele meldingsplicht voor aanbieders van informatie- en communicatiediensten (artikel 39-8 PIPA), niet van toepassing op gepseudonimiseerde informatie, wanneer die wordt verwerkt voor statistische doeleinden, wetenschappelijk onderzoek of archivering in het algemeen belang (artikel 28-7 PIPA) ([112]). In overeenstemming met de benadering van artikel 11, lid 2 (in samenhang met overweging 57) van Verordening (EU) 2016/679 wordt dit gerechtvaardigd door het feit dat de verwerkingsverantwoordelijke, om de transparantie te waarborgen of individuele rechten te verlenen, zou moeten nagaan of (en zo ja welke) gegevens betrekking hebben op de persoon die het verzoek indient, hetgeen uitdrukkelijk verboden is op grond van de PIPA (artikel 28-5, lid 1, PIPA). Bovendien zou, wanneer een dergelijke heridentificatie de pseudonimisering voor de volledige (gepseudonimiseerde) gegevensset ongedaan maakt, de persoonlijke informatie van alle andere betrokken personen aan grotere risico's worden blootgesteld. Terwijl Verordening (EU) 2016/679 verwijst naar situaties waarin re-identificatie praktisch onmogelijk is, kiest de PIPA voor een strengere aanpak door re-identificatie uitdrukkelijk te verbieden in alle situaties waarin gepseudonimiseerde informatie wordt verwerkt.

(83) Het Koreaanse systeem, zoals beschreven in de overwegingen 74 tot en met 82, bevat derhalve voorschriften over de rechten van betrokkenen die een beschermingsniveau bieden dat in wezen gelijkwaardig is aan dat van Verordening (EU) 2016/679.

([109]) Zie ook artikel 30, lid 1, punt 5, PIPA over het privacybeleid, dat onder meer informatie moet bevatten over de rechten waarover de betrokkene beschikt en hoe die kunnen worden uitgeoefend.

([110]) Zie ook artikel 39-7, lid 2, PIPA met betrekking tot aanbieders van informatie- en communicatiediensten.

([111]) In het uitzonderlijke geval waarin de Koreaanse bedrijfsexploitant een directe relatie met de betrokkene in de EU heeft, komt dit daarentegen doorgaans doordat hij of zij zich direct tot de betrokkene in de Europese Unie heeft gericht door goederen of diensten aan te bieden of zijn of haar gedrag te volgen. In dit scenario valt de Koreaanse bedrijfsexploitant zelf binnen de werkingssfeer van Verordening (EU) 2016/679 (artikel 3, lid 2) en moet hij dus direct voldoen aan de gegevensbeschermingswetgeving van de EU.

([112]) Zie ook Kennisgeving 2021-5, waarin wordt bevestigd dat deel III van de PIPA (met inbegrip van artikel 28-7) alleen van toepassing is wanneer gepseudonimiseerde informatie wordt verwerkt voor wetenschappelijk onderzoek, statistische doeleinden of archivering in het algemeen belang, zie deel 4 van bijlage I bij dit besluit.

2.3.9. *Verdere doorgiften*

(84) Het beschermingsniveau dat wordt geboden voor persoonsgegevens die worden doorgegeven vanuit de Unie naar verwerkingsverantwoordelijken in de Republiek Korea mag niet worden ondermijnd door de verdere doorgifte van dergelijke gegevens aan ontvangers in een derde land.

(85) Dergelijke "verdere doorgiften" vormen internationale doorgiften vanuit de Republiek Korea vanuit het oogpunt van de Koreaanse verwerkingsverantwoordelijke. In dit verband wordt in de PIPA onderscheid gemaakt tussen het uitbesteden van de verwerking aan een opdrachtnemer (d.w.z. een verwerker) en het verstrekken van persoonsgegevens aan derden ([113]).

(86) Ten eerste moet de Koreaanse verwerkingsverantwoordelijke de naleving van de bepalingen van de PIPA inzake uitbesteding (artikel 26 PIPA) waarborgen wanneer de verwerking van persoonsgegevens wordt uitbesteed aan een entiteit in een derde land. Dit omvat het voorzien in een wettelijk bindend instrument aan de hand waarvan onder meer de verwerking door de opdrachtnemer wordt beperkt tot het doel van de uitbestede werkzaamheden, technische en beheerswaarborgen worden opgelegd en subverwerking wordt beperkt (zie artikel 26, lid 1, PIPA), en het bekendmaken van informatie over de uitbestede werkzaamheden. De verwerkingsverantwoordelijke is bovendien verplicht de opdrachtnemer te scholen ("educate") over de noodzakelijke beveiligingsmaatregelen en het noodzakelijke toezicht, onder meer door middel van inspecties, de naleving van alle verplichtingen van de verwerkingsverantwoordelijke uit hoofde van de PIPA ([114]) en de overeenkomst voor de uitbesteding.

(87) Wanneer de opdrachtnemer schade veroorzaakt door de persoonsgegevens op een wijze te verwerken die strijdig is met de PIPA, wordt dit met het oog op de aansprakelijkheid toegerekend aan de verwerkingsverantwoordelijke, zoals het geval zou zijn bij werknemers van de verwerkingsverantwoordelijke (artikel 26, lid 6, PIPA). De Koreaanse verwerkingsverantwoordelijke blijft derhalve verantwoordelijk voor de uitbestede persoonsgegevens en moet ervoor zorgen dat de verwerker in het buitenland de informatie overeenkomstig de PIPA verwerkt. Indien de opdrachtnemer de informatie verwerkt op een wijze die in strijd is met de PIPA, kan de Koreaanse verwerkingsverantwoordelijke aansprakelijk worden gesteld voor het niet nakomen van zijn verplichting om de naleving van de PIPA te waarborgen, zoals door middel van toezicht op de opdrachtnemer. De waarborgen die zijn opgenomen in de uitbestedingsovereenkomst en de aansprakelijkheid van de Koreaanse verwerkingsverantwoordelijke voor de acties van de opdrachtnemer waarborgen de continuïteit van de bescherming wanneer persoonsgegevens worden doorgegeven aan een entiteit buiten Korea.

(88) Ten tweede mogen Koreaanse verwerkingsverantwoordelijken persoonsgegevens verstrekken aan derden buiten Korea. Hoewel de PIPA een aantal rechtsgrondslagen bevat die de verstrekking aan derden in het algemeen toestaan, moet de verwerkingsverantwoordelijke wanneer de derde zich buiten Korea bevindt in principe ([115]) de toestemming van de betrokkene verkrijgen ([116]) nadat hij deze informatie heeft verstrekt over 1) het soort persoonsgegevens, 2) de ontvanger van de persoonsgegevens, 3) het doel van de doorgifte in de zin van het doel van de door de ontvanger beoogde verwerking, 4) de bewaarperiode voor de verwerking door de ontvanger en 5) het feit dat de betrokkene de toestemming kan weigeren (artikel 17, leden 2 en 3, PIPA). Kennisgeving nr. 2021-5 vereist in het deel over transparantie (zie overweging 70) dat natuurlijke personen worden geïnformeerd over het derde land waaraan hun gegevens zullen worden verstrekt. Zo wordt gewaarborgd dat betrokkenen in de Unie een volledig geïnformeerde beslissing kunnen nemen over het al dan niet instemmen met een verstrekking naar het buitenland. Bovendien mag de verwerkingsverantwoordelijke geen overeenkomst sluiten met de derde ontvanger die in strijd is met de PIPA, wat betekent dat de overeenkomst geen verplichtingen mag bevatten die strijdig zouden zijn met de vereisten die bij de PIPA aan de verwerkingsverantwoordelijke zijn opgelegd ([117]).

([113]) Er zijn specifieke regels van toepassing op aanbieders van informatie- en communicatiediensten. Overeenkomstig artikel 39-12 PIPA moeten aanbieders van informatie- en communicatiediensten in beginsel toestemming van de gebruiker verkrijgen voor alle doorgiften van persoonsinformatie naar het buitenland. Wanneer de persoonsinformatie wordt doorgegeven als onderdeel van de uitbesteding van de verwerking, waaronder voor opslag, is toestemming niet vereist wanneer de betrokkenen vooraf direct of door middel van een openbare kennisgeving en op gemakkelijk toegankelijke wijze op de hoogte zijn gesteld van 1) de bijzonderheden van de informatie die zal worden doorgegeven, 2) het land waarnaar de informatie zal worden doorgegeven (evenals de datum en methode van de doorgifte), 3) de naam van de ontvanger en 4) het doel van het gebruik en de bewaring door de ontvanger (artikel 39-12, lid 3, PIPA). Daarnaast zijn de algemene vereisten voor uitbesteding in dat geval van toepassing. Voor elke doorgifte moet worden voorzien in specifieke waarborgen met betrekking tot de beveiliging, de afhandeling van klachten en geschillen en andere maatregelen die nodig zijn om de informatie van gebruikers te beschermen (artikel 48-10 van het PIPA-uitvoeringsdecreet).

([114]) Zie ook artikel 26, lid 7, PIPA, waarin is bepaald dat de artikelen 15 tot en met 25, 27 tot en met 31, 33 tot en met 38 en 50 mutatis mutandis van toepassing zijn op de verwerker.

([115]) De verstrekking van persoonsinformatie van gebruikers door aanbieders van informatie- en communicatiediensten aan derden vereist altijd de toestemming van de gebruiker (artikel 39-12, lid 2, PIPA).

([116]) Zoals meer in detail uiteengezet in voetnoot 51, kan een dergelijke toestemming alleen geldig zijn als zij vrijelijk wordt gegeven en geïnformeerd en specifiek is.

([117]) Zie ook artikel 39-12, lid 1, PIPA met betrekking tot aanbieders van informatie- en communicatiediensten.

(89) Zonder toestemming van de betrokkene mogen persoonsgegevens aan een derde (in het buitenland) worden verstrekt wanneer het doel van de verstrekking binnen het toepassingsgebied blijft dat redelijkerwijs verband houdt met het oorspronkelijke doel waarvoor de gegevens zijn verzameld (artikel 17, lid 4, PIPA, zie overweging 36). Bij het besluit of persoonsgegevens al dan niet voor een gerelateerd doel worden doorgegeven, moet de verwerkingsverantwoordelijke rekening houden met de vraag of de verstrekking nadelen voor de betrokkene oplevert en of de noodzakelijke beveiligingsmaatregelen (zoals encryptie) zijn genomen. Gezien het feit dat het derde land waaraan de persoonsgegevens worden doorgegeven mogelijk geen vergelijkbare bescherming biedt zoals die op grond van de PIPA, wordt in Kennisgeving nr. 2021-5, deel 2, erkend dat dergelijke nadelen kunnen ontstaan en slechts kunnen worden voorkomen wanneer de Koreaanse verwerkingsverantwoordelijke en de ontvanger in het buitenland door middel van een wettelijk bindend instrument (zoals een overeenkomst) een beschermingsniveau waarborgen dat gelijkwaardig is aan de PIPA, ook met betrekking tot de rechten van betrokkenen.

(90) Voor verstrekking voor een ander doel, dat wil zeggen het verstrekken van gegevens aan een derde voor een nieuw (ongerelateerd) doel, die alleen mag plaatsvinden op een van de in artikel 18, lid 2, PIPA genoemde gronden, gelden speciale regels, zoals beschreven in overweging 39. Zelfs onder deze omstandigheden wordt de verstrekking aan een derde echter uitgesloten wanneer deze waarschijnlijk "op oneerlijke wijze" inbreuk zou maken op de belangen van de betrokkene of een derde, wat vereist dat de belangen tegen elkaar worden afgewogen. De verwerkingsverantwoordelijke moet op grond van artikel 18, lid 5, PIPA bovendien aanvullende waarborgen toepassen, waaronder bijvoorbeeld een verzoek richten aan de derde om het doel en de methode van de verwerking te beperken of te voorzien in specifieke beveiligingsmaatregelen. Nogmaals, gezien het feit dat het derde land waaraan de persoonsgegevens worden doorgegeven mogelijk geen vergelijkbare bescherming biedt zoals die op grond van de PIPA, wordt in Kennisgeving nr. 2021-5, deel 2, erkend dat een dergelijke oneerlijke inbreuk op de belangen van de betrokkene of een derde kan ontstaan en slechts kan worden voorkomen wanneer de Koreaanse verwerkingsverantwoordelijke en de ontvanger in het buitenland door middel van een wettelijk bindend instrument (zoals een overeenkomst) een beschermingsniveau waarborgen dat gelijkwaardig is aan de PIPA, ook met betrekking tot de rechten van betrokkenen.

(91) De regels in de overwegingen 86 tot en met 90 waarborgen derhalve de continuïteit van de bescherming wanneer persoonsgegevens verder worden doorgegeven (aan een "opdrachtnemer" of derde) vanuit de Republiek Korea op een wijze die in wezen overeenkomt met die waarin is voorzien uit hoofde van Verordening (EU) 2016/679.

2.3.10. *Verantwoording*

(92) Volgens het verantwoordingsbeginsel moeten entiteiten die gegevens verwerken passende technische en organisatorische maatregelen nemen om doeltreffend hun verplichtingen inzake gegevensbescherming te kunnen naleven, en moeten zij de naleving daarvan kunnen aantonen, in het bijzonder ten overstaan van de bevoegde toezichthoudende autoriteit.

(93) Volgens artikel 3, leden 6 en 8, PIPA moet de verwerkingsverantwoordelijke persoonsgegevens verwerken op zodanige wijze dat de mogelijkheid dat inbreuk wordt gemaakt op de privacy van de betrokkene tot een minimum wordt beperkt en moet hij ernaar streven het vertrouwen van de betrokkene te verkrijgen door de taken en verantwoordelijkheden als voorzien in de PIPA en andere gerelateerde wetten na te leven en uit te voeren. Dit omvat de vaststelling van een intern beheersplan (artikel 29 PIPA) en de passende opleiding van en passend toezicht op het personeel (artikel 28 PIPA).

(94) Om de verantwoording te waarborgen is in artikel 31 PIPA juncto artikel 32 van het PIPA-uitvoeringsdecreet een verplichting voor verwerkingsverantwoordelijken vastgesteld om een privacyfunctionaris aan te wijzen die de verwerking van persoonsinformatie volledig op zich neemt. Die privacyfunctionaris heeft met name de opdracht de volgende taken uit te voeren: 1) het vaststellen en uitvoeren van een plan voor de bescherming van de persoonsgegevens en het opstellen van het privacybeleid; 2) het houden van regelmatige enquêtes over de stand van zaken en praktijken van de verwerking van persoonsgegevens, met het oog op de verbetering van eventuele tekortkomingen; 3) het afhandelen van klachten en schadevergoedingen; 4) het vaststellen van een intern controlesysteem om de verstrekking en het misbruik of oneigenlijk gebruik van persoonsgegevens te voorkomen; 5) het opstellen en uitvoeren van een opleidingsprogramma; 6) het beschermen, controleren en beheren van bestanden met persoonsgegevens, en 7) het vernietigen van persoonsgegevens zodra het doel van de verwerking is verwezenlijkt of de bewaarperiode is verstreken. Bij het uitvoeren van deze taken kan de privacyfunctionaris de stand van zaken van de verwerking van persoonsgegevens en gerelateerde systemen inspecteren en om informatie hierover verzoeken (artikel 31, lid 3, PIPA). Wanneer de privacyfunctionaris kennis neemt van een schending van de PIPA of andere relevante wetten inzake gegevensbescherming, neemt hij onmiddellijk corrigerende maatregelen en meldt hij dergelijke maatregelen, indien nodig, bij het management (het hoofd) van de verwerkingsverantwoordelijke (artikel 31, lid 4, PIPA). Overeenkomstig artikel 31, lid 5, PIPA mag de privacyfunctionaris geen ongerechtvaardigde nadelen ondervinden als gevolg van het uitvoeren van deze taken.

(95) Verwerkingsverantwoordelijken moeten er daarnaast op proactieve wijze naar streven een privacyeffectbeoordeling uit te voeren wanneer het gebruik van bestanden met persoonsgegevens een risico voor de privacy met zich meebrengt (artikel 33, lid 8, PIPA). Op basis van artikel 33, leden 1 en 2, PIPA juncto de artikelen 35, 36 en 38 van het PIPA-uitvoeringsdecreet zijn factoren zoals het soort en de aard van de verwerkte gegevens (met name de vraag of het gaat om gevoelige informatie), de omvang, de bewaarperiode en de waarschijnlijkheid van gegevenslekken relevant bij de beoordeling van de mate van het risico voor de rechten van betrokkenen. Het doel van de privacyeffectbeoordeling is ervoor te zorgen dat de risicofactoren voor de privacy en eventuele beveiligings- of andere tegenmaatregelen worden geanalyseerd en dat wordt gewezen op zaken die moeten worden verbeterd (zie artikel 33, lid 1, PIPA juncto artikel 38 van het PIPA-uitvoeringsdecreet).

(96) Overheidsinstanties zijn verplicht een effectbeoordeling uit te voeren wanneer zij bepaalde bestanden met persoonsgegevens verwerken die een groter risico op mogelijke schendingen van de privacy met zich meebrengen (artikel 33, lid 1, PIPA). Overeenkomstig artikel 35 van het PIPA-uitvoeringsdecreet is dit onder andere het geval voor bestanden die gevoelige informatie over ten minste 50 000 betrokkenen bevatten, bestanden die aan andere bestanden zullen worden gekoppeld en als gevolg daarvan de informatie van ten minste 500 000 betrokkenen zullen bevatten of bestanden die informatie bevatten van ten minste één miljoen betrokkenen. De resultaten van een effectbeoordeling door een overheidsinstantie moeten worden meegedeeld aan de PIPC (artikel 33, lid 1, PIPA), die een advies kan opstellen (artikel 33, lid 3, PIPA).

(97) Tot slot is in artikel 13 PIPA bepaald dat de PIPC beleid vaststelt dat noodzakelijk is voor de bevordering en ondersteuning van zelf-gereguleerde gegevensbeschermingsactiviteiten door verwerkingsverantwoordelijken, onder meer door middel van opleidingen over gegevensbescherming, de bevordering en ondersteuning van organisaties die zich bezighouden met gegevensbescherming en de ondersteuning van verwerkingsverantwoordelijken bij het vaststellen en uitvoeren van regels in verband met zelfregulering. Bovendien zal de PIPC het systeem ePRIVACY Mark invoeren en bevorderen. In dit opzicht voorziet artikel 32-2 PIPA juncto de artikelen 34-2 tot en met 34-8 van het PIPA-uitvoeringsdecreet in de mogelijkheid om te certificeren dat de verwerking van de persoonsgegevens en de beveiligingssystemen van verwerkingsverantwoordelijken in overeenstemming zijn met de vereisten van de PIPA. Volgens deze regels kan een certificering ([118]) worden toegekend (voor een periode van drie jaar) wanneer de verwerkingsverantwoordelijke voldoet aan de criteria voor certificering die door de PIPC zijn bepaald, waaronder de vaststelling van beheers-, technische en fysieke waarborgen ter bescherming van de persoonsgegevens ([119]). De PIPC moet de voor de certificering relevante systemen van de verwerkingsverantwoordelijke ten minste een keer per jaar onderzoeken om te beoordelen of de doeltreffendheid ervan is gehandhaafd, wat kan leiden tot de intrekking van de certificering (artikel 32, lid 4, PIPA juncto artikel 34-5 van het PIPA-uitvoeringsdecreet; het zogenaamde "follow-upbeheer").

(98) In het Koreaanse kader wordt het beginsel van verantwoording derhalve uitgevoerd op een wijze die een niveau van bescherming waarborgt dat in wezen overeenkomt met dat van Verordening (EU) 2016/679, door onder andere te voorzien in verschillende mechanismen voor het waarborgen en aantonen van de naleving van de PIPA.

2.3.11. *Speciale regels voor de verwerking van persoonlijke kredietinformatie*

(99) Zoals beschreven in overweging 13 zijn in de Wet inzake het gebruik en de bescherming van kredietinformatie (*Act on the Use and Protection of Credit Information* — CIA) specifieke regels vastgesteld voor de verwerking van persoonlijke kredietinformatie door marktdeelnemers. Bij het verwerken van persoonlijke kredietinformatie moeten marktdeelnemers derhalve de algemene vereisten van de PIPA naleven, tenzij de CIA specifiekere regels bevat. Dit zal bijvoorbeeld het geval zijn wanneer zij informatie verwerken in verband met een creditcard of bankrekening in het kader van een commerciële transactie met een natuurlijke persoon. Als sectorale wetgeving voor de verwerking van kredietinformatie (zowel persoonlijke als niet-persoonlijke informatie) worden in de CIA niet alleen specifieke waarborgen voor de gegevensbescherming opgelegd (bijvoorbeeld in termen van transparantie en beveiliging), maar worden ook de specifieke omstandigheden waarin persoonlijke kredietinformatie mag worden verwerkt meer in het algemeen geregeld. Dit komt met name tot uiting in de gedetailleerde vereisten voor het gebruik, de verstrekking van gegevens aan derden en het bewaren van dergelijke gegevens.

(100) Net zoals in de PIPA, komen in de CIA de beginselen van wettigheid en evenredigheid tot uiting. Ten eerste staat artikel 15, lid 1, CIA als algemeen vereiste de verzameling van persoonlijke kredietinformatie slechts toe als dit op redelijke en eerlijke wijze gebeurt en in een zo beperkt mogelijke mate die nodig is voor een welbepaald doel, overeenkomstig artikel 3, leden 1 en 2, PIPA. Ten tweede is in de CIA de wettigheid van de verwerking van persoonlijke kredietinformatie specifiek gereguleerd, door de verzameling, het gebruik en de verstrekking ervan aan een derde te beperken en deze verwerkingsactiviteiten over het algemeen te verbinden met het vereiste van toestemming van de betrokkene.

([118]) Daarnaast mag de verwerkingsverantwoordelijke het door de PIPC verstrekte merkteken voor de bescherming van persoonsinformatie gebruiken wanneer hij de certificering in het kader van zijn zakelijke activiteiten wil vermelden of promoten. Zie artikel 34-7 van het PIPA-uitvoeringsdecreet.

([119]) Sinds november 2018 wordt het "Personal Information & Information Security Management System" (ISMS-P — Beheerssysteem voor persoonsinformatie & informatiebeveiliging) ontwikkeld, dat certificeert dat verwerkingsverantwoordelijken een alomvattend beheerssysteem gebruiken.

(101) Persoonlijke kredietinformatie mag worden verzameld op basis van een van de gronden waarin in de PIPA is voorzien of om specifieke redenen die zijn uiteengezet in de CIA. Gezien het feit dat artikel 45 van Verordening (EU) 2016/679 een doorgifte van persoonsgegevens door een verwerkingsverantwoordelijke of verwerker in de Unie veronderstelt, maar geen betrekking heeft op de directe verzameling (van de betrokkene of van een website) door een verwerkingsverantwoordelijke in Korea, zijn slechts toestemming en de in de PIPA genoemde gronden relevant voor dit besluit. Deze gronden omvatten met name scenario's waarin de doorgifte noodzakelijk is voor het uitvoeren van een overeenkomst met de betrokkene of voor de legitieme belangen van de Koreaanse verwerkingsverantwoordelijke (artikel 15, lid 1, punten 4 en 6, PIPA) ([120]).

(102) Zodra persoonlijke kredietinformatie is verzameld, mag deze worden gebruikt 1) voor het oorspronkelijke doel waarvoor deze (direct) door de betrokkene werd verstrekt ([121]); 2) voor een doel dat verenigbaar is met het oorspronkelijke doel van de verzameling ([122]); 3) om te bepalen of een commerciële relatie kan worden aangegaan of in stand kan worden gehouden waarom de betrokkene heeft verzocht ([123]); 4) met het oog op statistieken, onderzoek en archivering in het openbaar belang ([124]) indien de informatie gepseudonimiseerd is ([125]); 5) indien verdere toestemming is verkregen of 6) in overeenstemming met de wet.

(103) Indien een marktdeelnemer persoonlijke kredietinformatie aan een derde wil verstrekken, moet hij de toestemming van de betrokkene verkrijgen ([126]) nadat hij deze heeft geïnformeerd over de ontvanger van de gegevens, het doel van de verwerking door de ontvanger, de details van de gegevens die zullen worden verstrekt, de periode van opslag door de ontvanger en het recht om de toestemming te weigeren (artikel 32, lid 1, CIA en artikel 28, lid 2, van het CIA-uitvoeringsdecreet) ([127]). Dit vereiste van toestemming is in specifieke situaties niet van toepassing, dat wil zeggen wanneer persoonlijke kredietinformatie wordt verstrekt ([128]): 1) aan een opdrachtnemer met het oog op uitbesteding ([129]); 2) aan een derde in het geval van een bedrijfsoverdracht, -splitsing of -fusie; 3) met het oog op statistieken, onderzoek en archivering in het openbaar belang wanneer de informatie gepseudonimiseerd is; 4) voor een doel dat verenigbaar is met het oorspronkelijke doel van de verzameling; 5) aan een derde die de informatie gebruikt om een schuld van de betrokkene te innen ([130]); 6) om een gerechtelijk bevel na te leven; 7) aan een aanklager/ambtenaar bij de gerechtelijke politie in een noodgeval waarin het leven van de betrokkene in

([120]) De CIA bevat ook andere rechtsgrondslagen voor de verzameling, dat wil zeggen wanneer deze bij wet vereist is, wanneer de informatie openbaar is gemaakt door een overheidsinstelling overeenkomstig de wetgeving inzake de vrijheid van informatie of wanneer de informatie beschikbaar is op een sociaal netwerk. Om de laatste reden te kunnen gebruiken, moet de marktdeelnemer aantonen dat de verzameling binnen de reikwijdte van de toestemming van de betrokkene blijft, op basis van een redelijke ("objectieve") uitlegging en rekening houdend met de aard van de gegevens, de intentie en het doel van het beschikbaar stellen ervan op het sociale netwerk en de vraag of het doel van de verzameling "zeer relevant" is voor dat doel enz. (artikel 13 van het CIA-uitvoeringsdecreet). Zoals uitgelegd in overweging 101 zijn deze redenen in beginsel echter niet relevant in het geval van een doorgifte.

([121]) Bijvoorbeeld wanneer kredietinformatie wordt gegenereerd/verzameld in het kader van een commerciële transactie met de betrokkene. Deze reden kan echter niet worden aangewend om persoonlijke kredietinformatie te gebruiken ten behoeve van direct marketing (zie artikel 33, lid 1, punt 3, CIA).

([122]) Om vast te stellen of het gebruiksdoel verenigbaar is met het oorspronkelijke doel van de verzameling, moet rekening worden gehouden met de volgende factoren: 1) het verband (de "relevantie") tussen de twee doelen; 2) de wijze waarop de informatie is verzameld; 3) de impact van het gebruik op de betrokkene, en 4) de vraag of er passende beveiligingsmaatregelen, zoals pseudonimisering, zijn genomen (vgl. artikel 32, lid 6, punt 9-4, CIA).

([123]) Een verwerkingsverantwoordelijke moet bijvoorbeeld eventueel rekening houden met persoonlijke kredietinformatie die hij van een natuurlijke persoon heeft ontvangen om te besluiten of een lening aan deze persoon kan worden verlengd.

([124]) Artikel 33 CIA, juncto artikel 32, lid 6, punten 9-2, 9-4 en 10, CIA.

([125]) Pseudonimisering wordt in artikel 2, lid 15, CIA gedefinieerd als de verwerking van persoonlijke kredietinformatie op zodanige wijze dat de betrokkenen niet langer kunnen worden geïdentificeerd op basis van de informatie, tenzij deze met aanvullende informatie wordt gecombineerd. Hoewel de CIA specifieke waarborgen bevat voor de verwerking van gepseudonimiseerde informatie met het oog op statistieken, onderzoek en archivering in het openbaar belang (artikel 40-2 CIA), zijn deze regels niet van toepassing op commerciële organisaties. Laatstgenoemden vallen in plaats daarvan onder de specifieke vereisten van deel III van de PIPA, zoals beschreven in de overwegingen 42 tot en met 48. In artikel 40-3 CIA wordt de verwerking van gepseudonimiseerde kredietinformatie — wanneer deze plaatsvindt met het oog op statistieken, wetenschappelijk onderzoek of archivering in het openbaar belang — bovendien vrijgesteld van de vereisten inzake transparantie en individuele rechten, op vergelijkbare wijze als in artikel 28-7 PIPA en onderworpen aan de waarborgen van deel III van de PIPA, zoals nader beschreven in de overwegingen 42 tot en met 48.

([126]) Dit geldt niet wanneer de informatie aan een derde wordt verstrekt met het oog op de nauwkeurigheid en bijwerking van de persoonlijke kredietinformatie, zolang de verstrekking binnen het oorspronkelijke doel van de verwerking blijft (artikel 32, lid 1, CIA). Dit kan bijvoorbeeld het geval zijn wanneer actuele informatie wordt verstrekt aan een kredietbeoordelingsbureau om ervoor te zorgen dat diens gegevens juist zijn.

([127]) Indien het praktisch gezien niet mogelijk is om de bovengenoemde informatie te verstrekken, kan het volstaan om de betrokkene voor de vereiste informatie te verwijzen naar de derde-ontvanger.

([128]) Gezien het feit dat doorgiften van persoonlijke kredietinformatie naar het buitenland niet specifiek zijn geregeld in de CIA, moeten dergelijke doorgiften in overeenstemming zijn met de waarborgen voor verdere doorgiften zoals opgelegd in deel 2 van Kennisgeving nr. 2021-5.

([129]) De verwerking van persoonlijke kredietinformatie mag alleen worden uitbesteed op basis van een schriftelijke overeenkomst en overeenkomstig de vereisten van artikel 26, leden 1, 2, 3 en 5, PIPA, zoals beschreven in overweging 20 (artikel 17 CIA en artikel 14 van het CIA-uitvoeringsdecreet). De opdrachtnemer mag de informatie niet gebruiken buiten de reikwijdte van de uitbestede taken en de uitbestedende onderneming moet voorzien in specifieke beveiligingsvereisten (bv. encryptie) en de opdrachtnemer aanleren hoe deze kan voorkomen dat de kredietinformatie verloren gaat, wordt gestolen, bekendgemaakt, gewijzigd of gecompromitteerd.

([130]) Zie ook artikel 28, lid 10, punten 1, 2 en 6, van het CIA-uitvoeringsdecreet.

gevaar is of hij/zij waarschijnlijk lichamelijk letsel zal oplopen en er geen tijd is om een gerechtelijk bevel af te geven ([131]); 8) aan bevoegde belastingautoriteiten om te voldoen aan belastingwetten, of 9) in overeenstemming met andere wetten. Wanneer informatie op deze gronden wordt verstrekt, moet de betrokkene hiervan vooraf in kennis worden gesteld (artikel 32, lid 7, CIA).

(104) In de CIA wordt ook de duur van de verwerking van persoonlijke kredietinformatie op basis van een van deze gronden voor gebruik of verstrekking aan een derde na het einde van de commerciële relatie met de betrokkene specifiek geregeld ([132]). Alleen informatie die noodzakelijk was om die relatie aan te gaan of te handhaven, mag worden bewaard, mits wordt voorzien in aanvullende waarborgen (de informatie moet gescheiden worden bewaard van kredietinformatie die verband houdt met natuurlijke personen met wie nog een commerciële relatie bestaat, zij moet worden beschermd door middel van specifieke beveiligingsmaatregelen en mag slechts toegankelijk zijn voor bevoegde personen) ([133]). Alle andere gegevens moeten worden verwijderd (artikel 17-2, lid 1, punt 2, van het CIA-uitvoeringsdecreet). Om te bepalen welke gegevens noodzakelijk waren voor de commerciële relatie, moet rekening worden gehouden met verschillende factoren, waaronder de vraag of het zonder de gegevens mogelijk was geweest om de relatie aan te gaan en of deze direct verband houden met de goederen of diensten die aan de betrokkene zijn geleverd (artikel 17-2, lid 2, van het CIA-uitvoeringsdecreet).

(105) Zelfs in gevallen waarin persoonlijke kredietinformatie in principe mag worden bewaard na het einde van de commerciële relatie, moet deze binnen drie maanden na het verwezenlijken van het verdere doel van de verwerking ([134]) of, in ieder geval, na vijf jaar worden verwijderd (artikel 20-2 CIA). In een beperkt aantal omstandigheden mag persoonlijke kredietinformatie langer dan vijf jaar worden bewaard, met name wanneer dit nodig is om een wettelijke verplichting na te komen; wanneer dit nodig is met het oog op de essentiële belangen in verband met het leven, de lichamelijke integriteit of de eigendom van een persoon; om gepseudonimiseerde informatie (die is gebruikt voor wetenschappelijk onderzoek, statistieken of archivering in het openbaar belang) te archiveren, of voor verzekeringsdoeleinden (met name voor verzekeringsbetalingen of om verzekeringsfraude te voorkomen) ([135]). In deze uitzonderlijke gevallen zijn specifieke waarborgen van toepassing (zoals de kennisgeving aan de betrokkene over het verdere gebruik, de scheiding tussen de bewaarde informatie en de informatie die verband houdt met natuurlijke personen met wie nog steeds een commerciële relatie bestaat en de beperking van de toegangsrechten, zie artikel 17-2, leden 1 en 2, van het CIA-uitvoeringsdecreet).

(106) In de CIA zijn ook de beginselen van juistheid en gegevenskwaliteit nader gespecificeerd, waarbij wordt vereist dat de persoonlijke kredietinformatie "geregistreerd, aangepast en beheerd" wordt om ervoor te zorgen dat deze juist en actueel is (artikel 18, lid 1, CIA en artikel 15, lid 3, van het CIA-uitvoeringsdecreet) ([136]). Wanneer zij kredietinformatie aan bepaalde andere entiteiten (zoals kredietbeoordelingsbureaus) verstrekken, zijn marktdeelnemers bovendien specifiek verplicht de juistheid van de informatie te verifiëren om ervoor te zorgen dat door de ontvanger slechts juiste informatie wordt geregistreerd en beheerd (artikel 15, lid 1, van het CIA-uitvoeringsdecreet juncto artikel 18, lid 1, CIA). Meer in het algemeen vereist de CIA dat een register wordt bijgehouden met informatie over de verzameling, het gebruik, de verstrekking aan derden en de vernietiging van persoonlijke kredietinformatie (artikel 20, lid 2, CIA) ([137]).

(107) Voor de verwerking van persoonlijke kredietinformatie gelden bovendien specifieke vereisten met betrekking tot de gegevensbeveiliging. De CIA vereist met name dat technologische, fysieke en organisatorische maatregelen worden uitgevoerd om de onrechtmatige toegang tot computersystemen te voorkomen, evenals de wijziging, vernietiging of andere risico's voor de verwerkte gegevens (bijvoorbeeld door middel van toegangscontroles, zie artikel 19 CIA en artikel 16 van het CIA-uitvoeringsdecreet). Daarnaast moet een overeenkomst worden gesloten waarin specifieke beveiligingsmaatregelen worden vastgesteld wanneer persoonlijke kredietinformatie wordt uitgewisseld met een derde (artikel 19, lid 2, CIA). Wanneer inbreuk op de persoonlijke kredietinformatie wordt gemaakt, moeten maatregelen worden genomen om eventuele schade tot een minimum te beperken en moeten de betrokkenen onverwijld in kennis worden gesteld (artikel 39-4, leden 1 en 2, CIA). Daarnaast moet de PIPC worden geïnformeerd over de aan natuurlijke personen verstrekte kennisgeving en de uitgevoerde maatregelen (artikel 39-4, lid 4, CIA).

([131]) In dat geval moet onverwijld worden verzocht om een bevel. Indien het bevel niet binnen 36 uur wordt uitgevaardigd, moeten de ontvangen gegevens onverwijld worden verwijderd (artikel 32, lid 6, punt 6, CIA).

([132]) Bijvoorbeeld omdat de contractuele verplichtingen zijn nagekomen, een van de partijen gebruik heeft gemaakt van haar recht op opzegging enz., zie artikel 17-2, lid 5, van het CIA-uitvoeringsdecreet.

([133]) Artikel 20-2, lid 1, CIA en artikel 17-2, lid 1, punt 1, van het CIA-uitvoeringsdecreet.

([134]) Met deze periode wordt rekening gehouden met het feit dat verwijdering vaak niet onmiddellijk mogelijk is, maar normaal gesproken bepaalde stappen vereist (bv. het scheiden van de te verwijderen gegevens van andere gegevens en het uitvoeren van de verwijdering zonder dat dit gevolgen heeft voor de stabiliteit van informatiesystemen) die enige tijd in beslag nemen.

([135]) Artikel 20-2, lid 2, CIA.

([136]) In artikel 18, lid 2, CIA en artikel 15, lid 4, van het CIA-uitvoeringsdecreet zijn specifiekere regels vastgelegd met betrekking tot dit vereiste om een register bij te houden, bv. voor registers met informatie die nadelig kan zijn voor een betrokkene, zoals informatie over criminaliteit en faillissementen.

([137]) Wat betreft de andere verantwoordingsmechanismen vereist de CIA dat bepaalde organisaties (bv. coöperatieven en overheidsbedrijven, zie artikel 21, lid 2, van het CIA-uitvoeringsdecreet) een "beheerder/hoeder van kredietinformatie" benoemen die verantwoordelijk is voor het toezicht op de naleving van de CIA en die de taken van de "privacyfunctionaris" uit hoofde van de PIPA uitvoert (artikel 20, leden 3 en 4, CIA).

(108) In de CIA worden ook specifieke transparantieverplichtingen opgelegd die moeten worden nagekomen voor het verkrijgen van toestemming voor het gebruik of de verstrekking van persoonlijke kredietinformatie (artikel 32, lid 4, en artikel 34-2 CIA en artikel 30-3 van het CIA-uitvoeringsdecreet) en, meer in het algemeen, voordat informatie aan een derde wordt verstrekt (artikel 32, lid 7, CIA) ([138]). Daarnaast hebben natuurlijke personen het recht om op verzoek informatie te krijgen over het gebruik en de verstrekking van hun kredietinformatie aan derden in de drie jaar voorafgaande aan het verzoek (met inbegrip van het doel en de data van een dergelijk gebruik/dergelijke verstrekking) ([139]).

(109) Op grond van de CIA hebben natuurlijke personen ook een recht op toegang tot hun persoonlijke kredietinformatie (artikel 38, lid 1, CIA) en op correctie van onjuiste gegevens (artikel 38, leden 2 en 3, CIA) ([140]). Bovendien voorziet de CIA naast het algemene recht op wissing op grond van de PIPA (zie overweging 77), in een specifiek recht op het wissen van persoonlijke kredietinformatie die langer is bewaard dan de in overweging 104 genoemde bewaarperiode, dat wil zeggen vijf jaar (voor persoonlijke kredietinformatie die moest worden bewaard om een commerciële relatie aan te gaan of in stand te houden) of drie maanden (voor andere soorten persoonlijke kredietinformatie) ([141]). Een verzoek om wissing kan bij wijze van uitzondering worden geweigerd wanneer verdere bewaring noodzakelijk is in de omstandigheden zoals beschreven in overweging 105. Indien een betrokkene verzoekt om wissing, maar een van de uitzonderingen van toepassing is, moeten specifieke waarborgen worden toegepast op de desbetreffende kredietinformatie (artikel 38-3, lid 3, CIA en artikel 33-3 van het CIA-uitvoeringsdecreet). De informatie moet bijvoorbeeld gescheiden van andere informatie worden bewaard, mag slechts worden ingezien door een bevoegde persoon en moet worden onderworpen aan specifieke beveiligingsmaatregelen.

(110) Naast de in overweging 109 genoemde rechten waarborgt de CIA het recht van natuurlijke personen om een verwerkingsverantwoordelijke te verzoeken geen contact meer met hen op te nemen met het oog op direct marketing (artikel 37, lid 2, van de wet) en het recht op gegevensoverdraagbaarheid. Wat het laatste recht betreft, staat de CIA natuurlijke personen toe te verzoeken om de overdracht van hun persoonlijke kredietinformatie aan henzelf of bepaalde derden (zoals financiële instellingen en kredietbeoordelingsbureaus). De persoonlijke kredietinformatie moet worden verwerkt en overgedragen aan de derde in een formaat dat kan worden verwerkt door een apparaat voor informatieverwerking (zoals een computer).

(111) Voor zover de CIA specifieke regels bevat ten opzichte van de PIPA is de Commissie derhalve van mening dat ook deze regels een niveau van bescherming waarborgen dat in wezen overeenkomt met dat van Verordening (EU) 2016/679.

2.4. **Toezicht en handhaving**

(112) Om ervoor te zorgen dat in de praktijk een passend niveau van bescherming van persoonsgegevens wordt gewaarborgd, moet er worden voorzien in een onafhankelijke toezichthoudende autoriteit met bevoegdheden tot monitoring en handhaving van de naleving van de gegevensbeschermingsvoorschriften. Deze autoriteit moet bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden volledig onafhankelijk en onpartijdig handelen.

2.4.1. *Onafhankelijk toezicht*

(113) In de Republiek Korea is de PIPC de onafhankelijke autoriteit die belast is met de monitoring en handhaving van de PIPA. De PIPC bestaat uit een voorzitter, een vicevoorzitter en zeven commissarissen. De voorzitter en vicevoorzitter worden benoemd door de president, op aanbeveling van de premier. Van de commissarissen worden er twee benoemd door de president op aanbeveling van de voorzitter en vijf op aanbeveling van de Nationale Vergadering (waarvan twee op aanbeveling van de politieke partij waartoe de president behoort en drie

([138]) Dit omvat een algemeen vereiste van kennisgeving (artikel 32, lid 7, CIA) en een specifieke transparantieverplichting wanneer informatie aan de hand waarvan de kredietwaardigheid van een natuurlijke persoon kan worden bepaald, wordt verstrekt aan bepaalde entiteiten, zoals kredietbeoordelingsbureaus en agentschappen die kredietinformatie verzamelen (artikel 35-3 CIA en artikel 30-3 van het CIA-uitvoeringsdecreet) of wanneer een commerciële transactie wordt geweigerd of beëindigd op basis van de van een derde ontvangen persoonlijke kredietinformatie (artikel 36 CIA en artikel 31 van het CIA-uitvoeringsdecreet).

([139]) Artikel 35, CIA. Bepaalde commerciële organisaties, bv. coöperatieven en overheidsbedrijven (artikel 21, lid 2, van het CIA-uitvoeringsdecreet) moeten voldoen aan aanvullende transparantievereisten, bv. om bepaalde informatie openbaar beschikbaar te stellen (artikel 31 CIA) en om betrokkenen te informeren over mogelijke nadelen voor hun kredietscore wanneer zij financiële transacties aangaan die een kredietrisico met zich meebrengen (artikel 35-2 CIA).

([140]) Wat betreft de voorwaarden voor en uitzonderingen op de rechten op toegang en correctie zijn de regels van de PIPA (zoals beschreven in de overwegingen 76 en 77) van toepassing. Daarnaast zijn verdere modaliteiten vastgelegd in artikel 38, leden 4 tot en met 8, CIA en artikel 33 van het CIA-uitvoeringsdecreet. Meer bepaald moet een marktdeelnemer die onjuiste kredietinformatie heeft gecorrigeerd of verwijderd de betrokkene hiervan in kennis stellen. Daarnaast moeten eventuele derden aan wie deze informatie binnen de zes hieraan voorafgaande maanden is verstrekt, in kennis worden gesteld en moet de betrokkene daarover worden geïnformeerd. Indien een betrokkene niet tevreden is met de manier waarop een verzoek om correctie is afgehandeld, kan hij of zij een verzoek indienen bij de PIPC, die de acties van de verwerkingsverantwoordelijke verifieert en corrigerende maatregelen kan opleggen.

([141]) Artikel 38-3 CIA.

op aanbeveling van andere politieke partijen (artikel 7-2, lid 2, PIPA), hetgeen bijdraagt tot het tegengaan van partijdigheid in het benoemingsproces) ([142]). Deze procedure is in overeenstemming met de vereisten voor de benoeming van leden van gegevensbeschermingsautoriteiten in de Unie (artikel 53, lid 1, van Verordening (EU) 2016/679). Bovendien moeten alle commissarissen afzien van zakelijke activiteiten met een winstoogmerk, politieke activiteiten en functies bij de overheid of de Nationale Vergadering (artikel 7-6 en artikel 7-7, lid 1, punt 3, PIPA) ([143]). Alle commissarissen zijn onderworpen aan specifieke voorschriften waardoor zij niet kunnen deelnemen aan overleg in geval van mogelijke belangenconflicten (artikel 7-11 PIPA). De PIPC wordt ondersteund door een secretariaat (artikel 7-13) en kan subcommissies oprichten (bestaande uit drie commissarissen) om minder ernstige schendingen en terugkerende zaken te behandelen (artikel 7-12 PIPA).

(114) Elk lid van de PIPC wordt voor een periode van drie jaar benoemd en kan één keer worden herbenoemd (artikel 7-4, lid 1, PIPA). Commissarissen mogen slechts onder specifieke omstandigheden uit hun functie worden ontheven, namelijk wanneer zij niet langer in staat zijn hun taken te vervullen als gevolg van een langdurige geestelijke of fysieke handicap, wanneer zij handelen in strijd met de wet of voldoen aan een van de gronden voor ontzegging van het mandaat ([144]) (artikel 7-5 PIPA). Dit biedt hun institutionele bescherming bij de uitoefening van hun taken.

(115) Meer in het algemeen waarborgt artikel 7, lid 1, PIPA de onafhankelijkheid van de PIPC uitdrukkelijk en vereist artikel 7-5, lid 2, PIPA dat commissarissen hun taken op onafhankelijke wijze uitoefenen, in overeenstemming met de wet en hun geweten ([145]). De beschreven institutionele en procedurele waarborgen, onder meer die in verband met de benoeming en het ontslag van haar leden, waarborgen dat de PIPC volledig onafhankelijk handelt, zonder externe invloeden of instructies. Bovendien stelt de PIPC als centraal administratief agentschap jaarlijks een eigen begroting voor (die door het Ministerie van Financiën wordt gecontroleerd als onderdeel van de totale nationale begroting vóór goedkeuring door de Nationale Vergadering) en is de PIPC belast met het eigen personeelsbeheer. De PIPC heeft een huidige begroting van ongeveer 35 miljoen euro en telt 154 personeelsleden (waaronder 40 werknemers die gespecialiseerd zijn in informatie- en communicatietechnologie, 32 werknemers die zich bezighouden met onderzoeken en 40 juridische deskundigen).

(116) De taken en bevoegdheden van de PIPC zijn voornamelijk opgenomen in de artikelen 7-8 en 7-9 en in de artikelen 61 tot en met 66 PIPA ([146]). De taken van de PIPC omvatten met name het geven van advies over wet- en regelgeving in verband met de gegevensbescherming, het ontwikkelen van gegevensbeschermingsbeleid en -richtsnoeren, het onderzoeken van inbreuken op individuele rechten, het afhandelen van klachten en bemiddelen in geschillen, het handhaven van de naleving van de PIPA, het waarborgen van opleiding en bevordering op het gebied van gegevensbescherming en het onderhouden van contacten en het samenwerken met gegevensbeschermingsautoriteiten in derde landen ([147]).

(117) Op basis van artikel 68 PIPA juncto artikel 62 van het PIPA-uitvoeringsdecreet zijn bepaalde taken van de PIPC gedelegeerd aan het Koreaans Agentschap voor internet en veiligheid, namelijk: 1) onderwijs en voorlichting, 2) opleiding van deskundigen en ontwikkeling van criteria voor privacyeffectbeoordelingen, 3) de afhandeling van verzoeken om aanwijzing van een zogenaamde instelling voor de privacyeffectbeoordeling, 4) de afhandeling van verzoeken om indirecte toegang tot persoonsgegevens die in het bezit zijn van overheidsinstanties (artikel 35, lid 2, PIPA) en 5) het verzoeken om materiaal en uitvoeren van inspecties met betrekking tot klachten die zijn

([142]) Alleen personen die aan de volgende criteria voldoen, kunnen als PIPC-commissaris worden benoemd: hoge ambtenaren die verantwoordelijk zijn voor aangelegenheden in verband met de persoonsinformatie; voormalige rechters, openbaar aanklagers of advocaten met ten minste tien jaar werkervaring; voormalige managers met ervaring op het gebied van gegevensbescherming die langer dan drie jaar werkzaam zijn geweest bij een overheidsinstantie of -organisatie of die door een dergelijke instantie of organisatie zijn aanbevolen, en voormalig hoofddocenten met deskundigheid op het gebied van gegevensbescherming die ten minste vijf jaar in een academische instelling hebben gewerkt (artikel 7-2 PIPA).

([143]) Zie ook artikel 4-2 van het PIPA-uitvoeringsdecreet.

([144]) Zie artikel 7-7 PIPA, waarin is bepaald dat niet-Koreaanse onderdanen en leden van politieke partijen geen lid van de PIPC kunnen worden. Hetzelfde geldt voor personen aan wie bepaalde soorten strafrechtelijke sancties zijn opgelegd, die in de laatste vijf jaar uit hun functie zijn ontheven in het kader van disciplinaire maatregelen enz. (artikel 7-7 PIPA juncto artikel 33 van de Ambtenarenwet).

([145]) Terwijl in artikel 7, lid 2, PIPA wordt verwezen naar de algemene bevoegdheid van de premier op grond van artikel 18 van de Wet op de overheidsorganisatie om — met goedkeuring van de president — onrechtmatige of onrechtvaardige beschikkingen van een centrale bestuursinstantie op te schorten of in te trekken, is een dergelijke bevoegdheid niet toegekend in verband met de onderzoeks- en handhavingsbevoegdheden van de PIPC (zie artikel 7, lid 2, punten 1 en 2, PIPA). Volgens toelichting van de Koreaanse regering is artikel 18 van de Wet op de overheidsorganisatie bedoeld om de premier de mogelijkheid te bieden om te handelen in buitengewone omstandigheden, bijvoorbeeld om te bemiddelen bij een geschil tussen verschillende overheidsagentschappen. De premier heeft echter nog nooit gebruikgemaakt van deze bevoegdheid sinds deze bepaling in 1963 werd goedgekeurd.

([146]) Indien nodig voor de uitvoering van de taken overeenkomstig artikel 7-9, lid 1, PIPA mag de PIPC het advies van relevante ambtenaren, deskundigen op het gebied van gegevensbescherming, maatschappelijke organisaties en relevante bedrijfsexploitanten vragen. De PIPC mag daarnaast verzoeken om relevant materiaal en kan aanbevelingen voor verbetering doen en controleren of deze worden uitgevoerd (artikel 7-9, leden 2 tot en met 5, PIPA).

([147]) Zie ook artikel 9 PIPA (driejaarlijks masterplan voor de bescherming van persoonsinformatie), artikel 12 PIPA (standaardrichtsnoeren voor de bescherming van persoonsinformatie) en artikel 13 PIPA (beleid voor de bevordering en ondersteuning van zelfregulering).

ontvangen via het zogenaamde Privacy Call Centre. In het kader van de afhandeling van klachten door het Privacy Call Centre stuurt het Koreaans Agentschap voor internet en veiligheid de zaak door naar de PIPC of het Openbaar Ministerie wanneer het vaststelt dat een wet is geschonden. De mogelijkheid om een klacht in te dienen bij het Privacy Call Centre belet betrokkenen niet direct een klacht in te dienen bij de PIPC of zich tot de PIPC te wenden wanneer zij van mening zijn dat het Koreaans Agentschap voor internet en veiligheid hun klacht niet naar tevredenheid heeft behandeld.

2.4.2. *Handhaving, met inbegrip van sancties*

(118) Om de naleving van de PIPA te waarborgen, heeft de wetgever de PIPC zowel onderzoeks- als handhavingsbevoegdheden gegeven, die uiteenlopen van aanbevelingen tot administratieve boetes. Deze bevoegdheden worden verder aangevuld door een stelsel van strafrechtelijke sancties.

(119) Wat de onderzoeksbevoegdheden betreft, kan de PIPC inspecties ter plaatse uitvoeren en verantwoordelijken voor de verwerking van persoonsgegevens verzoeken om al het relevante materiaal (zoals voorwerpen en documenten) wanneer zij vermoedt dat er sprake is van een schending van de PIPA of wanneer er een schending is gemeld of wanneer dit nodig is voor de bescherming van de rechten van betrokkenen tegen inbreuken (artikel 63 PIPA juncto artikel 60 van het PIPA-uitvoeringsdecreet) ([148]).

(120) Wat de handhaving betreft, kan de PIPC op grond van artikel 61, lid 2, PIPA advies verlenen aan verwerkingsverantwoordelijken over manieren om het beschermingsniveau van de persoonsgegevens tijdens specifieke verwerkingsactiviteiten te verbeteren. Verwerkingsverantwoordelijken moeten te goeder trouw inspanningen leveren om dat advies uit te voeren en zij moeten de PIPC informeren over het resultaat hiervan. Wanneer er redelijke gronden zijn om aan te nemen dat een schending van de PIPA heeft plaatsgevonden en niet handelen waarschijnlijk zal leiden tot schade die moeilijk kan worden hersteld, kan de PIPC bovendien corrigerende maatregelen opleggen (artikel 61, lid 1, PIPA) ([149]). In deel 5 van Kennisgeving nr. 2021-5 (bijlage I) wordt op bindende wijze verduidelijkt dat aan deze voorwaarden wordt voldaan in verband met de schending van bepalingen van de PIPA die de privacyrechten van betrokkenen beschermen met betrekking tot de persoonsinformatie ([150]). De maatregelen die de PIPC kan nemen, omvatten het gelasten van de stopzetting van het gedrag dat de schending veroorzaakt, de tijdelijke opschorting van de gegevensverwerking of andere noodzakelijke maatregelen. Het niet naleven van een corrigerende maatregel kan leiden tot een sanctie in de vorm van een boete van maximaal 50 miljoen KRW (artikel 75, lid 2, punt 13, PIPA).

(121) Met betrekking tot bepaalde overheidsinstanties (zoals de Nationale Vergadering, centrale bestuursinstanties, lokale overheden en de rechtbanken) is in artikel 64, lid 4, PIPA bepaald dat de PIPC de in overweging 120 genoemde corrigerende maatregelen kan aanbevelen en dat deze instanties die aanbeveling moeten naleven, tenzij er sprake is van buitengewone omstandigheden. Volgens deel 5 van Kennisgeving nr. 2021-5 wordt hiermee verwezen naar buitengewone feitelijke of juridische omstandigheden waarvan de PIPC niet op de hoogte was toen zij haar aanbeveling deed. De betrokken overheidsinstantie mag zich slechts beroepen op dergelijke buitengewone omstandigheden wanneer zij duidelijk aantoont dat er geen inbreuk heeft plaatsgevonden en de PIPC vaststelt dat dit inderdaad niet het geval is. Wanneer er wel een inbreuk heeft plaatsgevonden, moet de overheidsinstantie de aanbeveling van de PIPC volgen en is zij verplicht om corrigerende maatregelen te nemen om de actie onmiddellijk te stoppen en de schade te vergoeden in het uitzonderlijke geval waarin desondanks een illegale handeling werd verricht.

(122) De PIPC kan ook andere bestuursinstanties met een specifieke bevoegdheid uit hoofde van sectorale wetgeving (bv. gezondheidszorg, onderwijs) verzoeken om – alleen of samen met de PIPC – een onderzoek uit te voeren naar (vermoede) privacyschendingen door verwerkingsverantwoordelijken die actief zijn in de desbetreffende, onder hun jurisdictie vallende sectoren, en om corrigerende maatregelen op te leggen (artikel 63, leden 4 en 5, PIPA). In dat geval bepaalt de PIPC de gronden, het voorwerp en de reikwijdte van het onderzoek ([151]). De betrokken bestuursinstantie moet op haar beurt een inspectieplan indienen bij de PIPC en de PIPC in kennis stellen van het resultaat van de inspectie. De PIPC kan een specifieke corrigerende maatregel aanbevelen, die het betrokken agentschap moet trachten uit te voeren. Een dergelijk verzoek beperkt in ieder geval de bevoegdheid van de PIPC om haar eigen onderzoek te verrichten of sancties op te leggen niet.

([148]) De PIPC mag bovendien het terrein van de verwerkingsverantwoordelijke betreden om de status van de zakelijke activiteiten, registers, documenten enz. te controleren (artikel 63, lid 2, PIPA). Zie ook artikel 45-3 CIA en artikel 36-4 van het CIA-uitvoeringsdecreet met betrekking tot de bevoegdheden van de PIPC op grond van die wet.

([149]) Zie ook artikel 45-4 CIA met betrekking tot de bevoegdheden van de PIPC uit hoofde van de CIA.

([150]) In deel 5 van de kennisgeving is bepaald dat zwaarwegende gronden om aan te nemen dat een inbreuk in verband met persoonsinformatie heeft plaatsgevonden en niet handelen waarschijnlijk zal leiden tot schade die moeilijk kan worden hersteld in de zin van artikel 64, leden 1 en 2, PIPA, verwijst naar een schending van de beginselen, rechten en plichten die in de wet zijn opgenomen om de rechten van natuurlijke personen in verband met persoonsinformatie te beschermen. Hetzelfde geldt voor de bevoegdheden van de PIPC uit hoofde van artikel 45-4 CIA.

([151]) Artikel 60 van het PIPA-uitvoeringsdecreet.

(123) Naast zijn corrigerende bevoegdheden kan de PIPC administratieve boetes van 10 tot 50 miljoen KRW opleggen voor inbreuken op diverse vereisten van de PIPA (artikel 75 PIPA) ([152]). Dit omvat onder meer het niet naleven van de vereisten van de wettigheid van de verwerking, het niet nemen van de noodzakelijke beveiligingsmaatregelen, het niet in kennis stellen van betrokkenen in het geval van een gegevenslek, het niet naleven van de vereisten voor subverwerking, het niet vaststellen en bekendmaken van een privacybeleid, het niet aanwijzen van een privacyfunctionaris of het niet handelen op verzoek van de betrokkene in het kader van de uitoefening van diens individuele rechten, evenals bepaalde procedurele inbreuken (niet samenwerken tijdens een onderzoek). In geval van inbreuken op verschillende bepalingen van de PIPA door dezelfde verwerkingsverantwoordelijke kan voor elke inbreuk een boete worden opgelegd en zal bij de vaststelling van de hoogte van de boete rekening worden gehouden met het aantal getroffen personen.

(124) De PIPC kan bovendien een strafrechtelijke klacht indienen bij de bevoegde onderzoeksinstantie (zoals een aanklager, zie artikel 65, lid 1, PIPA) wanneer er redelijke gronden zijn om te vermoeden dat inbreuk is gepleegd op de PIPA of andere wetten in verband met de gegevensbescherming. De PIPC kan de verwerkingsverantwoordelijke bovendien adviseren disciplinaire maatregelen te nemen tegen de verantwoordelijke persoon (waaronder de verantwoordelijke manager, zie artikel 65, lid 2, PIPA). Wanneer de verwerkingsverantwoordelijke een dergelijk advies ontvangt, moet hij dit naleven ([153]) en de PIPC schriftelijk in kennis stellen van het resultaat (artikel 65 PIPA juncto artikel 58 van het PIPA-uitvoeringsdecreet).

(125) Ten aanzien van advies overeenkomstig artikel 61, corrigerende maatregelen overeenkomstig artikel 64, een beschuldiging of advies tot het nemen van disciplinaire maatregelen overeenkomstig artikel 65 en het opleggen van administratieve boetes overeenkomstig artikel 75 PIPA, kan de PIPC de feiten — dat wil zeggen de inbreuk, de entiteit die inbreuk op de wet heeft gemaakt en de opgelegde maatregel(en) — bekendmaken door deze op haar website of in een algemeen, nationaal dagblad te publiceren (artikel 66 PIPA juncto artikel 61, lid 1, van het PIPA-uitvoeringsdecreet) ([154]).

(126) Tot slot wordt de naleving van de gegevensbeschermingsvereisten van de PIPA (en van andere wetten in verband met de gegevensbescherming) ondersteund door een stelsel van strafrechtelijke sancties. In dit verband bevatten de artikelen 70 tot en met 73 PIPA sanctiebepalingen die kunnen leiden tot het opleggen van een boete (van 20 tot 100 miljoen KRW) of een gevangenisstraf (met een maximumstraf van 2 tot 10 jaar). Relevante inbreuken zijn onder meer het gebruik van persoonsgegevens of het verstrekken van dergelijke gegevens aan een derde zonder de noodzakelijke toestemming, de verwerking van gevoelige informatie in strijd met het verbod van artikel 23, lid 1, PIPA, de niet-naleving van de toepasselijke veiligheidsvereisten met als gevolg het verlies, de diefstal, de onthulling, de vervalsing, de wijziging of de beschadiging van persoonsgegevens, het niet nemen van de noodzakelijke maatregelen om persoonsgegevens te corrigeren, te wissen of op te schorten of de onrechtmatige doorgifte van persoonsgegevens aan een derde land ([155]). Op grond van artikel 74 PIPA zijn in elk van deze gevallen de werknemer, de vertegenwoordiger van de verwerkingsverantwoordelijke en de verwerkingsverantwoordelijke zelf aansprakelijk ([156]).

(127) Naast de strafrechtelijke sancties waarin is voorzien in de PIPA kan het misbruik van persoonsgegevens ook een strafbaar feit in de zin van het wetboek van strafrecht zijn. Dit is met name het geval met betrekking tot de schending van het briefgeheim, geheime documenten of elektronische registers (artikel 316), het verstrekken van informatie die valt onder het beroepsgeheim (artikel 317), fraude met gebruik van computers (artikel 347-2) en verduistering en vertrouwensbreuken (artikel 355).

(128) Het Koreaanse systeem combineert dus verschillende soorten sancties, van corrigerende maatregelen en administratieve boetes tot strafrechtelijke sancties, die waarschijnlijk een bijzonder sterk afschrikkend effect zullen hebben op verwerkingsverantwoordelijken en de personen die de gegevens behandelen. De PIPC begon na haar oprichting in 2020 meteen gebruik te maken van haar bevoegdheden. Uit het jaarverslag 2021 van de

([152]) Indien systemen voor de verwerking en bescherming van persoonsinformatie die door een verwerkingsverantwoordelijke worden gebruikt, zijn gecertificeerd als zijnde in overeenstemming met de PIPA, maar in feite niet is voldaan aan de certificeringscriteria overeenkomstig artikel 34-2, lid 1, van het PIPA-uitvoeringsdecreet of wanneer er sprake is van een ernstige inbreuk op een wet in verband met de bescherming van de persoonsinformatie, kan de PIPC de certificering intrekken (artikel 32-2, leden 3 en 5, PIPA). De PIPC stelt de verwerkingsverantwoordelijke op de hoogte van die intrekking en kondigt deze publiekelijk aan of maakt deze bekend op haar website of in het staatsblad (artikel 34-4 van het PIPA-uitvoeringsdecreet). Voor schendingen van de CIA is ook voorzien in administratieve boetes (artikel 52 CIA) en strafrechtelijke sancties (artikel 50 CIA).

([153]) Overeenkomstig artikel 58, lid 2, van het PIPA-uitvoeringsdecreet moet de verwerkingsverantwoordelijke de PIPC voorzien van een met redenen omklede rechtvaardiging wanneer bijzondere omstandigheden ertoe leiden dat de naleving van het advies in de praktijk onuitvoerbaar is.

([154]) Bij het besluiten of zij dergelijke informatie openbaar maakt, houdt de PIPC rekening met de inhoud en de ernst van de schending, de duur en frequentie ervan en de gevolgen ervan (omvang van de schade). De betrokken entiteit wordt vooraf in kennis gesteld en krijgt de mogelijkheid zich te verdedigen. Zie artikel 61, leden 2 en 3, van het PIPA-uitvoeringsdecreet.

([155]) Zie artikel 71, punt 2, juncto artikel 18, lid 1, PIPA (niet-naleving van de voorwaarden van artikel 17, lid 3, PIPA, waarnaar wordt verwezen in artikel 18, lid 1). Zie ook artikel 75, lid 2, punt 1 juncto artikel 17, lid 2, PIPA (niet verstrekken van noodzakelijke informatie aan de betrokkene overeenkomstig artikel 17, lid 2, PIPA, waarnaar wordt verwezen in artikel 17, lid 3).

([156]) Artikel 74-2 PIPA staat bovendien de inbeslagname toe van geld, goederen of andere opbrengsten als gevolg van de schending of, wanneer de inbeslagname niet mogelijk is, de inning van de onrechtmatig verkregen voordelen.

PIPC blijkt dat de PIPC reeds een aantal aanbevelingen en corrigerende bevelen heeft doen uitgaan en administratieve boetes heeft opgelegd, zowel jegens de overheidssector (ongeveer 34 overheidsinstanties) als tegen particuliere marktdeelnemers (ongeveer 140 bedrijven) ([157]). Twee bekende zaken in dit verband waren bijvoorbeeld een zaak in december 2020 waarin zij een boete van 6,7 miljard KRW oplegde aan een bedrijf vanwege de schending van verschillende bepalingen van de PIPA (waaronder beveiligingsvereisten, toestemmingsvereisten voor de verstrekking aan een derde en de transparantie) ([158]) en een zaak in april 2020 waarin zij een boete van 103,3 miljoen KRW oplegde aan een bedrijf voor AI-technologie wegens schending van onder meer de regels inzake de rechtmatigheid van de verwerking, en met name de toestemming, en de verwerking van gepseudonimiseerde informatie ([159]). In augustus 2021 heeft de PIPC een ander onderzoek afgerond naar de activiteiten van drie ondernemingen dat heeft geleid tot corrigerende maatregelen en het opleggen van boetes ten belope van 6,47 miljard KWR (onder meer omdat de ondernemingen personen niet in kennis hebben gesteld van de openbaarmaking van hun persoonsgegevens aan derden, waarbij ook sprake was van doorgiften aan derde landen) ([160]). Zuid-Korea had bovendien vóór de recente hervorming reeds een goede staat van dienst wat betreft de handhaving, waarbij de verantwoordelijke autoriteiten gebruikmaakten van het volledige scala aan handhavingsmaatregelen, waaronder administratieve boetes, corrigerende maatregelen en het publiekelijk aan de kaak stellen van verschillende verwerkingsverantwoordelijken, waaronder aanbieders van communicatiediensten (Koreaanse Communicatiecommissie) en marktdeelnemers, financiële instellingen, overheidsinstanties, universiteiten en ziekenhuizen (ministerie van Binnenlandse Zaken en Veiligheid) ([161]). Op basis hiervan concludeert de Commissie dat het Koreaanse systeem de doeltreffende handhaving van de gegevensbeschermingsvoorschriften in de praktijk waarborgt en daarmee een beschermingsniveau garandeert dat in wezen overeenkomt met dat van Verordening (EU) 2016/679.

2.5. **Verhaalsmogelijkheden**

(129) Om een passende bescherming en vooral de handhaving van individuele rechten te waarborgen, moeten aan de betrokkene doeltreffende administratieve en gerechtelijke verhaalsmogelijkheden worden verstrekt, met inbegrip van een recht op schadeloosstelling.

(130) Het Koreaanse systeem voorziet in verschillende mechanismen voor natuurlijke personen om hun rechten doeltreffend uit te oefenen en (gerechtelijk) verhaal te halen.

(131) Allereerst kunnen personen die menen dat hun gegevensbeschermingsrechten of -belangen zijn geschonden, zich wenden tot de betreffende verwerkingsverantwoordelijke. Overeenkomstig artikel 30, lid 1, punt 5, PIPA, omvat het privacybeleid van de verwerkingsverantwoordelijke onder meer informatie over de rechten van betrokkenen en hoe deze kunnen worden uitgeoefend. Daarnaast bevat het contactgegevens, zoals de naam en het telefoonnummer van de privacyfunctionaris of de voor de gegevensbescherming verantwoordelijke afdeling, voor het indienen van eventuele klachten ("grieven"). Binnen de organisatie van de verwerkingsverantwoordelijke is de privacyfunctionaris belast met de behandeling van klachten, het nemen van corrigerende maatregelen in geval van een inbreuk op de persoonlijke levenssfeer, en schadeloosstelling (artikel 31, lid 2, punt 3, en lid 4, PIPA). Deze laatste is bijvoorbeeld van belang wanneer de verwerkingsverantwoordelijke in geval van een gegevenslek de betrokkene het/de contactpunt(en) moet meedelen zodat deze, onder meer, eventuele schade kan melden (artikel 34, lid 1, punt 5, PIPA).

(132) Daarnaast biedt de PIPA verschillende verhaalsmogelijkheden aan betrokkenen ten aanzien van de verwerkingsverantwoordelijken. Ten eerste kan iedere persoon die meent dat zijn of haar gegevensbeschermingsrechten of -belangen door de verwerkingsverantwoordelijke zijn geschonden deze inbreuk rechtstreeks melden aan de PIPC en/of aan een van de door de PIPC aangewezen gespecialiseerde instellingen voor de ontvangst en behandeling van klachten; hiertoe behoort het Koreaans Agentschap voor internet en veiligheid, dat hiervoor een callcenter voor persoonsinformatie gebruikt (het zogenaamde "Privacy Call Centre") (artikel 62, leden 1 en 2, PIPA, juncto artikel 59 van het PIPA-uitvoeringsdecreet). Het Privacy Call Centre onderzoekt en stelt inbreuken vast, geeft advies in verband met de verwerking van persoonsgegevens (artikel 62, lid 3, PIPA) en kan inbreuken melden aan

([157]) Zie het jaarverslag 2021 van de PIPC 2021, blz. 50-55 (alleen beschikbaar in het Koreaans), op https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Zie https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK (alleen beschikbaar in het Koreaans).

([159]) Zie https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8 (alleen beschikbaar in het Koreaans).

([160]) Zie (alleen beschikbaar in het Koreaans): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Zie bv. het jaarverslag 2020 op https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 (alleen beschikbaar in het Koreaans) en de voorbeelden in het Engels op https://www.privacy.go.kr/eng/enforcement_02.do.

de PIPC (maar kan zelf geen handhavingsmaatregelen nemen). Het Privacy Call Centre ontvangt een groot aantal klachten/verzoeken (bv. 177 457 in 2020, 159 255 in 2019 en 164 497 in 2018) ([162]). Volgens informatie van de PIPC ontving het PIPC zelf tussen augustus 2020 en augustus 2021 ongeveer 1 000 klachten. Naar aanleiding van een klacht kan de PIPC komen met een advies voor verbeteringen, corrigerende maatregelen, een "inbeschuldigingstelling" bij de bevoegde onderzoeksinstantie (met inbegrip van een openbaar aanklager) of een advies voor tuchtmaatregelen (zie de artikelen 61, 64 en 65 PIPA). Beslissingen van de PIPC (zoals een weigering om een klacht te behandelen of een inhoudelijke afwijzing van een klacht) kunnen worden aangevochten op grond van de Wet administratieve procesvoering ([163]).

(133) Ten tweede kunnen betrokkenen volgens de artikelen 40 tot en met 50, PIPA, juncto de artikelen 48-14 tot en met 57 van het PIPA-uitvoeringsdecreet, vorderingen voorleggen aan een zogenaamd "Comité voor geschillenbeslechting", dat is samengesteld uit vertegenwoordigers die door de voorzitter van de PIPC zijn benoemd uit leden van de hoogste uitvoerende dienst van de PIPC, en uit personen die op grond van hun ervaring op het gebied van gegevensbescherming zijn benoemd uit bepaalde in aanmerking komende groepen (zie artikel 40, leden 2, 3 en 7, PIPA en artikel 48-14 van het PIPA-uitvoeringsdecreet) ([164]). De mogelijkheid om gebruik te maken van bemiddeling voor het Comité voor geschillenbeslechting biedt een alternatieve mogelijkheid om verhaal te halen, maar beperkt niet het recht van de persoon om zich in plaats daarvan tot de PIPC of de rechter te wenden. Om de zaak te onderzoeken, kan het Comité de partijen bij het geschil verzoeken het nodige materiaal te verstrekken en/of relevante getuigen op te roepen om voor het Comité te verschijnen (artikel 45 PIPA). Zodra de zaak is opgehelderd, stelt het Comité een ontwerp van een bemiddelingsbesluit ([165]) op waarover een meerderheid van zijn leden het eens moet zijn. Het ontwerp van bemiddeling kan opschorting van de inbreuk, de noodzakelijke rechtsmiddelen (met inbegrip van restitutie of schadeloosstelling) omvatten, alsmede alle maatregelen die nodig zijn om herhaling van dezelfde of soortgelijke inbreuk(en) te voorkomen (artikel 47, lid 1, PIPA). Wanneer beide partijen met het bemiddelingsbesluit instemmen, heeft dit dezelfde werking als een schikking voor de rechtbank (artikel 47, lid 5, PIPA). Beide partijen kunnen een gerechtelijke procedure inleiden tijdens de bemiddelingsprocedure, in welk geval deze laatste wordt opgeschort (zie artikel 48, lid 2, PIPA) ([166]). Uit de jaarlijkse cijfers van de PIPC blijkt dat personen regelmatig gebruikmaken van de procedure voor het Comité voor geschillenbeslechting, wat vaak tot een succesvol resultaat leidt. Zo heeft het Comité in 2020 126 zaken behandeld, waarvan er 89 bij het Comité werden opgelost (in 77 zaken kwamen de partijen reeds vóór het einde van de bemiddelingsprocedure tot overeenstemming en in 12 zaken werd het bemiddelingsvoorstel door de partijen aanvaard), wat resulteerde in een bemiddelingspercentage van 70,6 % ([167]). In 2019 behandelde het Comité 139 zaken, waarvan er 92 werden opgelost, wat leidde tot een bemiddelingspercentage van 62,2 %.

(134) Wanneer ten minste vijftig personen schade hebben geleden of hun rechten op gegevensbescherming op dezelfde of soortgelijke wijze zijn geschonden ten gevolge van hetzelfde (soort) incident ([168]), kan een betrokkene of een organisatie voor gegevensbescherming bovendien om collectieve geschillenbemiddeling verzoeken namens een dergelijke collectiviteit; andere betrokkenen kunnen verzoeken om deel te nemen aan deze bemiddeling, die door het Comité voor geschillenbeslechting openbaar wordt aangekondigd (artikel 49, leden 1, 2 en 3, PIPA, juncto de artikelen 52, 53 en 54 van het PIPA-uitvoeringsdecreet) ([169]). Het Comité voor geschillenbeslechting kan minstens

([162]) Zie het jaarverslag 2021 van de PIPC, blz. 174. In 2020 hadden dergelijke klachten bijvoorbeeld betrekking op het zonder toestemming verzamelen van gegevens, het niet naleven van transparantieverplichtingen, schendingen van de PIPA door verwerkers, ontoereikende veiligheidsmaatregelen, het niet beantwoorden van verzoeken van betrokkenen, en algemene vragen.

([163]) Met name kunnen betrokkenen beroep instellen tegen de uitoefening of weigering van de uitoefening van overheidsbevoegdheden door een bestuursinstantie (artikel 2, lid 1, punt 1, artikel 3, punt 1, Wet administratieve procesvoering). Nadere informatie over de procedurele aspecten, met inbegrip van ontvankelijkheidseisen, wordt verstrekt in overweging 181.

([164]) Alle leden hebben een vaste ambtstermijn en kunnen alleen om gegronde redenen worden ontslagen (zie de artikelen 40, lid 5, en 41 PIPA). Ook bevat artikel 42 PIPA waarborgen ter bescherming tegen belangenconflicten.

([165]) Zie artikel 44 PIPA. Daarnaast kan het Comité een ontwerp voor een schikking voorstellen en een schikking zonder bemiddeling aanbevelen (zie artikel 46 PIPA).

([166]) Ook kan het Comité bemiddeling weigeren indien het van oordeel is dat deze niet geschikt is met het oog op de aard van het geschil, of omdat het verzoek om bemiddeling met oneerlijke bedoelingen is ingediend (artikel 48 PIPA).

([167]) Zie het jaarverslag van de PIPC van 2021, blz. 179 en180. Deze zaken betroffen onder meer inbreuken op de verplichting om toestemming te verkrijgen voor het verzamelen van gegevens, het doelbindingsbeginsel en de rechten van betrokkenen.

([168]) Zie artikel 49, lid 1, PIPA, waarin is bepaald dat de betrokkenen "op identieke of soortgelijke wijze" schade moeten lijden of een inbreuk op hun rechten moeten ondergaan, en artikel 52, punt 2, van het PIPA-uitvoeringsdecreet waarin als voorwaarde is gesteld dat belangrijke elementen van het incident in feite of in rechte gemeenschappelijk zijn.

([169]) Bovendien kunnen zelfs personen die geen partij zijn, baat hebben bij een collectieve-bemiddelingsbesluit dat door de verwerkingsverantwoordelijke wordt aanvaard, in die zin dat het Comité voor geschillenbeslechting de verwerkingsverantwoordelijke kan adviseren een schadevergoedingsplan op te stellen en in te dienen dat (ook) op hen betrekking heeft (artikel 49, lid 5, PIPA).

één persoon die het meest geschikt is om het gemeenschappelijk belang te vertegenwoordigen als vertegenwoordigende partij aanwijzen (artikel 49, lid 4, PIPA). Wanneer de verwerkingsverantwoordelijke de collectieve geschillenbeslechting afwijst of het bemiddelingsbesluit niet aanvaardt, kunnen bepaalde organisaties ([170]) een collectieve rechtszaak aanspannen om de inbreuk aan te pakken (artikelen 51 tot en met 57 PIPA).

(135) Ten derde heeft de betrokkene in geval van een inbreuk op de persoonlijke levenssfeer die hem of haar "schade" toebrengt, recht om verhaal te halen door middel van een "snelle en eerlijke procedure" (artikel 4, punt 5, en artikel 39 PIPA) ([171]). De verwerkingsverantwoordelijke kan zich vrijpleiten door aan te tonen dat er geen sprake is van schuld ("kwade opzet" of nalatigheid). Wanneer de betrokkene schade lijdt als gevolg van verlies, diefstal, verspreiding, vervalsing, wijziging of beschadiging van zijn of haar persoonsgegevens, kan de rechter een vergoeding vaststellen van ten hoogste driemaal de feitelijke schade, waarbij rekening wordt gehouden met een aantal factoren (artikel 39, leden 3 en 4, PIPA). Als alternatief kan de betrokkene een "redelijke" schadevergoeding eisen van ten hoogste 3 miljoen KRW (artikel 39-2, leden 1 en 2, PIPA). Bovendien kan, overeenkomstig het burgerlijk wetboek, schadevergoeding worden geëist van eenieder die door een onrechtmatige daad, opzettelijk of uit nalatigheid, een ander schade berokkent of letsel toebrengt ([172]) of van een eenieder die de persoon, de vrijheid of de reputatie van een ander heeft geschaad of een andere persoon geestelijk leed heeft toegebracht ([173]). Deze aansprakelijkheid uit onrechtmatige daad als gevolg van de inbreuk op de gegevensbeschermingsvoorschriften is bevestigd door het Hooggerechtshof ([174]). Indien schade is veroorzaakt door het onrechtmatig handelen van een overheidsinstantie, kan bovendien een vordering tot schadevergoeding worden ingesteld op grond van de Wet inzake overheidscompensatie ([175]). Een vordering op grond van de Wet inzake overheidscompensatie kan worden ingediend bij een gespecialiseerde "raad voor schadevergoeding", of rechtstreeks bij de Koreaanse rechtbanken ([176]). Aansprakelijkheid van de staat dekt ook immateriële schade (zoals geestelijk lijden) ([177]). Als het slachtoffer een buitenlands onderdaan is, is de Wet inzake overheidscompensatie van toepassing zolang zijn of haar land van herkomst ook voorziet in overheidscompensatie voor Koreaanse onderdanen ([178]).

(136) Ten vierde heeft het Hooggerechtshof erkend dat betrokkenen het recht hebben een dwangmiddel tot rechtsherstel te vorderen wegens inbreuken op hun rechten uit hoofde van de grondwet, waaronder het recht op de bescherming van persoonsgegevens ([179]). In dit verband kan een rechter bijvoorbeeld de verwerkingsverantwoordelijken gelasten een onwettige activiteit op te schorten of stop te zetten. Daarnaast kan het recht op gegevensbescherming, met inbegrip van de door de PIPA beschermde rechten, worden gehandhaafd door middel van burgerlijke rechtsvordering. Deze horizontale toepassing van de grondwettelijke bescherming van de persoonlijke levenssfeer op betrekkingen tussen particuliere partijen is door het Hooggerechtshof erkend ([180]).

([170]) Namelijk, consumentengroepen of ngo's zonder winstoogmerk met een bepaald aantal leden, die gegevensbescherming tot doel hebben (in geval van een ngo echter met de aanvullende eis dat ten minste honderd betrokkenen die dezelfde (soort) inbreuk hebben ondervonden, een verzoek hebben ingediend om een collectieve rechtszaak aan te spannen). Zie artikel 51 PIPA.

([171]) In de artikelen 43 tot en met 43-3 CIA is ook de aansprakelijkheid vastgelegd voor het vergoeden van schade die voortvloeit uit schendingen van die wet.

([172]) Artikel 750 burgerlijk wetboek.

([173]) Artikel 751, lid 1, burgerlijk wetboek.

([174]) Zie bijvoorbeeld Beslissing 2015Da251539, 251546, 251553, 251560, 251577 van het Hooggerechtshof van 30 mei 2018. Daarnaast heeft het Hooggerechtshof bevestigd dat gegevenslekken kunnen leiden tot een toekenning van schadevergoeding op grond van het burgerlijk wetboek, zie Beslissing 2011Da59834, 59858, 59841 van het Hooggerechtshof van 26 december 2012 (Engelse samenvatting beschikbaar op: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). In deze zaak heeft het Hooggerechtshof verduidelijkt dat om te beoordelen of een persoon emotionele schade heeft geleden die als vergoedbare schade kan worden aangemerkt, verschillende factoren in aanmerking moeten worden genomen, zoals het type en de kenmerken van de gelekte informatie, de identificeerbaarheid van de persoon als gevolg van het gegevenslek, de mogelijke toegang tot de gegevens door derden, de mate waarin de persoonsinformatie is verspreid, of dit tot verdere inbreuken op individuele rechten heeft geleid, de wijze waarop de persoonsinformatie werd beheerd en beschermd enz.

([175]) Op basis van de Wet inzake overheidscompensatie kunnen betrokkenen een aanvraag indienen voor vergoeding van schade die door ambtenaren bij de uitoefening van hun officiële taken in strijd met de wet is toegebracht (artikel 2, lid 1, van de wet).

([176]) Artikelen 9 en 12 van de Wet inzake overheidscompensatie. De wet stelt districtsraden in (voorgezeten door de substituut-aanklager van het overeenkomstige parket), een centrale raad (voorgezeten door de viceminister van Justitie) en een speciale raad (belast met vorderingen tot schadevergoeding voor schade toegebracht door militairen of burgerpersoneel bij de krijgsmacht, voorgezeten door de viceminister van Nationale Defensie). Vorderingen tot schadevergoeding worden in beginsel behandeld door de districtsraden, die in bepaalde omstandigheden zaken moeten doorsturen naar de centrale/speciale raad, bijvoorbeeld wanneer de schadevergoeding een bepaald bedrag overschrijdt of wanneer een persoon om een nieuwe beraadslaging verzoekt. Alle raden bestaan uit leden die door de minister van Justitie worden benoemd (bv. uit ambtenaren van het ministerie van Justitie, rechterlijke ambtenaren, advocaten en personen die deskundig zijn op het gebied van staatscompensatie) en zijn onderworpen aan specifieke regels inzake belangenconflicten (zie artikel 7 van het uitvoeringsdecreet bij de Wet inzake overheidscompensatie).

([177]) Zie artikel 8 van de Wet inzake overheidscompensatie (waarin wordt verwezen naar het burgerlijk wetboek), alsmede artikel 751 van het burgerlijk wetboek.

([178]) Artikel 7 van de Wet inzake overheidscompensatie.

([179]) Beslissing 93Da40614 van het Hooggerechtshof van 12 april 1996, en Beslissing 2008Da42430 van 2 september 2011 (Engelse samenvatting beschikbaar op https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Zie bijvoorbeeld Beslissing 2008Da42430 van het Hooggerechtshof van 2 september 2011, (Engelse samenvatting beschikbaar op https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Tot slot kunnen betrokkenen op grond van het wetboek van strafvordering (artikel 223) een strafrechtelijke klacht indienen bij een openbaar aanklager of bij een ambtenaar van de gerechtelijke politie ([181]).

(138) Het Koreaanse systeem biedt derhalve verschillende mogelijkheden om verhaal te halen, van laagdrempelige en goedkope opties (bijvoorbeeld door contact op te nemen met het Privacy Call Centre of via (collectieve) bemiddeling) tot administratieve (voor de PIPC) en gerechtelijke alternatieven, met onder meer de mogelijkheid om schadeloosstelling te verkrijgen.

3. TOEGANG TOT EN GEBRUIK VAN UIT DE EUROPESE UNIE DOORGEGEVEN PERSOONSGEGEVENS DOOR OVERHEIDSINSTANTIES IN DE REPUBLIEK KOREA

(139) De Commissie heeft ook de beperkingen en waarborgen beoordeeld, inclusief de mechanismen voor toezicht en individueel verhaal in het Koreaanse recht met betrekking tot de verzameling en het daaropvolgende gebruik van persoonsgegevens die door Koreaanse overheidsinstanties in het openbaar belang, met name voor de handhaving van het strafrecht en de nationale veiligheid, worden doorgegeven aan verwerkingsverantwoordelijken in Korea (overheidstoegang). In dit verband heeft de Koreaanse regering de Commissie op het hoogste niveau van ministeries en andere overheidsinstanties ondertekende officiële verklaringen, garanties en toezeggingen verstrekt die in bijlage II bij dit besluit zijn opgenomen.

(140) Bij de beoordeling van de vraag of de voorwaarden waaronder overheidstoegang tot gegevens die op grond van dit besluit aan Korea worden doorgegeven "in feite overeenkomend" zijn met artikel 45, lid 1, van Verordening (EU) 2016/679, zoals uitgelegd door het Hof van Justitie van de Europese Unie (het "Hof") in het licht van het Handvest van de grondrechten, heeft de Commissie met name rekening gehouden met de volgende criteria.

(141) Ten eerste moet elke beperking van het recht op bescherming van persoonsgegevens bij wet worden geregeld en moet de rechtsgrondslag die de aantasting van een dergelijk recht mogelijk maakt, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht bepalen ([182]).

(142) Ten tweede moet, om te voldoen aan het evenredigheidsvereiste, dat inhoudt dat afwijkingen en beperkingen van de bescherming van persoonsgegevens slechts van toepassing mogen zijn voor zover zulks in een democratische samenleving strikt noodzakelijk is om specifieke doelstellingen van algemeen belang te verwezenlijken die gelijkwaardig zijn aan die welke door de EU worden erkend, de wetgeving van het betrokken derde land die de inmenging toestaat, duidelijke en nauwkeurige regels betreffende de werkingssfeer en de toepassing van de betrokken maatregelen vaststellen en minimumwaarborgen opleggen, opdat de personen wier gegevens zijn doorgegeven, over voldoende waarborgen beschikken om hun persoonsgegevens doeltreffend te beschermen tegen het risico van misbruik ([183]). De wetgeving moet met name aangeven in welke omstandigheden en onder welke voorwaarden een maatregel kan worden genomen die voorziet in de verwerking van dergelijke gegevens ([184]), en moet de naleving van dergelijke vereisten aan onafhankelijk toezicht onderwerpen ([185]).

(143) In de derde plaats moeten de wetgeving en de daarin gestelde eisen juridisch bindend zijn volgens het binnenlands recht. Dit betreft allereerst de autoriteiten van het derde land in kwestie, maar deze wettelijke eisen moeten ook voor de rechter afdwingbaar zijn ten opzichte van die autoriteiten ([186]). Betrokkenen moeten met name de mogelijkheid hebben een rechtsvordering in te stellen bij een onafhankelijke en onpartijdige rechterlijke instantie om inzage te krijgen in hun persoonsgegevens of om deze gegevens te laten corrigeren of wissen ([187]).

3.1. **Algemeen rechtskader**

(144) De beperkingen en waarborgen die gelden voor de verzameling en het daaropvolgende gebruik van persoonsgegevens door Koreaanse overheidsinstanties vloeien voort uit het overkoepelende grondwettelijke kader, specifieke wetten die hun activiteiten op het gebied van de handhaving van het strafrecht en de nationale veiligheid reguleren, alsmede de regels die specifiek van toepassing zijn op de verwerking van persoonsgegevens.

([181]) Zoals toegelicht in overweging 127, kan misbruik van gegevens op grond van het wetboek van strafrecht een strafbaar feit vormen.

([182]) Zie Schrems II, punten 174–175, en de aangehaalde rechtspraak. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, het arrest van het Hof (grote kamer) van 6 oktober 2020, Privacy International, Zaak C-623/17, ECLI:EU:C:2020:790, punt 65, en het arrest van het Hof (grote kamer) 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 175.

([183]) Zie Schrems II, punten 176 en 181, en de aangehaalde rechtspraak. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, Privacy International, punt 68, en La Quadrature du Net e.a., punt 132.

([184]) Zie Schrems II, punt 176. Zie ook, wat de toegang van overheidsinstanties van de lidstaten betreft, Privacy International, punt 68, en La Quadrature du Net e.a., punt 132.

([185]) Zie Schrems II, punt 179.

([186]) Zie Schrems II, punten 181 en182.

([187]) Zie Schrems I, punt 95 en Schrems II, punt 194. In dat verband heeft het Hof met name benadrukt dat artikel 47 van het Handvest van de grondrechten (dat het recht op een doeltreffende voorziening in rechte bij een onafhankelijk en onpartijdig gerecht waarborgt), deel uitmaakt van "het binnen de Unie vereiste beschermingsniveau en [dat] de Commissie de naleving [ervan] moet vaststellen alvorens een adequaatheidsbesluit op grond van artikel 45, lid 1, AVG vast te stellen" (Schrems II, punt 186).

(145) Ten eerste gelden voor de toegang tot persoonsgegevens door de Koreaanse overheid de algemene beginselen van legaliteit, noodzakelijkheid en evenredigheid die uit de Koreaanse grondwet voortvloeien ([188]). Met name mogen fundamentele rechten en vrijheden (waaronder het recht op privacy en het recht op briefgeheim) ([189]) alleen bij wet worden beperkt wanneer dat noodzakelijk is voor de nationale veiligheid of de handhaving van de openbare orde met het oog op het openbaar welzijn. Dergelijke beperkingen mogen de wezenlijke inhoud van het recht of de vrijheid in kwestie niet aantasten. Wat specifiek onderzoeken en inbeslagnemingen betreft, bepaalt de grondwet dat deze alleen mogen plaatsvinden zoals bij wet bepaald, op basis van een door een rechter afgegeven bevel en met inachtneming van een goede rechtsbedeling ([190]). Tot slot kunnen betrokkenen hun rechten en vrijheden voor het Grondwettelijk Hof inroepen wanneer zij menen dat deze door de overheid tijdens de uitoefening van haar bevoegdheden zijn geschonden ([191]). Ook personen die schade hebben geleden door een onrechtmatige handeling van een ambtenaar tijdens de uitoefening van zijn ambt, hebben het recht een billijke vergoeding te vorderen ([192]).

(146) Ten tweede komen, zoals in de punten 3.2.1 en 3.3.1 meer in detail is beschreven, de in overweging 145 genoemde algemene beginselen ook tot uiting in de specifieke wetten die de bevoegdheden van de rechtshandhavingsinstanties en de nationale veiligheidsinstanties regelen. Met betrekking tot strafrechtelijk onderzoek bepaalt het wetboek van strafvordering (*Criminal Procedure Act*, hierna "CPA" genoemd) bijvoorbeeld dat verplichte maatregelen alleen mogen worden genomen wanneer het CPA daarin uitdrukkelijk voorziet en voor zover zij niet verder gaan dan wat nodig is om het doel van het onderzoek te verwezenlijken ([193]). Evenzo verbiedt artikel 3 van de Wet op de bescherming van de communicatieprivacy (Communications Privacy Protection Act, hierna "CPPA" genoemd) de toegang tot privécommunicatie, tenzij dit op grond van de wet gebeurt en met inachtneming van de daarin vastgestelde beperkingen en waarborgen. Op het gebied van de nationale veiligheid bepaalt de Wet op de Nationale Inlichtingendienst (*National Intelligence Service Act*, hierna "NIS-wet" genoemd) dat elke toegang tot communicatie- of locatiegegevens in overeenstemming moet zijn met de wet en dat machtsmisbruik en wetsovertredingen strafrechtelijk moeten worden bestraft ([194]).

(147) Ten derde is de verwerking van persoonsgegevens door overheidsinstanties, ook ten behoeve van de rechtshandhaving en nationale veiligheid, onderworpen aan de gegevensbeschermingsvoorschriften van de PIPA ([195]). Als algemeen beginsel is in artikel 5, lid 1, PIPA bepaald dat overheidsinstanties een beleid moeten ontwikkelen ter voorkoming van misbruik en oneigenlijk gebruik van persoonsinformatie, willekeurige surveillance en tracering enz. en ter versterking van de menselijke waardigheid en de persoonlijke levenssfeer. Bovendien moet elke verwerkingsverantwoordelijke persoonsgegevens op zodanige wijze verwerken dat de mogelijkheid dat inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkene tot een minimum wordt beperkt (artikel 3, lid 6, PIPA).

(148) Alle voorschriften van de PIPA, zoals uitvoerig beschreven in deel 2, zijn van toepassing op de verwerking van persoonsgegevens ten behoeve van de rechtshandhaving. Dit omvat de kernbeginselen (zoals rechtmatigheid en behoorlijkheid, doelbinding, juistheid, minimale gegevensverwerking, opslagbeperking, beveiliging en transparantie), verplichtingen (bijvoorbeeld met betrekking tot de melding van gegevenslekken en gevoelige gegevens) en rechten (om toegang, correctie, verwijdering en opschorting te verkrijgen).

(149) Hoewel de verwerking van persoonsgegevens ten behoeve van de nationale veiligheid onder een beperktere reeks voorschriften van de PIPA valt, zijn de kernbeginselen, alsmede de regels inzake toezicht, handhaving en verhaal van toepassing ([196]). Met name zijn in de artikelen 3 en 4, PIPA de algemene gegevensbeschermingsbeginselen (rechtmatigheid en behoorlijkheid, doelbinding, juistheid, minimale gegevensverwerking, beveiliging en transparantie) en de individuele rechten (het recht op informatie, het recht op toegang, en het recht op correctie, verwijdering en opschorting) vastgelegd ([197]). Artikel 4, lid 5, PIPA biedt betrokkenen daarnaast het recht op passende verhaalsmogelijkheden met een snelle en eerlijke procedure in geval van schade die voortvloeit uit de

([188]) Zie punt 1.1 van bijlage II.
([189]) Artikel 37, lid 2, van de grondwet.
([190]) Artikel 16 en artikel 12, lid 3, van de grondwet. In artikel 12, lid 3, van de grondwet worden voorts de uitzonderlijke omstandigheden genoemd waarin onderzoeken of inbeslagnemingen zonder een rechterlijk bevel mogen plaatsvinden (hoewel een bevel achteraf vereist blijft), namelijk in geval van heterdaad of, voor strafbare feiten waarop een gevangenisstraf van ten minste drie jaar staat, wanneer het risico bestaat dat bewijsmateriaal zal worden vernietigd of de verdachte zal verdwijnen.
([191]) Artikel 68, lid 1, van de Wet op het Grondwettelijk Hof.
([192]) Artikel 29, lid 1, van de grondwet.
([193]) Artikel 199, lid 1, CPA. Meer in het algemeen moeten overheidsinstanties bij de uitoefening van hun bevoegdheden op grond van het CPA de grondrechten van verdachten van strafbare feiten en van alle andere betrokkenen eerbiedigen (artikel 198, lid 2, CPA).
([194]) Artikel 14 van de NIS-wet.
([195]) Zie punt 1.2 van bijlage II.
([196]) Artikel 58, lid 1, punt 2, PIPA. Zie ook punt 6 van Kennisgeving nr. 2021-5 (bijlage I). Deze vrijstelling van sommige bepalingen van de PIPA is alleen van toepassing wanneer persoonsgegevens worden verwerkt ten behoeve van de nationale veiligheid. Zodra de nationale veiligheidssituatie die de gegevensverwerking rechtvaardigt, is beëindigd, kan niet langer beroep op de vrijstelling worden gedaan en zijn alle PIPA-vereisten van toepassing.
([197]) Dergelijke rechten mogen alleen worden beperkt wanneer de wet daarin voorziet, voor zover en zolang dat noodzakelijk en evenredig is om een belangrijke doelstelling van openbaar belang te beschermen, of wanneer de toekenning van het recht schade kan toebrengen aan het leven of de lichamelijke integriteit van derden, of een ongerechtvaardigde inbreuk kan vormen op eigendoms- of andere belangen van derden. Zie punt 6 van Kennisgeving nr. 2021-5.

verwerking van hun persoonsgegevens. Dit wordt aangevuld met specifiekere verplichtingen om persoonsgegevens slechts te verwerken in de mate waarin en voor zolang zij noodzakelijk zijn om het beoogde doel te bereiken, om de nodige maatregelen te treffen om een veilig gegevensbeheer en een passende verwerking te waarborgen (zoals technische, bestuurlijke en fysieke waarborgen), alsook om maatregelen te treffen voor een passende behandeling van individuele grieven (klachten) ([198]). Tot slot zijn de algemene beginselen van wettigheid, noodzakelijkheid en evenredigheid uit de Koreaanse grondwet (zie overweging 145) ook van toepassing op de verwerking van persoonsgegevens met het oog op de nationale veiligheid.

(150) Deze algemene beperkingen en waarborgen kunnen door betrokkenen worden ingeroepen voor onafhankelijke toezichthoudende instanties (bv. de PIPC en/of de Nationale Mensenrechtencommissie, zie de overwegingen 177 en 178) en rechtbanken (zie overwegingen 179 tot en met 183) om rechtsherstel te verkrijgen.

3.2. **Toegang van en gebruik door de Koreaanse overheidsdiensten met het oog op de handhaving van het strafrecht**

(151) De Koreaanse wet legt een aantal beperkingen op aan de toegang tot en het gebruik van persoonsgegevens met het oog op de handhaving van het strafrecht, en voorziet in toezichts- en verhaalsmechanismen die in overeenstemming zijn met de in de overwegingen 141 tot en met 143 van dit besluit bedoelde vereisten. De voorwaarden waaronder deze toegang kan plaatsvinden en de waarborgen die van toepassing zijn op het gebruik van die bevoegdheden worden in de volgende punten in detail beoordeeld.

3.2.1. *Rechtsgrondslagen, beperkingen en waarborgen*

(152) Door Koreaanse verwerkingsverantwoordelijken verwerkte persoonsgegevens die op grond van dit besluit uit de EU zouden worden doorgegeven ([199]), kunnen door Koreaanse autoriteiten worden verzameld voor de handhaving van het strafrecht in het kader van een onderzoek of inbeslagneming (op grond van het CPA), door middel van toegang tot communicatiegegevens (op grond van de CPPA), of door abonneegegevens te verkrijgen via verzoeken om vrijwillige verstrekking (op grond van de Wet op de telecommunicatieactiviteiten —*Telecommunications Business Act*, hierna "TBA" genoemd) ([200]).

3.2.1.1. Onderzoeken en inbeslagnemingen

(153) Het CPA bepaalt dat een onderzoek of inbeslagneming alleen mag plaatsvinden indien een persoon wordt verdacht van een misdrijf, indien het onderzoek of de inbeslagneming noodzakelijk is voor het gerechtelijk onderzoek en indien er een verband bestaat tussen dat onderzoek en de te fouilleren persoon of het te doorzoeken of in beslag te nemen voorwerp ([201]). Voorts mag een onderzoek of inbeslagneming (zoals elke verplichte maatregel) slechts worden toegestaan/uitgevoerd in een mate die niet verder gaat dan noodzakelijk is ([202]). Indien een doorzoeking betrekking heeft op een computerschijf of een ander medium voor gegevensopslag, worden in beginsel alleen de noodzakelijke gegevens zelf (gekopieerd of afgedrukt) in beslag genomen en niet het hele medium ([203]). Dit laatste mag alleen gebeuren wanneer het in wezen onmogelijk wordt geacht de vereiste gegevens afzonderlijk af te drukken of te kopiëren, of wanneer het in wezen onmogelijk wordt geacht het doel van de doorzoeking op een andere manier te bereiken ([204]). Het CPA bevat derhalve duidelijke en precieze regels over de reikwijdte en de toepassing van deze maatregelen, en zorgt er zo voor dat de inmenging in de rechten van personen in geval van een onderzoek of inbeslagneming beperkt blijft tot wat noodzakelijk is voor een specifiek strafrechtelijk onderzoek en in verhouding staat tot het nagestreefde doel.

([198]) Artikel 58, lid 4, PIPA.

([199]) Zie punt 2.1 van bijlage II. In de officiële verklaring van de Koreaanse regering (punt 2.1 van bijlage II) wordt ook verwezen naar de mogelijkheid om op grond van de Wet inzake de verslaglegging over en het gebruik van bepaalde informatie over financiële transacties (*Act on Reporting and Using Specified Financial Transaction Information*, "ARUSFTI"), informatie over financiële transacties te verzamelen met het oog op de voorkoming van het witwassen van geld en de financiering van terrorisme. De ARUSFTI legt echter alleen verplichtingen tot verstrekking op aan verwerkingsverantwoordelijken die persoonlijke kredietinformatie verwerken op grond van de CIA en die onderworpen zijn aan het toezicht van de Commissie financiële diensten (zie overweging 13). Aangezien de verwerking van persoonlijke kredietinformatie door dergelijke verwerkingsverantwoordelijken buiten de werkingssfeer van dit besluit valt, is de ARUSFTI niet relevant voor de onderhavige beoordeling.

([200]) In artikel 3, CPPA wordt ook de Wet op de militaire rechtbank genoemd als mogelijke rechtsgrondslag voor de verzameling van communicatiegegevens. Die wet regelt echter de verzameling van gegevens over militair personeel en kan slechts in een beperkt aantal gevallen van toepassing zijn op burgers (wanneer militairen en burgers bijvoorbeeld samen een misdrijf zouden plegen, of wanneer een individu een misdrijf pleegt tegen de krijgsmacht, kan een procedure voor een militaire rechtbank worden ingeleid, zie artikel 2, Wet op de militaire rechtbank). In ieder geval bevat die wet algemene bepalingen inzake onderzoeken en inbeslagnemingen die vergelijkbaar zijn met die van het CPA (zie bijvoorbeeld de artikelen 146 tot en met 149 en 153 tot en met 156 van de Wet op de militaire rechtbank) en waarin bijvoorbeeld is voorzien dat poststukken alleen mogen worden verzameld wanneer dat nodig is voor een onderzoek en op grond van een bevel van de militaire rechtbank. Voor zover elektronische communicatie zou worden verzameld op basis van deze wet, zouden de beperkingen en waarborgen van de CPPA van toepassing zijn. Zie punt 2.2.2. van bijlage II en voetnoot 50.

([201]) Artikel 215, leden 1 en 2, CPA. Zie ook artikel 106, lid 1, artikel 107 en artikel 109, CPA, waarin wordt bepaald dat rechtbanken onderzoeken en inbeslagnemingen mogen verrichten zolang de betrokken voorwerpen of personen geacht worden verband te houden met een specifieke zaak. Zie punt 2.2.1.2 van bijlage II.

([202]) Artikel 199, lid 1, CPA.

([203]) Artikel 106, lid 3, CPA.

([204]) Artikel 106, lid 3, CPA.

(154) Wat de procedurele waarborgen betreft, vereist het CPA dat voor het uitvoeren van een onderzoek of inbeslagneming een rechterlijk bevel wordt verkregen ([205]). Een onderzoek of inbeslagneming zonder rechterlijk bevel is slechts bij uitzondering toegestaan, namelijk in dringende omstandigheden ([206]), ter plaatse bij de aanhouding of inhechtenisneming van een verdachte van een strafbaar feit ([207]), of wanneer een voorwerp is weggegooid of vrijwillig wordt overgelegd door een verdachte van een strafbaar feit of een derde (wat persoonsgegevens betreft, door de betrokkene zelf) ([208]). Op onwettige onderzoeken en inbeslagnemingen staan strafrechtelijke sancties ([209]) en iedere vorm van bewijs die in strijd met het CPA is verkregen, wordt als ontoelaatbaar beschouwd ([210]). Tot slot moeten de betrokkenen altijd onverwijld in kennis worden gesteld van een onderzoek of inbeslagneming (met inbegrip van een inbeslagneming van hun gegevens) ([211]), hetgeen de uitoefening van de materiële rechten van de betrokkene en het recht op verhaal zal vergemakkelijken (zie met name de mogelijkheid om de uitvoering van een bevel tot inbeslagneming aan te vechten, zie overweging 180).

3.2.1.2. Toegang tot communicatiegegevens

(155) Op grond van de CPPA kunnen de Koreaanse strafrechtelijke handhavingsinstanties twee soorten maatregelen nemen ([212]): enerzijds de verzameling van "communicatiebevestigende gegevens" ([213]), waaronder de datum van de telecommunicatie, de begin- en eindtijd ervan, het aantal uitgaande en inkomende gesprekken, alsmede het abonneenummer van de andere partij, de gebruiksfrequentie, logbestanden over het gebruik van telecommunicatiediensten en locatiegegevens (bijvoorbeeld afkomstig van zendmasten waar signalen worden ontvangen), en, anderzijds, "communicatiebeperkende maatregelen", die zowel betrekking hebben op de verzameling van de inhoud van traditionele post als op de rechtstreekse onderschepping van de inhoud van telecommunicatie ([214]).

(156) Communicatiebevestigende gegevens mogen alleen worden ingezien wanneer dat nodig is om een strafrechtelijk onderzoek in te stellen of een vonnis ten uitvoer te leggen ([215]), op basis van een rechterlijk bevel ([216]). In dit verband vereist de CPPA dat gedetailleerde informatie wordt verstrekt, zowel in het verzoek om het bevel (bv. over de redenen voor het verzoek, de relatie met het voorwerp/de abonnee en de noodzakelijke gegevens), als in het bevel zelf (bv. over de doelstelling, het voorwerp en de reikwijdte van de maatregel) ([217]). Het verzamelen van gegevens zonder rechterlijk bevel mag alleen plaatsvinden wanneer het om dringende redenen onmogelijk is

([205]) Artikel 113 en artikel 215, leden 1 en 2, CPA. Bij het aanvragen van een rechterlijk bevel moet de betrokken autoriteit materiaal overleggen waaruit blijkt dat er redenen zijn om iemand ervan te verdenken een strafbaar feit te hebben gepleegd, dat het onderzoek, de inspectie of de inbeslagneming noodzakelijk is en dat de in beslag te nemen voorwerpen bestaan (artikel 108, lid 1, verordening betreffende de strafrechtelijke procedure). In het bevel zelf moeten onder meer de namen van de verdachte en het strafbare feit worden vermeld; de plaats, de persoon die moet worden gefouilleerd of de voorwerpen die moeten worden doorzocht of in beslag moeten worden genomen; de datum van afgifte, en de effectieve toepassingsduur (artikel 114, lid 1, juncto artikel 219, CPA). Zie punt 2.2.1.2 van bijlage II.

([206]) Dat wil zeggen, wanneer het onmogelijk is een bevel te verkrijgen wegens een dringende reden op de plaats van een strafbaar feit (artikel 216, lid 3, CPA); in dat geval moet vervolgens toch onverwijld een bevel worden verkregen (artikel 216, lid 3, CPA).

([207]) Artikel 216, leden 1 en 2, CPA.

([208]) Artikel 218, CPA. Bovendien worden, zoals uiteengezet in punt 2.2.1.2 van bijlage II, vrijwillig overgelegde voorwerpen alleen als bewijs in een gerechtelijke procedure toegelaten indien er geen redelijke twijfel bestaat over de vrijwilligheid van de overlegging, hetgeen door de openbaar aanklager moet worden aangetoond.

([209]) Artikel 321 van het wetboek van strafrecht.

([210]) Artikel 308-2 CPA. Bovendien mag een persoon (en zijn/haar raadsman) aanwezig zijn wanneer een bevel tot onderzoek of inbeslagneming wordt uitgevoerd en mag hij/zij dus ook verzet aantekenen op het ogenblik dat het bevel wordt uitgevoerd (artikelen 121 en 219 CPA).

([211]) Artikelen 121 en 122 CPA (met betrekking tot doorzoekingen), en artikel 219 juncto artikel 106, lid 4, CPA (met betrekking tot inbeslagnemingen).

([212]) Zie ook punt 2.2.2.1 van bijlage II. Dergelijke maatregelen kunnen worden genomen met de gedwongen medewerking van telecommunicatie-exploitanten waarbij aan deze exploitanten een schriftelijke toestemming van een rechtbank moet worden overhandigd (artikel 9, lid 2, CPPA), die door de exploitanten moet worden bewaard (artikel 15-2 CPPA en artikel 12 van het CPPA-uitvoeringsdecreet). Telecommunicatieaanbieders mogen hun medewerking weigeren wanneer de in de schriftelijke toestemming van de rechter vermelde informatie over de persoon in kwestie (bijvoorbeeld het telefoonnummer van de persoon) onjuist is, en mogen onder geen beding wachtwoorden bekendmaken die voor telecommunicatie worden gebruikt (artikel 9, lid 4, CPPA).

([213]) Artikel 2, lid 11, CPPA.

([214]) Zie artikel 2, lid 6, CPPA, waarin wordt verwezen naar "censuur" (het openen van post zonder toestemming van de betrokken partij of het met andere middelen kennisnemen, opnemen of achterhouden van de inhoud daarvan) en artikel 2, lid 7, CPPA, dat betrekking heeft op "aftapping" (het verwerven of opnemen van de inhoud van telecommunicatie door het beluisteren of gelijktijdig lezen van de geluiden, woorden, symbolen of beelden van de berichten met behulp van elektronische en mechanische middelen zonder toestemming van de betrokken partij, of het verstoren van de transmissie en ontvangst daarvan).

([215]) Artikel 13, lid 1, CPPA. Zie ook punt 2.2.2.3 van bijlage II. Bovendien mogen realtime traceergegevens van locaties en communicatiebevestigende gegevens over een specifiek basisstation alleen worden verzameld voor het onderzoek naar ernstige strafbare feiten of wanneer het anders moeilijk zou zijn om de uitvoering van een strafbaar feit te voorkomen of bewijsmateriaal te verzamelen (artikel 13, lid 2, CPPA). Hiermee wordt tegemoetgekomen aan de noodzaak om, overeenkomstig het evenredigheidsbeginsel, te voorzien in aanvullende waarborgen in geval van maatregelen die bijzondere inbreuk op de persoonlijke levenssfeer maken.

([216]) Artikelen 6 en 13 CPPA.

([217]) Zie artikel 13, leden 3 en 9, juncto artikel 6, leden 4 en 6, CPPA.

toestemming van de rechter te krijgen; in dat geval moet het bevel onmiddellijk na het verzoek om de gegevens worden verkregen en aan de telecommunicatieaanbieder worden overhandigd ([218]). Mocht de rechter achteraf weigeren om toestemming te verlenen, dan moeten de verzamelde gegevens worden vernietigd ([219]).

(157) Wat de aanvullende waarborgen met betrekking tot de verzameling van communicatiebevestigende gegevens betreft, legt de CPPA specifieke eisen op inzake het bijhouden van registers en transparantie ([220]). Met name moeten zowel de strafrechtelijke handhavingsinstanties ([221]) als de telecommunicatieaanbieders ([222]) een register bijhouden van de verzoeken en de verstrekte gegevens. Daarnaast moeten strafrechtelijke handhavingsinstanties betrokkenen in beginsel in kennis stellen van het feit dat hun communicatiebevestigende gegevens zijn verzameld ([223]). Deze kennisgeving kan alleen in uitzonderlijke omstandigheden worden uitgesteld op grond van toestemming van de directeur van een bevoegd arrondissementsparket ([224]). Die toestemming kan alleen worden verleend wanneer de kennisgeving 1) de nationale veiligheid, de openbare veiligheid en de openbare orde in gevaar kan brengen; 2) de dood of lichamelijk letsel kan veroorzaken; 3) een eerlijke rechtsgang kan belemmeren (bijvoorbeeld door bewijsmateriaal te vernietigen of getuigen te bedreigen), of 4) de verdachte, de slachtoffers of andere personen die met de zaak te maken hebben, in diskrediet kan brengen, of inbreuk op hun persoonlijke levenssfeer kan maken. In die gevallen moet de kennisgeving worden gedaan binnen dertig dagen nadat de reden(en) voor uitstel niet langer bestaat (bestaan) ([225]). Na de kennisgeving hebben betrokkenen het recht om informatie te verkrijgen over de redenen voor het verzamelen van hun gegevens ([226]).

(158) Er gelden strengere regels voor communicatiebeperkende maatregelen, die alleen mogen worden toegepast wanneer er gegronde redenen zijn om te vermoeden dat bepaalde ernstige strafbare feiten die specifiek in de CPPA worden genoemd, worden beraamd, worden gepleegd of zijn gepleegd ([227]). Bovendien mogen communicatiebeperkende maatregelen alleen worden genomen als laatste redmiddel en wanneer het moeilijk is om op een andere manier het plegen van een misdrijf te voorkomen, een misdadiger te arresteren of bewijsmateriaal te verzamelen ([228]). Zij moeten onmiddellijk worden stopgezet zodra zij niet langer nodig zijn, om ervoor te zorgen dat de inbreuk op de communicatieprivacy zo beperkt mogelijk blijft ([229]). Informatie die op onwettige wijze is verkregen door middel van communicatiebeperkende maatregelen wordt niet als bewijs toegelaten in gerechtelijke of tuchtrechtelijke procedures ([230]).

(159) Wat de procedurele waarborgen betreft, vereist de CPPA dat voor het uitvoeren van communicatiebeperkende maatregelen een rechterlijk bevel wordt verkregen ([231]). Ook in deze gevallen vereist de CPPA dat het verzoek om een rechterlijk bevel en het bevel zelf gedetailleerde informatie bevatten ([232]), onder meer over de rechtvaardiging van het verzoek, alsook over de te verzamelen communicaties (die van de verdachte tegen wie een onderzoek loopt, moeten zijn) ([233]). Dergelijke maatregelen kunnen alleen zonder rechterlijk bevel worden genomen in geval van een onmiddellijke dreiging van georganiseerde criminaliteit of wanneer een ander ernstig misdrijf dat rechtstreeks de dood of ernstig letsel kan veroorzaken, ophanden is en er sprake is van een noodsituatie waardoor

([218]) Artikel 13, lid 2, CPPA.
([219]) Artikel 13, lid 3, CPPA.
([220]) Zie punt 2.2.2.3 van bijlage II.
([221]) Artikel 13, leden 5 en 6, CPPA.
([222]) Artikel 13, lid 7, CPPA. Ook moeten telecommunicatieaanbieders tweemaal per jaar aan het ministerie van Wetenschap en ICT verslag uitbrengen over de verstrekking van communicatiebevestigende gegevens.
([223]) Zie Artikel 13-3, lid 7, juncto artikel 9-2 CPPA. Met name moeten betrokkenen in kennis worden gesteld binnen dertig dagen nadat een beslissing is genomen om (niet) tot vervolging over te gaan of binnen dertig dagen vanaf het verstrijken van één jaar nadat een beslissing tot opschorting van een tenlastelegging is genomen (hoewel de kennisgeving in ieder geval moet plaatsvinden binnen dertig dagen vanaf het verstrijken van één jaar nadat de informatie is verzameld), zie artikel 13-3, lid 1, CPPA.
([224]) Artikel 13-3, leden 2 en 3, CPPA.
([225]) Artikel 13-3, lid 4, CPPA.
([226]) Artikel 13-3, lid 5, CPPA. Op verzoek van de persoon in kwestie moet een openbaar aanklager of een ambtenaar van de gerechtelijke politie de redenen schriftelijk meedelen binnen dertig dagen na ontvangst van het verzoek, tenzij een van de uitzonderingen voor uitstel van de kennisgeving van toepassing is (artikel 13-3, lid 6, CPPA).
([227]) Bijvoorbeeld oproer, drugsgerelateerde misdrijven, misdrijven met explosieven, alsmede misdrijven in verband met de nationale veiligheid, diplomatieke betrekkingen, of militaire bases en installaties, zie artikel 5, lid 1, CPPA. Zie ook punt 2.2.2.2 van bijlage II.
([228]) Artikel 3, lid 2, en artikel 5, lid 1, CPPA.
([229]) Artikel 2 van het CPPA-uitvoeringsdecreet.
([230]) Artikel 4, CPPA.
([231]) Artikel 6, leden 1, 2, 5 en 6, CPPA.
([232]) Een verzoek om een rechterlijk bevel moet een beschrijving bevatten van 1) de inhoudelijke redenen om (op het eerste gezicht) te vermoeden dat een van de genoemde strafbare feiten wordt gepland, wordt gepleegd of is gepleegd, alsmede ondersteunend materiaal; 2) de communicatiebeperkende maatregelen alsmede hun voorwerp, reikwijdte, doelstelling en de periode waarin zij feitelijk worden toegepast, en 3) de plaats waar de maatregelen zouden worden uitgevoerd en de wijze waarop zij zouden worden uitgevoerd (artikel 6, lid 4, CPPA en artikel 4, lid 1, van het CPPA-uitvoeringsdecreet). In het bevel zelf moeten de maatregelen worden gespecificeerd, alsmede hun voorwerp, reikwijdte, feitelijke periode, plaats van uitvoering en de wijze waarop zij worden uitgevoerd (artikel 6, lid 6, CPPA).
([233]) Een communicatiebeperkende maatregel moet gericht zijn op specifieke poststukken of telecommunicatie van of naar de verdachte, of op poststukken of telecommunicatie van of naar de verdachte gedurende een bepaalde periode (artikel 5, lid 2, CPPA).

het onmogelijk is de normale procedure te volgen ([234]). In dat geval moet echter onmiddellijk nadat de maatregel is genomen een verzoek om een bevel worden ingediend ([235]). De communicatiebeperkende maatregelen mogen ten hoogste twee maanden worden toegepast ([236]) en mogen alleen met toestemming van de rechter worden verlengd als nog steeds aan de voorwaarden voor de toepassing van de maatregelen wordt voldaan ([237]). De verlengingsperiode mag in totaal niet langer duren dan één jaar, of drie jaar voor bepaalde bijzonder ernstige strafbare feiten (zoals strafbare feiten in verband met oproer, buitenlandse agressie, nationale veiligheid) ([238]).

(160) Zoals het geval is voor het verzamelen van communicatiebevestigende gegevens, schrijft de CPPA voor dat telecommunicatieaanbieders ([239]) en rechtshandhavingsinstanties ([240]) een register bijhouden van de uitvoering van communicatiebeperkende maatregelen, evenals de kennnisgeving aan de betrokkene, hetgeen bij wijze van uitzondering kan worden uitgesteld wanneer dat om zwaarwegende redenen van algemeen belang noodzakelijk is ([241]).

(161) Tot slot staan er strafrechtelijke sancties op niet-naleving van verschillende beperkingen en waarborgen van de CPPA (waaronder bijvoorbeeld de verplichtingen inzake het verkrijgen van een bevel, het bijhouden van registers en het in kennis stellen van de betrokkene), zowel wat betreft het verzamelen van communicatiebevestigende gegevens als wat betreft het gebruik van communicatiebeperkende maatregelen ([242]).

(162) De bevoegdheden van de strafrechtelijke handhavingsinstanties om op basis van de CPPA communicatiegegevens te verzamelen (zowel de inhoud van de communicatie als de communicatiebevestigende gegevens) zijn derhalve afgebakend door duidelijke en precieze regels, en zijn onderworpen aan een aantal waarborgen. Deze waarborgen garanderen met name het toezicht op de uitvoering van dergelijke maatregelen, zowel vooraf (via voorafgaande toestemming van de rechter), als achteraf (door middel van registratie- en rapportagevereisten), en vergemakkelijken de toegang van betrokkenen tot doeltreffende rechtsmiddelen (door ervoor te zorgen dat zij worden geïnformeerd over het verzamelen van hun gegevens).

3.2.1.3. Verzoeken om vrijwillige verstrekking van abonneegegevens

(163) De Koreaanse rechtshandhavingsinstanties kunnen niet alleen een beroep doen op de in de overwegingen 153 tot en met 162 beschreven verplichte maatregelen, maar zij kunnen telecommunicatieaanbieders ook vragen om "communicatiegegevens" op vrijwillige basis, ter ondersteuning van een strafrechtelijke procedure, een onderzoek of de uitvoering van een vonnis (artikel 83, lid 3, TBA). Deze mogelijkheid bestaat alleen met betrekking tot beperkte gegevensreeksen, namelijk de naam, het burgerregistratienummer, het adres en het telefoonnummer van gebruikers, de data waarop gebruikers zich abonneren of hun abonnement beëindigen, alsmede gebruikersidentificatiecodes (d.w.z. codes die worden gebruikt om de rechtmatige gebruiker van computersystemen of communicatienetwerken te identificeren) ([243]). Aangezien alleen natuurlijke personen aan wie rechtstreeks diensten van een Koreaanse telecommunicatieaanbieder worden verleend, als "gebruikers" worden beschouwd ([244]), vallen EU-burgers wier gegevens aan de Republiek Korea zijn doorgegeven, normaal gesproken niet in deze categorie ([245]).

(164) Voor dergelijke vrijwillige verstrekkingen gelden verschillende beperkingen, zowel wat betreft de uitoefening van bevoegdheden door de rechtshandhavingsinstantie als de reactie van de telecommunicatie-exploitant. Als algemene eis geldt dat rechtshandhavingsinstanties moeten handelen overeenkomstig de grondwettelijke beginselen van noodzakelijkheid en evenredigheid (artikel 12, lid 1, en artikel 37, lid 2, van de grondwet), ook wanneer zij om informatie op vrijwillige basis verzoeken. Daarnaast moeten zij de PIPA naleven, met name door uitsluitend persoonsgegevens te verzamelen voor zover deze nodig zijn om een gerechtvaardigd doel te bereiken, op een

([234]) Artikel 8, lid 1, CPPA. Het verzamelen van informatie in noodsituaties moet echter altijd plaatsvinden in overeenstemming met een "verklaring inzake censuur/aftapping in noodsituaties" en de instantie die de informatie verzamelt, moet een register bijhouden van alle noodmaatregelen (artikel 8, lid 4, CPPA).

([235]) Het verzamelen moet onmiddellijk worden gestaakt wanneer de rechtshandhavingsinstantie er niet in slaagt binnen 36 uur toestemming van de rechter te verkrijgen (artikel 8, lid 2, CPPA); in dat geval wordt de verzamelde informatie in beginsel vernietigd, zoals in punt 2.2.2.2 van bijlage II wordt uitgelegd. De rechtbank moet ook worden geïnformeerd wanneer noodmaatregelen binnen dusdanig korte tijd zijn uitgevoerd dat de toestemming niet langer nodig is (bv. wanneer de verdachte onmiddellijk na het begin van de onderschepping wordt gearresteerd, zie artikel 8, lid 5, CPPA). In dat geval moet aan de rechter informatie worden verstrekt over de doelstelling, het voorwerp, de reikwijdte, de periode, de plaats van uitvoering en de wijze van verzameling, alsmede de redenen waarom geen verzoek om toestemming van de rechter is ingediend (artikel 8, leden 6 en 7, CPPA).

([236]) Artikel 6, lid 7, CPPA. Wanneer het doel van de maatregelen vóór het einde van die periode wordt bereikt, moeten de maatregelen onmiddellijk worden stopgezet.

([237]) Artikel 6, leden 7 en 8, CPPA.

([238]) Artikel 6, lid 8, CPPA.

([239]) Artikel 9, lid 3, CPPA.

([240]) Artikel 18, lid 1, van het CPPA-uitvoeringsdecreet.

([241]) Met name moet de openbaar aanklager de betrokkene binnen dertig dagen na het uitvaardigen van een tenlastelegging of een beslissing om niet tot tenlastelegging of aanhouding over te gaan, hiervan in kennis stellen (artikel 9-2, lid 1, CPPA). Deze kennisgeving kan worden uitgesteld met de goedkeuring van het hoofd van het arrondissementsparket, wanneer zij de nationale veiligheid ernstig in gevaar zou kunnen brengen of de openbare veiligheid en orde zou kunnen verstoren, of zou kunnen leiden tot materiële schade aan het leven en de lichamelijke integriteit van anderen (artikel 9-2, leden 4, 5 en 6, CPPA).

([242]) Artikelen 17 en 16 CPPA.

([243]) Artikel 83, lid 3, TBA. Zie ook punt 2.2.3 van bijlage II.

([244]) Artikel 2, lid 9, TBA.

([245]) Zie ook punt 2.2.3 van bijlage II.

wijze die de gevolgen voor de persoonlijke levenssfeer van personen tot een minimum beperkt (zoals artikel 3, leden 1 en 6, PIPA). Meer in het bijzonder moeten verzoeken om communicatiegegevens te verkrijgen op basis van de TBA schriftelijk worden gedaan en moeten de redenen voor het verzoek, het verband met de betrokken gebruiker en de reikwijdte van de gevraagde gegevens worden vermeld ([246]).

(165) Telecommunicatieaanbieders zijn niet verplicht dergelijke verzoeken in te willigen en mogen dit alleen doen in overeenstemming met de PIPA. Dit betekent met name dat zij de verschillende in het geding zijnde belangen tegen elkaar moeten afwegen en de gegevens niet mogen verstrekken indien dit waarschijnlijk op oneerlijke wijze inbreuk zou maken op de belangen van de betrokkene of van derden ([247]). Dit zou bijvoorbeeld het geval zijn als duidelijk is dat de verzoekende autoriteit misbruik heeft gemaakt van haar bevoegdheid ([248]). Telecommunicatie-exploitanten moeten registers bijhouden van verstrekkingen in het kader van de TBA en tweemaal per jaar verslag uitbrengen aan de minister van Wetenschap en ICT ([249]).

(166) Bovendien moeten telecommunicatieaanbieders, overeenkomstig punt 3 van Kennisgeving nr. 2021-5 (bijlage I), de betrokkene in beginsel in kennis stellen wanneer zij vrijwillig aan een verzoek voldoen ([250]). Dit zal de betrokkene dan weer in staat stellen zijn of haar rechten uit te oefenen en, indien zijn/haar gegevens op onrechtmatige wijze zijn verstrekt, verhaal te halen, hetzij ten aanzien van de verwerkingsverantwoordelijke (bijvoorbeeld omdat de gegevens in strijd met de PIPA zijn verstrekt of omdat is ingegaan op een verzoek dat duidelijk onevenredig was), hetzij ten aanzien van de rechtshandhavingsinstantie (bijvoorbeeld omdat is gehandeld buiten de grenzen van wat noodzakelijk en evenredig is of omdat de procedurele voorschriften van de TBA niet in acht zijn genomen).

3.2.2. *Verder gebruik van de verzamelde informatie*

(167) De verwerking van door Koreaanse strafrechtelijke handhavingsinstanties verzamelde persoonsgegevens is onderworpen aan alle voorschriften van de PIPA, ook met betrekking tot doelbinding (artikel 3, leden 1 en 2, PIPA), rechtmatigheid van gebruik en verstrekking aan derden (artikelen 15, 17 en 18 PIPA), internationale doorgiften (artikelen 17 en 18 PIPA, juncto Kennisgeving nr. 2021-5, deel 2) ([251]), evenredigheid/minimale gegevensverwerking (artikel 3, leden 1 en 6, PIPA) en opslagbeperking (artikel 21 PIPA) ([252]).

(168) Met betrekking tot de inhoud van communicatie die is verkregen door de uitvoering van communicatiebeperkende maatregelen, beperkt de CPPA uitdrukkelijk het mogelijke gebruik ervan tot het onderzoeken, vervolgen of voorkomen van ernstige strafbare feiten ([253]); tuchtrechtelijke procedures voor dezelfde strafbare feiten; vorderingen tot schadevergoeding van een partij bij de communicatie of wanneer dit specifiek is toegestaan door andere wetgeving ([254]). Bovendien mag de inhoud van via internet verzonden telecommunicatie alleen worden bewaard met toestemming van de rechter die de communicatiebeperkende maatregelen heeft toegestaan ([255]), met het oog op het gebruik ervan voor het onderzoeken, vervolgen of voorkomen van ernstige strafbare feiten ([256]). Meer in het algemeen verbiedt de CPPA de verstrekking van vertrouwelijke informatie die is verkregen door communicatiebeperkende maatregelen, en het gebruik van dergelijke informatie om de reputatie te schaden van degenen op wie de maatregelen betrekking hadden ([257]).

3.2.3. *Toezicht*

(169) In Korea wordt door verschillende instanties toezicht gehouden op de activiteiten van de strafrechtelijke handhavingsinstanties ([258]).

([246]) Artikel 83, lid 4, TBA. Wanneer het om dringende redenen onmogelijk is een schriftelijk verzoek in te dienen, moet het schriftelijke verzoek worden ingediend zodra de reden voor de urgentie is vervallen (artikel 83, lid 4, TBA).
([247]) Artikel 18, lid 2, PIPA.
([248]) Beslissing nr. 2012Da105482 van het Hooggerechtshof van donderdag 10 maart 2016. Zie ook punt 2.2.3 van bijlage II over deze beslissing van het Hooggerechtshof.
([249]) Artikel 83, leden 5 en 6, TBA.
([250]) Op dit vereiste gelden beperkte en speciale uitzonderingen, met name indien en zolang de kennisgeving een lopend strafrechtelijk onderzoek in gevaar zou brengen, of het leven of de lichamelijke integriteit van een andere persoon zou kunnen schaden, wanneer deze rechten of belangen duidelijk zwaarder wegen dan de rechten van de betrokkene. Zie deel 3, iii), lid 1 van de kennisgeving.
([251]) De Koreaanse overheid is met name verplicht om door middel van een juridisch bindend instrument te zorgen voor een beschermingsniveau dat gelijkwaardig is aan dat van de PIPA (zie ook overweging 90).
([252]) Zie ook punt 1.2 van bijlage II.
([253]) Zie overweging 158.
([254]) Artikel 12, CPPA. Zie punt 2.2.2.2 van bijlage II.
([255]) De openbaar aanklager of politieambtenaar die de communicatiebeperkende maatregelen uitvoert, moet binnen 14 dagen na het einde van de maatregelen de te bewaren telecommunicatie selecteren en de rechter om toestemming vragen (in geval van een politieambtenaar moet het verzoek worden ingediend bij een openbaar aanklager, die op zijn beurt het verzoek bij de rechter indient), zie artikel 12-2, leden 1 en 2, CPPA.
([256]) Een verzoek om een dergelijke toestemming moet informatie bevatten over de communicatiebeperkende maatregelen, een samenvatting van de resultaten van de maatregelen, de redenen voor het bewaren (samen met ondersteunend materiaal) en de te bewaren telecommunicatie (artikel 12-2, lid 3, CPPA). Indien geen verzoek wordt ingediend, moeten de verkregen gegevens worden gewist binnen 14 dagen na het einde van de communicatiebeperkende maatregel (artikel 12-2, lid 5, CPPA), en indien het verzoek wordt afgewezen, binnen zeven dagen (artikel 12-2, lid 5, CPPA). In beide gevallen moet binnen zeven dagen een verslag over deze verwijdering worden ingediend bij de rechter die de verzameling heeft toegestaan.
([257]) Artikel 11, lid 2, van het CPPA-uitvoeringsdecreet.
([258]) Zie punt 2.3 van bijlage II.

(170) Ten eerste staat de politie onder intern toezicht van een inspecteur-generaal ([259]), die een controle van wettigheid uitvoert, ook met betrekking tot mogelijke schendingen van de mensenrechten. De inspecteur-generaal is aangesteld voor de uitvoering van de Wet inzake controles in de publieke sector, die de oprichting van interne-controleorganen aanmoedigt en specifieke voorschriften bevat inzake hun samenstelling en taken. De wet schrijft met name voor dat het hoofd van een interne-controleorgaan voor een periode van twee tot vijf jaar wordt benoemd uit personen buiten de betrokken autoriteit (zoals voormalige rechters, professoren) ([260]), alleen om gegronde redenen kan worden ontslagen (bijvoorbeeld wanneer hij om gezondheidsredenen niet in staat is zijn taken uit te voeren, of wanneer tegen hem een tuchtmaatregel is genomen) ([261]) en dat zijn onafhankelijkheid zoveel mogelijk wordt gewaarborgd ([262]). Op het belemmeren van een interne controle staan administratieve geldboeten ([263]). Controleverslagen (die aanbevelingen, verzoeken om tuchtmaatregelen en verzoeken om schadevergoeding of correctie kunnen bevatten) worden meegedeeld aan het hoofd van de betrokken overheidsinstantie en aan de Controle- en Inspectieraad (*Board of Audit and Inspection*, hierna "BAI" genoemd) ([264]), en worden in het algemeen openbaar gemaakt ([265]). De resultaten van de uitvoering van het verslag moeten ook worden meegedeeld aan de BAI ([266]) (zie overweging 173 over de toezichthoudende rol en bevoegdheden van de BAI).

(171) Ten tweede ziet de PIPC erop toe dat de gegevensverwerking door strafrechtelijke handhavingsinstanties in overeenstemming is met de PIPA en met andere wetten die de persoonlijke levenssfeer van personen beschermen, met inbegrip van de wetten die de verzameling van (elektronisch) bewijsmateriaal met het oog op de handhaving van het strafrecht regelen, zoals beschreven in punt 3.2.1 ([267]). Aangezien het toezicht van de PIPC zich uitstrekt tot de rechtmatigheid en behoorlijkheid van de verzameling en verwerking van gegevens (artikel 3, lid 1, PIPA), die worden geschonden indien toegang wordt verkregen tot persoonsgegevens en zij worden gebruikt in strijd met deze wetten ([268]), kan de PIPC ook nagaan of de in punt 3.2.1. beschreven beperkingen en waarborgen worden nageleefd en kan zij de naleving ervan afdwingen ([269]). Bij de uitoefening van deze toezichthoudende rol kan de PIPC gebruik maken van al haar corrigerende en onderzoeksbevoegdheden, zoals uitvoerig beschreven in punt 2.4.2. Reeds vóór de recente hervorming van de PIPA (d.w.z. in haar vorige toezichthoudende rol voor de publieke sector) heeft de PIPC verschillende activiteiten van toezicht uitgevoerd op de verwerking van persoonsgegevens door strafrechtelijke handhavingsinstanties, bv. in het kader van het verhoor van verdachten (zaak nr. 2013-16 van 26 augustus 2013), met betrekking tot het verstrekken van kennisgevingen aan personen over het opleggen van administratieve geldboeten (zaak nr. 2015-02-04 van 26 januari 2015), het delen van gegevens met andere autoriteiten (zaak nr. 2018-15-146 van 9 juli 2018, zaak nr. 2018-25-308 van 10 december 2018; zaak nr. 2019-02-015 van 29 januari 2019), het verzamelen van vingerafdrukken of foto's (zaak nr. 2019-17-273 van 9 september 2019), het gebruik van drones (zaak nr. 2020-01-004 van 13 januari 2020). In die zaken onderzocht de PIPC de naleving van verschillende bepalingen van de PIPA (bv. de rechtmatigheid van de verwerking, de beginselen van doelbinding en minimale verwerking van de gegevens), maar ook van relevante bepalingen van andere wetten, zoals het wetboek van strafvordering, en deed zij, waar nodig, aanbevelingen om de verwerking in overeenstemming te brengen met de gegevensbeschermingsvoorschriften.

(172) Ten derde is er onafhankelijk toezicht door de Nationale Mensenrechtencommissie (*National Human Rights Commission*, hierna "NHRC" genoemd) ([270]), die schendingen van het recht op privacy en het recht op briefgeheim kan onderzoeken als onderdeel van haar algemene mandaat voor de bescherming van de grondrechten van de artikelen 10 tot en met 22 van de grondwet. De NHRC bestaat uit elf commissarissen die aan specifieke kwalificaties moeten voldoen ([271]) en die door de president worden benoemd volgens bij wet vastgestelde procedures. Met name worden vier commissarissen benoemd op voordracht van de Nationale Vergadering, vier op voordracht van de president en drie op voordracht van de opperrechter van het Hooggerechtshof ([272]). De voorzitter wordt door de president benoemd uit de commissarissen en moet worden bevestigd door de Nationale Vergadering ([273]). De commissarissen (met inbegrip van de voorzitter) worden benoemd voor een hernieuwbare

([259]) Zie punt 2.3.1 van bijlage II. Zie ook https://www.police.go.kr/eng/knpa/org/org01.jsp
([260]) Evenzo worden controleurs benoemd op basis van specifieke voorwaarden die in de wet zijn vastgelegd, zie de artikelen 16 e.v. van de Wet inzake controles in de publieke sector.
([261]) Artikelen 8 tot en met 11 van de Wet inzake controles in de publieke sector.
([262]) Artikel 7 van de Wet inzake controles in de publieke sector.
([263]) Artikel 41 van de Wet inzake controles in de publieke sector.
([264]) Artikel 23, lid 1, van de Wet inzake controles in de publieke sector.
([265]) Artikel 26 van de Wet inzake controles in de publieke sector.
([266]) Artikel 23, lid 3, van de Wet inzake controles in de publieke sector.
([267]) Zie artikel 7-8, leden 3 en 4, en artikel 7-9, lid 5, PIPA.
([268]) Zie Kennisgeving nr. 2021-5 van de PIPC, deel 6 (bijlage I).
([269]) Zie ook punt 2.3.4 van bijlage II.
([270]) Artikel 1 van de Wet inzake de Mensenrechtencommissie ("NHRC-wet").
([271]) Om te worden benoemd, moet een commissaris 1) ten minste tien jaar werkzaam zijn geweest aan een universiteit of een erkend onderzoeksinstituut, op ten minste het niveau van geassocieerd hoogleraar; 2) gedurende ten minste tien jaar een functie hebben bekleed als rechter, openbaar aanklager of advocaat; 3) zich gedurende ten minste tien jaar met mensenrechten hebben bezighouden (bv. voor een non-profit-, niet-gouvernementele of internationale organisatie), of 4) zijn aanbevolen door groeperingen uit het maatschappelijk middenveld (artikel 5, lid 3, van de NHRC-wet). Bovendien is het de commissarissen na hun benoeming verboden tegelijkertijd een functie te bekleden in de Nationale Vergadering, lokale raden, of de staats- of lokale overheid (als ambtenaar), zie artikel 10 van de NHRC-wet.
([272]) Artikel 5, leden 1 en 2, van de NHRC-wet.
([273]) Artikel 5, lid 5, van de NHRC-wet.

termijn van drie jaar en kunnen alleen worden ontslagen wanneer zij tot een gevangenisstraf zijn veroordeeld of niet langer in staat zijn hun taken uit te voeren als gevolg van langdurige fysieke of mentale zwakte (in dat geval moet twee derde van de commissarissen instemmen met het ontslag) ([274]). In het kader van een onderzoek kan de NHRC verzoeken om overlegging van relevant materiaal, inspecties uitvoeren en personen dagvaarden om te getuigen ([275]). Wat de corrigerende bevoegdheden betreft, kan de NHRC (openbare) aanbevelingen doen om specifieke beleidslijnen en praktijken te verbeteren of te corrigeren, waarop de overheidsinstanties moeten reageren met een voorstel voor een uitvoeringsplan ([276]). Indien de betrokken instantie geen gevolg geeft aan deze aanbevelingen, moet zij de commissie daarvan in kennis stellen ([277]), die op haar beurt dit nalaten kan bekendmaken aan de Nationale Vergadering, en/of openbaar kan maken. Volgens de officiële verklaring van de Koreaanse regering (punt 2.3.5 van bijlage II) leven de Koreaanse autoriteiten de aanbevelingen van de NHRC over het algemeen na en zijn zij zeer gestimuleerd om dit te doen aangezien de uitvoering hiervan wordt beoordeeld als onderdeel van een algemene, doorlopende evaluatie onder het gezag van het kabinet van de premier. Uit de jaarlijkse cijfers over haar activiteiten blijkt dat de NHRC actief toezicht houdt op de activiteiten van de strafrechtelijke handhavingsinstanties, hetzij op basis van individuele verzoeken, hetzij door middel van onderzoek ambtshalve ([278]).

(173) Ten vierde wordt het algemene toezicht op de wettigheid van de activiteiten van overheidsinstanties uitgeoefend door de BAI, die de inkomsten en uitgaven van de staat onderzoekt, maar ook meer in het algemeen toeziet op de naleving van de plichten van overheidsinstanties met het oog op de verbetering van de werking van het openbaar bestuur ([279]). De BAI is formeel opgericht onder de president van de Republiek Korea, maar behoudt een onafhankelijke status wat zijn taken betreft ([280]). Bovendien is de raad volledig onafhankelijk wat betreft de benoeming, het ontslag en de organisatie van zijn personeel en het opstellen van zijn begroting ([281]). De BAI bestaat uit een voorzitter (benoemd door de president, met instemming van de Nationale Vergadering) ([282]) en zes commissarissen (op aanbeveling van de voorzitter benoemd door de president) ([283]), die moeten voldoen aan specifieke, bij wet vastgestelde kwalificaties ([284]) en alleen kunnen worden ontslagen in geval van afzetting, veroordeling tot gevangenisstraf of onvermogen om hun taken uit te voeren als gevolg van langdurige geestelijke of lichamelijke zwakheid ([285]). De BAI voert jaarlijks een algemene controle uit, maar kan ook specifieke controles uitvoeren in verband met zaken die van bijzonder belang zijn. Bij het uitvoeren van een controle of inspectie kan de BAI verzoeken om overlegging van documenten en om de aanwezigheid van bepaalde personen ([286]). De BAI kan aanbevelingen doen, om tuchtmaatregelen verzoeken of een strafklacht indienen ([287]).

(174) Tot slot oefent de Nationale Vergadering parlementair toezicht uit op overheidsinstanties door middel van onderzoeken en inspecties ([288]) van hun activiteiten ([289]). Zij kan om de openbaarmaking van documenten verzoeken, de verschijning van getuigen afdwingen ([290]), corrigerende maatregelen aanbevelen (indien zij tot de

([274]) Artikelen 7, lid 1, en 8, van de NHRC-wet.

([275]) Artikel 36 van de NHRC-wet. Overeenkomstig artikel 6, lid 7, van de wet kan het overleggen van materiaal of artikelen worden geweigerd indien daardoor de staatsgeheimhouding zou worden geschaad, wat een aanzienlijk effect zou kunnen hebben op de staatsveiligheid of de diplomatieke betrekkingen, of een ernstige belemmering zou vormen voor een strafrechtelijk onderzoek of een lopende gerechtelijke procedure. In dergelijke gevallen kan de commissie het hoofd van de betrokken instantie (die te goeder trouw moet handelen) om nadere informatie verzoeken, wanneer dat nodig is om te kunnen beoordelen of de weigering tot informatieverstrekking gerechtvaardigd is.

([276]) Artikel 25, leden 1 en 3, van de NHRC-wet.

([277]) Artikel 25, lid 4, van de NHRC-wet.

([278]) Tussen 2015 en 2019 ontving de NHRC bijvoorbeeld jaarlijks tussen 1 380 en 1 699 verzoekschriften tegen strafrechtelijke handhavingsinstanties en nam zij een even hoog aantal in behandeling (zo behandelde zij in 2018 1 546 klachten tegen de politie en in 2019 1 249 klachten); zij voerde ook ambtshalve verscheidene onderzoeken uit, zoals nader is beschreven in het NHRC-jaarverslag 2018 (beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) en het jaarverslag 2019 (beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Artikelen 20 en 24 van de Wet inzake de Controle- en Inspectieraad ("BAI-wet"). Zie punt 2.3.2 van bijlage II.

([280]) Artikel 2, lid 1, van de BAI-wet.

([281]) Artikel 2, lid 2, van de BAI-wet.

([282]) Artikel 4, lid 1, van de BAI-wet.

([283]) Artikelen 5, lid1, en 6, van de BAI-wet.

([284]) Bijvoorbeeld, gedurende ten minste tien jaar rechter, openbaar aanklager of advocaat zijn geweest, gedurende ten minste acht jaar als ambtenaar of hoogleraar of in een hogere functie aan een universiteit hebben gewerkt, of gedurende ten minste tien jaar in een beursgenoteerde onderneming of overheidsinstelling hebben gewerkt (waarvan minstens vijf jaar als leidinggevend functionaris), zie artikel 7 van de BAI-wet. Daarnaast is het de commissarissen verboden deel te nemen aan politieke activiteiten, en gelijktijdig functies te bekleden in de Nationale Vergadering, bestuursinstanties, organisaties die onderworpen zijn aan controle en inspectie door de BAI of een andere bezoldigde functie of positie te vervullen (artikel 9 van de BAI-wet).

([285]) Artikel 8 van de BAI-wet.

([286]) Zie bv. artikel 27 van de BAI-wet.

([287]) Artikelen 24 en 31 tot en met 35 van de BAI-wet.

([288]) Artikel 128 van de Wet inzake de Nationale Vergadering en de artikelen 2, 3 en 15 van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie. Dit omvat jaarlijkse inspecties van overheidszaken als geheel, maar ook onderzoeken van specifieke zaken.

([289]) Zie punt 2.2.3 van bijlage.

([290]) Artikel 10, lid 1, van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie. Zie ook artikelen 128 en 129 van de Wet inzake de Nationale Vergadering.

conclusie komt dat onwettige of ongepaste activiteiten hebben plaatsgevonden) ([291]) en de resultaten van haar bevindingen openbaar maken ([292]). Wanneer de Nationale Vergadering verlangt dat er corrigerende maatregelen worden genomen — die bijvoorbeeld het toekennen van schadevergoeding, het nemen van tuchtmaatregelen of het verbeteren van interne procedures kunnen omvatten — is de betrokken overheidsinstantie verplicht onverwijld te handelen en over het resultaat verslag uit te brengen aan de Nationale Vergadering ([293]).

3.2.4. *Verhaalsmogelijkheden*

(175) Het Koreaanse systeem biedt verschillende (gerechtelijke) alternatieven om verhaal te halen, met inbegrip van de mogelijkheid om schadeloosstelling te verkrijgen.

(176) Ten eerste biedt de PIPA betrokkenen een recht op toegang, correctie, verwijdering en opschorting met betrekking tot de persoonsgegevens die worden verwerkt met het oog op de handhaving van het strafrecht ([294]).

(177) Ten tweede kunnen betrokkenen gebruik maken van de verschillende verhaalsmogelijkheden die de PIPA biedt, indien hun gegevens door een strafrechtelijke handhavingsinstantie zijn verwerkt in strijd met de PIPA of met de beperkingen en waarborgen voor het verzamelen van persoonsgegevens in andere wetten (d.w.z. het CPA of de CPPA, zie overweging 171). Natuurlijke personen kunnen met name een klacht indienen bij de PIPC (onder meer via het Privacy Call Centre van het Koreaans Agentschap voor internet en veiligheid ([295])) of het Comité voor geschillenbeslechting in verband met persoonsinformatie ([296]). Voor deze verhaalsmogelijkheden gelden geen verdere ontvankelijkheidsvereisten. Op grond van de Wet administratieve procesvoering kunnen natuurlijke personen voorts in beroep gaan tegen beslissingen of het uitblijven van maatregelen van de PIPC (zie overweging 132).

(178) Ten derde kan elk individu ([297]) een klacht indienen bij de NHRC over een schending van het recht op privacy- en gegevensbescherming door een Koreaanse strafrechtelijke handhavingsinstantie. De NHRC kan de correctie of verbetering aanbevelen van relevante wetten, instellingen, beleidslijnen of praktijken ([298]), of de uitvoering van rechtsmiddelen zoals bemiddeling ([299]), stopzetting van de schending van mensenrechten, schadeloosstelling en maatregelen om herhaling van dezelfde of soortgelijke schendingen te voorkomen ([300]). Volgens de officiële verklaring van de Koreaanse regering (punt 2.4.2 van bijlage II) kan dit ook het verwijderen van onrechtmatig verzamelde persoonsgegevens inhouden. Hoewel de NHRC niet bevoegd is om bindende beslissingen af te geven, biedt zij een informelere, goedkopere en gemakkelijker toegankelijke verhaalsmogelijkheid, met name omdat, zoals uiteengezet in punt 2.4.2 van bijlage II, voor het onderzoek van een klacht niet hoeft te worden aangetoond dat er sprake is van feitelijke schade ([301]). Dit zorgt ervoor dat klachten van natuurlijke personen over het verzamelen van hun gegevens kunnen worden onderzocht, zelfs als een persoon niet in staat is aan te tonen dat zijn/haar gegevens daadwerkelijk zijn verzameld (bv. omdat de betrokkene nog niet in kennis is gesteld). Uit de jaarlijkse activiteitenverslagen van de NHRC blijkt dat betrokkenen in de praktijk ook gebruik maken van deze mogelijkheid om activiteiten van strafrechtelijke handhavingsinstanties aan te vechten, onder meer met betrekking tot de behandeling van persoonsgegevens ([302]). Als een persoon niet tevreden is met het resultaat van een procedure voor de NHRC, kan hij of zij de besluiten van de NHRC (zoals een besluit om het onderzoek van

([291]) Artikel 16, lid 2, van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([292]) Artikel 12-2 van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([293]) Artikel 16, lid 3, van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([294]) Dit recht kan rechtstreeks bij de bevoegde instantie worden uitgeoefend, of niet rechtstreeks via de PIPC (artikel 35, lid 2, PIPA). Zoals meer in detail wordt beschreven in de overwegingen 76 tot en met 78, kunnen uitzonderingen op deze rechten alleen gelden wanneer dit noodzakelijk is om zwaarwegende (openbare) belangen te beschermen.
([295]) Artikel 62, PIPA.
([296]) Artikelen 40 tot en met 50 PIPA en de artikelen 48-2 tot en met 58 van het PIPA-uitvoeringsdecreet. Zie ook punt 2.4.1 van bijlage II.
([297]) Zoals uiteengezet in punt 2.4.2 van bijlage II, verwijst artikel 4 van de NHRC-wet weliswaar naar staatsburgers en buitenlanders die in de Republiek Korea verblijven, maar verwijst de term "verblijven" eerder naar een concept van jurisdictie dan van grondgebied. Wanneer de grondrechten van een buitenlander buiten Korea door nationale instellingen in Korea worden geschonden, kan die persoon dan ook een klacht indienen bij de NHRC. Dit zou het geval zijn wanneer er op onrechtmatige wijze door Koreaanse overheidsinstanties toegang wordt verkregen tot persoonsgegevens van een buitenlander die aan Korea zijn doorgegeven. Zie met name de uitleg op https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2
([298]) Artikel 44 van de NHRC-wet.
([299]) Een persoon kan ook verzoeken de klacht op te lossen door middel van bemiddeling, zie de artikelen 42 e.v. van de NRHC-wet.
([300]) Artikel 42, lid 4, van de NHRC-wet. Bovendien kan de NHRC dringende verlichtingsmaatregelen nemen in het geval van een aanhoudende inbreuk die waarschijnlijk schade zal veroorzaken, die moeilijk te verhelpen is wanneer er niets aan wordt gedaan, zie artikel 48 van de NHRC-wet.
([301]) Een klacht moet in beginsel binnen een jaar na de inbreuk worden ingediend, maar de NHRC kan nog steeds besluiten een klacht te onderzoeken die na die periode is ingediend, zolang de strafrechtelijke of civielrechtelijke verjaringstermijn niet is verstreken (artikel 32, lid 1, punt 4, van de NHRC-wet).
([302]) Zo heeft de NHRC in het verleden klachten behandeld en aanbevelingen gedaan met betrekking tot onrechtmatige inbeslagnemingen en een schending van de verplichting om betrokkenen te informeren over een inbeslagneming (zie blz. 80 en 91 van het NHRC-jaarverslag 2018, beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), alsook de onrechtmatige verwerking van persoonsinformatie door de politie, het Openbaar Ministerie en de rechter (zie blz. 157-158 van het NHRC-jaarverslag 2019, beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, en blz. 76 van het jaarverslag 2019, beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

een klacht niet voort te zetten ([303])) en aanbevelingen aanvechten voor de Koreaanse rechtbanken op grond van de Wet administratieve procesvoering (zie overweging 181) ([304]). Bovendien kan een procedure voor de NHRC de toegang tot de rechter verder vergemakkelijken, aangezien een persoon verder verhaal zou kunnen zoeken tegen de overheidsinstantie die zijn/haar gegevens onrechtmatig heeft verwerkt op basis van de bevindingen van de NHRC, overeenkomstig de in de overwegingen 181 tot en met 183 beschreven procedures.

(179) Tot slot zijn er verschillende voorzieningen in rechte beschikbaar, waarmee natuurlijke personen zich kunnen beroepen op de in punt 3.2.1 beschreven beperkingen en waarborgen om verhaal te halen ([305]).

(180) Met betrekking tot inbeslagnemingen (met inbegrip van gegevens) voorziet het CPA in de mogelijkheid om tegen de uitvoering van een bevel bezwaar aan te tekenen of deze aan te vechten door middel van een "quasiklacht", door bij de bevoegde rechter een verzoekschrift in te dienen met het verzoek tot nietigverklaring of wijziging van een beslissing van een openbaar aanklager of politieambtenaar ([306]).

(181) Meer in het algemeen kunnen natuurlijke personen het handelen ([307]) of nalaten ([308]) van overheidsinstanties (met inbegrip van strafrechtelijke handhavingsinstanties) aanvechten op grond van de Wet administratieve procesvoering ([309]). Administratieve maatregelen worden beschouwd als een "voor beroep vatbare beslissing" indien zij rechtstreeks van invloed zijn op de burgerrechten en -plichten ([310]), hetgeen, zoals de Koreaanse regering heeft bevestigd (punt 2.4.3 van bijlage II), het geval is voor maatregelen om persoonsgegevens te verzamelen, hetzij rechtstreeks (bijvoorbeeld door het onderscheppen van communicatie), hetzij door middel van bindende verzoeken om verstrekking (bijvoorbeeld aan een dienstverlener), hetzij door middel van verzoeken om vrijwillige medewerking. Een klacht op grond van de Wet administratieve procesvoering kan maar ontvankelijk zijn als een natuurlijke persoon een wettig belang heeft bij het instellen van de vordering ([311]). Volgens de rechtspraak van het Hooggerechtshof wordt onder "wettig belang" verstaan een "wettelijk beschermd belang", d.w.z. een direct en specifiek belang dat wordt beschermd door de wet- en regelgeving waarop administratieve beslissingen zijn gebaseerd (d.w.z. geen algemene, indirecte en abstracte belangen van het publiek) ([312]). Natuurlijke personen hebben een dergelijk wettig belang in geval van inbreuk op de beperkingen en waarborgen die van toepassing zijn op het verzamelen van hun persoonsgegevens met het oog op de handhaving van het strafrecht (op grond van specifieke wetten of de PIPA). Op grond van de Wet administratieve procesvoering kan een rechter beslissen een onwettige beslissing in te trekken of te wijzigen, een verklaring van nietigheid af te geven (d.w.z. een verklaring dat de beslissing geen rechtsgevolgen heeft of niet in de rechtsorde is voorzien) of een verklaring dat een nalatigheid onwettig is ([313]). Een definitieve uitspraak op grond van de Wet administratieve procesvoering is bindend voor de partijen ([314]).

([303]) Indien de NHRC bijvoorbeeld in uitzonderlijke gevallen niet in staat is om bepaalde materialen of faciliteiten te inspecteren omdat hiermee staatsgeheimen zijn gemoeid die een aanzienlijke invloed kunnen hebben op de staatsveiligheid of diplomatieke betrekkingen, of wanneer de inspectie een ernstige belemmering zou vormen voor een strafrechtelijk onderzoek of lopende gerechtelijke procedure, en indien dit de NHRC verhindert om het onderzoek uit te voeren dat nodig is om de gegrondheid van het ontvangen verzoek te beoordelen, zal de NHRC de persoon in kwestie informeren over de redenen waarom de klacht werd afgewezen, overeenkomstig artikel 39 van de NHRC-wet. In dit geval kan de betrokkene de beslissing van de NHRC aanvechten op grond van de Wet administratieve procesvoering.

([304]) Zie bv. Beslissing 2007Nu27259 van het Hof van Seoul van 18 april 2008, bevestigd bij Beslissing 2008Du7854 van het Hooggerechtshof van 9 oktober 2008; Beslissing 2017Nu69382 van het Hof van Seoul van 2 februari 2018.

([305]) Zie punt 2.4.3 van bijlage II.

([306]) Artikel 417 CPA, juncto artikel 414, lid 2, CPA. Zie ook Beslissing nr. 97Mo66 van het Hooggerechtshof van 29 september 1997.

([307]) De Wet administratieve procesvoering spreekt van een "beslissing", dat wil zeggen de uitoefening of de weigering van de uitoefening van een overheidsbevoegdheid in een specifiek geval.

([308]) In het kader van de Wet administratieve procesvoering gaat het om het langdurig nalaten van een bestuursinstantie om een bepaalde beslissing te nemen, wat in strijd is met een wettelijke verplichting daartoe.

([309]) Een administratief beroep kan in eerste instantie worden ingesteld bij commissies van administratief beroep die door bepaalde overheidsinstanties zijn ingesteld (bv. de Nationale Inlichtingendienst, de NHRC), of bij de Centrale Commissie voor hoger beroep in bestuurszaken die is ingesteld door de Commissie voor corruptiebestrijding en burgerrechten (artikel 6 van de Wet inzake hoger beroep in bestuurszaken, en artikel 18, lid 1, van de Wet administratieve procesvoering), als een informelere verhaalsmogelijkheid. Een vordering kan echter ook rechtstreeks bij de Koreaanse rechter worden ingesteld op grond van de Wet administratieve procesvoering.

([310]) Beslissing 98Du18435 van het Hooggerechtshof van 22 oktober 1999, Beslissing 99Du1113 van het Hooggerechtshof van 8 september 2000, en Beslissing 2010Du3541 van het Hooggerechtshof van 27 september 2012.

([311]) Artikelen 12, 35 en 36 van de Wet administratieve procesvoering. Daarnaast moet een verzoek tot intrekking/wijziging van een beslissing en een verzoek om de onrechtmatigheid van een nalatigheid te bevestigen, worden ingediend binnen negentig dagen na de datum waarop de betrokkene kennis heeft gekregen van de beslissing/nalatigheid en in beginsel niet later dan één jaar na de datum waarop de beslissing is genomen of de nalatigheid heeft plaatsgevonden, tenzij er gerechtvaardigde redenen zijn om dat niet te doen (artikelen 20 en 38, lid 2, van de Wet administratieve procesvoering). Het begrip "gerechtvaardigde redenen" is door het Hooggerechtshof ruim uitgelegd en vereist dat wordt beoordeeld of het, gelet op alle omstandigheden van het geval, maatschappelijk aanvaardbaar is dat een klacht te laat wordt ingediend (Beslissing 90Nu6521 van het Hooggerechtshof van 28 juni 1991). Zoals de Koreaanse regering in punt 2.4.3 van bijlage II heeft bevestigd, gaat het hierbij onder meer (maar niet uitsluitend) om redenen voor de vertraging die niet aan de betrokken partij kunnen worden toegerekend (d.w.z. situaties waarop de klager geen invloed heeft, bijvoorbeeld wanneer hij of zij niet in kennis is gesteld van het verzamelen van zijn of haar persoonsinformatie) of om overmacht (bijvoorbeeld een natuurramp, oorlog).

([312]) Beslissing nr. 2006Du330 van het Hooggerechtshof van zondag 26 maart 2006.

([313]) Artikelen 2 en 4 van de Wet administratieve procesvoering.

([314]) Artikel 30, lid 1, van de Wet administratieve procesvoering.

(182) Naast het aanvechten van overheidsoptreden via administratieve procesvoering, kunnen betrokkenen ook een grondwettelijke klacht indienen bij het Grondwettelijk Hof met betrekking tot elke inbreuk op hun fundamentele rechten als gevolg van de uitoefening of niet-uitoefening van overheidsbevoegdheid (met uitzondering van rechterlijke beslissingen) ([315]). Indien andere verhaalsmogelijkheden beschikbaar zijn, moeten deze eerst worden uitgeput. Volgens de rechtspraak van het Grondwettelijk Hof kunnen buitenlandse onderdanen een grondwettelijke klacht indienen voor zover hun grondrechten door de Koreaanse grondwet worden erkend (zie de uitleg in punt 1.1) ([316]). Het Grondwettelijk Hof kan de uitoefening van de overheidsbevoegdheid die de inbreuk heeft veroorzaakt, ongeldig verklaren of bevestigen dat een bepaalde nalatigheid ongrondwettelijk is ([317]). In dat geval is de betrokken overheid verplicht maatregelen te nemen om zich naar de beslissing van het Hof te voegen.

(183) Daarnaast kunnen betrokkenen bij de Koreaanse rechtbanken schadevergoeding verkrijgen. Dit omvat in de eerste plaats de mogelijkheid om schadevergoeding te vorderen voor inbreuken op de PIPA door strafrechtelijke handhavingsinstanties, overeenkomstig artikel 39 (zie ook overweging 135). Meer in het algemeen kunnen betrokkenen op grond van de Wet inzake overheidscompensatie (zie ook overweging 135) een vergoeding eisen van de schade die ambtenaren bij de uitoefening van hun ambt in strijd met de wet hebben toegebracht ([318]).

(184) De in de overwegingen 176 tot en met 183 genoemde mechanismen bieden betrokkenen doeltreffende administratieve en gerechtelijke verhaalsmogelijkheden, waardoor zij met name hun rechten kunnen doen gelden, waaronder het recht op inzage in hun persoonsgegevens of op rectificatie of wissing van die gegevens.

3.3. **Toegang van en gebruik door de Koreaanse overheidsdiensten ten behoeve van de nationale veiligheid**

(185) De Koreaanse wet omvat een aantal beperkingen en waarborgen met betrekking tot de toegang tot en het gebruik van persoonsgegevens met het oog op de nationale veiligheid, en voorziet in toezichts- en verhaalsmechanismen op dit gebied die in overeenstemming zijn met de in de overwegingen 141 tot en met 143 van dit besluit bedoelde vereisten. De voorwaarden waaronder deze toegang kan plaatsvinden en de waarborgen die van toepassing zijn op het gebruik van deze bevoegdheden worden in de volgende punten in detail beoordeeld.

3.3.1. *Rechtsgrondslagen, beperkingen en waarborgen*

(186) In de Republiek Korea kunnen persoonsgegevens ten behoeve van de nationale veiligheid worden geraadpleegd op basis van de CPPA, de TBA en de Wet inzake terrorismebestrijding ter bescherming van de burgers en de openbare veiligheid ("Wet terrorismebestrijding") ([319]). De belangrijkste autoriteit ([320]) met bevoegdheden op het gebied van de nationale veiligheid is de Nationale Inlichtingendienst (*National Intelligence Service*, "NIS") ([321]). De verzameling en het gebruik van persoonsgegevens door de Nationale Inlichtingendienst moeten voldoen aan de

([315]) Artikel 68, lid 1, van de Wet op het Grondwettelijk Hof. Grondwettelijke klachten moeten worden ingediend binnen negentig dagen nadat de betrokkene kennis heeft gekregen van de inbreuk, en binnen één jaar nadat deze zich heeft voorgedaan. Zoals ook uiteengezet in punt 2.4.3 van bijlage II zal, aangezien de procedure van de Wet administratieve procesvoering op grond van artikel 40 van de Wet op het Grondwettelijk Hof wordt toegepast op geschillen in het kader van de Wet op het Grondwettelijk Hof, een klacht nog steeds ontvankelijk zijn indien er "gerechtvaardigde redenen" zijn, zoals uitgelegd volgens de in voetnoot 312 beschreven rechtspraak van het Hooggerechtshof. Indien eerst andere rechtsmiddelen moeten worden uitgeput, moet een grondwettelijke klacht worden ingediend binnen dertig dagen na de definitieve beslissing over een dergelijk rechtsmiddel (artikel 69 van de Wet op het Grondwettelijk Hof).

([316]) Beslissing nr. 99HeonMa194 van het Grondwettelijk Hof van 29 november 2001.

([317]) Artikel 75, lid 3, van de Wet op het Grondwettelijk Hof.

([318]) Artikel 2, lid 1, van de Wet inzake overheidscompensatie.

([319]) Zie punt 3.1 van bijlage II.

([320]) In uitzonderlijke omstandigheden mogen ook de politie en het Openbaar Ministerie persoonsinformatie verzamelen ten behoeve van de nationale veiligheid (zie voetnoot 327 en punt 3.2.1.2 van bijlage II). Daarnaast heeft de Koreaanse militaire inlichtingendienst (het Commando ondersteuning defensie en veiligheid, dat onder het ministerie van Defensie valt) bevoegdheden op het gebied van de nationale veiligheid. Zoals uiteengezet in punt 3.1 van bijlage II is deze dienst echter alleen verantwoordelijk voor militaire inlichtingen en voert hij alleen surveillance uit op burgers wanneer dit noodzakelijk is voor de uitvoering van zijn militaire taken. Met name kan de dienst alleen onderzoek doen naar militair personeel, civiele werknemers van de krijgsmacht, personen in militaire opleiding, personen in militaire reserve- of rekruteringsdienst, en krijgsgevangenen (artikel 1 van de Wet op de militaire rechtbank). Bij het verzamelen van communicatiegegevens met het oog op de nationale veiligheid is het Commando ondersteuning defensie en veiligheid onderworpen aan de beperkingen en waarborgen die zijn vastgelegd in de CPPA en het bijbehorende uitvoeringsdecreet.

([321]) De Nationale Inlichtingendienst heeft tot taak informatie over het buitenland te verzamelen, samen te stellen en te verspreiden (d. w.z. algemene informatie over trends en ontwikkelingen met betrekking tot het buitenland, of de activiteiten van overheidsactoren); inlichtingen met betrekking tot de bestrijding van spionage (met inbegrip van militaire en industriële spionage), terrorisme en de activiteiten van internationale criminele organisaties; inlichtingen over bepaalde soorten strafbare feiten die gericht zijn tegen de openbare en de nationale veiligheid (bv. binnenlands oproer, buitenlandse agressie) en inlichtingen in verband met de taak om de cyberveiligheid te waarborgen en cyberaanvallen en -dreigingen te voorkomen of te bestrijden (artikel 4, lid 2, van de NIS-wet). Zie ook punt 3.1 van bijlage II.

toepasselijke wettelijke voorschriften (waaronder de PIPA en de CPPA) ([322]) en aan de algemene richtsnoeren die door de president zijn opgesteld en door de Nationale Vergadering zijn getoetst ([323]). Als algemeen beginsel geldt dat de Nationale Inlichtingendienst politieke neutraliteit moet behouden en de vrijheid en rechten van natuurlijke personen moet beschermen ([324]). Bovendien mag het personeel van de Nationale Inlichtingendienst geen misbruik maken van zijn officiële bevoegdheid om instellingen, organisaties of personen te dwingen iets te doen waartoe zij (wettelijk) niet verplicht zijn, noch mag het iemand belemmeren bij de uitoefening van zijn of haar rechten ([325]).

3.3.1.1. Toegang tot communicatiegegevens

(187) Op basis van de CPPA mogen de Koreaanse overheidsinstanties ([326]) communicatiebevestigende gegevens (d.w.z. de datum van de telecommunicatie, de begin- en eindtijd ervan, het aantal uitgaande en inkomende gesprekken, alsmede het abonneenummer van de andere partij, de gebruiksfrequentie, logbestanden over het gebruik van telecommunicatiediensten en locatiegegevens, zie overweging 155) en de inhoud van de communicatie (door middel van communicatiebeperkende maatregelen, zie overweging 155) verzamelen met het oog op de nationale veiligheid (zoals bepaald in het mandaat van de Nationale Inlichtingendienst, zie voetnoot 322 hierboven). Deze bevoegdheden strekken zich uit tot twee soorten informatie: 1) communicatie waarbij een partij of beide partijen Koreaans onderdaan zijn ([327]), en 2) communicatie van a) landen die de Republiek Korea vijandig gezind zijn; b) buitenlandse instanties, groepen of onderdanen die ervan verdacht worden betrokken te zijn bij anti-Koreaanse activiteiten ([328]), of c) leden van groepen die op het Koreaanse schiereiland opereren maar zich feitelijk aan de soevereiniteit van de Republiek Korea onttrekken en hun in het buitenland gevestigde overkoepelende groepen ([329]). Communicatie van EU-onderdanen die op grond van dit besluit uit de Europese Unie aan de Republiek Korea wordt doorgegeven, kan derhalve uit hoofde van de CPPA alleen ten behoeve van de nationale veiligheid worden verzameld (onder de in de overwegingen 188 tot en met 192 genoemde voorwaarden) wanneer het gaat om communicatie tussen een EU-onderdaan en een Koreaans onderdaan, of, indien het communicatie betreft tussen uitsluitend niet-Koreaanse onderdanen, wanneer deze onder een van de drie genoemde categorieën 2a), b) en c) valt.

(188) In beide situaties mogen alleen communicatiebevestigende gegevens worden verzameld ter voorkoming van bedreigingen van de nationale veiligheid ([330]), terwijl communicatiebeperkende maatregelen alleen mogen worden genomen wanneer er een ernstig risico voor de nationale veiligheid bestaat en de verzameling noodzakelijk is om dit te voorkomen ([331]). Voorts mag uitsluitend als laatste redmiddel toegang worden verkregen tot de inhoud van de communicatie en moet ernaar worden gestreefd de inbreuk op de communicatieprivacy tot een minimum te beperken ([332]), zodat deze evenredig blijft aan het nagestreefde doel van nationale veiligheid. Het verzamelen van zowel de inhoud van de communicatie als de communicatiebevestigende gegevens mag slechts hoogstens vier maanden worden voortgezet en moet onmiddellijk worden stopgezet wanneer het nagestreefde doel eerder wordt bereikt ([333]). Indien de desbetreffende voorwaarden vervuld blijven, kan de periode met voorafgaande toestemming van een rechter (voor de in overweging 189 beschreven maatregelen) of van de president (voor de in overweging 190 beschreven maatregelen) ([334]) met maximaal vier maanden worden verlengd.

(189) Dezelfde procedurele waarborgen zijn van toepassing op het verzamelen van communicatiebevestigende gegevens en de inhoud van de communicatie ([335]). Met name wanneer ten minste een van de bij de communicatie betrokken personen een Koreaans onderdaan is, moet de inlichtingendienst een schriftelijk verzoek indienen bij het Bureau van de procureur-generaal, dat op zijn beurt een bevel moet aanvragen bij een hooggeplaatste

([322]) Zie ook de artikelen 14, 22 en 23 van de NIS-wet.
([323]) Artikel 4, lid 2, van de NIS-wet.
([324]) Artikel 3, lid 1, artikel 6, lid 2, en de artikelen 11 en 21 van de NIS-wet. Zie ook de regels in verband met belangenconflicten, met name de artikelen 10 en 12 van de NIS-wet.
([325]) Artikel 13 van de NIS-wet.
([326]) Dit omvat de inlichtingendiensten (d.w.z. de Nationale Inlichtingendienst en het Commando ondersteuning defensie en veiligheid) en de politie/het Openbaar Ministerie.
([327]) Artikel 7, lid 1, punt 1, CPPA.
([328]) Zoals de Koreaanse regering in voetnoot 244 van bijlage II heeft uitgelegd, gaat het om activiteiten die een bedreiging vormen voor het bestaan en de veiligheid van de natie, de democratische orde of het voortbestaan en de vrijheid van het volk.
([329]) Artikel 7, lid 1, punt 2, CPPA.
([330]) Artikel 13-4 CPPA.
([331]) Artikel 7, lid 1, CPPA.
([332]) Artikel 3, lid 2, CPPA. Bovendien moeten de communicatiebeperkende maatregelen onmiddellijk worden stopgezet zodra zij niet langer noodzakelijk zijn, zodat de eventuele inbreuk op de communicatiegeheimen van de betrokkene tot een minimum wordt beperkt (artikel 2 van het CPPA-uitvoeringsdecreet).
([333]) Artikel 7, lid 2, CPPA.
([334]) Het verzoek om toestemming voor verlenging van de surveillancemaatregelen moet schriftelijk worden ingediend, met opgave van de redenen waarom om verlenging wordt verzocht en met overlegging van ondersteunend materiaal (artikel 7, lid 2, CPPA en artikel 5 van het CPPA-uitvoeringsdecreet).
([335]) Zie artikel 13-4, lid 2, CPPA en artikel 37, lid 4, van het CPPA-uitvoeringsdecreet, op grond waarvan de procedures die gelden voor het verzamelen van de inhoud van communicatie ook van toepassing zijn op het verzamelen van de communicatiebevestigende gegevens. Zie ook punt 3.2.1.1.1 van bijlage II.

rechter van het Hof ([336]). De CPPA bevat een lijst van de informatie die moet worden verstrekt in het verzoek aan de openbaar aanklager, de aanvraag voor het bevel en het bevel zelf, dat met name de motivering van het verzoek en de belangrijkste redenen voor verdenking, ondersteunend materiaal, alsmede informatie over het doel, het voorwerp (d.w.z. de betrokkene(n)), de reikwijdte en de duur van de voorgestelde maatregel omvat ([337]). Het verzamelen zonder bevel kan alleen plaatsvinden indien er sprake is van een samenzwering die een bedreiging vormt voor de nationale veiligheid en er een noodsituatie bestaat waardoor het onmogelijk is de bovengenoemde procedures te volgen ([338]). Maar ook in dat geval moet onmiddellijk nadat de maatregel is genomen, een verzoek om een rechterlijk bevel worden ingediend ([339]). De CPPA omschrijft dus duidelijk de reikwijdte van en de voorwaarden voor deze vormen van verzameling, en onderwerpt ze aan specifieke (procedurele) waarborgen (waaronder voorafgaande toestemming van de rechter), die ervoor zorgen dat het gebruik van dergelijke maatregelen beperkt blijft tot wat noodzakelijk en evenredig is. Bovendien sluit de eis om gedetailleerde informatie te verstrekken in zowel het verzoek om een bevel als het bevel zelf, de mogelijkheid van onbeperkte toegang uit.

(190) Voor communicatie tussen niet-Koreaanse onderdanen die onder een van de drie in overweging 187 genoemde specifieke categorieën vallen, moet een aanvraag worden ingediend bij de directeur van de Nationale Inlichtingendienst, die, na te hebben nagegaan of de voorgestelde maatregelen passend zijn, de president van de Republiek Korea om voorafgaande schriftelijke toestemming moet vragen ([340]). Het door de inlichtingendienst opgestelde verzoek moet dezelfde gedetailleerde informatie bevatten als een verzoek om een rechterlijk bevel (zie overweging 189), met name wat betreft de motivering van het verzoek en de belangrijkste redenen voor verdenking, ondersteunend materiaal en informatie over de doelstellingen, de betrokkene(n), de reikwijdte en de duur van de voorgestelde maatregelen ([341]). In noodsituaties ([342]) moet vooraf toestemming worden verkregen van de minister onder wie de betrokken inlichtingendienst ressorteert, hoewel de inlichtingendienst onmiddellijk nadat de noodmaatregelen zijn genomen de goedkeuring van de president moet vragen ([343]). Ook wat het verzamelen van communicatie tussen uitsluitend niet-Koreaanse onderdanen betreft, beperkt de CPPA derhalve het gebruik van dergelijke maatregelen tot hetgeen noodzakelijk en evenredig is, door duidelijk de beperkte categorieën personen af te bakenen die aan dergelijke maatregelen kunnen worden onderworpen en door gedetailleerde criteria vast te stellen die door inlichtingendiensten moeten worden aangetoond om een verzoek tot de verzameling van informatie te rechtvaardigen. Bovendien wordt zo opnieuw de mogelijkheid van onbeperkte toegang uitgesloten. Hoewel er geen sprake is van voorafgaande onafhankelijke goedkeuring van dergelijke maatregelen, is onafhankelijk toezicht achteraf wel gewaarborgd, met name door de PIPC en de NHRC (zie bijvoorbeeld de overwegingen 199 en 200).

(191) De CPPA legt voorts verscheidene aanvullende waarborgen op die bijdragen tot het toezicht achteraf en de toegang van personen tot doeltreffende voorzieningen in rechte vergemakkelijken. Ten eerste voorziet de CPPA met betrekking tot elke vorm van verzameling ten behoeve van de nationale veiligheid in verschillende registratie- en rapportageverplichtingen. Met name moeten inlichtingendiensten bij een verzoek om medewerking van particuliere exploitanten het rechterlijk bevel/de presidentiële toestemming of een kopie van de omslag van een verklaring van censuur in noodsituaties overleggen, die de betreffende entiteit in haar dossiers moet bewaren ([344]). Wanneer particuliere exploitanten worden gedwongen mee te werken, moeten zowel de verzoekende overheidsinstantie als de betrokken exploitant een administratie bijhouden met betrekking tot het doel en

([336]) Artikel 6, leden 5 en 8, en artikel 7, lid 1, punt 1, en lid 3, CPPA, juncto artikel 7, leden 3 en 4, van het CPPA-uitvoeringsdecreet.

([337]) Zie artikel 7, lid 3, en artikel 6, lid 4, CPPA (voor het verzoek van de inlichtingendienst), artikel 4 van het CPPA-uitvoeringsdecreet (voor het verzoek van de openbaar aanklager) en artikel 6, lid 6, en artikel 7, lid 3, CPPA (voor het bevel).

([338]) Artikel 8, CPPA.

([339]) Artikel 8, leden 2 en 8, CPPA. Indien binnen 36 uur nadat de maatregelen zijn genomen geen toestemming van de rechter is verkregen, moet de verzameling onmiddellijk worden stopgezet In gevallen waarin de surveillance binnen korte tijd wordt beëindigd, waardoor geen toestemming van de rechter kan worden gevraagd, moet het hoofd van het bevoegde Bureau van de procureur-generaal een door de inlichtingendienst opgestelde kennisgeving van noodmaatregelen sturen aan het hoofd van de bevoegde rechtbank, die op basis daarvan de rechtmatigheid van de verzameling kan toetsen (artikel 8, leden 5 en 7, CPPA). In deze kennisgeving moeten het doel, het voorwerp, de reikwijdte, de periode, de plaats van uitvoering en de methode van surveillance worden aangegeven, alsmede de redenen waarom geen verzoek is ingediend voordat de maatregel werd genomen (artikel 8, lid 6, CPPA). Meer in het algemeen mogen inlichtingendiensten alleen noodmaatregelen nemen overeenkomstig een "verklaring inzake censuur/aftapping in noodsituaties" en moeten zij een register bijhouden van dergelijke maatregelen (artikel 8, lid 4, CPPA).

([340]) Artikel 8, leden 1 en 2, van het CPPA-uitvoeringsdecreet.

([341]) Artikel 8, lid 3, van het CPPA-uitvoeringsdecreet, juncto artikel 6, lid 4, CPPA.

([342]) Dat wil zeggen, in gevallen waarin de maatregel gericht is op een samenzwering die de nationale veiligheid bedreigt, er onvoldoende tijd is om de goedkeuring van de president te verkrijgen en het niet nemen van noodmaatregelen de nationale veiligheid kan schaden (artikel 8, lid 8, CPPA).

([343]) Artikel 8, lid 9, CPPA. De verzameling moet onmiddellijk worden stopgezet indien de toestemming niet binnen 36 uur vanaf het tijdstip waarop de aanvraag is ingediend, wordt verkregen.

([344]) Artikel 9, lid 2, CPPA en artikel 12 van het CPPA-uitvoeringsdecreet. Zie artikel 13 van het CPPA-uitvoeringsdecreet over de mogelijkheid om de medewerking van postkantoren en aanbieders van telecommunicatiediensten af te dwingen. Particuliere exploitanten die worden verzocht informatie te verstrekken, kunnen dit weigeren wanneer het bevel/de toestemming of de verklaring inzake de censuur in noodsituaties betrekking heeft op de verkeerde identificator (bv. een telefoonnummer dat aan een andere persoon toebehoort dan de geïdentificeerde persoon). In ieder geval mogen zij geen wachtwoorden bekendmaken die voor communicatie worden gebruikt (artikel 9, lid 4, CPPA).

het voorwerp van de maatregelen, alsmede de datum van uitvoering ([345]). Bovendien moeten de inlichtingendiensten bij de directeur van de Nationale Inlichtingendienst verslag uitbrengen over de informatie die zij hebben verzameld en over het resultaat van de surveillance ([346]).

(192) Ten tweede moeten betrokkenen ervan in kennis worden gesteld dat hun gegevens worden verzameld (communicatiebevestigende gegevens of de inhoud van de communicatie) ten behoeve van de nationale veiligheid, indien het gaat om communicatie waarbij ten minste één van de partijen Koreaans onderdaan is ([347]). Deze kennisgeving moet schriftelijk geschieden binnen dertig dagen na de datum waarop de gegevensverzameling is beëindigd (ook wanneer de gegevens overeenkomstig de noodprocedure zijn verkregen) en mag alleen worden uitgesteld indien en zolang dit de nationale veiligheid in gevaar zou brengen of het leven en de fysieke veiligheid van personen zou schaden ([348]). Ongeacht deze kennisgeving hebben betrokkenen verschillende verhaalsmogelijkheden, zoals nader wordt toegelicht in punt 3.3.4.

3.3.1.2. Verzameling van informatie over terreurverdachten

(193) In de Wet terrorismebestrijding is bepaald dat de Nationale Inlichtingendienst gegevens mag verzamelen over terreurverdachten ([349]), overeenkomstig de beperkingen en waarborgen die in andere wetten zijn vastgelegd ([350]). De Nationale Inlichtingendienst kan met name communicatiegegevens (op basis van de CPPA) en andere persoonsinformatie (via een verzoek om vrijwillige verstrekking) verkrijgen ([351]). Met betrekking tot het verzamelen van communicatiegegevens (d.w.z. de inhoud van de communicatie of de communicatiebevestigende gegevens) gelden de beperkingen en waarborgen die in punt 3.3.1.1 zijn beschreven, met inbegrip van het vereiste van een door de rechter goedgekeurd bevel. Wat verzoeken om vrijwillige verstrekking van andere soorten persoonsgegevens van terreurverdachten betreft, moet de Nationale Inlichtingendienst voldoen aan de vereisten van de grondwet en de PIPA inzake noodzaak en evenredigheid (zie overweging 164) ([352]). Verwerkingsverantwoordelijken die dergelijke verzoeken ontvangen, kunnen daaraan op vrijwillige basis voldoen onder de voorwaarden van de PIPA (bijvoorbeeld overeenkomstig het beginsel van minimale gegevensverwerking en door het beperken van de gevolgen voor de persoonlijke levenssfeer van de betrokkene) ([353]). In dat geval moeten zij ook voldoen aan de uit Kennisgeving nr. 2021-5 voortvloeiende verplichting om de betrokkene hiervan in kennis te stellen (zie overweging 166).

([345]) Voor communicatiebeperkende maatregelen moeten dergelijke gegevens drie jaar worden bewaard, zie artikel 9, lid 3, CPPA en artikel 17, lid 2, van het CPPA-uitvoeringsdecreet. Met betrekking tot communicatiebevestigende gegevens moeten inlichtingendiensten registreren dat een verzoek om dergelijke gegevens is gedaan en moeten zij het schriftelijke verzoek zelf en de instelling die hiervan gebruik heeft gemaakt, registreren (artikel 13, lid 5, en artikel 13-4, lid 3, CPPA). Aanbieders van telecommunicatiediensten moeten gedurende zeven jaar een register bijhouden en tweemaal per jaar aan de minister van Wetenschap en ICT verslag uitbrengen over de frequentie van deze verstrekkingen (artikel 9, lid 3, CPPA, juncto artikel 13, lid 7, CPPA, en artikel 37, lid 4, en artikel 39 van het CPPA-uitvoeringsdecreet).

([346]) Artikel 18, lid 3, van het CPPA-uitvoeringsdecreet.

([347]) Artikel 9-2, lid 3, en artikel 13-4, CPPA. In de kennisgeving moet het volgende worden vermeld: 1) het feit dat de informatie is verzameld, 2) de uitvoerende instantie en 3) de uitvoeringsperiode.

([348]) Artikel 9-2, lid 4, CPPA. In dat geval moet de kennisgeving worden gedaan binnen dertig dagen vanaf het moment dat de redenen voor uitstel niet langer bestaan (zie artikel 13-4, lid 2, en artikel 9-2, lid 6, CPPA).

([349]) Dat wil zeggen, leden van een terroristische groepering (zoals aangeduid door de Verenigde Naties, zie artikel 2, lid 2, van de Wet terrorismebestrijding); personen die ideeën of tactieken van een terroristische groepering propageren en verspreiden, fondsen voor terrorisme werven of daaraan bijdragen, of zich bezighouden met andere activiteiten in het kader van de voorbereiding, samenzwering, propaganda of aanzetting tot terrorisme, of personen ten aanzien van wie er goede gronden bestaan om te vermoeden dat zij dergelijke activiteiten hebben verricht (artikel 2, lid 3, van de Wet terrorismebestrijding). "Terrorisme" wordt in artikel 2, lid 1, van de Wet terrorismebestrijding gedefinieerd als gedrag dat erop is gericht om de uitoefening van het gezag van de staat, een lokale overheid of een buitenlandse overheid (met inbegrip van internationale organisaties) te belemmeren, om deze tot actie te dwingen zonder dat daartoe een wettelijke verplichting bestaat, of om het publiek te bedreigen. Dergelijk gedrag kan bijvoorbeeld bestaan uit het doden, ontvoeren of gijzelen van een persoon; het kapen/in bezit nemen, vernietigen of beschadigen van een schip of vliegtuig; het gebruik van biochemische, explosieve of brandwapens met het oogmerk de dood, ernstig letsel of schade te veroorzaken, en het misbruiken van nucleaire of radioactieve stoffen.

([350]) Artikel 9, leden 1 en 3, van de Wet terrorismebestrijding.

([351]) Hoewel in de Wet terrorismebestrijding ook wordt verwezen naar de mogelijkheid om op basis van de Wet inzake immigratie en douane informatie te verzamelen over het binnenkomen in en het verlaten van de Republiek Korea, voorzien deze wetten momenteel niet in een dergelijke bevoegdheid (zie punt 3.2.2.1 van bijlage II). In ieder geval zouden zij in beginsel niet van toepassing zijn op gegevens die op grond van dit besluit worden doorgegeven, aangezien zij normaal gesproken betrekking hebben op informatie die rechtstreeks door de Koreaanse autoriteiten wordt verzameld (in plaats van toegang tot gegevens die eerder door de Europese Unie aan Koreaanse verwerkingsverantwoordelijken zijn doorgegeven). Daarnaast wordt in de Wet terrorismebestrijding de Wet inzake de verslaglegging over en het gebruik van bepaalde informatie over financiële transacties (ARUSFTI) genoemd als rechtsgrondslag voor het verzamelen van informatie over financiële transacties. Zoals in voetnoot 200 wordt uitgelegd, vallen de soorten gegevens die op basis van deze wet kunnen worden verkregen, echter niet binnen de werkingssfeer van dit besluit. Tot slot bepaalt de Wet terrorismebestrijding ook dat de Nationale Inlichtingendienst locatiegegevens kan verzamelen door middel van niet-bindende verzoeken, in welk geval de verstrekkers van de locatiegegevens deze informatie vrijwillig zouden kunnen verstrekken onder de voorwaarden van de PIPA (zoals beschreven in overweging 193) en de Wet locatiegegevens. Zoals ook in voetnoot 17 wordt uitgelegd, zouden locatiegegevens op basis van dit besluit echter niet door de Europese Unie aan Koreaanse verwerkingsverantwoordelijken worden doorgegeven, maar eerder binnen Korea worden voortgebracht.

([352]) Zie punt 3.2.2.2 van bijlage II.

([353]) Zie artikel 58, lid 4, PIPA, waarin is bepaald dat persoonsinformatie moet worden verwerkt in de mate die minimaal noodzakelijk is om het beoogde doel te bereiken, en artikel 3, lid 6, PIPA, waarin is bepaald dat de persoonsinformatie op zodanige wijze moet worden verwerkt dat de kans dat inbreuk wordt gemaakt op de persoonlijke levenssfeer van de persoon tot een minimum wordt herleid. Zie ook artikel 59, punten 2 en 3, PIPA, waarin is bepaald dat het de verwerkingsverantwoordelijken verboden is om zonder toestemming persoonsinformatie aan derden te verstrekken.

3.3.1.3. Verzoeken om vrijwillige verstrekking van abonneegegevens

(194) Op basis van de TBA mogen telecommunicatieaanbieders vrijwillig abonneegegevens verstrekken (zie overweging 163) op verzoek van een inlichtingendienst, die met de verzameling van dergelijke informatie beoogt om een bedreiging van de nationale veiligheid te voorkomen ([354]). Voor dergelijke verzoeken van de Nationale Inlichtingendienst gelden dezelfde beperkingen (die voortvloeien uit de grondwet, de PIPA en de TBA) als op het gebied van de handhaving van het strafrecht, zoals uiteengezet in overweging 164 ([355]). Telecommunicatieaanbieders zijn niet verplicht hieraan te voldoen en kunnen dit alleen doen onder de in de PIPA gestelde voorwaarden (met name overeenkomstig het beginsel van minimale gegevensverwerking en door het beperken van de gevolgen voor de persoonlijke levenssfeer van de persoon, zie ook overweging 193). Met betrekking tot het registreren van gegevens en de kennisgeving aan de betrokkene gelden dezelfde eisen als op het gebied van de handhaving van het strafrecht (zie overwegingen 165 en 166).

3.3.2. *Verder gebruik van de verzamelde informatie*

(195) Voor de verwerking van persoonsgegevens die door de Koreaanse autoriteiten zijn verzameld ten behoeve van de nationale veiligheid, gelden de beginselen van doelbinding (artikel 3, leden 1 en 2, PIPA), rechtmatigheid en behoorlijkheid van de verwerking (artikel 3, lid 1, PIPA), evenredigheid/minimale gegevensverwerking (artikel 3, leden 1 en 6, en artikel 58, PIPA), juistheid (artikel 3, lid 3, PIPA), transparantie (artikel 3, lid 5, PIPA), beveiliging (artikel 58, lid 4, PIPA) en opslagbeperking (artikel 58, lid 4, PIPA) ([356]). De eventuele verstrekking van persoonsgegevens aan derden (waaronder derde landen) kan alleen plaatsvinden in overeenstemming met deze beginselen (met name die van doelbinding en minimale gegevensverwerking), nadat is beoordeeld of de beginselen van noodzakelijkheid en evenredigheid (artikel 37, lid 2, van de grondwet) zijn geëerbiedigd, en met inachtneming van de gevolgen voor de rechten van de betrokken personen (artikel 3, lid 6, PIPA).

(196) Wat de inhoud van de communicatie en de communicatiebevestigende gegevens betreft, beperkt de CPPA het gebruik hiervan verder tot gerechtelijke procedures, wanneer een bij de communicatie betrokken partij zich daarop beroept in het kader van een vordering tot schadevergoeding of tot toegestaan gebruik krachtens andere wetgeving ([357]).

3.3.3. *Toezicht*

(197) De activiteiten van de Koreaanse nationale veiligheidsinstanties staan onder toezicht van verschillende organen ([358]).

(198) Ten eerste voorziet de Wet terrorismebestrijding in specifieke toezichtsmechanismen voor activiteiten van terrorismebestrijding, waaronder het verzamelen van gegevens over terreurverdachten. Op het niveau van de uitvoerende macht wordt op terrorismebestrijdingsactiviteiten met name toezicht gehouden door de Commissie terrorismebestrijding ([359]), waaraan de directeur van de Nationale Inlichtingendienst verslag moet uitbrengen over het onderzoeken en opsporen van terreurverdachten om informatie of materiaal te verzamelen dat nodig is voor terrorismebestrijdingsactiviteiten ([360]). Daarnaast houdt de mensenrechtenfunctionaris specifiek toezicht op de naleving van de grondrechten bij terrorismebestrijdingsactiviteiten ([361]). De mensenrechtenfunctionaris wordt benoemd door de voorzitter van de Commissie terrorismebestrijding uit personen die voldoen aan specifieke kwalificaties, die zijn vastgelegd in het uitvoeringsdecreet van de Wet terrorismebestrijding ([362]), voor een (verlengbare) termijn van twee jaar, en kan alleen op specifieke, beperkte gronden en om gegronde redenen uit zijn functie worden ontheven ([363]). Bij de uitoefening van zijn toezichtsfunctie kan de mensenrechtenfunctionaris

([354]) Artikel 83, lid 3, TBA.
([355]) Zie ook punt 3.2.3 van bijlage II.
([356]) Zie punt 1.2 van bijlage II.
([357]) Artikel 5, leden 1 en 2, artikel 12 en 13-5, CPPA.
([358]) Zie punt 3.3 van bijlage II.
([359]) Artikel 5, lid 3, van de Wet terrorismebestrijding. De Commissie wordt voorgezeten door de premier en bestaat uit verschillende ministers en hoofden van overheidsinstanties, zoals de ministers van Buitenlandse Zaken, Justitie, Nationale Defensie, en Binnenlandse Zaken en Veiligheid, de directeur van de Nationale Inlichtingendienst en de commissaris-generaal van de Nationale Politie (artikel 3, lid 1, van het uitvoeringsdecreet van de Wet terrorismebestrijding).
([360]) Artikel 9, lid 4, van de Wet terrorismebestrijding.
([361]) Artikel 7 van de Wet terrorismebestrijding.
([362]) Namelijk uit advocaten die ten minste tien jaar werkervaring hebben of deskundig zijn op het gebied van mensenrechten en (ten minste) tien jaar als universitair hoofddocent werkzaam zijn of zijn geweest, of die als hooggeplaatst ambtenaar werkzaam zijn geweest bij de staatsoverheid of bij plaatselijke overheden, of die ten minste tien jaar werkervaring hebben op het gebied van mensenrechten, bijvoorbeeld bij een niet-gouvernementele organisatie (artikel 7, lid 1, van het uitvoeringsdecreet van de Wet terrorismebestrijding).
([363]) Bijvoorbeeld wanneer hij/zij in staat van beschuldiging is gesteld in een strafzaak die verband houdt met zijn/haar functie, wanneer hij/zij vertrouwelijke informatie openbaar maakt, of wegens langdurige geestelijke of lichamelijke ongeschiktheid (artikel 7, lid 3, van het uitvoeringsdecreet van de Wet terrorismebestrijding).

algemene aanbevelingen doen ter verbetering van de bescherming van de mensenrechten ([364]) en specifieke aanbevelingen voor corrigerende maatregelen indien een schending van de mensenrechten is vastgesteld ([365]). De overheidsinstanties zijn verplicht de mensenrechtenfunctionaris te informeren over het gevolg dat aan zijn aanbevelingen is gegeven ([366]).

(199) Ten tweede houdt de PIPC toezicht op de naleving van de gegevensbeschermingsvoorschriften door de nationale veiligheidsinstanties, wat zowel de toepasselijke bepalingen van de PIPA (zie overweging 149) omvat als de beperkingen en waarborgen die gelden voor het verzamelen van persoonsgegevens op grond van andere wetten (de CPPA, de Wet terrorismebestrijding en de TBA, zie ook overweging 171) ([367]). Bij de uitoefening van deze toezichthoudende rol kan de PIPC gebruik maken van al haar corrigerende en onderzoeksbevoegdheden, zoals uitvoerig beschreven in punt 2.4.2.

(200) Ten derde zijn de activiteiten van de nationale veiligheidsinstanties onderworpen aan het onafhankelijke toezicht van de NHRC, overeenkomstig de in overweging 172 beschreven procedures ([368]).

(201) Ten vierde strekt de toezichtsfunctie van de Controle- en Inspectieraad zich ook uit tot de nationale veiligheidsinstanties, hoewel de Nationale Inlichtingendienst in uitzonderlijke omstandigheden kan weigeren bepaalde informatie of materiaal te verstrekken, namelijk wanneer deze staatsgeheimen vormen en openbaarmaking ervan ernstige gevolgen zou hebben voor de nationale veiligheid ([369]).

(202) Tot slot wordt het parlementaire toezicht op de activiteiten van de Nationale Inlichtingendienst uitgeoefend door de Nationale Vergadering (via een gespecialiseerde Inlichtingencommissie) ([370]). De CPPA voorziet in een specifieke toezichthoudende rol voor de Nationale Vergadering met betrekking tot het gebruik van communicatiebeperkende maatregelen ten behoeve van de nationale veiligheid ([371]). De Nationale Vergadering kan met name ter plaatse inspecties uitvoeren van afluisterapparatuur en kan zowel van de Nationale Inlichtingendienst als van telecommunicatie-exploitanten die de inhoud van communicatie hebben verstrekt, verlangen dat zij daarover verslag uitbrengen. De Nationale Vergadering kan ook haar algemene toezichtstaken uitoefenen (overeenkomstig de in overweging 174 beschreven procedures). De NIS-wet bepaalt dat de directeur van de Nationale Inlichtingendienst onverwijld moet reageren wanneer de Inlichtingencommissie om een verslag over een specifieke aangelegenheid verzoekt ([372]), met specifieke voorschriften voor bepaalde bijzonder gevoelige informatie. Concreet kan de directeur van de Nationale Inlichtingendienst alleen in uitzonderlijke omstandigheden weigeren te antwoorden of voor de Inlichtingencommissie te getuigen, namelijk wanneer het verzoek betrekking heeft op staatsgeheimen betreffende militaire, diplomatieke of Noord-Korea-gerelateerde aangelegenheden waarvan de openbaarmaking ernstige gevolgen zou kunnen hebben voor de "nationale lotsbestemming" van het land ([373]). In dat geval kan de Inlichtingencommissie de premier om uitleg vragen en als binnen zeven dagen geen uitleg wordt gegeven, mag het antwoord of de getuigenis niet worden geweigerd.

3.3.4. *Verhaalsmogelijkheden*

(203) Ook op het gebied van de nationale veiligheid biedt het Koreaanse systeem verschillende (gerechtelijke) alternatieven om verhaal te halen, met inbegrip van de mogelijkheid om schadeloosstelling te verkrijgen. Deze mechanismen bieden betrokkenen doeltreffende administratieve en gerechtelijke verhaalsmogelijkheden, waardoor zij met name hun rechten kunnen doen gelden, waaronder het recht op inzage in hun persoonsgegevens of op rectificatie of wissing van die gegevens.

(204) Ten eerste kunnen natuurlijke personen overeenkomstig artikel 3, lid 5, en artikel 4, leden 1, 3 en 4, PIPA, hun recht op toegang, correctie, verwijdering en opschorting uitoefenen ten aanzien van de nationale veiligheidsinstanties. In deel 6 van Kennisgeving nr. 2021-5 (bijlage I bij dit besluit) wordt verder verduidelijkt hoe deze rechten van toepassing zijn in de context van gegevensverwerking ten behoeve van de nationale veiligheid. Met

([364]) Artikel 8, lid 1, van het uitvoeringsdecreet van de Wet terrorismebestrijding.
([365]) Artikel 9, lid 1, van het uitvoeringsdecreet van de Wet terrorismebestrijding. De mensenrechtenfunctionaris beslist autonoom over het al dan niet vaststellen van aanbevelingen, maar is verplicht deze aanbevelingen te melden aan de voorzitter van de Commissie terrorismebestrijding.
([366]) Artikel 9, lid 2, van het uitvoeringsdecreet van de Wet terrorismebestrijding. Volgens de officiële verklaring van de Koreaanse regering zou het niet uitvoeren van een aanbeveling van de mensenrechtenfunctionaris worden doorverwezen naar de Commissie terrorismebestrijding, met inbegrip van de premier, hoewel er zich tot dusver geen gevallen hebben voorgedaan waarin aanbevelingen van die functionaris niet zijn uitgevoerd (zie punt 3.3.1 van bijlage II).
([367]) Punt 3.3.4 van bijlage II.
([368]) Specifiek met betrekking tot de Nationale Inlichtingendienst heeft de NHRC in het verleden ambtshalve onderzoeken uitgevoerd en een aantal individuele klachten behandeld. Zie bijvoorbeeld het NHRC-jaarverslag 2018, blz. 128 (beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) en het NHRC-jaarverslag 2019, blz. 70 (beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Artikel 13, lid 1, van de NIS-wet.
([370]) Artikelen 36 en 37, lid 1, Wet inzake de Nationale Vergadering.
([371]) Artikel 15, CPPA.
([372]) Artikel 15, lid 2, van de NIS-wet.
([373]) Artikel 17, lid 2, van de NIS-wet. "Staatsgeheimen" worden gedefinieerd als (vertrouwelijke) feiten, goederen of kennis die niet aan andere landen of andere organisaties mogen worden bekendgemaakt om ernstig nadeel voor de nationale veiligheid te voorkomen, en waartoe slechts beperkte toegang is toegestaan. Zie artikel 13, lid 4, van de NIS-wet.

name mag een nationale veiligheidsinstantie de uitoefening van het recht alleen beperken of ontzeggen voor zover en zolang dit noodzakelijk en evenredig is voor de bescherming van een belangrijke doelstelling van openbaar belang (bijvoorbeeld voor zover en zolang de verlening van het recht een lopend onderzoek in gevaar zou brengen of de nationale veiligheid zou bedreigen), of wanneer de verlening van het recht schade kan toebrengen aan het leven of de lichamelijke integriteit van een derde. Het inroepen van een dergelijke beperking vereist derhalve een afweging van de rechten en belangen van het individu tegen het betrokken openbaar belang en mag in geen geval de wezenlijke inhoud van het recht aantasten (artikel 37, lid 2, van de grondwet). Wanneer het verzoek wordt afgewezen of beperkt, moet de betrokkene onverwijld in kennis worden gesteld van de redenen daarvoor.

(205) Ten tweede hebben natuurlijke personen het recht om op grond van de PIPA verhaal te halen indien hun gegevens door een nationale veiligheidsinstantie zijn verwerkt in strijd met de PIPA of de beperkingen en waarborgen in andere wetten die betrekking hebben op het verzamelen van persoonsgegevens (met name de CPPA, zie overweging 171) ([374]). Dit recht kan worden uitgeoefend door een klacht in te dienen bij de PIPC (onder meer via het Privacy Call Centre van het Koreaans Agentschap voor internet en veiligheid) ([375]). Om gemakkelijker verhaal te kunnen halen bij de Koreaanse nationale veiligheidsautoriteiten, kunnen EU-burgers bovendien via hun nationale gegevensbeschermingsautoriteit een klacht indienen bij de PIPC ([376]). In dat geval zal de PIPC de betrokkene via de nationale gegevensbeschermingsautoriteit op de hoogte brengen zodra het onderzoek is afgesloten (en, in voorkomend geval, informatie verstrekken over de opgelegde corrigerende maatregelen). Op grond van de Wet administratieve procesvoering kunnen natuurlijke personen voorts in beroep gaan tegen beslissingen of het uitblijven van maatregelen van de PIPC (zie overweging 132).

(206) Ten derde kunnen natuurlijke personen bij de mensenrechtenfunctionaris een klacht indienen over de inbreuk op hun recht op bescherming van de persoonlijke levenssfeer/gegevensbescherming in het kader van terrorismebestrijdingsactiviteiten (d.w.z. op grond van de Wet terrorismebestrijding) ([377]), en kan die functionaris vervolgens corrigerende maatregelen aanbevelen. Aangezien er voor de mensenrechtenfunctionaris geen ontvankelijkheidseisen gelden, wordt een klacht zelfs in behandeling genomen als de betrokkene niet kan aantonen dat hij/zij daadwerkelijk is benadeeld (bijvoorbeeld omdat zijn/haar gegevens onrechtmatig zouden zijn verzameld door een nationale veiligheidsinstantie) ([378]). De betrokken instantie moet de mensenrechtenfunctionaris in kennis stellen van alle maatregelen die zij ter uitvoering van zijn aanbevelingen heeft genomen.

(207) Ten vierde kunnen natuurlijke personen bij de NHRC een klacht indienen over het verzamelen van hun gegevens door de nationale veiligheidsdiensten en verhaal halen volgens de in overweging 178 beschreven procedure ([379]).

(208) Tot slot zijn er verschillende voorzieningen in rechte beschikbaar ([380]), waarmee betrokkenen zich kunnen beroepen op de in punt 3.3.1 beschreven beperkingen en waarborgen om verhaal te halen. Zij kunnen met name de wettigheid van handelingen van nationale veiligheidsinstanties aanvechten op basis van de Wet administratieve procesvoering (overeenkomstig de in overweging 181 beschreven procedure) of de Wet op het grondwettelijk Hof (zie overweging 182). Daarnaast kunnen zij schadevergoeding krijgen op basis van de Wet inzake overheidscompensatie (zoals nader beschreven in overweging 183).

4. **CONCLUSIE**

(209) De Commissie is van oordeel dat de Republiek Korea — door middel van de PIPA, de speciale regels die voor bepaalde sectoren gelden (zoals onderzocht in punt 2) en de aanvullende waarborgen van Kennisgeving nr. 2021-5 (bijlage I) — een niveau van bescherming van vanuit de Europese Unie doorgegeven persoonsgegevens waarborgt dat in wezen gelijkwaardig is aan dat van Verordening (EU) 2016/679.

(210) Bovendien is de Commissie van oordeel dat, als geheel genomen, de toezichtsmechanismen en de verhaalsmogelijkheden waarin het Koreaanse recht voorziet, het mogelijk maken om inbreuken op de gegevensbeschermingsvoorschriften door verwerkingsverantwoordelijken in Korea in de praktijk vast te stellen en aan te pakken, en de betrokkene rechtsmiddelen bieden om toegang te krijgen tot zijn/haar persoonsgegevens en, uiteindelijk, om deze gegevens te laten corrigeren of wissen.

([374]) Artikel 58, lid 4, en artikel 4, lid 5, PIPA. Zie punt 3.4.2 van bijlage II.
([375]) Artikel 62 en artikel 63, lid 2, PIPA.
([376]) Kennisgeving nr. 2021-5 (deel 6, bijlage I).
([377]) Artikel 8, lid 1, punt 2, van het uitvoeringsdecreet van de Wet terrorismebestrijding.
([378]) Zie punt 3.4.1 van bijlage II.
([379]) De NHRC ontvangt bijvoorbeeld regelmatig klachten tegen de Nationale Inlichtingendienst, zie de cijfers in het NHRC-jaarverslag 2019 over het aantal klachten dat tussen 2015 en 2019 is ontvangen, blz. 70 (beschikbaar op https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Zie punt 3.4.4 van bijlage II.

(211) Tot slot is de Commissie op grond van de beschikbare informatie over de Koreaanse rechtsorde, met inbegrip van de verklaringen, garanties en toezeggingen van de Koreaanse regering in bijlage II, van oordeel dat elke inmenging in de grondrechten van particulieren van wie persoonsgegevens van de Europese Unie naar de Republiek Korea worden doorgegeven, door Koreaanse overheidsinstanties voor doeleinden van openbaar belang, meer in het bijzonder handhaving van het strafrecht en nationale veiligheid, beperkt is tot hetgeen strikt noodzakelijk is om de betrokken legitieme doelstelling te bereiken, en dat tegen dergelijke inmenging doeltreffende rechtsbescherming voorhanden is.

(212) In het licht van de bevindingen van dit besluit is de Commissie dan ook van oordeel dat de Republiek Korea een passend beschermingsniveau waarborgt in de zin van artikel 45 van Verordening (EU) 2016/679, uitgelegd in het licht van het Handvest van de grondrechten van de Europese Unie, voor vanuit de Europese Unie aan verwerkingsverantwoordelijken in de Republiek Korea doorgegeven persoonsgegevens die aan de PIPA zijn onderworpen, met uitzondering van religieuze organisaties voor zover zij persoonsgegevens voor hun zendingswerk verwerken; politieke organisaties, voor zover zij persoonsgegevens verwerken in het kader van de voordracht van kandidaten en verwerkingsverantwoordelijken die onder het toezicht van de Commissie financiële diensten vallen voor de verwerking van persoonlijke kredietinformatie uit hoofde van de Wet kredietinformatie, voor zover zij dergelijke informatie verwerken.

5. GEVOLGEN VAN DIT BESLUIT EN INGRIJPEN VAN GEGEVENSBESCHERMINGSAUTORITEITEN

(213) De lidstaten en hun organen moeten de maatregelen nemen die noodzakelijk zijn om te voldoen aan de handelingen van de instellingen van de Europese Unie, aangezien deze laatste vermoed worden rechtsgeldig te zijn en bijgevolg rechtsgevolgen in het leven roepen zolang zij niet zijn ingetrokken, nietig verklaard in een beroep tot nietigverklaring of ongeldig verklaard na een prejudiciële verwijzing of op een exceptie van onwettigheid.

(214) Daarom is een krachtens artikel 45, lid 3, van Verordening (EU) 2016/679 vastgesteld adequaatheidsbesluit van de Commissie bindend voor alle organen van de lidstaten waartoe het is gericht, met inbegrip van hun onafhankelijke toezichthoudende autoriteiten. Met name kunnen doorgiften van een verwerkingsverantwoordelijke of verwerker in de Europese Unie aan verwerkingsverantwoordelijken in de Republiek Korea plaatsvinden zonder dat verdere toestemming noodzakelijk is.

(215) Er zij aan herinnerd dat, overeenkomstig artikel 58, lid 5, van Verordening (EU) 2016/679 en zoals door het Hof van Justitie uitgelegd in het arrest in de zaak Schrems ([381]), wanneer een nationale gegevensbeschermingsautoriteit, ook na ontvangst van een klacht, de verenigbaarheid van een adequaatheidsbesluit van de Commissie met de grondrechten van de persoon op privacy en gegevensbescherming in twijfel trekt, het nationale recht moet voorzien in een rechtsmiddel voor die persoon om die grieven aan een nationale rechter voor te leggen die eventueel bij prejudiciële verwijzing het Hof van Justitie om beoordeling moet verzoeken ([382]).

6. TOEZICHT EN TOETSING VAN DIT BESLUIT

(216) Volgens de rechtspraak van het Hof van Justitie ([383]), en zoals is erkend in artikel 45, lid 4, van Verordening (EU) 2016/679, moet de Commissie na de vaststelling van een adequaatheidsbesluit doorlopend toezicht houden op relevante ontwikkelingen in het derde land, teneinde te beoordelen of dit derde land een in wezen gelijkwaardig beschermingsniveau blijft waarborgen. Een dergelijke controle is hoe dan ook vereist wanneer de Commissie informatie ontvangt die aanleiding geeft tot gerechtvaardigde twijfel dienaangaande.

(217) Derhalve moet de Commissie voortdurend volgen wat de situatie is in de Republiek Korea met betrekking tot het rechtskader en de dagelijkse praktijk aangaande de verwerking van persoonsgegevens die in dit besluit zijn beoordeeld, inclusief de naleving door de Koreaanse autoriteiten van de verklaringen, garanties en toezeggingen in bijlage II. Om dit proces te vergemakkelijken, worden de Koreaanse autoriteiten verzocht de Commissie te informeren over materiële ontwikkelingen die voor dit besluit van belang zijn, zowel wat de verwerking van persoonsgegevens door bedrijfsexploitanten en overheidsinstanties als de beperkingen en waarborgen die gelden voor de toegang tot persoonsgegevens door overheidsinstanties betreft.

([381]) Schrems, punt 65.

([382]) Schrems, punt 65: "In dat verband staat het aan de nationale wetgever om in beroepsgangen te voorzien waarmee bedoelde autoriteit de grieven die zij gegrond acht aan de nationale rechter kan voorleggen, zodat die laatste, wanneer hij de twijfel ten aanzien van de geldigheid van de beschikking van de Commissie deelt, de vraag naar de geldigheid van die beschikking prejudicieel kan verwijzen."

([383]) Schrems, punt 76.

(218) Teneinde de Commissie in staat te stellen haar toezichthoudende taak doeltreffend uit te voeren, moeten de lidstaten de Commissie bovendien in kennis stellen van relevante maatregelen van de nationale gegevensbeschermingsautoriteiten, met name inzake vragen of klachten van betrokkenen uit de EU betreffende de doorgifte van persoonsgegevens vanuit de Europese Unie aan verwerkingsverantwoordelijken in de Republiek Korea. Voorts moet de Commissie worden geïnformeerd over eventuele aanwijzingen dat de maatregelen van de Koreaanse overheidsinstanties die verantwoordelijk zijn voor de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten, of voor de nationale veiligheid, met inbegrip van toezichthoudende instanties, niet het vereiste beschermingsniveau waarborgen.

(219) Ingevolge artikel 45, lid 3, van Verordening (EU) 2016/679 ([384]), en in het licht van het feit dat het door de Koreaanse rechtsorde geboden beschermingsniveau kan veranderen, moet de Commissie na de vaststelling van dit besluit periodiek toetsen of de vaststellingen met betrekking tot de adequaatheid van het door de Republiek Korea geboden beschermingsniveau nog steeds feitelijk en rechtens gerechtvaardigd zijn.

(220) Te dien einde moet dit besluit binnen drie jaar na de inwerkingtreding ervan een eerste keer worden getoetst. Na die eerste toetsing, en afhankelijk van het resultaat daarvan, zal de Commissie in nauw overleg met het comité dat is ingesteld bij artikel 93, lid 1, van Verordening (EU) 2016/679 besluiten of de cyclus van drie jaar moet worden gehandhaafd. De daaropvolgende toetsingen moeten hoe dan ook ten minste om de vier jaar plaatsvinden ([385]). De toetsing moet betrekking hebben op alle aspecten van de werking van dit besluit, en met name op de toepassing van de aanvullende waarborgen in bijlage I bij dit besluit, met bijzondere aandacht voor de bescherming die wordt geboden in geval van verdere doorgifte; relevante ontwikkelingen in de rechtspraak; de regels inzake de verwerking van gepseudonimiseerde informatie ten behoeve van statistieken, wetenschappelijk onderzoek en archivering in het algemeen belang, alsook de toepassing van de uitzonderingen uit hoofde van artikel 28, lid 7, PIPA; de doeltreffendheid van de uitoefening van de individuele rechten, ook ten aanzien van de onlangs hervormde PIPC, en de toepassing van uitzonderingen op die rechten; de toepassing van de gedeeltelijke vrijstellingen in het kader van de PIPA; alsmede de beperkingen en waarborgen met betrekking tot de toegang van de overheid (zoals uiteengezet in bijlage II bij dit besluit), met inbegrip van de samenwerking van de PIPC met de gegevensbeschermingsautoriteiten van de EU inzake klachten van natuurlijke personen. Ook moet zij betrekking hebben op de doeltreffendheid van toezicht en handhaving, wat de PIPA betreft en op het gebied van de handhaving van het strafrecht en de nationale veiligheid (in het bijzonder door de PIPC en de NHRC).

(221) Voor het verrichten van de toetsing moet de Commissie samenkomen met de PIPC, in voorkomend geval samen met andere Koreaanse autoriteiten die verantwoordelijk zijn voor de toegang van de overheid, met inbegrip van relevante toezichtsorganen. Aan die bijeenkomst moet kunnen worden deelgenomen door vertegenwoordigers van de leden van het Europees Comité voor gegevensbescherming. In het kader van de toetsing moet de Commissie de PIPC verzoeken om uitvoerige informatie over alle aspecten die relevant zijn voor de vaststelling van adequaatheid, onder meer over de beperkingen en waarborgen met betrekking tot de overheidstoegang ([386]). De Commissie moet ook uitleg vragen over alle door haar ontvangen informatie die relevant is voor dit besluit, waaronder openbare rapporten van de Koreaanse autoriteiten of andere belanghebbenden in Korea, het Europees Comité voor gegevensbescherming, afzonderlijke gegevensbeschermingsautoriteiten, maatschappelijke groeperingen, berichten in de media of alle andere beschikbare informatiebronnen.

(222) Op basis van de toetsing moet de Commissie een openbaar verslag opstellen dat bij het Europees Parlement en de Raad moet worden ingediend.

7. OPSCHORTING, INTREKKING OF WIJZIGING VAN DIT BESLUIT

(223) Wanneer uit de beschikbare informatie, met name informatie die voortvloeit uit het toezicht op dit besluit of verstrekt wordt door de autoriteiten in de Republiek Korea of in de lidstaten, blijkt dat het door de Republiek Korea geboden beschermingsniveau niet langer passend is, moet de Commissie de bevoegde Koreaaanse autoriteiten onverwijld daarvan in kennis stellen en verzoeken dat binnen een opgegeven, redelijke termijn geschikte maatregelen worden genomen.

(224) Indien de bevoegde Koreaanse autoriteiten die maatregelen bij het verstrijken van die opgegeven termijn niet hebben genomen of anderszins niet aannemelijk hebben kunnen maken dat dit besluit op een passend beschermingsniveau gebaseerd blijft, leidt de Commissie de in artikel 93, lid 2, van Verordening (EU) 2016/679 bedoelde procedure in teneinde dit besluit geheel of gedeeltelijk op te schorten of in te trekken.

(225) Als alternatief zal de Commissie die procedure inleiden met het oog op wijziging van dit besluit, met name door voor gegevensdoorgiften aanvullende voorwaarden te stellen of door de reikwijdte van de vaststelling van adequaatheid te beperken tot gegevensdoorgiften waarvoor een passend beschermingsniveau blijft gewaarborgd.

([384]) Artikel 45, lid 3, van Verordening (EU) 2016/679 bepaalt: "De uitvoeringshandeling voorziet in een mechanisme voor periodieke toetsing, […] waarbij alle relevante ontwikkelingen in het derde land of de internationale organisatie in aanmerking worden genomen."

([385]) Artikel 45, lid 3, van Verordening (EU) 2016/679 bepaalt dat "minstens om de vier jaar" een periodieke toetsing moet plaatsvinden. Zie ook het Europees Comité voor gegevensbescherming, Adequaatheidsreferentie, WP 254 rev. 01.

([386]) Zie bijlage II bij dit besluit.

(226) De Commissie moet de procedure tot schorsing of intrekking met name inleiden als er aanwijzingen zijn dat de aanvullende waarborgen in bijlage I niet worden nageleefd door de bedrijfsexploitanten die persoonsgegevens ontvangen op grond van dit besluit en/of niet daadwerkelijk ten uitvoer worden gelegd, of dat de Koreaanse autoriteiten de verklaringen, garanties en toezeggingen in bijlage II bij dit besluit niet naleven.

(227) De Commissie moet tevens de inleiding van de procedure tot wijziging, schorsing of intrekking van dit besluit overwegen indien, in de context van de toetsing of anderszins, de bevoegde Koreaanse autoriteiten niet de informatie of verduidelijking verstrekken die nodig is voor de beoordeling van het niveau van de bescherming van persoonsgegevens die worden doorgegeven van de Europese Unie aan de Republiek Korea, of van de naleving van dit besluit. In dit verband moet de Commissie rekening houden met de mate waarin relevante informatie kan worden verkregen uit andere bronnen.

(228) De Commissie zal om naar behoren gerechtvaardigde dwingende urgente redenen gebruikmaken van de mogelijkheid om overeenkomstig de in artikel 93, lid 3, van Verordening (EU) 2016/679 bedoelde procedure onmiddellijk toepasselijke uitvoeringshandelingen tot opschorting, intrekking of wijziging van het besluit vast te stellen.

8. **SLOTOVERWEGINGEN**

(229) Het Europees Comité voor gegevensbescherming heeft zijn advies bekendgemaakt ([387]), waarmee bij het opstellen van dit besluit rekening is gehouden.

(230) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 93, lid 1, van Verordening (EU) 2016/679 ingestelde comité,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

1. Voor de toepassing van artikel 45 van Verordening (EU) 2016/679 waarborgt de Republiek Korea een passend beschermingsniveau voor persoonsgegevens die van de Europese Unie worden doorgegeven aan entiteiten in de Republiek Korea overeenkomstig de Wet bescherming persoonsinformatie, zoals aangevuld met de aanvullende waarborgen vermeld in bijlage I, tezamen met de officiële verklaringen, garanties en toezeggingen die zijn opgenomen in bijlage II.

2. Dit besluit heeft geen betrekking op persoonsgegevens die worden doorgegeven aan ontvangers die behoren tot een van de volgende categorieën, voor zover alle of sommige van de doeleinden van de verwerking van de persoonsgegevens beantwoorden aan één van de genoemde doeleinden, respectievelijk:

a) religieuze organisaties voor zover zij persoonsgegevens verwerken voor hun zendingswerk;

b) politieke partijen voor zover zij persoonsgegevens verwerken in het kader van de voordracht van kandidaten;

c) entiteiten die onder het toezicht van de Commissie financiële diensten vallen voor de verwerking van persoonlijke kredietinformatie uit hoofde van de Wet kredietinformatie, voor zover zij dergelijke informatie verwerken.

Artikel 2

Wanneer de bevoegde autoriteiten in de lidstaten, om personen te beschermen in verband met de verwerking van hun persoonsgegevens, hun bevoegdheden uit hoofde van artikel 58 van Verordening (EU) 2016/679 uitoefenen met betrekking tot gegevensdoorgiften die onder het in artikel 1 van dit besluit vastgestelde toepassingsgebied vallen, stelt de betrokken lidstaat de Commissie daarvan onverwijld in kennis.

Artikel 3

1. De Commissie houdt voortdurend toezicht op de toepassing van het rechtskader waarop dit besluit is gebaseerd, met inbegrip van de voorwaarden waaronder verdere doorgiften plaatsvinden, individuele rechten worden uitgeoefend en de Koreaanse overheidsinstanties toegang hebben tot de op grond van dit besluit doorgegeven gegevens, teneinde te beoordelen of de Republiek Korea een passend beschermingsniveau in de zin van artikel 1 blijft waarborgen.

([387]) Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea, beschikbaar op: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. De lidstaten en de Commissie stellen elkaar in kennis van gevallen waarin de Commissie bescherming persoonsinformatie of enige andere bevoegde Koreaanse autoriteit niet garandeert dat het rechtskader waarop dit besluit is gebaseerd wordt geëerbiedigd.

3. De lidstaten en de Commissie stellen elkaar in kennis van eventuele aanwijzingen dat ingrepen van de Koreaanse overheidsdiensten in het recht van natuurlijke personen op de bescherming van hun persoonsgegevens verder gaan dan hetgeen strikt noodzakelijk is, of dat er geen doeltreffende rechtsbescherming tegen dergelijke ingrepen is.

4. Binnen drie jaar na de datum van kennisgeving van dit besluit aan de lidstaten en daarna ten minste om de vier jaar, zal de Commissie de vaststelling in artikel 1, lid 1, evalueren op basis van alle beschikbare informatie, met inbegrip van de informatie die in het kader van de met de betrokken Koreaanse autoriteiten uitgevoerde toetsing is ontvangen.

5. Wanneer de Commissie aanwijzingen heeft dat een passend beschermingsniveau niet langer wordt gewaarborgd, stelt zij de bevoegde Koreaanse autoriteiten daarvan in kennis. Indien noodzakelijk, kan zij, in overeenstemming met artikel 45, lid 5, van Verordening (EU) 2016/679, besluiten dit besluit te schorsen, te wijzigen of in te trekken, of de werkingssfeer ervan te beperken, met name wanneer er aanwijzingen zijn dat:

a) verwerkingsverantwoordelijken in de Republiek Korea die uit hoofde van dit besluit persoonsgegevens uit de Europese Unie hebben ontvangen, de aanvullende waarborgen in bijlage I bij dit besluit niet naleven, of er dienaangaande onvoldoende toezicht en handhaving is;

b) de Koreaanse overheidsinstanties de verklaringen, garanties en toezeggingen die zijn opgenomen in bijlage II niet naleven, onder meer wat betreft de voorwaarden voor en de beperkingen van het verzamelen van en de toegang tot uit hoofde van dit besluit doorgegeven persoonsgegevens voor Koreaanse overheidsinstanties met het oog op de handhaving van het strafrecht of de nationale veiligheid.

De Commissie kan dergelijke maatregelen ook vaststellen indien zij door het gebrek aan medewerking van de Koreaanse regering niet kan bepalen of de Republiek Korea een passend beschermingsniveau blijft waarborgen.

Artikel 4

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 17 december 2021.

Voor de Commissie
Didier REYNDERS
Lid van de Commissie

BIJLAGE I

AANVULLENDE VOORSCHRIFTEN VOOR DE UITLEGGING EN TOEPASSING VAN DE WET BESCHERMING PERSOONSINFORMATIE IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS DIE ZIJN DOORGEGEVEN AAN KOREA

Inhoud

I. **Beschrijving**

Korea en de Europese Unie (hierna "EU" genoemd) hebben discussies over de adequaatheid gevoerd naar aanleiding waarvan de Europese Commissie heeft vastgesteld dat Korea een passend beschermingsniveau voor persoonsgegevens waarborgt overeenkomstig artikel 45 AVG.

De Commissie bescherming persoonsinformatie (*Personal Information Protection Commission* — PIPC) heeft in dit verband deze kennisgeving goedgekeurd op basis van artikel 5 (Verplichtingen van de staat enz.) en artikel 14 (Internationale samenwerking) [1] van de Wet bescherming persoonsinformatie (*Personal Information Protection Act* — PIPA) om de uitlegging, toepassing en handhaving van een aantal bepalingen van de Wet te verduidelijken, onder meer in verband met de verwerking van aan Korea doorgegeven persoonsgegevens op basis van het adequaatheidsbesluit van de EU.

Omdat deze kennisgeving de status van bestuursrechtelijk voorschrift heeft, dat het bevoegde bestuursrechtelijke agentschap vaststelt en bekendmaakt ter verduidelijking van de normen voor de uitlegging, toepassing en handhaving van de Wet bescherming persoonsinformatie in het Koreaanse rechtssysteem, is zij wettelijk bindend voor de verantwoordelijke voor de verwerking van persoonsinformatie in die zin dat een schending van deze kennisgeving kan worden beschouwd als schending van de desbetreffende bepalingen van de PIPA. Daarnaast hebben betrokkenen het recht verhaal te halen bij de Commissie bescherming persoonsinformatie of de rechter wanneer persoonlijke rechten en belangen worden geschonden als gevolg van een inbreuk op deze kennisgeving.

Bijgevolg wordt overeenkomstig artikel 64, leden 1 en 2, van de Wet aangenomen dat er zwaarwegende gronden zijn om aan te nemen dat een inbreuk in verband met persoonsinformatie heeft plaatsgevonden en dat niet handelen waarschijnlijk zal leiden tot schade die moeilijk kan worden hersteld wanneer de verantwoordelijke voor de verwerking van persoonsinformatie, die de persoonsinformatie verwerkt die overeenkomstig het adequaatheidsbesluit van de EU aan Korea is doorgegeven, geen maatregelen neemt om deze kennisgeving na te leven. In dergelijke gevallen kan de Commissie bescherming persoonsinformatie of een gerelateerde centrale bestuursinstantie op grond van de bevoegdheid die

[1] In artikel 14 van de Wet bescherming persoonsinformatie is bepaald dat de Koreaanse regering bevoegd is om beleid vast te stellen ter verbetering van het beschermingsniveau voor persoonsinformatie in de internationale omgeving en ter voorkoming van inbreuken op de rechten van betrokkenen als gevolg van de grensoverschrijdende doorgifte van persoonsinformatie.

deze bepaling verleent de betrokken verantwoordelijke voor de verwerking van persoonsinformatie gelasten corrigerende maatregelen enz. te nemen en, afhankelijk van de specifieke schending van de wet, ook een dienovereenkomstige straf (sanctie, administratieve boete enz.) opleggen.

II. **Definities**

In deze voorziening worden de volgende definities gebruikt:

i) "Wet": de Wet bescherming persoonsinformatie (Wet nr. 16930, gewijzigd op 4 februari 2020 en ten uitvoer gelegd op 5 augustus 2020), ook afgekort als PIPA (*Personal Information Protection Act*);

ii) "presidentieel decreet": uitvoeringsdecreet van de Wet bescherming persoonsinformatie (Presidentieel decreet nr. 30509 van 3 maart 2020, waarbij andere wetten worden gewijzigd);

iii) "betrokkene": een persoon die kan worden geïdentificeerd aan de hand van de verwerkte informatie en daarmee het onderwerp van deze informatie wordt;

iv) "verantwoordelijke voor de verwerking van persoonsinformatie": een overheidsinstantie, rechtspersoon, organisatie, individu enz. die/dat in het kader van zijn/haar activiteiten direct of indirect persoonsinformatie verwerkt;

v) "EU": de EU (per eind februari 2020 27 lidstaten [2], dat wil zeggen België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië en Zweden), alsook landen die op grond van de EER-Overeenkomst met de EU zijn geassocieerd (IJsland, Liechtenstein, Noorwegen);

vi) "AVG": de algemene verordening gegevensbescherming (Verordening (EU) 2016/679), de algemene wet van de EU voor de bescherming van persoonsinformatie;

vii) "adequaatheidsbesluit": overeenkomstig artikel 45, lid 3, AVG, wanneer de Europese Commissie heeft besloten dat een derde land, een gebied in een derde land, één of meer gebieden of een internationale organisatie een passend beschermingsniveau voor persoonsinformatie waarborgt.

III. **Aanvullende voorschriften**

1. **Beperking van het gebruik en het verstrekken van persoonsgegevens voor een ander dan het beoogde doel (artikelen 3, 15 en 18 van de Wet)**

<Wet bescherming persoonsinformatie

(Wet nr. 16930, gedeeltelijk gewijzigd op 4 februari 2020)>

Artikel 3 (Beginselen voor de bescherming van persoonsinformatie) 1) De verantwoordelijke voor de verwerking van persoonsinformatie specificeert uitdrukkelijk voor welke doeleinden de persoonsinformatie wordt verwerkt; hij verzamelt de persoonsinformatie op rechtmatige en behoorlijke wijze in de mate die minimaal noodzakelijk is voor die doeleinden.

2) De verantwoordelijke voor de verwerking van persoonsinformatie verwerkt de persoonsinformatie op passende wijze zoals nodig voor de doeleinden waarvoor de persoonsinformatie wordt verwerkt en gebruikt de persoonsinformatie niet voor andere doeleinden.

Artikel 15 (Verzameling en gebruik van persoonsinformatie) 1) Een verantwoordelijke voor de verwerking van persoonsinformatie mag in de volgende omstandigheden persoonsinformatie verzamelen en deze gebruiken binnen het toepassingsgebied van het doel waarvoor zij is verzameld:

1. wanneer toestemming is verkregen van een betrokkene;

2. wanneer er bijzondere wettelijke bepalingen bestaan of dit onvermijdelijk is om aan wettelijke verplichtingen te voldoen;

3. wanneer dit onvermijdelijk is voor de uitvoering van de taken van een overheidsinstelling die vallen binnen haar bij wet enz. voorgeschreven bevoegdheid;

4. wanneer dit onvermijdelijk is voor het uitvoeren van een overeenkomst met een betrokkene;

[2] Tot het einde van de overgangsperiode viel ook het Verenigd Koninkrijk onder deze definitie, zoals bepaald in de artikelen 126, 127 en 132 van het Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie (2019/C 384 I/01).

5. wanneer dit duidelijk noodzakelijk wordt geacht om het leven, de lichamelijke integriteit of de eigendomsbelangen van de betrokkene of een derde partij te beschermen tegen onmiddellijk gevaar indien de betrokkene of diens wettelijke vertegenwoordiger niet in staat is om zijn of haar wil kenbaar te maken, of geen voorafgaande toestemming kan worden verkregen als gevolg van een onbekend adres enz.;
6. wanneer dit noodzakelijk is om het rechtmatige belang van een verantwoordelijke voor de verwerking van persoonsinformatie te verwezenlijken indien dat belang duidelijk zwaarder weegt dan de rechten van de betrokkene. In dergelijke gevallen is de verwerking slechts toegestaan in de mate waarin de verwerking wezenlijk verband houdt met het gerechtvaardigde belang van de verantwoordelijke voor de verwerking van persoonsinformatie en mag deze niet verder gaan dan wat redelijk is.

Artikel 18 (Beperking van het gebruik en het verstrekken van persoonsinformatie voor een ander dan het beoogde doel) 1) Verantwoordelijken voor de verwerking van persoonsinformatie gebruiken de persoonsinformatie niet buiten het toepassingsgebied als bepaald in artikel 15, lid 1, en artikel 39-3, leden 1 en 2, en verstrekken deze niet aan derden buiten het toepassingsgebied als bepaald in artikel 17, leden 1 en 3.

2) Onverminderd lid 1 mag een verantwoordelijke voor de verwerking van persoonsinformatie persoonsinformatie voor andere doeleinden gebruiken of verstrekken aan een derde wanneer een van de volgende punten van toepassing is, tenzij hiermee waarschijnlijk op oneerlijke wijze inbreuk zou worden gemaakt op de belangen van een betrokkene of derde: op aanbieders van informatie- en communicatiediensten [zoals uiteengezet in artikel 2, lid 1, punt 3, van de Wet inzake de bevordering van het gebruik van informatie- en communicatienetwerken en de bescherming van informatie enz., hierna geldt hetzelfde] die de persoonsinformatie van gebruikers verwerken [zoals uiteengezet in artikel 2, lid 1, punt 4, van de Wet inzake de bevordering van het gebruik van informatie- en communicatienetwerken en de bescherming van informatie enz.; hierna geldt hetzelfde] zijn uitsluitend de punten 1 en 2 van toepassing, terwijl de punten 5 tot en met 9 uitsluitend van toepassing zijn op overheidsinstanties:

1. er is aanvullende toestemming verkregen van een betrokkene;
2. er bestaan andere bijzondere wettelijke bepalingen;
3. dit wordt duidelijk noodzakelijk geacht om het leven, de lichamelijke integriteit of de eigendomsbelangen van de betrokkene of een derde partij te beschermen tegen onmiddellijk gevaar indien de betrokkene of diens wettelijke vertegenwoordiger niet in staat is om zijn of haar wil kenbaar te maken, of geen voorafgaande toestemming kan worden verkregen als gevolg van een onbekend adres;
4. geschrapt;<bij Wet nr. 16930 van 4 februari 2020>
5. het is onmogelijk om de taken uit te voeren die onder zijn bij wet voorgeschreven bevoegdheid vallen, tenzij de verantwoordelijke voor verwerking van persoonsinformatie de persoonsinformatie gebruikt voor een ander dan het beoogde doel, of deze verstrekt aan een derde en de beraadslaging en afhandeling van de commissie hierop van toepassing is;
6. het is noodzakelijk om de persoonsinformatie te verstrekken aan een buitenlandse regering of internationale organisatie om een verdrag of andere internationale overeenkomst uit te voeren;
7. het is noodzakelijk voor het onderzoek van een misdaad, een tenlastelegging en vervolging;
8. het is noodzakelijk voor een rechtbank om de taken in verband met een proces uit te voeren;
9. het is noodzakelijk voor de handhaving van een straf, voorwaardelijke straf en verzekerde bewaring.

weggelaten (3) ~ (4)

(5) Wanneer een verantwoordelijke voor de verwerking van persoonsinformatie aan een derde partij persoonsinformatie verstrekt met een ander dan het beoogde doel in een van de in lid 2 omschreven gevallen, verzoekt de verantwoordelijke voor de verwerking van persoonsinformatie de ontvanger van de persoonsinformatie het doel en de methode van gebruik en andere noodzakelijke aangelegenheden te beperken of te zorgen voor de noodzakelijke waarborgen om de veiligheid van de persoonsinformatie te verzekeren. In dergelijke gevallen neemt de persoon die een dergelijk verzoek ontvangt de noodzakelijke maatregelen om de veiligheid van de persoonsinformatie te waarborgen.

i) In artikel 3, leden 1 en 2, van de Wet wordt het beginsel voorgeschreven dat een verantwoordelijke voor de verwerking van persoonsinformatie slechts het minimum aan persoonsinformatie mag verzamelen dat noodzakelijk is voor de rechtmatige verwerking van de persoonsinformatie en deze informatie niet voor een ander dan het beoogde doel mag gebruiken ([3]).

ii) Overeenkomstig dit beginsel wordt in artikel 15, lid 1, van de Wet voorgeschreven dat wanneer een verantwoordelijke voor de verwerking van persoonsinformatie persoonsinformatie verzamelt, deze informatie mag worden gebruikt binnen het doel van de verzameling en wordt in artikel 18, lid 1, voorgeschreven dat persoonsinformatie niet mag worden gebruikt voor andere doeleinden dan het doel van de verzameling en niet aan een derde mag worden verstrekt.

([3]) Aangezien in deze bepalingen algemene beginselen zijn uiteengezet die van toepassing zijn op alle verwerkingen van persoonsinformatie, ook wanneer een dergelijke verwerking specifiek wordt geregeld in andere wetten, zijn de verduidelijkingen van dit punt ook van toepassing op gevallen waarin persoonsgegevens worden verwerkt op basis van andere wetten (zie bv. artikel 15, lid 1, van de Wet kredietinformatie, waarin specifiek wordt verwezen naar deze bepalingen).

iii) Bovendien moet er, zelfs wanneer persoonsinformatie voor een ander dan het beoogde doel mag worden gebruikt of aan een derde mag worden verstrekt in de uitzonderlijke gevallen ([4]) als beschreven in de punten van artikel 18, lid 2, van de Wet, overeenkomstig lid 5 om worden verzocht dat het doel of de methode van het gebruik wordt beperkt, zodat de persoonsinformatie op veilige wijze kan worden verwerkt, of moeten er maatregelen worden genomen die noodzakelijk zijn om de veiligheid van de persoonsinformatie te beschermen.

iv) De bovenstaande bepalingen worden op gelijke wijze toegepast op de verwerking van alle persoonsinformatie die binnen het rechtsgebied van Korea van een derde land wordt ontvangen, ongeacht de nationaliteit van de betrokkene.

v) Wanneer bijvoorbeeld een verantwoordelijke voor de verwerking van persoonsinformatie in de EU persoonsinformatie doorgeeft aan een Koreaanse verantwoordelijke voor de verwerking van persoonsinformatie in overeenstemming met het adequaatheidsbesluit van de Europese Commissie, wordt het doel van de doorgifte van de persoonsinformatie van de EU-verantwoordelijke voor de verwerking van persoonsinformatie beschouwd als het doel van de verzameling van de persoonsinformatie van de Koreaanse verantwoordelijke voor de verwerking van persoonsinformatie en mag de Koreaanse verantwoordelijke voor de verwerking van de persoonsinformatie de persoonsinformatie in dergelijke gevallen alleen gebruiken of aan een derde verstrekken binnen het doel van de verzameling, met uitzondering van de uitzonderlijke gevallen als beschreven in artikel 18, lid 2, punten 1 tot en met 9, van de Wet.

2. **Beperking van de verdere doorgifte van persoonsgegevens (artikel 17, leden 3 en 4, en artikel 18 van de Wet)**

<Wet bescherming persoonsinformatie
(Wet nr. 16930, gedeeltelijk gewijzigd op 4 februari 2020)>

Artikel 17 (Verstrekken van persoonsinformatie) 1) weggelaten

2) Een verantwoordelijke voor de verwerking van persoonsinformatie informeert een betrokkene over de volgende zaken wanneer hij de toestemming verkrijgt op grond van lid 1, punt 1. Hetzelfde geldt wanneer het volgende is aangepast:

1. de ontvanger van de persoonsinformatie;
2. het doel waarvoor de ontvanger van de persoonsinformatie die informatie gebruikt;
3. bijzonderheden van de persoonsinformatie die moet worden verstrekt;
4. de periode waarin de ontvanger de persoonsinformatie bewaart en gebruikt, en
5. het feit dat de betrokkene het recht heeft de toestemming te weigeren en, in voorkomend geval, de nadelen van een dergelijke weigering van toestemming.

3) De verantwoordelijke voor de verwerking van persoonsinformatie informeert de betrokkene over de in lid 2 bedoelde zaken en verkrijgt de toestemming van de betrokkene wanneer hij de persoonsinformatie aan een derde in een ander land wil verstrekken; hij sluit geen overeenkomst voor de grensoverschrijdende doorgifte van persoonsinformatie die in strijd is met deze Wet.

4) Verantwoordelijken voor de verwerking van persoonsinformatie mogen persoonsinformatie verstrekken zonder toestemming van een betrokkene binnen het toepassingsgebied dat redelijkerwijs verband houdt met het oorspronkelijke doel waarvoor de persoonsinformatie werd verzameld, in overeenstemming met het bepaalde in het presidentieel decreet, waarbij rekening wordt gehouden met de vraag of dit nadelen oplevert voor de betrokkene, of de noodzakelijke maatregelen zijn genomen om de veiligheid te waarborgen, zoals encryptie enz.

※ Zie bladzijden 3, 4 en 5 voor artikel 18.

< **Uitvoeringsdecreet van de Wet bescherming persoonsinformatie**

([Datum van uitvoering: 5 februari 2021.] [Presidentieel decreet nr. 30892 van 4 augustus 2020, waarbij andere wetten worden gewijzigd])>

Artikel 14-2 (Normen voor aanvullend gebruik/aanvullende verstrekking van persoonsinformatie enz.)

1) Wanneer een verantwoordelijke voor de verwerking van persoonsinformatie persoonsinformatie gebruikt of verstrekt (hierna "aanvullend gebruik of aanvullende verstrekking van persoonsinformatie" genoemd) zonder toestemming van de betrokkene overeenkomstig artikel 15, lid 3, van de Wet of artikel 17, lid 4, van de Wet, neemt de verantwoordelijke voor de verwerking van persoonsinformatie de volgende vragen in aanmerking:

1. of dit redelijk is in verband met het oorspronkelijke doel waarvoor de persoonsinformatie werd verzameld;
2. of aanvullend gebruik of de aanvullende verstrekking van persoonsinformatie in het licht van de omstandigheden waaronder de persoonsinformatie werd verzameld en de verwerkingspraktijken voorzienbaar is;
3. of het aanvullende gebruik of de aanvullende verstrekking van persoonsinformatie niet leidt tot een oneerlijke inbreuk op de belangen van de betrokkene, en
4. of de vereiste maatregelen zijn genomen om de veiligheid te waarborgen, zoals pseudonimisering of encryptie.

([4]) Op aanbieders van informatie- en communicatiediensten zijn slechts de punten 1 en 2 van artikel 18, lid 2, van toepassing. De punten 5 tot en met 9 zijn uitsluitend van toepassing op overheidsinstanties.

2) De verantwoordelijke voor de verwerking van persoonsinformatie maakt de criteria voor de beoordeling van de punten van lid 1 vooraf bekend in het privacybeleid op grond van artikel 30, lid 1, van de Wet en de privacyfunctionaris op grond van artikel 31, lid 1, van de Wet controleert of de verwerkingsverantwoordelijke voor de persoonsinformatie aanvullende persoonsinformatie gebruikt of verstrekt overeenkomstig de desbetreffende normen.

i) Indien de verantwoordelijke voor de verwerking van persoonsinformatie persoonsinformatie verstrekt aan een derde in het buitenland, moet hij de betrokkenen vooraf informeren over alle in artikel 17, lid 2, van de Wet beschreven zaken en hun toestemming verkrijgen, behalve in gevallen die vallen onder de punten 1 of 2. Er mag geen overeenkomst betreffende de grensoverschrijdende verstrekking van persoonsgegevens worden gesloten die in strijd is met deze Wet.
   1) Wanneer persoonsinformatie wordt verstrekt binnen de redelijke grenzen van het oorspronkelijke doel van de verzameling overeenkomstig artikel 17, lid 4, van de Wet. De gevallen waarop deze bepaling kan worden toegepast, zijn echter beperkt tot gevallen waarin de normen voor het aanvullend gebruik en de aanvullende verstrekking van persoonsinformatie, zoals beschreven in artikel 14-2 van het uitvoeringsdecreet, worden nageleefd. Daarnaast moet de verantwoordelijke voor de verwerking van persoonsinformatie de vragen in aanmerking nemen of de verstrekking van persoonsinformatie nadelige gevolgen kan hebben voor betrokkenen en of hij de noodzakelijke maatregelen ter waarborging van de veiligheid heeft genomen, zoals encryptie.
   2) Wanneer persoonsinformatie aan een derde kan worden verstrekt in de uitzonderlijke gevallen als bedoeld in artikel 18, lid 2, van de Wet (zie bladzijde 3 tot en met 5). Zelfs in dergelijke gevallen geldt echter dat wanneer de verstrekking van dergelijke persoonsinformatie waarschijnlijk op oneerlijke wijze zou leiden tot een inbreuk op de belangen van de betrokkene of een derde, deze persoonsinformatie niet aan een derde mag worden verstrekt. De aanbieder van persoonsinformatie moet de ontvanger van de persoonsinformatie bovendien verzoeken het doel of de methode van het gebruik van de persoonsinformatie te beperken of maatregelen te nemen die noodzakelijk zijn ter waarborging van de veiligheid van deze informatie, zodat de persoonsinformatie op veilige wijze kan worden verwerkt.

ii) Wanneer persoonsinformatie wordt verstrekt aan een derde in het buitenland, is het mogelijk dat hiervoor niet hetzelfde niveau van bescherming wordt gewaarborgd als door de Wet bescherming persoonsinformatie van Korea als gevolg van verschillen in de systemen voor de bescherming van persoonsinformatie van verschillende landen. Deze gevallen zullen dienovereenkomstig worden beschouwd als "gevallen waarin sprake kan zijn van nadelige gevolgen voor de betrokkene" als bedoeld in artikel 17, lid 4, van de Wet of als "gevallen waarin de belangen van een betrokkene of derde op oneerlijke wijze worden geschonden", zoals bedoeld in artikel 18, lid 2, van de Wet en artikel 14-2 van het uitvoeringsdecreet van deze Wet ([5]). Om de vereisten van deze bepalingen na te komen, moeten de verantwoordelijke voor de verwerking van persoonsinformatie en de derde derhalve uitdrukkelijk een beschermingsniveau waarborgen dat gelijkwaardig is aan dat van de Wet, met inbegrip van de waarborging van het uitoefenen van de rechten door de betrokkene in wettelijk bindende documenten zoals overeenkomsten, zelfs nadat de informatie naar het buitenland is overgedragen.

3. **Kennisgeving voor de gegevens wanneer geen persoonsgegevens zijn verkregen van de betrokkene (artikel 20 van de Wet)**

<Wet bescherming persoonsinformatie

(Wet nr. 16930, gedeeltelijk gewijzigd op 4 februari 2020)>

Artikel 20 (Kennisgeving over bronnen enz. van persoonsinformatie die van derden wordt verkregen) 1) Wanneer een verantwoordelijke voor de verwerking van persoonsinformatie persoonsinformatie verwerkt die van derden is verkregen, stelt de verantwoordelijke voor de verwerking van persoonsinformatie de betrokkene op diens verzoek onverwijld op de hoogte van de volgende zaken:

1. de bron van de verzamelde persoonsinformatie;
2. het doel van de verwerking van de persoonsinformatie;
3. het feit dat de betrokkene het recht heeft de opschorting van de verwerking van de persoonsinformatie te verlangen, zoals voorgeschreven in artikel 37.

2) Onverminderd lid 1 stelt de verantwoordelijke voor de verwerking van persoonsinformatie die voldoet aan de criteria als voorgeschreven bij het presidentieel decreet, rekening houdend met de soort en de hoeveelheid verwerkte persoonsinformatie, het aantal werknemers, het aantal verkopen enz., de betrokkene in kennis van de in lid 1 bedoelde zaken wanneer hij persoonsinformatie van derden verzamelt en deze verwerkt overeenkomstig artikel 17, lid 1, punt 1. Dit geldt niet wanneer de door de verantwoordelijke voor de verwerking van persoonsinformatie verzamelde informatie geen persoonsinformatie bevat aan de hand waarvan de betrokkene in kennis kan worden gesteld, zoals contactgegevens.

([5]) Overeenkomstig artikel 18, lid 2, punt 2, PIPA geldt dit ook wanneer persoonsinformatie wordt verstrekt aan derden in het buitenland op basis van bepalingen in andere wetten (zoals de Wet kredietinformatie).

3) Noodzakelijke informatie in verband met het tijdstip, de methode en procedure van de kennisgeving aan de betrokkene overeenkomstig de hoofdzin van lid 2 wordt voorgeschreven in het presidentieel decreet.

4) Lid 1 en de hoofdzin van lid 2 zijn in de volgende gevallen niet van toepassing: dit is alleen het geval wanneer dit duidelijk zwaarder weegt dan de rechten van betrokkenen uit hoofde van deze Wet:

1. wanneer persoonsinformatie waarvoor een kennisgevingsverzoek wordt ingediend, is opgenomen in de bestanden met persoonsinformatie als bedoeld in een van de punten van artikel 32, lid 2;
2. wanneer een dergelijke kennisgeving waarschijnlijk schade zal veroorzaken voor het leven of de lichamelijke integriteit van een andere persoon of oneerlijke schade zal toebrengen aan de eigendom en andere belangen van een andere persoon.

i) Wanneer de verantwoordelijke voor de verwerking van de persoonsinformatie de uit de EU doorgegeven persoonsinformatie ontvangt op basis van het adequaatheidsbesluit ([6]), moet hij de volgende informatie onder de punten 1 tot en met 5 onverwijld en in ieder geval niet later dan één maand na de doorgifte verstrekken aan de betrokkene:

1) de naam en contactgegevens van de personen die de persoonsinformatie doorgeven en ontvangen;

2) de onderdelen of categorieën doorgegeven persoonsinformatie;

3) het doel van de verzameling en het gebruik van de persoonsinformatie (zoals vastgesteld door de gegevensexporteur overeenkomstig punt 1 van deze kennisgeving);

4) de bewaartermijn van de persoonsinformatie;

5) informatie over de rechten van de betrokkene in verband met de verwerking van de persoonsinformatie, de methode en de procedure van de uitoefening van de rechten en de nadelige gevolgen wanneer de uitoefening van de rechten nadelige gevolgen oplevert.

ii) Wanneer de verantwoordelijke voor de verwerking van persoonsinformatie de onder i) bedoelde persoonsinformatie verstrekt aan een derde in de Republiek Korea of het buitenland moet hij de onder de punten 1 tot en met 5 bedoelde informatie aan de betrokkene verstrekken voordat de persoonsinformatie wordt verstrekt:

1) de naam en contactgegevens van de personen die de persoonsinformatie verstrekken en ontvangen;

2) de onderdelen of categorieën verstrekte persoonsinformatie;

3) het land waaraan de persoonsinformatie wordt verstrekt en de beoogde datum en de methode van de verstrekking ervan (alleen voor gevallen waarin de persoonsinformatie wordt verstrekt aan een derde in het buitenland);

4) het doel van de verstrekker van de persoonsinformatie en de rechtsgrond voor het verstrekken van de persoonsinformatie;

5) informatie over de rechten van de betrokkene in verband met de verwerking van de persoonsinformatie, de methode en de procedure van de uitoefening van de rechten en de nadelige gevolgen wanneer de uitoefening van de rechten nadelige gevolgen oplevert.

iii) De verantwoordelijke voor de verwerking van persoonsinformatie mag de punten i) of ii) niet toepassen wanneer er sprake is van de omstandigheden als bedoeld onder de volgende punten 1 tot en met 4:

1) wanneer de persoonsinformatie waarvoor kennisgeving vereist is, is opgenomen in een van de volgende bestanden met persoonsinformatie als bedoeld in artikel 32, lid 2, van de Wet voorzover de bij deze bepaling beschermde belangen duidelijk zwaarder wegen dan de rechten van de betrokkene en slechts zolang de kennisgeving een risico zou vormen voor het nastreven van de op het spel staande belangen, bijvoorbeeld door lopende strafrechtelijke onderzoeken of de nationale veiligheid in gevaar te brengen;

2) wanneer en zolang de kennisgeving waarschijnlijk zou leiden tot schade voor het leven of de lichamelijke integriteit van een andere persoon of de eigendomsbelangen van een andere persoon op oneerlijke wijze zou schenden wanneer deze rechten of belangen duidelijk zwaarder wegen dan de rechten van de betrokkene;

3) wanneer de betrokkene reeds beschikt over de informatie die de verantwoordelijke voor de verwerking van persoonsinformatie moet verstrekken overeenkomstig punt i) of punt ii);

4) wanneer de verantwoordelijke voor de verwerking van persoonsinformatie niet beschikt over contactgegevens van de betrokkene of buitensporige inspanningen moet verrichten om contact op te nemen met de betrokkene, ook in het kader van de verwerking onder de in deel 3 van de PIPA uiteengezette voorwaarden. Bij het bepalen of het mogelijk is om contact op te nemen met de betrokkene en of dit buitensporige inspanningen vereist, moet rekening worden gehouden met de mogelijkheid om samen te werken met de gegevensexporteur in de EU.

([6]) De onder i), ii) en iii) vermelde verplichtingen zijn op gelijke wijze van toepassing wanneer de verantwoordelijke voor de verwerking van persoonsinformatie uit de EU op basis van het adequaatheidsbesluit ontvangt dergelijke informatie op basis van andere wetten, zoals de Wet kredietinformatie, verwerkt.

4. **Toepassingsgebied van de speciale uitzondering op de verwerking van gepseudonimiseerde informatie (artikelen 28-2, 28-3, 28-4, 28-5, 28-6, 28-7, artikel 3 en artikel 58-2, van de Wet)**

<Wet bescherming persoonsinformatie
(Wet nr. 16930, gedeeltelijk gewijzigd op 4 februari 2020)>
Hoofdstuk III Verwerking van persoonsinformatie
DEEL 3 Speciale gevallen in verband met gepseudonimiseerde gegevens
Artikel 28-2 (Verwerking van gepseudonimiseerde gegevens) 1) Verantwoordelijken voor de verwerking van persoonsinformatie mogen gepseudonimiseerde informatie zonder toestemming van betrokkenen verwerken voor statistische doeleinden, wetenschappelijk onderzoek en archivering in het algemeen belang enz.
2) Verantwoordelijken voor de verwerking van persoonsinformatie nemen geen informatie op die kan worden gebruikt om een bepaalde natuurlijke persoon te identificeren wanneer zij overeenkomstig lid 1 gepseudonimiseerde informatie verstrekken aan een derde.
Artikel 28-3 (Beperking van de samenvoeging van pseudonieme gegevens) 1) Onverminderd artikel 28-2 wordt de samenvoeging van gepseudonimiseerde informatie die door verschillende verantwoordelijken voor de verwerking van persoonsinformatie wordt verwerkt voor statistische doeleinden, wetenschappelijk onderzoek en het bewaren van documenten in het algemeen belang enz. verricht door een gespecialiseerde instelling die wordt aangewezen door de Commissie bescherming persoonsinformatie of het hoofd van de desbetreffende centrale bestuursinstantie.
2) Verantwoordelijken voor de verwerking van persoonsinformatie die de samengevoegde informatie willen vrijgeven buiten de organisatie die de informatie heeft samengevoegd, moeten hiervoor na de verwerking van de informatie tot gepseudonimiseerde informatie of de in artikel 58-2 bedoelde vorm toestemming verkrijgen van het hoofd van de gespecialiseerde instelling.
3) Noodzakelijke aangelegenheden, waaronder de procedures en methoden voor de samenvoeging overeenkomstig lid 1, de normen en procedures voor het aanwijzen of intrekken van de aanwijzing van het bestuur en toezicht van een gespecialiseerde instelling en normen en procedures voor de export en goedkeuring overeenkomstig lid 2 worden bij presidentieel decreet vastgesteld.
Artikel 28-4 (Verplichting tot het nemen van veiligheidsmaatregelen voor gepseudonimiseerde gegevens) 1) Bij het verwerken van de gepseudonimiseerde informatie nemen verantwoordelijken voor de verwerking van persoonsinformatie de nodige technische, organisatorische en fysieke maatregelen, zoals het afzonderlijk opslaan en beheren van aanvullende informatie die nodig is om de informatie in de oorspronkelijke staat terug te brengen, om de veiligheid te waarborgen, zoals voorgeschreven bij presidentieel decreet, zodat de persoonsinformatie niet verloren gaat en niet wordt gestolen, onthuld, vervalst, gewijzigd of beschadigd.
2) Verantwoordelijken voor de verwerking van persoonsinformatie die de gepseudonimiseerde informatie willen verwerken stellen registers op en houden deze bij in verband met de bij presidentieel decreet voorgeschreven zaken, waaronder het doel van de verwerking van de gepseudonimiseerde informatie, en een derde-ontvanger wanneer gepseudonimiseerde informatie wordt verstrekt, om de verwerking van de gepseudonimiseerde informatie te beheren.
Artikel 28-5 (Verboden handelingen in verband met de verwerking van gepseudonimiseerde informatie) 1) Het verwerken van gepseudonimiseerde informatie met het oog op de identificatie van een bepaalde natuurlijke persoon is niet toegestaan.
2) Wanneer bij de verwerking van gepseudonimiseerde informatie informatie wordt gegenereerd aan de hand waarvan een bepaalde natuurlijke persoon kan worden geïdentificeerd, stopt de verantwoordelijke voor de verwerking van persoonsinformatie de verwerking van de informatie, haalt hij deze terug en vernietigt hij deze onmiddellijk.
Artikel 28-6 (Opleggen van een administratieve boete voor de verwerking van de gepseudonimiseerde informatie) 1) De Commissie bescherming persoonsinformatie mag aan de verwerkingsverantwoordelijke die in strijd met artikel 28-5, lid 1, gegevens heeft verwerkt met het oog op de identificatie van een specifieke natuurlijke persoon een boete opleggen die gelijk is aan minder dan drie procent van de totale omzet. Wanneer er geen sprake is van verkopen of het berekenen van de omzet lastig is, kan aan de verwerkingsverantwoordelijke een boete worden opgelegd van niet meer dan 400 miljoen KRW of drie procent van het kapitaal, waarbij het hoogste bedrag van toepassing is.
2) Artikel 34-2, leden 3 tot en met 5, zijn mutatis mutandis van toepassing op zaken die noodzakelijk zijn om administratieve boetes op te leggen en te innen.
Artikel 28-7 (Toepassingsgebied) @De artikelen 20, 21 en 27, artikel 34, lid 1, de artikelen 35 tot en met 37, artikel 39-3, artikel 39-4 en de artikelen 39-6 tot en met 39-8 zijn niet van toepassing op gepseudonimiseerde informatie.
Hoofdstuk I Algemene bepalingen
Artikel 3 (Beginselen voor de bescherming van persoonsinformatie) 1) De verantwoordelijke voor de verwerking van persoonsinformatie specificeert uitdrukkelijk voor welke doeleinden de persoonsinformatie wordt verwerkt; hij verzamelt de persoonsinformatie op rechtmatige en behoorlijke wijze in de mate die minimaal noodzakelijk is voor die doeleinden.
2) De verantwoordelijke voor de verwerking van persoonsinformatie verwerkt de persoonsinformatie op passende wijze zoals nodig voor de doeleinden waarvoor de persoonsinformatie wordt verwerkt en gebruikt de persoonsinformatie niet voor andere doeleinden.

3) De verantwoordelijke voor de verwerking van persoonsinformatie zorgt ervoor dat de persoonsinformatie juist, volledig en actueel is voor zover nodig in verband met het doel waarvoor de persoonsinformatie wordt verwerkt.

4) De verantwoordelijke voor de verwerking van persoonsinformatie beheert de persoonsinformatie op veilige wijze, in overeenstemming met de verwerkingsmethoden, soorten enz. van de persoonsinformatie, rekening houdend met de mogelijkheid van inbreuken op de rechten van de betrokkene en de ernst van de desbetreffende risico's.

5) De verantwoordelijke voor de verwerking van persoonsinformatie maakt zijn privacybeleid en andere zaken in verband met de verwerking van de persoonsinformatie openbaar en waarborgt de rechten van de betrokkene, zoals het recht op toegang tot de eigen persoonsinformatie.

6) De verantwoordelijke voor de verwerking van persoonsinformatie verwerkt persoonsinformatie op zodanige wijze dat de mogelijkheid dat inbreuk wordt gemaakt op de privacy van een betrokkene tot een minimum wordt beperkt.

7) Indien het nog steeds mogelijk is om het doel van de verzameling van de persoonsinformatie te verwezenlijken door geanonimiseerde of gepseudonimiseerde informatie te verwerken, streeft de verantwoordelijke voor de verwerking van persoonsinformatie ernaar de persoonsinformatie te verwerken door middel van anonimisering, indien mogelijk, of door middel van pseudonimisering, indien het niet mogelijk is om het doel van de verzameling van de persoonsinformatie te verwezenlijken aan de hand van anonimisering.

8) De verantwoordelijke voor de verwerking van persoonsinformatie streeft ernaar het vertrouwen van betrokkenen te verkrijgen door de taken en verantwoordelijkheden als voorzien in deze Wet en andere gerelateerde wetten na te komen en uit te voeren.

Hoofdstuk IX Aanvullende bepalingen

Artikel 58-2 (Uitsluiting van toepassing) Deze Wet is niet van toepassing op informatie aan de hand waarvan een bepaalde natuurlijke persoon niet langer kan worden geïdentificeerd wanneer deze informatie met andere informatie wordt samengevoegd, waarbij de tijd, kosten, technologie enz. op redelijke wijze in aanmerking worden genomen. <Dit artikel is nieuw ingevoegd bij Wet nr. 16930 van 4 februari 2020>

i) Op grond van hoofdstuk III, deel 3, Speciale gevallen in verband met gepseudonimiseerde gegevens (artikelen 28-2 tot en met 28-7) is het toegestaan gepseudonimiseerde informatie zonder toestemming van de betrokkene te verwerken met het oog op het opstellen van statistieken, wetenschappelijk onderzoek, het bewaren van openbare archieven enz. (artikel 28-2), maar moet in dergelijke gevallen worden gezorgd voor passende waarborgen en verboden die noodzakelijk zijn om de rechten van betrokkenen te beschermen (artikelen 28-4 en 28-5), kunnen boetes worden opgelegd bij inbreuken (artikel 28-6) en zijn bepaalde waarborgen die anders uit hoofde van de PIPA zouden gelden, niet van toepassing (artikel 28-7).

ii) Deze bepalingen zijn niet van toepassing op gevallen waarin gepseudonimiseerde informatie voor andere doeleinden wordt verwerkt dan het opstellen van statistieken, wetenschappelijk onderzoek, het bewaren van openbare archieven enz. Wanneer persoonsinformatie van een EU-burger die aan Korea is doorgegeven overeenkomstig het adequaatheidsbesluit van de Europese Commissie voor andere doeleinden wordt gepseudonimiseerd dan het opstellen van statistieken, wetenschappelijk onderzoek, het bewaren van openbare archieven enz., zijn de speciale bepalingen van hoofdstuk III, deel 3, bijvoorbeeld niet van toepassing ([7]).

iii) Wanneer een verantwoordelijke voor de verwerking van persoonsinformatie gepseudonimiseerde informatie verwerkt met het oog op het opstellen van statistieken, wetenschappelijk onderzoek, het bewaren van openbare archieven enz. en de gepseudonimiseerde informatie niet wordt vernietigd zodra het specifieke doel van de verwerking is verwezenlijkt overeenkomstig artikel 37 van de grondwet en artikel 3 (Beginselen voor de bescherming van persoonsinformatie) van de Wet, anonimiseert hij deze informatie om ervoor te zorgen dat met deze informatie op zich of in combinatie met andere informatie niet langer een specifieke natuurlijke persoon kan worden geïdentificeerd, waarbij op redelijke wijze rekening wordt gehouden met de tijd, kosten, technologie enz. overeenkomstig artikel 58-2 van de PIPA.

5. **Corrigerende maatregelen enz. (artikel 64, leden 1, 2 en 4, van de Wet)**

<Wet bescherming persoonsinformatie

(Wet nr. 16930, gedeeltelijk gewijzigd op 4 februari 2020)>

Artikel 64 (Corrigerende maatregelen) 1) Wanneer de Commissie bescherming persoonsinformatie van mening is dat er zwaarwegende gronden zijn om aan te nemen dat een inbreuk in verband met persoonsinformatie heeft plaatsgevonden en niet handelen waarschijnlijk zal leiden tot schade die moeilijk kan worden hersteld, kan zij degene die inbreuk op deze wet heeft gemaakt (met uitzondering van centrale bestuursinstanties, lokale overheden, de Nationale Vergadering, het Hof, het Grondwettelijk Hof en de Nationale Verkiezingscommissie) gelasten een of meer van de volgende maatregelen te nemen:

1. het stoppen van de inbreuk in verband met de persoonsinformatie;

2. het tijdelijk opschorten van de verwerking van de persoonsinformatie;

([7]) De uitzondering van artikel 40-3 van de Wet kredietinformatie is op vergelijkbare wijze slechts van toepassing op de verwerking van gepseudonimiseerde kredietinformatie met het oog op het opstellen van statistieken, wetenschappelijk onderzoek en het bewaren van openbare archieven.

3. andere maatregelen die noodzakelijk zijn om de persoonsinformatie te beschermen en een inbreuk op de persoonsinformatie te voorkomen.

2) Wanneer het hoofd van een betrokken centrale bestuursinstantie van oordeel is dat er zwaarwegende gronden zijn om aan te nemen dat er een inbreuk op persoonsinformatie heeft plaatsgevonden en niet handelen waarschijnlijk zal leiden tot schade die moeilijk kan worden hersteld, kan hij een verantwoordelijke voor de verwerking van persoonsinformatie gelasten een of meer van de in lid 1 genoemde maatregelen te nemen overeenkomstig de wetten die onder de bevoegdheid van een dergelijke centrale bestuursinstantie vallen.

4) Wanneer een centrale bestuursinstantie, een lokale overheid, de Nationale Vergadering, het Hof, het Grondwettelijk Hof of de Nationale Verkiezingscommissie deze Wet schendt, kan de Commissie bescherming persoonsinformatie het hoofd van de betrokken instantie aanbevelen een of meerdere van de in lid 1 genoemde maatregelen te nemen. In dergelijke gevallen voldoet de instantie aan de ontvangen aanbeveling, tenzij er sprake is van uitzonderlijke omstandigheden.

i) In de vaste rechtspraak ([8]) ([9]) wordt "schade die moeilijk kan worden hersteld" uitgelegd als gevallen die schade kunnen toebrengen aan de persoonlijke rechten of persoonlijke levenssfeer van een natuurlijke persoon.

ii) Dienovereenkomstig verwijst "zwaarwegende gronden [...] om aan te nemen dat er een inbreuk op persoonsinformatie heeft plaatsgevonden en niet handelen waarschijnlijk zal leiden tot schade die moeilijk kan worden hersteld" zoals bepaald in artikel 64, leden 1 en 2, naar gevallen waarin een schending van het recht waarschijnlijk zal leiden tot een inbreuk op de rechten en vrijheid van personen in verband met persoonsinformatie. Dit geldt in alle gevallen waarin de beginselen, rechten en plichten worden geschonden die bij wet zijn vastgesteld ter bescherming van persoonsinformatie ([10]).

iii) Volgens artikel 64, lid 4, van de Wet bescherming persoonsinformatie betreft dit een maatregel in verband met een schending van deze Wet, dat wil zeggen een maatregel tegen een inbreuk op de PIPA.

Een centrale bestuursinstantie enz. is als openbare autoriteit gebonden aan de rechtsstaat, mag geen wetten schenden en is verplicht om corrigerende maatregelen te nemen om onder andere de actie onmiddellijk te stoppen en de schade te vergoeden in de uitzonderlijke gevallen waarin een illegale handeling desondanks werd verricht.

Een centrale bestuursinstantie moet dienovereenkomstig zelfs zonder tussenkomst van de Commissie bescherming persoonsinformatie overeenkomstig artikel 64, lid 4, PIPA een corrigerende maatregel tegen schendingen nemen zodra zij van een schending op de hoogte is.

In het bijzonder wordt het normaal gesproken objectief duidelijk voor de centrale bestuursinstantie enz. dat zij de wet heeft geschonden wanneer zij van de Commissie bescherming persoonsinformatie een aanbeveling voor een corrigerende maatregel ontvangt. Om te rechtvaardigen waarom zij van mening is dat een aanbeveling van de Commissie bescherming persoonsinformatie niet moet worden gevolgd, moet een centrale bestuursinstantie dan ook duidelijk bewijs overleggen dat zij de wet niet heeft geschonden. De aanbeveling moet worden gevolgd, tenzij de Commissie bescherming persoonsinformatie vaststelt dat dit inderdaad niet het geval is.

Bij deze overweging moeten de "uitzonderlijke omstandigheden" van artikel 64, lid 4, van de Wet bescherming persoonsinformatie strikt worden beperkt tot uitzonderlijke omstandigheden waarin duidelijke gronden voor centrale bestuursinstanties enz. bestaan om te bewijzen dat "deze Wet in werkelijkheid niet werd geschonden", zoals "gevallen waarin sprake is van uitzonderlijke omstandigheden (feitelijk of rechtens)" waarvan de Commissie bescherming persoonsinformatie niet op de hoogte was toen zij in eerste instantie haar aanbeveling deed en waarin de Commissie bescherming persoonsinformatie vaststelt dat inderdaad geen schending heeft plaatsgevonden.

6. **Toepassing van de PIPA op de verwerking van persoonsgegevens ten behoeve van de nationale veiligheid, met inbegrip van het onderzoek naar inbreuken en handhaving overeenkomstig de PIPA (artikelen 7-8, 7-9, 58, 3, 4 en 62 PIPA)**

<Wet bescherming persoonsinformatie

(Wet nr. 16930, gedeeltelijk gewijzigd op 4 februari 2020)>

Artikel 7-8 (Werkzaamheden van de Commissie bescherming persoonsinformatie) 1) De Commissie bescherming persoonsinformatie verricht de volgende werkzaamheden: […]

3. werkzaamheden met betrekking tot het onderzoek naar inbreuken op de rechten van betrokkenen en de hieruit voortvloeiende beschikkingen;
4. het afhandelen van klachten of correctieve procedures in verband met de verwerking van persoonsinformatie en bemiddeling bij geschillen over persoonsinformatie;

[…]

([8]) (Arrest 97Da10215,10222 van het Hooggerechtshof van 26 januari 1999) Wanneer de door de beschuldigde gepleegde strafbare feiten via de media bekend worden gemaakt, leidt dit waarschijnlijk tot onherstelbare geestelijke en lichamelijke schade, niet alleen voor het slachtoffer, d.w.z. de eiser, maar ook voor de personen in diens omgeving, waaronder familie.

([9]) (Arrest nr. 2006Na92006 van het Hof van Seoul van 16 januari 2008) Wanneer een lasterlijk artikel wordt gepubliceerd, leidt dit waarschijnlijk tot onherstelbare schade voor de desbetreffende persoon.

([10]) Dezelfde beginselen als uiteengezet in punt ii) zijn van toepassing op artikel 45-4 van de Wet kredietinformatie.

Artikel 7-9 (Zaken die vallen onder de beraadslaging en afhandeling van de Commissie bescherming persoonsinformatie) 1) De Commissie bescherming persoonsinformatie bespreekt de volgende zaken en handelt deze af: […]

5. zaken ten aanzien van de uitlegging en werking van de wet in verband met de bescherming van de persoonsinformatie;

[…]

Artikel 58 (Gedeeltelijke uitsluiting van toepassing) 1) De hoofdstukken III tot en met VII zijn niet van toepassing op de volgende persoonsinformatie:

1. persoonsinformatie die op grond van de Statistiekwet wordt verzameld voor de verwerking door overheidsinstellingen;
2. persoonsinformatie die wordt verzameld of waarom is verzocht met het oog op de analyse van informatie in verband met de nationale veiligheid;
3. persoonsinformatie die tijdelijk wordt verwerkt wanneer dit dringend noodzakelijk is met het oog op de openbare veiligheid, volksgezondheid enz.;
4. persoonsinformatie die wordt verzameld of gebruikt voor de eigen doeleinden van respectievelijk verslaggeving door de pers, zendingswerk van religieuze organisaties en de voordracht van kandidaten door politieke partijen.

[weggelaten 2) en 3)]

4) Wanneer persoonsinformatie wordt verwerkt overeenkomstig lid 1, verwerkt de verantwoordelijke voor de verwerking van persoonsinformatie in de mate die minimaal noodzakelijk is om het beoogde doel te bereiken, gedurende een tot een minimum beperkte periode; hij treft daarnaast de noodzakelijke voorbereidingen, zoals technische, beheers- en fysieke waarborgen, de individuele afhandeling van klachten en andere noodzakelijke maatregelen voor het veilige beheer en de passende verwerking van dergelijke persoonsinformatie.

Artikel 3 (Beginselen voor de bescherming van persoonsinformatie) 1) De verantwoordelijke voor de verwerking van persoonsinformatie specificeert uitdrukkelijk voor welke doeleinden de persoonsinformatie wordt verwerkt; hij verzamelt de persoonsinformatie op rechtmatige en behoorlijke wijze in de mate die minimaal noodzakelijk is voor die doeleinden.

2) De verantwoordelijke voor de verwerking van persoonsinformatie verwerkt de persoonsinformatie op passende wijze zoals nodig voor de doeleinden waarvoor de persoonsinformatie wordt verwerkt en gebruikt de persoonsinformatie niet voor andere doeleinden.

3) De verantwoordelijke voor de verwerking van persoonsinformatie zorgt ervoor dat de persoonsinformatie juist, volledig en actueel is voor zover nodig in verband met het doel waarvoor de persoonsinformatie wordt verwerkt.

4) De verantwoordelijke voor de verwerking van persoonsinformatie beheert de persoonsinformatie op veilige wijze, in overeenstemming met de verwerkingsmethoden, soorten enz. van de persoonsinformatie, rekening houdend met de mogelijkheid van inbreuken op de rechten van de betrokkene en de ernst van de desbetreffende risico's.

5) De verantwoordelijke voor de verwerking van persoonsinformatie maakt zijn privacybeleid en andere zaken in verband met de verwerking van de persoonsinformatie openbaar en waarborgt de rechten van de betrokkene, zoals het recht op toegang tot de eigen persoonsinformatie.

6) De verantwoordelijke voor de verwerking van persoonsinformatie verwerkt persoonsinformatie op zodanige wijze dat de mogelijkheid dat inbreuk wordt gemaakt op de privacy van een betrokkene tot een minimum wordt beperkt.

7) Indien het nog steeds mogelijk is om het doel van de verzameling van de persoonsinformatie te verwezenlijken door geanonimiseerde of gepseudonimiseerde informatie te verwerken, streeft de verantwoordelijke voor de verwerking van persoonsinformatie ernaar de persoonsinformatie te verwerken door middel van anonimisering, indien mogelijk, of door middel van pseudonimisering, indien het niet mogelijk is om het doel van de verzameling van de persoonsinformatie te verwezenlijken aan de hand van anonimisering.

8) De verantwoordelijke voor de verwerking van persoonsinformatie streeft ernaar het vertrouwen van betrokkenen te verkrijgen door de taken en verantwoordelijkheden als voorzien in deze Wet en andere gerelateerde wetten na te komen en uit te voeren.

Artikel 4 (Rechten van betrokkenen) Betrokkenen hebben de volgende rechten in verband met de verwerking van hun eigen persoonsinformatie:

1. het recht te worden geïnformeerd over de verwerking van die persoonsinformatie;
2. het recht te bepalen of zij instemmen met de verwerking van die persoonsinformatie en de reikwijdte van hun toestemming;
3. het recht op bevestiging van de vraag of de persoonsinformatie wordt verwerkt en om toegang te verzoeken (met inbegrip van het verstrekken van kopieën; dit geldt hierna ook) tot die persoonsinformatie;
4. het recht op opschorting van de verwerking en te verzoeken om de correctie, verwijdering en vernietiging van die persoonsinformatie;
5. het recht op een passend rechtsmiddel in verband met schade die voortvloeit uit de verwerking van die persoonsinformatie via een snelle en eerlijke procedure.

Artikel 62 (Verslaglegging over inbreuken) 1) Eenieder wiens rechten of belangen in verband met zijn persoonsinformatie worden geschonden in het kader van de verwerking van persoonsinformatie door een verantwoordelijke voor de verwerking van persoonsinformatie kan een dergelijke inbreuk melden bij de Commissie bescherming persoonsinformatie.
2) De Commissie bescherming persoonsinformatie kan een gespecialiseerde instelling aanwijzen om de klachten overeenkomstig lid 1 op efficiënte wijze in ontvangst te nemen en af te handelen zoals voorgeschreven bij presidentieel decreet. In die gevallen richt die gespecialiseerde instelling een callcenter voor inbreuken op de persoonsinformatie (hierna "Privacy Call Centre" genoemd) op en beheert zij dit.
3) Het Privacy Call Centre verricht de volgende taken:
1. het in ontvangst nemen van klachten en het verstrekken van advies in verband met de verwerking van persoonsinformatie;
2. het onderzoeken en bevestigen van incidenten en het horen van standpunten van de betrokken partijen;
3. bijkomende taken op grond van de leden 1 en 2.

4) De Commissie bescherming persoonsinformatie kan, indien noodzakelijk, haar ambtenaar naar de gespecialiseerde instelling die op grond van lid 2 is aangewezen, sturen overeenkomstig artikel 32-4 van de Staatsambtenarenwet om de incidenten op efficiënte wijze te onderzoeken en te bevestigen overeenkomstig lid 3, punt 2.

i) De verzameling van persoonsinformatie met het oog op de nationale veiligheid wordt geregeld in specifieke wetten die aan bevoegde autoriteiten (bv. de Nationale Inlichtingendienst) de bevoegdheid verlenen om onder bepaalde voorwaarden en met waarborgen communicatie te onderscheppen of om de bekendmaking hiervan te verzoeken (hierna "wetten betreffende de nationale veiligheid" genoemd). Deze wetten betreffende de nationale veiligheid omvatten onder meer de Wet op de bescherming van de communicatieprivacy, de Wet inzake terrorismebestrijding ter bescherming van burgers en de openbare veiligheid en de Wet op de telecommunicatieactiviteiten. De verzameling en verdere verwerking van persoonsinformatie moet bovendien voldoen aan de vereisten van de PIPA. In dit verband is in artikel 58, lid 1, punt 2, PIPA bepaald dat de hoofdstukken III tot en met VII niet van toepassing zijn op persoonsinformatie die wordt verzameld of waarom is verzocht met het oog op de analyse van informatie in verband met de nationale veiligheid. Deze gedeeltelijke uitzondering is daarom van toepassing op de verwerking van persoonsinformatie met het oog op de nationale veiligheid.
Hoofdstuk I (Algemene bepalingen), hoofdstuk II (Vaststelling van beleid ter bescherming van persoonsinformatie enz.), hoofdstuk VIII (Collectieve rechtszaak vanwege een gegevensinbreuk), hoofdstuk IX (Aanvullende bepalingen) en hoofdstuk X (Sanctiebepalingen) van de PIPA zijn echter wel van toepassing op de verwerking van dergelijke persoonsinformatie. Dit omvat de algemene beginselen voor gegevensbescherming van artikel 3 (Beginselen van de bescherming van persoonsinformatie) en de individuele rechten die worden gewaarborgd door artikel 4 PIPA (Rechten van betrokkenen).
Daarnaast is in artikel 58, lid 4, PIPA bepaald dat de verwerking van dergelijke informatie moet worden beperkt tot wat minimaal noodzakelijk is om het beoogde doel te bereiken, gedurende een tot een minimum beperkte periode; dit artikel vereist bovendien dat de verantwoordelijke voor de verwerking van persoonsinformatie zorgt voor de noodzakelijke maatregelen om een veilig gegevensbeheer en een passende verwerking te waarborgen, zoals technische, beheers- en fysieke waarborgen, evenals voor maatregelen voor de passende afhandeling van individuele klachten.
Tot slot zijn de bepalingen inzake de taken en bevoegdheden van de PIPC (met inbegrip van artikel 60-65 PIPA inzake de afhandeling van klachten en de vaststelling van aanbevelingen en corrigerende maatregelen), alsook de bepalingen inzake administratieve en strafrechtelijke sancties (artikel 70 e.v. PIPA) van toepassing. Overeenkomstig artikel 7-8, lid 1, punten 3 en 4, en artikel 7-9, lid 1, punt 5, PIPA hebben deze onderzoeks- en corrigerende bevoegdheden, ook wanneer zij worden uitgeoefend in het kader van de afhandeling van klachten, ook betrekking op mogelijke inbreuken op de voorschriften die zijn opgenomen in specifieke wetten waarin de beperkingen en waarborgen zijn uiteengezet in verband met de verzameling van persoonsinformatie, zoals de wetten betreffende de nationale veiligheid. Gezien de vereisten van artikel 3, lid 1, PIPA met betrekking tot de rechtmatige en behoorlijke verzameling van persoonsinformatie vormt een dergelijke inbreuk een schending van "deze Wet" in de zin van de artikelen 63 en 64, die de PIPC toestaat een onderzoek uit te voeren en corrigerende maatregelen te nemen ([11]).
De uitoefening van deze bevoegdheden door de PIPC vormt een aanvulling op, maar geen vervanging van, de bevoegdheden van de Nationale Mensenrechtencommissie op grond van de Wet inzake de Mensenrechtencommissie.
De toepassing van de kernbeginselen, rechten en verplichtingen van de PIPA op de verwerking van persoonsinformatie met het oog op de nationale veiligheid weerspiegelt de in de grondwet verankerde waarborgen in verband met de bescherming van het recht van natuurlijke personen op controle over hun eigen persoonsinformatie. Zoals door het Grondwettelijk Hof werd erkend, omvat dit het recht van een natuurlijke persoon ([12]) om zelf te beslissen wanneer, aan wie of door wie en in welke mate zijn informatie wordt bekendgemaakt of gebruikt. Dit is, aldus dit hof, een basisrecht ([13]) dat bestaat om de persoonlijke beslissingsvrijheid te beschermen tegen het risico dat wordt veroorzaakt door de uitbreiding van de taken van de staat en de informatiecommunicatietechnologie. Elke beperking van dat recht, bijvoorbeeld wanneer dit noodzakelijk is voor de bescherming van de nationale veiligheid, vereist een afweging van de rechten en belangen van het individu tegen het betrokken openbaar belang en mag de wezenlijke inhoud van het recht niet aantasten (artikel 37, lid 2, van de grondwet).

([11]) Zie wat corrigerende maatregelen overeenkomstig artikel 64 betreft ook deel 5 hierboven.
([12]) Arrest nr. 99HunMa513, 2004HunMa190 van het Grondwettelijk Hof van 26 mei 2005.
([13]) Arrest nr. 2003HunMa282 van het Grondwettelijk Hof van 21 juli 2005.

Bij het verwerken van persoonsinformatie met het oog op de nationale veiligheid moet de verwerkingsverantwoordelijke (bv. de Nationale Inlichtingendienst) derhalve onder meer het volgende doen:

1) uitdrukkelijk vermelden voor welke doeleinden de persoonsinformatie wordt verwerkt en de persoonsinformatie op rechtmatige en behoorlijke wijze verzamelen, waarbij deze tot het voor deze doeleinden noodzakelijke minimum wordt beperkt (artikel 3, lid 1, PIPA). Meer specifiek mag hij de persoonsinformatie alleen verzamelen en verder verwerken om de taken uit te voeren die hij op grond van de desbetreffende wetten heeft, zoals de Wet op de Nationale Inlichtingendienst;

2) de verwerking van de persoonsinformatie tot een minimum beperken, gedurende de minimumperiode die noodzakelijk is om het beoogde doel te bereiken (artikel 58, lid 4, PIPA); zodra het doel van de verwerking is bereikt, wordt de persoonsinformatie onomkeerbaar vernietigd door de verwerkingsverantwoordelijke, tenzij verdere bewaring specifiek is vereist op grond van een wet, in welk geval de desbetreffende persoonsinformatie gescheiden van andere persoonsinformatie wordt opgeslagen en beheerd, niet wordt gebruikt voor een ander dan in de wet beschreven doel en aan het einde van de bewaartermijn wordt vernietigd;

3) persoonsinformatie op passende wijze verwerken zoals nodig voor de doeleinden waarvoor de persoonsinformatie wordt verwerkt en de persoonsinformatie niet voor andere doeleinden gebruiken (artikel 3, lid 2, PIPA);

4) ervoor zorgen dat de persoonsinformatie juist, volledig en actueel is voor zover nodig in verband met het doel waarvoor de persoonsinformatie wordt verwerkt (artikel 3, lid 3, PIPA);

5) de persoonsinformatie op veilige wijze, in overeenstemming met de verwerkingsmethoden, soorten enz. van de persoonsinformatie, beheren, rekening houdend met de mogelijkheid van inbreuken op de rechten van de betrokkene en de ernst van de desbetreffende risico's (artikel 3, lid 4, PIPA);

6) zijn privacybeleid en andere zaken in verband met de verwerking van de persoonsinformatie openbaar maken (artikel 3, lid 5, PIPA);

7) persoonsinformatie op zodanige wijze verwerken dat de mogelijkheid dat inbreuk wordt gemaakt op de privacy van betrokkenen tot een minimum wordt beperkt (artikel 3, lid 6, PIPA).

ii) Overeenkomstig artikel 58, lid 4, PIPA treft de verwerkingsverantwoordelijke (bv. autoriteiten die bevoegd zijn voor de nationale veiligheid, zoals de Nationale Inlichtingendienst) de noodzakelijke regelingen, zoals het voorzien in technische, beheers- en fysieke waarborgen, om te zorgen voor de naleving van deze beginselen en de passende verwerking van persoonsinformatie. Dit kan bijvoorbeeld specifieke maatregelen omvatten om de veiligheid van de persoonsinformatie te waarborgen, zoals beperkingen van de toegang tot de persoonsinformatie, toegangscontroles, aanmeldingen, het voorzien in een speciale opleiding voor personeel over de omgang met persoonsinformatie enz.

Daarnaast hebben betrokkenen op grond van artikel 3, lid 5, en artikel 4 PIPA onder meer de volgende rechten met betrekking tot persoonsinformatie die met het oog op de nationale veiligheid wordt verwerkt:

1) het recht om uitsluitsel te verkrijgen over het al dan niet verwerken van hun persoonsinformatie en om informatie te verkrijgen over de verwerking, alsook het recht op toegang tot die informatie, met inbegrip van het verstrekken van kopieën (artikel 4, leden 1 en 3, PIPA);

2) het recht op opschorting van de verwerking en op de correctie, verwijdering en vernietiging van persoonsinformatie (artikel 4, lid 4, PIPA).

iii) Een betrokkene kan in het kader van de uitoefening van deze rechten direct bij de verwerkingsverantwoordelijke of indirect bij de Commissie bescherming persoonsinformatie een verzoek indienen en kan zijn vertegenwoordiger hiertoe opdracht geven. Wanneer de betrokkene een verzoek indient, kent de verwerkingsverantwoordelijke het recht onverwijld toe; hij kan dit recht echter uitstellen, beperken of ontzeggen wanneer specifiek in deze mogelijkheid is voorzien of dit onvermijdelijk is om aan andere wettelijke verplichtingen te voldoen voor zover en zolang dit noodzakelijk en evenredig is voor de bescherming van een belangrijke doelstelling van openbaar belang (bijvoorbeeld voor zover en zolang de verlening van het recht een lopend onderzoek in gevaar zou brengen of de nationale veiligheid zou bedreigen), of wanneer de verlening van het recht schade kan toebrengen aan het leven of de lichamelijke integriteit van een derde of een ongerechtvaardigde inbreuk kan vormen op eigendoms- of andere belangen van een derde. Wanneer het verzoek wordt afgewezen of beperkt, stelt de verwerkingsverantwoordelijke de betrokkene onverwijld in kennis van de redenen daarvoor. De verwerkingsverantwoordelijke bereidt de methode en procedure voor om betrokkenen in staat te stellen verzoeken in te dienen en maakt deze openbaar, zodat betrokkenen hiervan op de hoogte kunnen zijn.

Op grond van artikel 58, lid 4, PIPA (vereiste ter waarborging van de passende afhandeling van individuele klachten) en artikel 4, lid 5, PIPA (het recht op een passend rechtsmiddel in verband met schade die voortvloeit uit de verwerking van persoonsinformatie via een snelle en eerlijke procedure) hebben betrokkenen bovendien het recht om verhaal te halen. Dit omvat het recht om een vermeende inbreuk te melden bij het Centrum voor inbreuken op de persoonsinformatie (overeenkomstig artikel 62, lid 3, PIPA), bij de PIPC overeenkomstig artikel 62 PIPA een klacht in te dienen over een schending van rechten of belangen in verband met de persoonsinformatie van een natuurlijke persoon en gerechtelijk beroep in te stellen tegen besluiten of nalatigheid van de PIPC op grond van de Wet administratieve procesvoering. Daarnaast kunnen betrokkenen op grond van de Wet administratieve procesvoering beroep instellen wanneer hun rechten of belangen zijn geschonden als gevolg van een beschikking of nalatigheid van de verwerkingsverantwoordelijke (bv. onrechtmatige verzameling van persoonsgegevens) of kunnen zij een schadevergoeding verkrijgen overeenkomstig de Wet inzake overheidscompensatie. Deze verhaalsmiddelen zijn zowel beschikbaar voor mogelijke inbreuken op de voorschriften die zijn opgenomen in specifieke wetten waarin de beperkingen en waarborgen in verband met de verzameling van persoonsinformatie zijn vastgesteld, zoals de wetten betreffende de nationale veiligheid, als voor mogelijke inbreuken op de PIPA.

Een EU-burger kan bij de PIPC een klacht indienen via zijn nationale gegevensbeschermingsautoriteit en de PIPC zal de betrokkene informeren via de nationale gegevensbeschermingsautoriteit, nadat het onderzoek en de corrigerende maatregel (indien van toepassing) zijn afgerond.

BIJLAGE II

18 mei 2021

Zijne Excellentie de heer Didier Reynders, commissaris voor Justitie van de Europese Commissie

Excellentie,

Ik verheug mij over de constructieve besprekingen tussen Korea en de Europese Commissie om een kader tot stand te brengen voor de doorgifte van persoonsgegevens van de EU aan Korea.

Overeenkomstig het verzoek van de Europese Commissie aan de Koreaanse regering stuur ik u hierbij een overzicht van het juridische kader inzake de toegang tot informatie door de Koreaanse regering.

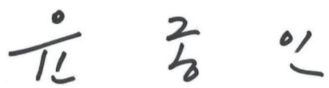
Dit document betreft veel ministeries en agentschappen van de Koreaanse overheid en met betrekking tot de inhoud van het document zijn de relevante ministeries en agentschappen (de Commissie bescherming persoonsinformatie, het ministerie van Justitie, de Nationale Inlichtingendienst, de Nationale Mensenrechtencommissie van Korea, het Nationaal Centrum voor terrorismebestrijding, de Koreaanse Financiële-Inlichtingeneenheid) verantwoordelijk voor de passages die binnen hun respectieve bevoegdheden vallen. Hieronder vindt u een lijst van de desbetreffende ministeries en agentschappen en degenen die bevoegd zijn tot ondertekening.

Vragen over dit document kunnen worden gericht tot de Commissie bescherming persoonsinformatie, die zal zorgen voor de coördinatie van de antwoorden tussen de betrokken ministeries en agentschappen.

Ik hoop dat dit document nuttig is voor de besluitvorming binnen de Europese Commissie.

Ik waardeer uw grote bijdrage op dit vlak tot nu toe.

Hoogachtend,



Yoon Jong In
voorzitter van de Commissie bescherming persoonsinformatie

Dit document is opgesteld door de Commissie bescherming persoonsinformatie en de volgende ministeries en agentschappen.

Park Jie Won
Voorzitter(directeur), Nationale Inlichtingendienst

Lee Jung Soo
Directeur-generaal, ministerie van Justitie

Choi Young Ae
Voorzitter, Nationale Mensenrechtencommissie van Korea

Kim Hyuck Soo
Directeur, Nationaal Centrum voor terrorismebestrijding

Kim, Jeong Kag
Commissaris, Koreaanse Financiële-Inlichtingeneenheid

Rechtskader voor de verzameling en het gebruik van persoonsgegevens door Koreaanse overheidsinstanties met het oog op de rechtshandhaving en de nationale veiligheid

Dit document bevat een overzicht van het juridische kader voor de verzameling en het gebruik van persoonsgegevens door de Koreaanse overheid met het oog op de handhaving van het strafrecht en de nationale veiligheid (hierna "overheidstoegang" genoemd), met name wat betreft de geldende rechtsgrondslag, toepasselijke voorwaarden (beperkingen) en waarborgen, alsook onafhankelijk toezicht en individuele verhaalsmogelijkheden.

1. ALGEMENE JURIDISCHE BEGINSELEN INZAKE OVERHEIDSTOEGANG

1.1. Grondwettelijk kader

In de grondwet van de Republiek Korea zijn het recht op privacy in het algemeen (artikel 17) en het recht op het briefgeheim in het bijzonder (artikel 18) vastgelegd. De staat heeft als taak deze grondrechten te beschermen ([1]). In de grondwet is verder bepaald dat de rechten en vrijheden van burgers slechts bij wet mogen worden beperkt en indien dat noodzakelijk is voor de nationale veiligheid of de handhaving van de openbare orde met het oog op het openbaar welzijn ([2]). Zelfs wanneer dergelijke beperkingen worden opgelegd, mogen deze geen gevolgen hebben voor de wezenlijke aspecten van de vrijheid of het recht ([3]). De Koreaanse rechters hebben deze bepalingen toegepast in zaken die betrekking hadden op de inmenging van de overheid in de persoonlijke levenssfeer. Het Hooggerechtshof oordeelde bijvoorbeeld dat de bewaking van burgers in strijd was met het grondrecht op privacy, waarbij het benadrukte dat burgers het recht op zelfbeschikking in verband met persoonsinformatie hebben ([4]). In een andere zaak oordeelde het Grondwettelijk Hof dat de privacy een grondrecht is dat voorziet in de bescherming tegen inmenging van de staat en observatie van het privéleven van burgers ([5]).

De Koreaanse grondwet waarborgt bovendien dat personen niet worden gearresteerd, vastgehouden, gefouilleerd of verhoord en dat er geen voorwerpen in beslag worden genomen tenzij in gevallen die bij wet zijn bepaald ([6]). Onderzoeken en inbeslagnemingen mogen bovendien slechts op grond van een gerechtelijk bevel, op verzoek van een aanklager en met eerbiediging van de juiste procedures worden uitgevoerd ([7]). In uitzonderlijke omstandigheden, dat wil zeggen wanneer een verdachte tijdens het plegen van een strafbaar feit wordt betrapt (op heterdaad) of wanneer het risico bestaat dat een verdachte van een strafbaar feit waarop een gevangenisstraf van drie jaar of meer staat zal ontsnappen of bewijs zal vernietigen, mogen de onderzoeksautoriteiten zonder bevel onderzoeken of inbeslagnemingen verrichten. In dat geval moeten zij achteraf een verzoek om een bevel indienen ([8]). Deze algemene beginselen zijn verder uitgewerkt in specifieke wetten die de strafprocedure en de bescherming van de communicatie betreffen (zie hieronder voor een gedetailleerd overzicht).

Met betrekking tot buitenlandse staatsburgers is in de grondwet bepaald dat hun status wordt gewaarborgd zoals voorgeschreven door het internationaal recht en verdragen ([9]). Verschillende internationale overeenkomsten waarbij Korea partij is, waarborgen privacyrechten, 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). Daarnaast heeft het Grondwettelijk Hof geoordeeld dat hoewel de grondwet in principe verwijst naar de rechten van "*staatsburgers*", buitenlandse onderdanen ook basisrechten genieten ([10]). Dit hof oordeelde met name dat de bescherming van de waardigheid en de waarde van een persoon als mens, alsook het recht te streven

([1]) Artikel 10 van de grondwet van de Republiek Korea, bekendgemaakt op 17 juli 1948 (hierna "de grondwet").
([2]) Artikel 37, lid 2, van de grondwet.
([3]) Artikel 37, lid 2, van de grondwet.
([4]) Beslissing nr. 96DA42789 van het Hooggerechtshof van Korea van 24 juli 1998.
([5]) Beslissing nr. 2002Hun-Ma51 van het Grondwettelijk Hof van 30 oktober 2003. In de Beslissingen 99Hun-Ma513 en 2004Hun-Ma190 (geconsolideerd) van 26 mei 2005 verduidelijkte het Grondwettelijk Hof op vergelijkbare wijze dat het recht op controle over de eigen persoonsinformatie een recht is van de persoon over wie deze informatie handelt om zelf te beslissen wanneer, aan wie of door wie en in welke mate zijn of haar informatie wordt verstrekt respectievelijk gebruikt. Hoewel het niet is gespecificeerd in de grondwet, is het volgens dit hof een basisrecht dat bestaat om de persoonlijke beslissingsvrijheid te beschermen tegen het risico dat wordt veroorzaakt door de uitbreiding van de taken van de staat en de informatiecommunicatietechnologie.
([6]) Artikel 12, lid 1, eerste zin, van de grondwet.
([7]) Artikel 16 en artikel 12, lid 3, van de grondwet.
([8]) Artikel 12, lid 3, van de grondwet.
([9]) Artikel 6, lid 2, van de grondwet.
([10]) Beslissing nr. 93Hun-MA120 van het Grondwettelijk Hof van donderdag 29 december 1994. Zie bijvoorbeeld ook Beslissing nr. 2014Hun-Ma346 van het Grondwettelijk Hof (31 mei 2018), waarbij het hof oordeelde dat het grondwettelijk recht op rechtsbijstand van een Sudanees onderdaan die op de luchthaven werd vastgehouden, was geschonden. In een andere zaak oordeelde het Grondwettelijk Hof dat de vrijheid om de eigen legale werkplek te kiezen nauw verband houdt met het recht om te streven naar geluk en met de menselijke waardigheid en waarde en derhalve niet beperkt is tot de eigen staatsburgers, maar ook kan worden gewaarborgd voor buitenlanders die legaal werkzaam zijn in de Republiek Korea (Beslissing nr. 2007Hun-Ma1083 van het Grondwettelijk Hof van 29 september 2011).

naar geluk, rechten zijn van ieder mens, niet alleen van de eigen staatsburgers ([11]). Het verduidelijkte ook dat het recht op controle van de eigen informatie wordt beschouwd als een basisrecht dat gebaseerd is op het recht op waardigheid, het streven naar geluk en het recht op een privéleven ([12]). Hoewel in de vaste rechtspraak het recht op privacy van niet-Koreaanse onderdanen tot nu toe nog niet specifiek is behandeld, is de algemeen geldende opvatting onder wetenschappers dat de artikelen 12 tot en met 22 van de grondwet (waaronder het recht op privacy en de persoonlijke vrijheid) "mensenrechten" zijn.

Tot slot voorziet de grondwet ook in een recht om een billijke schadevergoeding van overheidsinstanties te vorderen ([13]). Op basis van de Wet op het Grondwettelijk Hof kan elke persoon wiens door de grondwet gewaarborgde rechten zijn geschonden als gevolg van de uitoefening van een overheidsbevoegdheid (met uitzondering van uitspraken van de rechtbanken) een grondwettelijke klacht indienen bij het Grondwettelijk Hof ([14]).

1.2. **Algemene gegevensbeschermingsvoorschriften**

De algemene wet voor de gegevensbescherming in de Republiek Korea, de Wet bescherming persoonsinformatie (*Personal Information Protection Act* — PIPA), is zowel op de particuliere als de openbare sector van toepassing. In verband met overheidsinstanties wordt in de PIPA specifiek verwezen naar de verplichting om beleid op te stellen ter voorkoming van misbruik en oneigenlijk gebruik van persoonsinformatie, willekeurige surveillance en tracering enz. en ter versterking van de menselijke waardigheid en de persoonlijke levenssfeer ([15]).

De verwerking van persoonsgegevens met het oog op de rechtshandhaving valt volledig onder de vereisten van de PIPA. Dit houdt in dat de strafrechtelijke handhavingsinstanties de verplichtingen in verband met een rechtmatige verwerking moeten naleven, dat wil zeggen zich moeten laten leiden door een van de in de PIPA opgenomen rechtsgronden voor het verzamelen, gebruiken of verstrekken van persoonsinformatie (de artikelen 15 tot en met 18 PIPA) en dat zij de beginselen moeten naleven van doelbinding (artikel 3, leden 1 en 2, PIPA), evenredigheid/gegevensminimalisatie (artikel 3, leden 1 en 6, PIPA), de beperkte bewaring van gegevens (artikel 21 PIPA), gegevensbeveiliging, waaronder de kennisgeving over gegevenslekken (artikel 3, lid 4, en de artikelen 29 en 34 PIPA) en transparantie (artikel 3, leden 1 en 5, en de artikelen 20, 30 en 32 PIPA). Er zijn specifieke waarborgen van toepassing met betrekking tot gevoelige informatie (artikel 23 PIPA). Bovendien kunnen personen overeenkomstig artikel 3, lid 5, en artikel 4 PIPA, evenals de artikelen 35 tot en met 39-2 PIPA, hun rechten op toegang, correctie, verwijdering en opschorting uitoefenen ten opzichte van rechtshandhavingsinstanties.

Hoewel de PIPA dus volledig van toepassing is op de verwerking van persoonsgegevens met het oog op de handhaving van het strafrecht, bevat de wet een uitzondering voor de verwerking van persoonsgegevens met het oog op de nationale veiligheid. Overeenkomstig artikel 58, lid 1, punt 2, PIPA is bepaald dat de artikelen 15 tot en met 50 niet van toepassing zijn op persoonsinformatie die wordt verzameld of waarom is verzocht met het oog op de analyse van informatie in verband met de nationale veiligheid ([16]). Hoofdstuk I (Algemene bepalingen), hoofdstuk II (Vaststelling van beleid ter bescherming van persoonsinformatie enz.), hoofdstuk VIII (Collectieve rechtszaak vanwege een gegevensinbreuk), hoofdstuk IX (Aanvullende bepalingen) en hoofdstuk X (Sanctiebepalingen) van de PIPA blijven in dat geval echter wel van toepassing. Dit omvat de algemene beginselen voor gegevensbescherming van artikel 3 (Beginselen van de bescherming van persoonsinformatie) en de individuele rechten die worden gewaarborgd door artikel 4 PIPA (Rechten van betrokkenen). Dit betekent dat de belangrijkste beginselen en rechten ook op dit gebied gewaarborgd zijn. Daarnaast is in artikel 58, lid 4, PIPA bepaald dat de verwerking van dergelijke informatie moet worden beperkt tot wat minimaal noodzakelijk is om het beoogde doel te bereiken, gedurende een tot een minimum beperkte periode; dit artikel vereist ook dat de verantwoordelijke voor de verwerking van persoonsinformatie zorgt voor de noodzakelijke maatregelen om een veilig gegevensbeheer en een passende verwerking te waarborgen, zoals technische, beheers- en fysieke waarborgen, evenals maatregelen voor de passende afhandeling van individuele klachten.

In Kennisgeving nr. 2021-1 over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie heeft de Commissie bescherming persoonsinformatie (Personal Information Protection Commission — *PIPC*) verder verduidelijkt hoe de PIPA van toepassing is op de verwerking van persoonsgegevens met het oog op de nationale veiligheid, in het licht van deze gedeeltelijke vrijstelling ([17]). Dit omvat onder meer de rechten van personen (toegang, rectificatie, opschorting en verwijdering) en de gronden en grenzen voor de mogelijke beperkingen daarvan. Volgens de kennisgeving weerspiegelt de toepassing van de kernbeginselen, rechten en verplichtingen van de PIPA op de verwerking van persoonsinformatie met het oog op de nationale veiligheid de waarborgen waarin in de grondwet is voorzien in verband met de bescherming van het recht van natuurlijke personen op controle over hun eigen persoonsinformatie. Elke beperking van dat recht, bijvoorbeeld wanneer dit noodzakelijk is voor de

([11]) Beslissing nr. 99HeonMa494 van het Grondwettelijk Hof van 29 november 2001.
([12]) Zie bijvoorbeeld Beslissing nr. 99HunMa513 van het Grondwettelijk Hof.
([13]) Artikel 29, lid 1, van de grondwet.
([14]) Artikel 68, lid 1, van de Wet op het Grondwettelijk Hof.
([15]) Artikel 5, lid 1, PIPA.
([16]) Artikel 58, lid 1, punt 2, PIPA.
([17]) Kennisgeving nr. 2021-1 van de PIPC over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie, deel III, punt 6.

bescherming van de nationale veiligheid, vereist een afweging van de rechten en belangen van het individu tegen het betrokken openbaar belang en mag de wezenlijke inhoud van het recht niet aantasten (artikel 37, lid 2, van de grondwet).

2. OVERHEIDSTOEGANG MET HET OOG OP DE RECHTSHANDHAVING

2.1. Bevoegde overheidsinstanties op het gebied van de rechtshandhaving

Op basis van het Wetboek van strafvordering (*Criminal Procedure Act* — CPA), de Wet op de bescherming van de communicatieprivacy (*Communications Privacy Protection Act* — CPPA) en de Wet op de telecommunicatieactiviteiten (*Telecommunications Business Act* — TBA) mogen de politie, aanklagers en rechters persoonsgegevens verzamelen met het oog op de handhaving van het strafrecht. Voor zover deze bevoegdheid ook aan de Nationale Inlichtingendienst (*National Intelligence Service* — NIS) is verleend bij de Wet op de Nationale Inlichtingendienst (hierna de "NIS-wet" genoemd) moet deze dienst de bovengenoemde wetten naleven ([18]). Tot slot voorziet de Wet inzake de verslaglegging over en het gebruik van bepaalde informatie over financiële transacties (*Act on Reporting and Using Specified Financial Transaction Information* — ARUSFTI) in een rechtsgrond voor financiële instellingen om informatie te verstrekken aan de Koreaanse Financiële-Inlichtingeneenheid (*Korea Financial Intelligence Unit* — KOFIU) voor het voorkomen van het witwassen van geld en de financiering van terrorisme. Dit gespecialiseerde agentschap mag dergelijke informatie vervolgens verstrekken aan rechtshandhavingsinstanties. Deze openbaarmakingsverplichtingen gelden echter alleen voor verwerkingsverantwoordelijken die persoonlijke kredietinformatie verwerken overeenkomstig de Wet kredietinformatie en onder toezicht staan van de Commissie financiële diensten. Aangezien de verwerking van persoonlijke kredietinformatie door dergelijke verwerkingsverantwoordelijken is uitgesloten van het toepassingsgebied van het adequaatheidsbesluit, worden de beperkingen en waarborgen die in het kader van de ARUSFTI van toepassing zijn, in dit document niet nader beschreven.

2.2. Rechtsgrondslagen en beperkingen

Het CPA (zie 2.2.1), de CPPA (zie 2.2.2) en de TBA (zie 2.2.3) voorzien in rechtsgrondslagen voor de verzameling van persoonsinformatie met het oog op de rechtshandhaving en bevatten de toepasselijke beperkingen en waarborgen.

2.2.1. *Onderzoeken en inbeslagnemingen*

2.2.1.1. Rechtsgrondslag

Aanklagers en hoge ambtenaren bij de gerechtelijke politie mogen slechts voorwerpen inspecteren, personen fouilleren of voorwerpen in beslag nemen 1) wanneer een persoon wordt verdacht van het plegen van een strafbaar feit, 2) wanneer dit noodzakelijk is voor het onderzoek en 3) wanneer de voorwerpen die moeten worden geïnspecteerd, de personen die moeten worden gefouilleerd en de voorwerpen die in beslag moeten worden genomen, geacht worden verband te houden met de zaak ([19]). Ook rechters mogen doorzoekingen verrichten en voorwerpen in beslag nemen die als bewijs zullen worden gebruikt of die voor verbeurdverklaring in aanmerking komen, zolang dergelijke voorwerpen of personen geacht worden verband te houden met een specifieke zaak ([20]).

2.2.1.2. Beperkingen en waarborgen

Aanklagers en ambtenaren bij de gerechtelijke politie hebben de algemene verplichting de mensenrechten van verdachten in strafzaken en van eventuele andere betrokkenen te eerbiedigen ([21]). Daarnaast mogen verplichte maatregelen om het doel van het onderzoek te bereiken slechts worden genomen wanneer hierin uitdrukkelijk is voorzien in het CPA en als dit in een zo beperkt mogelijke mate gebeurt ([22]).

Fouilleringen, doorzoekingen, inspecties en inbeslagnemingen door politieambtenaren of aanklagers als onderdeel van een strafrechtelijk onderzoek mogen slechts plaatsvinden op basis van een rechterlijk bevel ([23]). De autoriteit die om een bevel verzoekt, moet bewijs indienen waaruit blijkt dat er redenen zijn om iemand ervan te verdenken een strafbaar feit te hebben gepleegd, dat het onderzoek of de inbeslagneming noodzakelijk is en dat de in beslag te nemen voorwerpen bestaan ([24]). In het bevel moeten naast andere elementen de namen van de verdachte en het strafbare feit; de plaats, de persoon die moet worden gefouilleerd of de voorwerpen die moeten worden doorzocht of in beslag moeten worden genomen; de datum van afgifte, en de feitelijke periode van toepassing worden vermeld ([25]). Wanneer de onderzoeken en inbeslagnemingen als onderdeel van een lopende gerechtelijke procedure, maar niet tijdens een openbare zitting plaatsvinden, moet ook vooraf een rechterlijk bevel worden verkregen ([26]). De betrokkene en diens advocaat worden vooraf op de hoogte gesteld van het onderzoek of de inbeslagneming en mogen aanwezig zijn wanneer het bevel wordt uitgevoerd ([27]).

([18]) Zie artikel 3 van de NIS-wet (Wet nr. 12948), waarin wordt verwezen naar strafrechtelijke onderzoeken in verband met bepaalde misdrijven, zoals oproer, rebellie en misdaden in verband met de nationale veiligheid (bv. spionage). De procedures van het CPA met betrekking tot onderzoeken en inbeslagnemingen zouden in een dergelijke context van toepassing zijn, terwijl de CPPA van toepassing zou zijn op de verzameling van communicatiegegevens (zie deel 3 over de bepalingen inzake de toegang tot communicatie met het oog op de nationale veiligheid).
([19]) Artikel 215, leden 1 en 2, CPA.
([20]) Artikel 106, lid 1, artikel 107 en artikel 109 CPA.
([21]) Artikel 198, lid 2, CPA.
([22]) Artikel 199, lid 1, CPA.
([23]) Artikel 215, leden 1 en 2, CPA.
([24]) Artikel 108, lid 1, van de verordening inzake strafvordering.
([25]) Artikel 114, lid 1, CPA, juncto artikel 219 CPA.
([26]) Artikel 113 CPA.
([27]) Artikelen 121 en 122 CPA.

Bij onderzoeken of inbeslagnemingen waarbij het te doorzoeken voorwerp een computerschijf of een ander medium voor gegevensopslag is, worden in beginsel alleen de gegevens zelf in beslag genomen (gekopieerd of afgedrukt) en niet het hele medium ([28]). Het medium voor gegevensopslag zelf mag slechts in beslag worden genomen wanneer het in wezen onmogelijk wordt geacht de vereiste gegevens afzonderlijk af te drukken of te kopiëren, of wanneer het in wezen onmogelijk wordt geacht het doel van de doorzoeking op een andere manier te bereiken ([29]). De betrokkene moet onverwijld op de hoogte worden gesteld van de inbeslagneming ([30]). Het CPA bevat geen uitzonderingen op deze kennisgevingsvereiste.

Onderzoeken, inspecties en inbeslagnemingen zonder bevel mogen slechts in een beperkt aantal situaties plaatsvinden. Ten eerste is dit het geval wanneer het onmogelijk is om een bevel te verkrijgen wegens een dringende reden op de plaats van een strafbaar feit ([31]). Achteraf moet echter onverwijld een bevel worden verkregen ([32]). Ten tweede mogen doorzoekingen en inspecties zonder bevel ter plaatse worden verricht wanneer een verdachte wordt aangehouden of in hechtenis wordt genomen ([33]). Tot slot mag een aanklager of hoge ambtenaar van de gerechtelijke politie een voorwerp zonder bevel in beslag nemen wanneer het voorwerp door een verdachte van een strafbaar feit of derde is weggegooid of vrijwillig werd verstrekt ([34]).

Bewijs dat in strijd met het CPA is verkregen, wordt als ontoelaatbaar beschouwd ([35]). Bovendien is in het Wetboek van strafrecht bepaald dat illegale fouilleringen van personen of doorzoekingen van de verblijfplaats van een persoon, een bewaakt gebouw, een structuur, auto, schip, vliegtuig of verblijfsruimte strafbaar zijn met een gevangenisstraf van maximaal drie jaar ([36]). Deze bepaling is derhalve ook van toepassing op gevallen waarin voorwerpen, zoals apparaten voor de gegevensopslag, in beslag worden genomen tijdens een illegale fouillering of doorzoeking.

2.2.2. *Verzameling van communicatiegegevens*

2.2.2.1. Rechtsgrondslag

De verzameling van communicatiegegevens valt onder een specifieke wet: de CPPA. In de CPPA is met name een verbod vastgesteld op het censureren van post, het aftappen van telecommunicatie, het verstrekken van communicatiebevestigende gegevens en het opnemen of afluisteren van gesprekken tussen andere personen die niet openbaar zijn gemaakt, tenzij dit gebeurt op basis van het CPA, de CPPA of de Wet op de militaire rechtbank ([37]). De term "*communicatie*" in de zin van de CPPA omvat zowel gewone post als telecommunicatie ([38]). In dit opzicht wordt in de CPPA een onderscheid gemaakt tussen "communicatiebeperkende maatregelen" ([39]) en het verzamelen van "communicatiebevestigende gegevens".

Het begrip communicatiebeperkende maatregelen omvat "*censuur*", dat wil zeggen de verzameling van de inhoud van traditionele poststukken, evenals "*aftapping*", dat wil zeggen, het direct onderscheppen (verkrijgen of opnemen) van de inhoud van telecommunicatie ([40]). Het begrip "*communicatiebevestigende gegevens*" omvat metagegevens over de telecommunicatie, waaronder de datum van de telecommunicatie, de begin- en eindtijd ervan, het aantal uitgaande en inkomende gesprekken en het abonneenummer van de andere partij, de gebruiksfrequentie, logbestanden over het gebruik van telecommunicatiediensten en locatiegegevens (bv. afkomstig van zendmasten waar signalen worden ontvangen) ([41]).

([28]) Artikel 106, lid 3, CPA.
([29]) Artikel 106, lid 3, CPA.
([30]) Artikel 219 CPA, juncto artikel 106, lid 4, CPA.
([31]) Artikel 216, lid 3, CPA.
([32]) Artikel 216, lid 3, CPA.
([33]) Artikel 216, leden 1 en 2, CPA.
([34]) Artikel 218, CPA. Wat persoonsinformatie betreft, heeft dit slechts betrekking op het vrijwillig verstrekken van de informatie door de betrokkene zelf en niet op het verstrekken door een verantwoordelijke voor de verwerking van persoonsinformatie die in het bezit is van dergelijke informatie (wat een specifieke rechtsgrondslag zou vereisen op grond van de Wet bescherming persoonsinformatie). Vrijwillig overgelegde voorwerpen worden alleen als bewijs in een gerechtelijke procedure toegelaten indien er geen redelijke twijfel bestaat over de vrijwilligheid van de overlegging, hetgeen door de openbaar aanklager moet worden aangetoond. Zie Beslissing nr. 2013Do11233 van het Hooggerechtshof van 10 maart 2016.
([35]) Artikel 308-2 CPA.
([36]) Artikel 321 van het Wetboek van strafrecht.
([37]) Artikel 3 CPPA. De Wet op de militaire rechtbank regelt in beginsel de verzameling van informatie over militair personeel en kan slechts in een beperkt aantal gevallen van toepassing zijn op burgers (bv. wanneer militairen en burgers samen een misdaad zouden plegen of wanneer een individu een strafbaar feit pleegt tegen de krijgsmacht, kan een procedure voor een militaire rechtbank worden ingeleid, zie artikel 2 van de Wet op de militaire rechtbank). De algemene bepalingen inzake onderzoeken en inbeslagnemingen zijn vergelijkbaar met die van het CPA, zie bijvoorbeeld de artikelen 146 tot en met 149 en 153 tot en met 156 van de Wet op de militaire rechtbank. Poststukken mogen bijvoorbeeld alleen worden verzameld wanneer dat nodig is voor een onderzoek en op grond van een bevel van de militaire rechtbank. Voor zover elektronische communicatie zou worden verzameld, zijn de beperkingen en waarborgen van de CPPA van toepassing.
([38]) Artikel 2, lid 1, CPPA, namelijk de overdracht of ontvangst van allerlei soorten geluiden, woorden, symbolen of beelden per kabel of vezelkabel of kabelloos of via een ander elektromagnetisch systeem, waaronder telefoons, e-mails, informatiediensten waarvoor een abonnement vereist is, faxen en semafoons.
([39]) Artikel 2, lid 7, en artikel 3, lid 2, CPPA.
([40]) "Censuur" wordt gedefinieerd als het openen van post zonder toestemming van de betrokken partij of het op andere wijze verkrijgen van kennis over, het opnemen of het achterhouden van de inhoud daarvan (artikel 2, lid 6, CPPA). "Aftapping" betekent het verwerven of opnemen van de inhoud van telecommunicatie door het beluisteren of gelijktijdig lezen van de geluiden, woorden, symbolen of beelden van de berichten met behulp van elektronische en mechanische middelen zonder toestemming van de betrokken partij of met storing van de overdracht, of het verstoren van de transmissie en ontvangst daarvan (artikel 2, lid 7, CPPA).
([41]) Artikel 2, lid 11, CPPA.

In de CPPA zijn de beperkingen en waarborgen uiteengezet voor de verzameling van beide soorten gegevens en op de niet-naleving van enkele van deze vereisten zijn strafrechtelijke sancties van toepassing ([42]).

2.2.2.2. Beperkingen en waarborgen die van toepassing zijn op de verzameling van de inhoud van communicatie (communicatiebeperkende maatregelen)

De verzameling van de inhoud van communicatie mag slechts plaatsvinden als aanvullend middel om een strafrechtelijk onderzoek mogelijk te maken (dat wil zeggen als laatste redmiddel) en er moeten inspanningen worden gedaan om de inbreuk op het communicatiegeheim van personen tot een minimum te beperken ([43]). In lijn met dit algemene beginsel mogen communicatiebeperkende maatregelen alleen worden gebruikt wanneer het moeilijk is om op andere wijze het plegen van een strafbaar feit te voorkomen, de dader te arresteren of het bewijs te verzamelen ([44]). Rechtshandhavingsinstanties die de inhoud van communicatie verzamelen, moeten deze verzameling onmiddellijk stopzetten zodra verdere toegang niet langer noodzakelijk wordt geacht, zodat ervoor wordt gezorgd dat de inbreuk op de privacy van de communicatie zo beperkt mogelijk blijft ([45]).

Communicatiebeperkende maatregelen mogen bovendien alleen worden toegepast wanneer er gegronde redenen zijn om te vermoeden dat bepaalde ernstige strafbare feiten die specifiek in de CPPA worden genoemd, worden beraamd, worden gepleegd of zijn gepleegd. Deze omvatten onder meer misdrijven zoals oproer, drugsgerelateerde misdrijven of misdrijven met explosieven, alsmede misdrijven in verband met de nationale veiligheid, diplomatieke betrekkingen of militaire bases en installaties ([46]). Een communicatiebeperkende maatregel moet gericht zijn op specifieke poststukken of telecommunicatie van of naar de verdachte, of op poststukken of telecommunicatie van of naar de verdachte gedurende een bepaalde periode ([47]).

Zelfs wanneer aan deze vereisten is voldaan, mag de verzameling van inhoudsgegevens slechts plaatsvinden op basis van een rechterlijk bevel. Een aanklager mag de rechter met name vragen om de verzameling van inhoudsgegevens in verband met de verdachte of persoon die wordt onderzocht, toe te staan ([48]). Een ambtenaar van de gerechtelijke politie mag op vergelijkbare wijze een aanklager om toestemming vragen, die op zijn beurt om een rechterlijk bevel kan verzoeken ([49]). Een verzoek om een bevel moet schriftelijk worden ingediend en bepaalde specifieke elementen bevatten. Het verzoek moet met name een beschrijving bevatten van 1) de inhoudelijke redenen om te vermoeden dat een van de genoemde strafbare feiten wordt gepland, wordt gepleegd of is gepleegd, alsmede ondersteunend materiaal waaruit blijkt dat er op het eerste gezicht sprake is van een verdenking; 2) de communicatiebeperkende maatregelen alsmede hun voorwerp, reikwijdte, doelstelling en de periode waarin zij feitelijk worden toegepast, en 3) de plaats waar de maatregelen zouden worden uitgevoerd en de wijze waarop zij zouden worden uitgevoerd ([50]).

Wanneer aan de wettelijke eisen is voldaan, kan de rechter schriftelijke toestemming verlenen om de communicatiebeperkende maatregelen uit te voeren met betrekking tot de verdachte of de persoon die wordt onderzocht ([51]). In dit bevel zijn de soorten maatregelen alsmede hun voorwerp, reikwijdte, feitelijke periode, plaats van uitvoering en de wijze van uitvoering vermeld ([52]).

Communicatiebeperkende maatregelen mogen alleen gedurende een periode van twee maanden worden uitgevoerd ([53]). Wanneer het doel van de maatregelen vóór het einde van die periode wordt bereikt, moeten de maatregelen onmiddellijk worden stopgezet. Indien nog steeds aan de vereiste voorwaarden wordt voldaan, kan echter binnen de periode van twee maanden ook een verzoek om verlenging van de toepassingsperiode van communicatiebeperkende maatregelen worden ingediend. Een dergelijk verzoek moet bewijs bevatten waaruit een kennelijke reden voor het verlengen van de maatregelen blijkt ([54]). De periode mag in totaal niet langer zijn dan één jaar, of drie jaar voor bepaalde bijzonder ernstige strafbare feiten (bv. strafbare feiten in verband met oproer, buitenlandse agressie, nationale veiligheid enz.) ([55]).

Rechtshandhavingsinstanties mogen de hulp van communicatie-exploitanten verlangen door de schriftelijke toestemming van de rechter aan hen te overleggen ([56]). Communicatie-exploitanten zijn verplicht mee te werken en moeten de ontvangen toestemming in hun dossiers bewaren ([57]). Zij mogen medewerking weigeren wanneer de informatie over de betrokken persoon zoals genoemd in de schriftelijke toestemming van de rechter (bijvoorbeeld het telefoonnummer van deze persoon) onjuist is. Het is voor hen bovendien onder alle omstandigheden verboden om wachtwoorden te verstrekken die voor telecommunicatie worden gebruikt ([58]).

([42]) Artikelen 16 en 17 CPPA. Dit geldt bijvoorbeeld voor de verzameling zonder bevel, het niet bijhouden van een register, het nalaten de verzameling stop te zetten wanneer er niet langer sprake is van een noodgeval of het nalaten de betrokkene in kennis te stellen.
([43]) Artikel 3, lid 2, CPPA.
([44]) Artikel 5, lid 1, CPPA.
([45]) Artikel 2 van het CPPA-uitvoeringsdecreet.
([46]) Artikel 5, lid 1, CPPA.
([47]) Artikel 5, lid 2, CPPA.
([48]) Artikel 6, lid 1, CPPA.
([49]) Artikel 6, lid 2, CPPA.
([50]) Artikel 6, lid 4, CPPA en artikel 4, lid 1, van het CPPA-uitvoeringsdecreet.
([51]) Artikel 6, leden 5 en 8, CPPA.
([52]) Artikel 6, lid 6, CPPA.
([53]) Artikel 6, lid 7, CPPA.
([54]) Artikel 6, lid 7, CPPA.
([55]) Artikel 6, lid 8, CPPA.
([56]) Artikel 9, lid 2, CPPA.
([57]) Artikel 15-2 CPPA en artikel 12 van het CPPA-uitvoeringsdecreet.
([58]) Artikel 9, lid 4, CPPA.

Iedereen die communicatiebeperkende maatregelen uitvoert of die wordt verzocht om medewerking moet een register bijhouden waarin de doelstellingen van de maatregelen, de uitvoering ervan, de datum waarop de medewerking werd verleend en het voorwerp worden gespecificeerd ([59]). Rechtshandhavingsinstanties die communicatiebeperkende maatregelen uitvoeren, moeten ook een register bijhouden, waarin de details en behaalde resultaten worden uiteengezet ([60]). Ambtenaren van de gerechtelijke politie moeten deze informatie verstrekken in de vorm van een verslag aan de aanklager wanneer zij een onderzoek afsluiten ([61]).

Wanneer een aanklager een tenlastelegging uitvaardigt in verband met een zaak waarin communicatiebeperkende maatregelen zijn toegepast of een beschikking om niet tot tenlastelegging of aanhouding van de betrokkene over te gaan (d.w.z. niet slechts een opschorting van de vervolging), moet de aanklager de persoon die het voorwerp van de communicatiebeperkende maatregelen was, in kennis stellen van het feit dat er communicatiebeperkende maatregelen zijn uitgevoerd en hierbij het uitvoerende agentschap en de periode van uitvoering vermelden. Een dergelijke kennisgeving moet binnen dertig dagen van de beschikking schriftelijk worden gedaan ([62]). De kennisgeving mag worden uitgesteld wanneer deze de nationale veiligheid ernstig in gevaar zou kunnen brengen of de openbare veiligheid en orde zou kunnen verstoren, of wanneer deze zou kunnen leiden tot materiële schade aan het leven en de lichamelijke integriteit van anderen ([63]). Wanneer hij de kennisgeving wil uitstellen, moet de aanklager of de ambtenaar van de gerechtelijke politie hiervoor toestemming krijgen van het hoofd van het arrondissementsparket ([64]). Zodra de redenen voor het uitstel niet langer bestaan, moet de kennisgeving binnen dertig dagen vanaf dat moment worden gedaan ([65]).

In de CPPA is ook een specifieke procedure uiteengezet voor het verzamelen van de inhoud van communicatie in noodsituaties. Rechtshandhavingsinstanties mogen met name de inhoud van communicatie verzamelen in geval van een onmiddellijke dreiging van georganiseerde criminaliteit of wanneer een ander ernstig strafbaar feit dat rechtstreeks de dood of ernstig letsel kan veroorzaken, ophanden is en er sprake is van een noodsituatie waardoor het onmogelijk is de normale procedure (zoals hierboven uiteengezet) te volgen ([66]). In een dergelijke noodsituatie mag een politieambtenaar of aanklager communicatiebeperkende maatregelen nemen zonder voorafgaande toestemming van de rechter, maar moet hij meteen na de uitvoering om rechterlijke toestemming verzoeken. Wanneer de rechtshandhavingsinstantie niet binnen 36 uur na uitvoering van de noodmaatregelen toestemming van de rechter verkrijgt, moet de verzameling onmiddellijk worden stopgezet en de verzamelde informatie normaal gesproken worden vernietigd ([67]). Politieambtenaren die noodsurveillance uitvoeren, doen dit onder toezicht van een aanklager, of moeten, indien het onmogelijk is om vooraf instructies van de aanklager te verkrijgen omdat snel moet worden gehandeld, onmiddellijk na aanvang van de uitvoering toestemming van de aanklager verkrijgen ([68]). De regels inzake de kennisgeving van de persoon zoals hierboven beschreven, zijn ook van toepassing op het verzamelen van de inhoud van communicatie in noodsituaties.

Het verzamelen van informatie in noodsituaties moet altijd plaatsvinden in overeenstemming met een "*verklaring inzake censuur/aftapping in noodsituaties*" en de instantie die de informatie verzamelt moet een register bijhouden van alle noodmaatregelen ([69]). Het verzoek aan een rechter om toestemming voor noodmaatregelen moet vergezeld gaan van een schriftelijk document waarin de noodzakelijke communicatiebeperkende maatregelen, het voorwerp, de reikwijdte, de periode, de plaats van uitvoering, de wijze van verzameling, en een uitleg over de manier waarop de desbetreffende communicatiebeperkende maatregelen in overeenstemming zijn met artikel 5, lid 1, CPPA ([70]) worden vermeld, samen met ondersteunende documenten.

In gevallen waarin noodmaatregelen binnen korte tijd worden afgerond, waardoor de toestemming van een rechter niet mogelijk is (bv. wanneer de verdachte onmiddellijk na het begin van de onderschepping wordt gearresteerd, waarna de onderschepping dus eindigt), doet het hoofd van het bevoegde Openbaar Ministerie de bevoegde rechter een kennisgeving van een noodmaatregel toekomen ([71]). In de kennisgeving moeten het doel, het voorwerp, de reikwijdte, de periode, de plaats van uitvoering en de wijze van verzameling, alsmede de redenen waarom geen verzoek om toestemming van de rechter is ingediend, worden uiteengezet ([72]). Deze kennisgeving stelt de ontvangende rechter in staat de wettigheid van de verzameling te onderzoeken en moet worden opgenomen in een register van kennisgevingen van noodmaatregelen.

([59]) Artikel 9, lid 3, CPPA.
([60]) Artikel 18, lid 1, van het CPPA-uitvoeringsdecreet.
([61]) Artikel 18, lid 2, van het CPPA-uitvoeringsdecreet.
([62]) Artikel 9-2, lid 1, CPPA.
([63]) Artikel 9-2, lid 4, CPPA.
([64]) Artikel 9-2, lid 5, CPPA.
([65]) Artikel 9-2, lid 6, CPPA.
([66]) Artikel 8, lid 1, CPPA.
([67]) Artikel 8, lid 2, CPPA.
([68]) Artikel 8, lid 3, CPPA en artikel 16, lid 3, van het CPPA-uitvoeringsdecreet.
([69]) Artikel 8, lid 4, CPPA.
([70]) Dat wil zeggen dat er een gegronde reden is om te vermoeden dat bepaalde ernstige strafbare feiten worden beraamd, worden gepleegd of zijn gepleegd en het onmogelijk is om op andere wijze het plegen van een strafbaar feit te voorkomen, de dader te arresteren of het bewijs te verzamelen.
([71]) Artikel 8, lid 5, CPPA.
([72]) Artikel 8, leden 6 en 7, CPPA.

Als algemeen vereiste mag de inhoud van communicatie die is verkregen door middel van de uitvoering van communicatiebeperkende maatregelen op basis van de CPPA slechts worden gebruikt om de specifieke bovengenoemde strafbare feiten te onderzoeken, te vervolgen of te voorkomen, in het kader van tuchtrechtelijke procedures voor deze strafbare feiten of een vordering tot schadevergoeding die is ingediend door een partij bij de communicatie of wanneer dit is toegestaan door andere wetgeving ([73]).

Wanneer telecommunicatie via het internet wordt verzameld, zijn specifieke waarborgen van toepassing ([74]). Dergelijke informatie mag alleen worden gebruikt om de ernstige strafbare feiten te onderzoeken die worden genoemd in artikel 5, lid 1, CPPA. Voor het bewaren van de informatie moet toestemming worden verkregen van de rechter die de communicatiebeperkende maatregelen heeft goedgekeurd ([75]). Een verzoek tot bewaring van informatie moet informatie bevatten over de communicatiebeperkende maatregelen, een samenvatting van de resultaten van de maatregelen, de redenen voor het bewaren (samen met ondersteunend materiaal) en de te bewaren telecommunicatie ([76]). Wanneer een dergelijk verzoek ontbreekt, moet de verkregen telecommunicatie binnen 14 dagen na afloop van de communicatiebeperkende maatregelen worden verwijderd ([77]). Indien een verzoek wordt afgewezen, moet de telecommunicatie binnen zeven dagen worden vernietigd ([78]). Wanneer telecommunicatie wordt verwijderd, moet binnen zeven dagen bij de rechter die de communicatiebeperkende maatregelen heeft goedgekeurd een verslag worden ingediend waarin de redenen voor het verwijderen en de details en het tijdstip ervan worden vermeld.

Meer in het algemeen wordt informatie die op onwettige wijze door middel van communicatiebeperkende maatregelen is verkregen niet als bewijs toegelaten in gerechtelijke of tuchtrechtelijke procedures ([79]). De CPPA verbiedt personen die communicatiebeperkende maatregelen nemen bovendien vertrouwelijke informatie bekend te maken die is verkregen in het kader van de uitvoering van dergelijke maatregelen en de verkregen informatie te gebruiken om de reputatie te schaden van de personen ten aanzien van wie de maatregelen worden uitgevoerd ([80]).

2.2.2.3. Beperkingen en waarborgen die van toepassing zijn op de verzameling van communicatiebevestigende informatie

Rechtshandhavingsinstanties kunnen op basis van de CPPA telecommunicatie-exploitanten verzoeken communicatiebevestigende gegevens te verstrekken wanneer dit nodig is om een onderzoek of een straf uit te voeren ([81]). In tegenstelling tot de verzameling van inhoudsgegevens, is de mogelijkheid om communicatiebevestigende gegevens te verzamelen niet beperkt tot bepaalde specifieke strafbare feiten. Net zoals bij inhoudsgegevens vereist de verzameling van communicatiebevestigende gegevens echter schriftelijke toestemming vooraf van een rechter, volgens dezelfde voorwaarden als hierboven beschreven ([82]). Wanneer het om dringende redenen onmogelijk is om toestemming van de rechter te verkrijgen, mogen communicatiebevestigende gegevens zonder bevel worden verzameld. In dat geval moet de toestemming onmiddellijk na het verzoek om de gegevens worden verkregen en aan de telecommunicatieaanbieder worden bezorgd ([83]). Wanneer geen toestemming achteraf wordt verkregen, moet de verzamelde informatie worden vernietigd ([84]).

Aanklagers, ambtenaren van de gerechtelijke politie en rechters moeten registers bijhouden van verzoeken om communicatiebevestigende gegevens ([85]). Daarnaast moeten telecommunicatieaanbieders twee keer per jaar aan de minister van Wetenschap en ICT verslag uitbrengen over het verstrekken van communicatiebevestigende gegevens en moeten zij daarvan registers bijhouden gedurende een periode van zeven jaar na de datum van verstrekking van de gegevens ([86]).

Natuurlijke personen worden in principe op de hoogte gesteld van het feit dat er communicatiebevestigende gegevens zijn verzameld ([87]). Het tijdstip van een dergelijke kennisgeving is afhankelijk van de omstandigheden van het onderzoek ([88]). Zodra een beslissing is genomen om (niet) te vervolgen, moet de kennisgeving binnen dertig dagen worden gedaan. Wanneer een tenlastelegging wordt opgeschort, moet de kennisgeving echter plaatsvinden binnen een jaar en dertig dagen nadat een dergelijke beslissing is genomen. De kennisgeving moet in ieder geval plaatsvinden binnen een jaar en dertig dagen nadat de informatie is verzameld.

De kennisgeving mag worden uitgesteld wanneer deze 1) de nationale veiligheid, de openbare veiligheid en de openbare orde in gevaar kan brengen; 2) de dood of lichamelijk letsel kan veroorzaken; 3) een eerlijke rechtsgang kan belemmeren

([73]) Artikel 12 CPPA.
([74]) Artikel 12-2 CPPA.
([75]) De aanklager of politieambtenaar die de communicatiebeperkende maatregelen uitvoert, moet binnen 14 dagen na afloop van de maatregelen de te bewaren telecommunicatie selecteren en de rechter om toestemming vragen (in geval van een politieambtenaar moet het verzoek worden ingediend bij een aanklager, die op zijn beurt het verzoek bij de rechter indient), zie artikel 12-2, leden 1 en 2, CPPA.
([76]) Artikel 12-2, lid 3, CPPA.
([77]) Artikel 12-2, lid 5, CPPA.
([78]) Artikel 12-2, lid 5, CPPA.
([79]) Artikel 4, CPPA.
([80]) Artikel 11, lid 2, van het CPPA-uitvoeringsdecreet.
([81]) Artikel 13, lid 1, CPPA.
([82]) Artikelen 6 en 13 CPPA.
([83]) Artikel 13, lid 2, CPPA. Net zoals bij dringende communicatiebeperkende maatregelen moet een document worden opgesteld waarin de details van de zaak (de verdachte, de te nemen maatregelen, het vermoede strafbare feit en de dringendheid) worden beschreven. Zie artikel 37, lid 5, van het CPPA-uitvoeringsdecreet.
([84]) Artikel 13, lid 3, CPPA.
([85]) Artikel 13, leden 5 en 6, CPPA.
([86]) Artikel 13, lid 7, CPPA.
([87]) Zie artikel 13-3, lid 7, juncto artikel 9-2 CPPA.
([88]) Artikel 13-3, lid 1, CPPA.

(bv. doordat deze de vernietiging van bewijsmateriaal of bedreiging van getuigen tot gevolg heeft), of 4) de verdachte, de slachtoffers of andere personen die met de zaak te maken hebben, in diskrediet kan brengen of inbreuk op hun persoonlijke levenssfeer kan maken ([89]). Een kennisgeving op een van de bovengenoemde gronden vereist toestemming van de directeur van een bevoegd arrondissementsparket ([90]). Zodra de redenen voor het uitstel niet langer bestaan, moet de kennisgeving binnen dertig dagen vanaf dat moment worden gedaan ([91]).

Natuurlijke personen die een kennisgeving hebben ontvangen, kunnen een schriftelijk verzoek indienen bij de aanklager of de ambtenaar van de gerechtelijke politie met betrekking tot de redenen voor de verzameling van de communicatiebevestigende gegevens ([92]). In dat geval moet de aanklager of de ambtenaar van de gerechtelijke politie binnen dertig dagen na ontvangst van het verzoek de redenen schriftelijk meedelen, tenzij een van de bovengenoemde gronden (uitzonderingen voor het uitstel van de kennisgeving) van toepassing is ([93]).

2.2.3. *Vrijwillige verstrekking door telecommunicatie-exploitanten*

Artikel 83, lid 3, TBA biedt telecommunicatie-exploitanten de mogelijkheid vrijwillig te voldoen aan een verzoek van een rechter, aanklager of hoofd van een onderzoeksinstantie om communicatiegegevens te verstrekken (ter ondersteuning van een strafrechtelijk proces, onderzoek of de uitvoering van een straf). In het kader van de TBA verwijst "*communicatiegegevens*" naar de naam, het burgerregistratienummer, het adres en het telefoonnummer van gebruikers, de data waarop gebruikers zich abonneren of hun abonnement beëindigen alsmede gebruikersidentificatiecodes (d.w.z. codes die worden gebruikt om de rechtmatige gebruiker van computersystemen of communicatienetwerken te identificeren) ([94]). In het kader van de TBA worden uitsluitend natuurlijke personen aan wie rechtstreeks diensten worden verleend door een Koreaanse telecommunicatieaanbieder als gebruikers beschouwd ([95]). Als gevolg hiervan zullen er waarschijnlijk weinig situaties zijn waarin natuurlijke personen uit de EU wier gegevens zijn doorgegeven aan de Republiek Korea op grond van de TBA als gebruikers worden beschouwd, aangezien deze personen normaal gesproken geen rechtstreekse overeenkomst sluiten met een Koreaanse telecommunicatie-exploitant.

Verzoeken om communicatiegegevens te verkrijgen op basis van de TBA moeten schriftelijk worden gedaan en de redenen voor het verzoek vermelden, evenals het verband met de betrokken gebruiker en de reikwijdte van de gevraagde gegevens ([96]). Wanneer het om dringende redenen onmogelijk is een schriftelijk verzoek in te dienen, moet het schriftelijke verzoek worden ingediend zodra de reden voor de urgentie is vervallen ([97]). Telecommunicatie-exploitanten die voldoen aan verzoeken om communicatiegegevens te verstrekken, moeten registers bijhouden waaruit blijkt dat de communicatiegegevens zijn verstrekt, samen met de bijbehorende stukken, zoals het schriftelijke verzoek ([98]). Telecommunicatie-exploitanten moeten bovendien twee keer per jaar aan de minister van Wetenschap en ICT verslag uitbrengen over het verstrekken van communicatiegegevens ([99]).

Op basis van de TBA bestaat er geen verplichting voor telecommunicatie-exploitanten om te voldoen aan verzoeken om communicatiegegevens te verstrekken. Elk verzoek moet daarom door de exploitant worden beoordeeld in het licht van de toepasselijke gegevensbeschermingsvoorschriften uit hoofde van de PIPA. Een telecommunicatie-exploitant moet met name rekening houden met de belangen van de betrokkene en mag geen informatie verstrekken wanneer dit waarschijnlijk op oneerlijke wijze inbreuk zou maken op de belangen van de betrokkene of van derden ([100]). Daarnaast moet de betrokkene overeenkomstig Kennisgeving nr. 2021-1 over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie op de hoogte worden gesteld van het verstrekken van de informatie. Een dergelijke kennisgeving mag in uitzonderlijke gevallen worden vertraagd, met name indien en zolang de kennisgeving een lopend strafrechtelijk onderzoek in gevaar zou brengen, of het leven of de lichamelijke integriteit van een andere persoon zou kunnen schaden, wanneer deze rechten of belangen duidelijk zwaarder wegen dan de rechten van de betrokkene ([101]).

Het Hooggerechtshof heeft in 2016 bevestigd dat het vrijwillig verstrekken van communicatiegegevens door telecommunicatie-exploitanten zonder bevel op basis van de TBA als zodanig geen schending vormt van het recht op de zelfbeschikking over informatie van de gebruiker van de telecommunicatiedienst. Het Hooggerechtshof heeft toen ook verduidelijkt dat er sprake zou zijn van een dergelijke schending wanneer het overduidelijk is dat het verzoekende agentschap misbruik heeft gemaakt van zijn autoriteit door te verzoeken communicatiegegevens te verstrekken en zodoende de belangen van de betrokkene of een derde heeft geschonden ([102]). Meer in het algemeen moet een verzoek om het vrijwillige verstrekken van informatie van een rechtshandhavingsinstantie op grond van de Koreaanse grondwet (artikel 12, lid 1, en artikel 37, lid 2) in overeenstemming zijn met de beginselen van rechtmatigheid, noodzakelijkheid en evenredigheid.

([89]) Artikel 13-3, lid 2, CPPA.
([90]) Artikel 13-3, lid 3, CPPA.
([91]) Artikel 13-3, lid 4, CPPA.
([92]) Artikel 13-3, lid 5, CPPA.
([93]) Artikel 13-3, lid 6, CPPA.
([94]) Artikel 83, lid 3, TBA.
([95]) Artikel 2, lid 9, TBA.
([96]) Artikel 83, lid 4, TBA.
([97]) Artikel 83, lid 4, TBA.
([98]) Artikel 83, lid 5, TBA.
([99]) Artikel 83, lid 6, TBA.
([100]) Artikel 18, lid 2, PIPA.
([101]) Kennisgeving nr. 2021-1 van de PIPC over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie, deel III, 2, punt iii).
([102]) Beslissing nr. 2012Da105482 van het Hooggerechtshof van 10 maart 2016.

2.3. **Toezicht**

Het toezicht op de strafrechtelijke handhavingsinstanties wordt uitgeoefend via verschillende mechanismen, door zowel interne als externe organen.

2.3.1. *Interne controles*

Overeenkomstig de Wet inzake controles in de publieke sector worden overheidsinstanties aangemoedigd een intern orgaan voor interne controles op te richten, dat onder meer als taak heeft de wettigheid te controleren ([103]). De onafhankelijkheid van de hoofden van dergelijke controleorganen moet zoveel mogelijk worden gewaarborgd ([104]). Meer specifiek worden personen benoemd die geen deel uitmaken van de betrokken autoriteit (bv. voormalige rechters, professoren), voor een periode van twee tot vijf jaar, en kunnen zij alleen om gegronde redenen worden ontslagen (bv. wanneer zij hun taken niet kunnen vervullen als gevolg van een geestelijke of lichamelijke aandoening of wanneer er tuchtmaatregelen tegen hen worden genomen) ([105]). Ook controleurs worden benoemd op basis van de specifieke voorwaarden van de Wet ([106]). Controleverslagen kunnen aanbevelingen of verzoeken om schadevergoeding of correctie bevatten, evenals berispingen en aanbevelingen of verzoeken om tuchtmaatregelen ([107]). Zij worden binnen zestig dagen na afronding van de controle meegedeeld aan het hoofd van de overheidsinstantie die wordt gecontroleerd, alsook aan de Controle- en Inspectieraad (zie punt 2.3.2) ([108]). De betrokken instantie moet de vereiste maatregelen uitvoeren en over de resultaten verslag uitbrengen aan de Controle- en Inspectieraad ([109]). Daarnaast worden de controleresultaten normaal gesproken openbaar gemaakt ([110]). Bij weigering of belemmering van een interne controle kunnen administratieve boetes worden opgelegd ([111]). Op het gebied van de strafrechtelijke handhaving gebruikt de nationale politie een systeem met een inspecteur-generaal voor interne controles om aan de bovengenoemde wetgeving te voldoen, ook met betrekking tot mogelijke schendingen van de mensenrechten ([112]).

2.3.2. *De Controle- en Inspectieraad*

De Controle- en Inspectieraad (*Board of controle and Inspection* — BAI) kan de activiteiten van overheidsinstanties inspecteren en, op basis van dergelijke inspecties, aanbevelingen doen, verzoeken om tuchtmaatregelen of een strafrechtelijke klacht indienen ([113]). De BAI is opgericht onder de bevoegdheid van de president van de Republiek Korea, maar heeft een onafhankelijke status in verband met zijn taken ([114]). Daarnaast vereist de Wet tot oprichting van de BAI dat aan de BAI een maximale onafhankelijkheid wordt toegekend in verband met de benoeming, het ontslag en de organisatie van zijn personeel, evenals in verband met de samenstelling van zijn begroting ([115]). De voorzitter van de BAI wordt benoemd door de president, met goedkeuring van de Nationale Vergadering ([116]). De zes overige commissarissen worden, op aanbeveling van de voorzitter, door de president benoemd voor een periode van vier jaar ([117]). De commissarissen (met inbegrip van de voorzitter) moeten beschikken over specifieke bij wet vastgelegde kwalificaties ([118]) en mogen slechts worden ontslagen in het geval van inbeschuldigingsstelling, een gevangenisstraf of het niet kunnen uitoefenen van hun taken als gevolg van een langdurige geestelijke of lichamelijke aandoening ([119]). Commissarissen mogen daarnaast niet deelnemen aan politieke activiteiten en niet tegelijkertijd een functie bekleden in de Nationale Vergadering, bestuursinstanties, organisaties die door de BAI worden gecontroleerd en geïnspecteerd of een andere bezoldigde functie of positie vervullen ([120]).

De BAI voert jaarlijks een algemene controle uit, maar kan ook specifieke controles verrichten in verband met kwesties van bijzonder belang. De BAI kan in de loop van een inspectie verzoeken om overlegging van documenten en om de aanwezigheid van bepaalde personen ([121]). Als onderdeel van een controle onderzoekt de BAI de inkomsten en uitgaven

([103]) De artikelen 3 en 5 van de Wet inzake controles in de publieke sector.
([104]) Artikel 7 van de Wet inzake controles in de publieke sector.
([105]) De artikelen 8 tot en met 11 van de Wet inzake controles in de publieke sector.
([106]) Artikel 16 en verder van de Wet inzake controles in de publieke sector.
([107]) Artikel 23, lid 2, van de Wet inzake controles in de publieke sector.
([108]) Artikel 23, lid 1, van de Wet inzake controles in de publieke sector.
([109]) Artikel 23, lid 3, van de Wet inzake controles in de publieke sector.
([110]) Artikel 26 van de Wet inzake controles in de publieke sector.
([111]) Artikel 41 van de Wet inzake controles in de publieke sector.
([112]) Zie met name de afdelingen onder de directeur-generaal voor Controles en Inspecties: https://www.police.go.kr/eng/knpa/org/org01.jsp
([113]) Artikel 24 en artikelen 31 tot en met 35 van de Wet inzake de Controle- en Inspectieraad (hierna "*BAI-wet*" genoemd).
([114]) Artikel 2, lid 1, van de BAI-wet.
([115]) Artikel 2, lid 2, van de BAI-wet.
([116]) Artikel 4, lid 1, van de BAI-wet.
([117]) Artikel 5, lid 1, en artikel 6 van de BAI-wet.
([118]) Bv. gedurende ten minste tien jaar rechter, openbaar aanklager of advocaat zijn geweest, gedurende ten minste acht jaar als ambtenaar of hoogleraar of in een hogere functie aan een universiteit hebben gewerkt, of gedurende ten minste tien jaar in een beursgenoteerde onderneming of overheidsinstelling hebben gewerkt (waarvan minstens vijf jaar als leidinggevend functionaris), zie artikel 7 van de BAI-wet.
([119]) Artikel 8 van de BAI-wet.
([120]) Artikel 9 van de BAI-wet.
([121]) Zie bv. artikel 27 van de BAI-wet.

van de staat en houdt hij ook toezicht op de algemene vervulling van de taken van overheidsinstanties en ambtenaren met het oog op de verbetering van de werking van het openbaar bestuur ([122]). Zijn toezicht gaat dus verder dan begrotingsaspecten en omvat ook een controle van de wettigheid.

2.3.3. *De Nationale Vergadering*

De Nationale Vergadering kan overheidsinstanties onderzoeken en inspecteren ([123]). Tijdens een onderzoek of inspectie kan de Nationale Vergadering verzoeken om de openbaarmaking van documenten en kan zij getuigen verplichten te verschijnen ([124]). Personen die in het kader van een onderzoek van de Nationale Vergadering meineed plegen, kunnen strafrechtelijk worden vervolgd (gevangenisstraf van maximaal tien jaar) ([125]). Het proces en de resultaten van inspecties kunnen openbaar worden gemaakt ([126]). Wanneer de Nationale Vergadering vaststelt dat er sprake is van onwettige of ongepaste activiteiten, mag zij de betrokken overheidsinstantie verzoeken corrigerende maatregelen te nemen, met inbegrip van de toekenning van een schadevergoeding, het nemen van tuchtmaatregelen en het verbeteren van de interne procedures ([127]). Naar aanleiding van een dergelijk verzoek moet de instantie onverwijld handelen en aan de Nationale Vergadering verslag uitbrengen over de resultaten ([128]).

2.3.4. *De Commissie bescherming persoonsinformatie*

De Commissie bescherming persoonsinformatie (hierna "PIPC" genoemd) houdt toezicht op de verwerking van persoonsinformatie door strafrechtelijke handhavingsinstanties in overeenstemming met de PIPA. Het toezicht van de PIPC heeft op grond van artikel 7-8, leden 3 en 4, en artikel 7-9, lid 5, PIPA ook betrekking op mogelijke inbreuken op de regels tot vaststelling van de beperkingen en waarborgen in verband met de verzameling van persoonsinformatie, met inbegrip van de beperkingen en waarborgen die zijn opgenomen in de specifieke wetten waarin de verzameling van (elektronisch) bewijs met het oog op de strafrechtelijke handhaving wordt geregeld (zie punt 2.2). Gezien de vereisten van artikel 3, lid 1, PIPA met betrekking tot de rechtmatige en behoorlijke verzameling van persoonsinformatie vormt een dergelijke inbreuk ook een schending van de PIPA, die de PIPC toestaat een onderzoek uit te voeren en corrigerende maatregelen te nemen ([129]).

Bij de uitoefening van haar toezichtstaak heeft de PIPC toegang tot alle relevante informatie ([130]). De PIPC kan advies verlenen aan rechtshandhavingsinstanties om het niveau van de bescherming van persoonsinformatie bij hun verwerkingsactiviteiten te verbeteren, corrigerende maatregelen opleggen (bv. om de gegevensverwerking op te schorten of noodzakelijke maatregelen te nemen om de persoonsinformatie te beschermen) of de autoriteit adviseren tuchtmaatregelen te nemen ([131]). Tot slot is voorzien in strafrechtelijke sancties voor bepaalde schendingen van de PIPA, zoals het onrechtmatige gebruik of de onrechtmatige verstrekking van persoonsinformatie aan derden of de onrechtmatige verwerking van gevoelige informatie ([132]). In dit verband kan de PIPC de zaak doorsturen naar het bevoegde onderzoeksorgaan (waaronder een aanklager) ([133]).

2.3.5. *Nationale Mensenrechtencommissie*

De Nationale Mensenrechtencommissie (*National Human Rights Commission* — hierna "NHRC" genoemd) — een onafhankelijk orgaan dat tot taak heeft de grondrechten te beschermen en te bevorderen ([134]) — is bevoegd om schendingen van de artikelen 10 tot en met 22 van de grondwet, die het recht op privacy en het briefgeheim omvatten, te onderzoeken en te verhelpen. De NHRC bestaat uit elf commissarissen, die worden benoemd op voordracht van de Nationale Vergadering (vier), de president (vier) en de president van het Hooggerechtshof (drie) ([135]). Om te kunnen worden benoemd, moet een commissaris 1) ten minste tien jaar werkzaam zijn geweest aan een universiteit of een erkend onderzoeksinstituut op ten minste het niveau van geassocieerd hoogleraar; 2) gedurende ten minste tien jaar een functie hebben bekleed als rechter, openbaar aanklager of advocaat; 3) zich gedurende ten minste tien jaar met mensenrechten hebben beziggehouden (bv. voor een non-profit-, niet-gouvernementele of internationale organisatie), of 4) zijn aanbevolen door groeperingen uit het maatschappelijk middenveld ([136]). De voorzitter wordt door de president benoemd uit

([122]) Artikelen 20 en 24 van de BAI-wet.
([123]) Artikel 128 van de Wet inzake de Nationale Vergadering en artikelen 2, 3 en 15 van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie. Dit omvat jaarlijkse inspecties van overheidszaken als geheel, en onderzoeken van specifieke zaken.
([124]) Artikel 10, lid 1, van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie. Zie ook artikelen 128 en 129 van de Wet inzake de Nationale Vergadering.
([125]) Artikel 14 van de Wet inzake de getuigenverklaring, beoordeling enz. voor de Nationale Vergadering.
([126]) Artikel 12-2 van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([127]) Artikel 16, lid 2, van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([128]) Artikel 16, lid 3, van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([129]) Zie Kennisgeving nr. 2021-1 van de PIPC over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie.
([130]) Artikel 63 PIPA.
([131]) Artikel 61, lid 2, artikel 65, leden 1 en 2, en artikel 64, lid 4, PIPA.
([132]) Artikelen 70 tot en met 74 PIPA.
([133]) Artikel 65, lid 1, PIPA.
([134]) Artikel 1 van de Wet inzake de Mensenrechtencommissie (hierna "*NHRC-wet*" genoemd).
([135]) Artikel 5, leden 1 en 2, van de NHRC-wet.
([136]) Artikel 5, lid 3, van de NHRC-wet.

de commissarissen en moet worden bevestigd door de Nationale Vergadering ([137]). De commissarissen (met inbegrip van de voorzitter) worden benoemd voor een hernieuwbare termijn van drie jaar en kunnen alleen worden ontslagen wanneer zij tot een gevangenisstraf zijn veroordeeld of niet langer in staat zijn hun taken uit te oefenen als gevolg van langdurige fysieke of mentale zwakte (in dat geval moet twee derde van de commissarissen instemmen met het ontslag) ([138]). De commissarissen van de NHRC mogen niet tegelijkertijd een functie bekleden in de Nationale Vergadering, lokale raden of bij een staats- of lokale overheid (als ambtenaar) ([139]).

De NHRC mag op eigen initiatief of op basis van een verzoekschrift van een persoon een onderzoek starten. De NHRC mag in het kader van haar onderzoek verzoeken om overlegging van relevante materialen, inspecties uitvoeren en personen dagvaarden om te getuigen ([140]). Naar aanleiding van een onderzoek kan de NHRC aanbevelingen doen om specifieke beleidsmaatregelen en praktijken te verbeteren of te corrigeren en deze openbaar maken ([141]). Overheidsinstanties moeten de NHRC binnen negentig dagen na ontvangst van dergelijke aanbevelingen op de hoogte stellen van een plan om deze uit te voeren ([142]). Wanneer de aanbevelingen niet worden uitgevoerd, moet de betrokken instantie de NHRC daarvan bovendien in kennis stellen ([143]). De NHRC mag een dergelijke niet-uitvoering melden bij de Nationale Vergadering en/of openbaar maken. Overheidsinstanties volgen aanbevelingen van de NHRC over het algemeen op en er bestaan sterke prikkels om dit te doen, aangezien de uitvoering ervan is beoordeeld als onderdeel van de algemene evaluatie door het Bureau voor de coördinatie van het overheidsbeleid onder de auspiciën van het kabinet van de premier.

2.4. **Individueel verhaal**

2.4.1. *Op grond van de PIPA beschikbare verhaalsmechanismen*

Natuurlijke personen kunnen hun rechten op toegang, correctie, verwijdering en opschorting uit hoofde van de PIPA uitoefenen in verband met persoonsinformatie die door strafrechtelijke handhavingsinstanties wordt verwerkt. Zij kunnen direct bij de betrokken instantie, of indirect via de PIPC, om toegang verzoeken ([144]). De bevoegde autoriteit mag de toegang slechts beperken of weigeren wanneer hierin bij wet is voorzien, wanneer de toegang waarschijnlijk schade zal toebrengen aan het leven of de lichamelijke integriteit van een derde, of deze waarschijnlijk zal leiden tot een ongerechtvaardigde inbreuk op de eigendoms- en andere belangen van een andere persoon (d.w.z. wanneer de belangen van die andere persoon zwaarder zouden doorwegen dan de belangen van de persoon die het verzoek indient) ([145]). Wanneer een verzoek om toegang wordt afgewezen, moet de betrokkene worden geïnformeerd over de redenen hiervoor en over de mogelijkheden om hiertegen in beroep te gaan ([146]). Een verzoek om informatie te corrigeren of te wissen kan op vergelijkbare wijze worden afgewezen wanneer hierin in andere wetten is voorzien. In dit geval moet de persoon worden geïnformeerd over de onderliggende redenen en de mogelijkheid om beroep aan te tekenen ([147]).

Wat verhaal betreft, kunnen natuurlijke personen een klacht indienen bij de PIPC, onder meer via het Privacy Call Centre dat wordt beheerd door het Koreaans Agentschap voor internet en veiligheid ([148]). Bovendien kunnen zij het Comité voor geschillenbeslechting in verband met persoonsinformatie laten bemiddelen ([149]). Deze verhaalsmechanismen zijn zowel beschikbaar voor mogelijke inbreuken op de regels van specifieke wetten waarin de beperkingen en waarborgen in verband met de verzameling van persoonsinformatie zijn vastgesteld (punt 2.2) als voor mogelijke inbreuken op de PIPA. Natuurlijke personen kunnen daarnaast beslissingen of het uitblijven van maatregelen van de PIPC aanvechten op grond van de Wet administratieve procesvoering (zie punt 2.4.3).

([137]) Artikel 5, lid 5, van de NHRC-wet.
([138]) Artikel 7, lid 1, en artikel 8 van de NHRC-wet.
([139]) Artikel 10 van de NHRC-wet.
([140]) Artikel 36 van de NHRC-wet. Overeenkomstig artikel 36, lid 7, van de wet kan het overleggen van materiaal of artikelen worden geweigerd indien daardoor de staatsgeheimhouding zou worden geschaad, wat een aanzienlijk effect zou kunnen hebben op de staatsveiligheid of de diplomatieke betrekkingen, of een ernstige belemmering zou vormen voor een strafrechtelijk onderzoek of een lopende gerechtelijke procedure. In dergelijke gevallen kan de NHRC een verzoek om aanvullende informatie richten aan het hoofd van de betrokken instantie (die te goeder trouw moet voldoen aan het verzoek), wanneer dat nodig is om te beoordelen of de weigering tot informatieverstrekking gerechtvaardigd is.
([141]) Artikel 25, lid 1, van de NHRC-wet.
([142]) Artikel 25, lid 3, van de NHRC-wet.
([143]) Artikel 25, lid 4, van de NHRC-wet.
([144]) Artikel 35, lid 2, PIPA.
([145]) Artikel 35, lid 4, PIPA.
([146]) Artikel 42, lid 2, van het PIPA-uitvoeringsdecreet.
([147]) Artikel 36, leden 1 en 2, PIPA en artikel 43, lid 3, van het PIPA-uitvoeringsdecreet.
([148]) Artikel 62, PIPA.
([149]) Artikelen 40 tot en met 50 PIPA en de artikelen 48-2 tot en met 57 van het PIPA-uitvoeringsdecreet.

2.4.2. *Verhaal voor de Nationale Mensenrechtencommissie*

De NHRC behandelt klachten van personen (zowel Koreaanse staatsburgers als buitenlanders) in verband met schendingen van de mensenrechten door overheidsinstanties ([150]). Er zijn geen vaste eisen voor personen om een klacht bij de NHRC in te dienen ([151]). De NHRC handelt daarom alle klachten af, zelfs wanneer de betrokkene tijdens het ontvankelijkheidsonderzoek niet kan aantonen dat hij/zij daadwerkelijk is benadeeld. In het kader van de verzameling van persoonsgegevens voor de handhaving van het strafrecht hoeft een natuurlijke persoon dan ook niet aan te tonen dat de Koreaanse overheidsinstanties zich daadwerkelijk toegang hebben verschaft tot zijn/haar persoonsinformatie opdat de klacht ontvankelijk zou zijn voor de NHRC. Personen kunnen ook een verzoek indienen om de klacht door middel van bemiddeling op te lossen ([152]).

Voor het onderzoeken van een klacht kan de NHRC gebruikmaken van haar onderzoeksbevoegdheden, onder meer het verzoeken om overlegging van relevant materiaal, het verrichten van inspecties en het dagvaarden van personen om te getuigen ([153]). Wanneer uit het onderzoek blijkt dat de desbetreffende wetten zijn geschonden, kan de NHRC de uitvoering van corrigerende maatregelen of de rectificatie of verbetering van relevante wetten, instellingen, beleidsmaatregelen of praktijken aanbevelen ([154]). Corrigerende maatregelen die kunnen worden voorgesteld, zijn onder meer bemiddeling, stopzetting van de mensenrechtenschending, schadevergoeding en maatregelen om herhaling van dezelfde of soortgelijke inbreuken te voorkomen ([155]). Wanneer de verzameling van persoonsinformatie op grond van de toepasselijke regels onrechtmatig is, kunnen de corrigerende maatregelen de verwijdering van de verzamelde persoonsinformatie omvatten. Indien het zeer waarschijnlijk wordt geacht dat de inbreuk nog steeds plaatsvindt en dat die aanhoudende inbreuk waarschijnlijk schade zal veroorzaken die moeilijk te verhelpen is wanneer er niets wordt gedaan, kan de NHRC dringende mitigerende maatregelen nemen ([156]).

Hoewel de NHRC niet bevoegd is om haar beslissingen af te dwingen, kunnen haar beslissingen (bv. een beslissing om het onderzoek van een klacht niet voort te zetten) ([157]) en aanbevelingen worden aangevochten voor een Koreaanse rechter op grond van de Wet administratieve procesvoering (zie punt 2.4.3 hieronder) ([158]). Daarnaast kunnen personen, wanneer uit de bevindingen van de NHRC blijkt dat hun persoonsgegevens op onrechtmatige wijze door een overheidsinstantie zijn verzameld, voor de Koreaanse rechter verhaal zoeken tegen die overheidsinstantie, bijvoorbeeld door bezwaar te maken tegen de verzameling op grond van de Wet administratieve procesvoering, door een grondwettelijke klacht in te dienen op grond van de Wet op het Grondwettelijk Hof of door te verzoeken om schadevergoeding op grond van de Wet inzake overheidscompensatie (zie punt 2.4.3 hieronder).

2.4.3. *Gerechtelijk beroep*

Natuurlijke personen kunnen de beperkingen en waarborgen zoals beschreven in de delen hierboven inroepen om op verschillende wijzen verhaal te halen voor de Koreaanse rechter.

Allereerst mogen de betrokken persoon en/of diens raadsman in overeenstemming met het CPA aanwezig zijn wanneer een bevel tot onderzoek of inbeslagneming wordt uitgevoerd en kan hij/zij derhalve bezwaar maken op het moment dat het bevel wordt uitgevoerd ([159]). Het CPA voorziet daarnaast in een zogenaamd "quasiklachtenmechanisme", dat personen in staat stelt de bevoegde rechter te verzoeken om een beslissing van een aanklager of politieambtenaar in verband met een inbeslagneming nietig te verklaren of te wijzigen ([160]). Zo worden personen in staat gesteld bezwaar te maken tegen de maatregelen die worden genomen om een bevel tot inbeslagneming uit te voeren.

([150]) Hoewel in artikel 4 van de NHRC-wet wordt verwezen naar staatsburgers en buitenlanders die in de Republiek Korea verblijven, verwijst het begrip "verblijven" eerder naar een concept van jurisdictie dan van grondgebied. Wanneer de grondrechten van een buitenlander buiten Korea door nationale instellingen in Korea worden geschonden, kan die persoon dan ook een klacht indienen bij de NHRC. Zie bijvoorbeeld de dienovereenkomstige vraag op de pagina met veelgestelde vragen van de NHRC, beschikbaar op: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2 Dit zou het geval zijn wanneer er op onrechtmatige wijze door Koreaanse overheidsinstanties toegang wordt verkregen tot persoonsgegevens van een buitenlander die aan Korea zijn doorgegeven.

([151]) Een klacht moet in beginsel binnen een jaar na de inbreuk worden ingediend, maar de NHRC kan nog steeds besluiten een klacht te onderzoeken die na die periode is ingediend, zolang de strafrechtelijke of civielrechtelijke verjaringstermijn niet is verstreken (artikel 32, lid 1, punt 4, van de NHRC-wet).

([152]) Artikelen 42 en verder van de NHRC-wet.

([153]) Artikelen 36 en 37 van de NHRC-wet.

([154]) Artikel 44 van de NHRC-wet.

([155]) Artikel 42, lid 4, van de NHRC-wet.

([156]) Artikel 48 van de NHRC-wet.

([157]) Indien de NHRC bij wijze van uitzondering bijvoorbeeld niet in staat is om bepaalde materialen of faciliteiten te inspecteren omdat deze staatsgeheimen betreffen die een aanzienlijk effect kunnen hebben op de staatsveiligheid of de diplomatieke betrekkingen, of wanneer de inspectie een ernstige belemmering zou vormen voor een strafrechtelijk onderzoek of een lopende gerechtelijke procedure (zie voetnoot 166) en wanneer dit ertoe leidt dat de NHRC het noodzakelijke onderzoek om te feiten van het ontvangen verzoek te beoordelen, niet kan uitvoeren, stelt zij de betrokkene in kennis van de redenen waarom de klacht is afgewezen, overeenkomstig artikel 39 van de NHRC-wet. In dit geval kan de betrokkene de beslissing van de NHRC aanvechten op grond van de Wet administratieve procesvoering.

([158]) Zie bijvoorbeeld Beslissing 2007Nu27259 van het Hof van Seoul van 18 april 2008, bevestigd bij Beslissing 2008Du7854 van het Hooggerechtshof van 9 oktober 2008; Beslissing 2017Nu69382 van het Hof van Seoul van 2 februari 2018.

([159]) Artikelen 121 en 219 CPA.

([160]) Artikel 417 CPA, juncto artikel 414, lid 2, CPA. Zie ook Beslissing nr. 97Mo66 van het Hooggerechtshof van 29 september 1997.

Daarnaast kunnen betrokkenen bij de Koreaanse rechtbanken schadevergoeding verkrijgen. Op basis van de Wet inzake overheidscompensatie kunnen betrokkenen een aanvraag indienen voor vergoeding van schade die door ambtenaren bij de uitoefening van hun officiële taken, in strijd met de wet is toegebracht ([161]). Een verzoek op grond van de Wet inzake overheidscompensatie kan worden ingediend bij een gespecialiseerde "raad voor schadevergoeding" of rechtstreeks bij de Koreaanse rechtbanken ([162]). Indien het slachtoffer een buitenlands onderdaan is, is de Wet inzake overheidscompensatie van toepassing zolang het land van herkomst van deze persoon ook voorziet in compensatie van de staat voor Koreaanse onderdanen ([163]). Volgens de jurisprudentie wordt aan deze voorwaarde voldaan wanneer de vereisten voor het indienen van een verzoek om schadevergoeding in het andere land niet te zeer verschillen tussen Korea en het andere land en over het algemeen niet strikter zijn dan de door Korea vastgestelde vereisten, waarbij er geen sprake is van wezenlijke en inhoudelijke verschillen ([164]). In het burgerlijk wetboek is de aansprakelijkheid van de overheid voor schadevergoeding geregeld. De aansprakelijkheid van de staat omvat ook niet-materiële schade (bijvoorbeeld geestelijk lijden) ([165]).

Voor schendingen van de gegevensbeschermingsvoorschriften voorziet de PIPA in een aanvullende gerechtelijke verhaalsmogelijkheid. Op grond van artikel 39 PIPA kan een natuurlijke persoon die schade heeft opgelopen als gevolg van een schending van de PIPA of van verlies, diefstal, openbaarmaking, vervalsing of wijziging van of schade aan zijn/haar persoonsinformatie schadevergoeding verkrijgen voor de rechter. Hiervoor geldt geen vergelijkbare eis van wederkerigheid zoals op grond van de Wet inzake overheidscompensatie.

Naast de schadevergoeding kan op grond van de Wet administratieve procesvoering administratief beroep worden aangetekend tegen het handelen of nalaten van bestuursinstanties. Personen kunnen bezwaar maken tegen een beschikking (d.w.z. het uitoefenen of weigeren uit te oefenen van een openbare bevoegdheid in een specifieke zaak) of nalaten (het langdurige nalaten van een bestuursinstantie om een bepaalde beschikking vast te stellen ondanks een wettelijke verplichting om dit te doen), wat kan leiden tot de intrekking of wijziging van een onwettige beschikking, een vaststelling van nietigheid (d.w.z. een vaststelling dat de beschikking geen rechtsgevolg heeft of niet bestaat in de rechtsorde) of een vaststelling dat het nalaten onwettig is ([166]). Om bezwaar te kunnen maken tegen een administratieve beschikking moet deze directe gevolgen hebben voor de burgerrechten en -plichten ([167]). Dit omvat maatregelen tot verzameling van persoonsgegevens, ongeacht of dit direct (bv. het onderscheppen van communicatie) of door middel van een verzoek om openbaarmaking (bv. aan een dienstverlener) is.

De bovengenoemde vorderingen kunnen in eerste instantie worden ingesteld bij commissies van administratief beroep die door bepaalde overheidsinstanties zijn opgericht (bv. de Nationale Inlichtingendienst, de NHRC) of bij de Centrale Commissie voor hoger beroep in bestuurszaken die is ingesteld door de Commissie voor corruptiebestrijding en burgerrechten ([168]). Een dergelijk administratief beroep biedt een alternatieve, informelere mogelijkheid om bezwaar te maken tegen een beschikking of nalatigheid van een overheidsinstantie. Een vordering kan echter ook rechtstreeks bij de Koreaanse rechter worden ingesteld op grond van de Wet administratieve procesvoering.

Een verzoek om intrekking/wijziging van een beschikking op grond van de Wet administratieve procesvoering kan worden ingediend door elke persoon met een wettelijk belang bij het verzoek om intrekking/wijziging of het herstel van zijn/haar rechten door de intrekking/wijziging in het geval dat de beschikking niet langer rechtsgevolgen heeft ([169]). Een proces om de nietigheid te bevestigen, kan op vergelijkbare wijze worden gestart door een persoon met een wettig belang bij een dergelijke bevestiging, terwijl een proces om de onwettigheid van nalaten te bevestigen, kan worden gestart door een persoon die een verzoek om een beschikking heeft ingediend en een wettig belang heeft bij het verzoek om de bevestiging van de onwettigheid van het nalaten ([170]). Volgens de rechtspraak van het Hooggerechtshof wordt onder "wettig belang" verstaan een "wettelijk beschermd belang", d.w.z. een direct en specifiek belang dat wordt beschermd door de wet- en regelgeving waarop administratieve beslissingen zijn gebaseerd (d.w.z. geen algemene, indirecte en abstracte belangen van het publiek) ([171]). Natuurlijke personen hebben derhalve een dergelijk wettig belang in geval van inbreuk op de beperkingen en waarborgen die van toepassing zijn op het verzamelen van hun persoonsgegevens met het oog op de handhaving van het strafrecht (op grond van specifieke wetten of de PIPA). Een definitieve uitspraak op grond van de Wet administratieve procesvoering is bindend voor de partijen ([172]).

Een verzoek tot intrekking/wijziging van een beslissing en een verzoek om de onrechtmatigheid van een nalatigheid te bevestigen moeten worden ingediend binnen negentig dagen na de datum waarop de betrokkene kennis heeft gekregen

([161]) Artikel 2, lid 1, van de Wet inzake overheidscompensatie.

([162]) Artikelen 9 en 12 van de Wet inzake overheidscompensatie. De wet stelt districtsraden in (voorgezeten door de substituut-aanklager van het overeenkomstige parket), een centrale raad (voorgezeten door de viceminister van Justitie) en een speciale raad (voorgezeten door de viceminister van Nationale Defensie en belast met vorderingen tot schadevergoeding voor schade toegebracht door militairen of burgerpersoneel bij de krijgsmacht). Vorderingen tot schadevergoeding worden in beginsel behandeld door de districtsraden, die in bepaalde omstandigheden zaken moeten doorsturen naar de centrale/speciale raad, bijvoorbeeld wanneer de schadevergoeding een bepaald bedrag overschrijdt of wanneer een persoon om een nieuwe beraadslaging verzoekt. Alle raden bestaan uit leden die door de minister van Justitie worden benoemd (bv. uit ambtenaren van het ministerie van Justitie, rechterlijke ambtenaren, advocaten en personen die deskundig zijn op het gebied van staatscompensatie) en zijn onderworpen aan specifieke regels inzake belangenconflicten (zie artikel 7 van het Uitvoeringsdecreet van de Wet inzake overheidscompensatie).

([163]) Artikel 7 van de Wet inzake overheidscompensatie.

([164]) Beslissing nr. 2013Da208388 van het Hooggerechtshof van donderdag 11 juni 2015.

([165]) Zie artikel 8 van de Wet inzake overheidscompensatie en artikel 751 van het burgerlijk wetboek.

([166]) Artikelen 2 en 4 van de Wet administratieve procesvoering.

([167]) Beslissing nr. 98Du18435 van het Hooggerechtshof van 22 oktober 1999, Beslissing nr. 99Du1113 van het Hooggerechtshof van 8 september 2000 en Beslissing nr. 2010Du3541 van het Hooggerechtshof van 27 september 2012.

([168]) Artikel 6 van de Wet inzake hoger beroep in bestuurszaken en Artikel 18, lid 1, van de Wet administratieve procesvoering.

([169]) Artikel 12 van de Wet administratieve procesvoering.

([170]) Artikelen 35 en 36 van de Wet administratieve procesvoering.

([171]) Beslissing nr. 2006Du330 van het Hooggerechtshof van 26 maart 2006.

([172]) Artikel 30, lid 1, van de Wet administratieve procesvoering.

van de beslissing/nalatigheid en in beginsel niet later dan één jaar na de datum waarop de beslissing is genomen of de nalatigheid heeft plaatsgevonden, tenzij er gerechtvaardigde redenen zijn om dat niet te doen ([173]). Volgens de jurisprudentie van het Hooggerechtshof moet het begrip "gerechtvaardigde redenen" ruim worden uitgelegd en vereist het dat wordt beoordeeld of het, gelet op alle omstandigheden van het geval, maatschappelijk aanvaardbaar is dat een klacht te laat wordt ingediend ([174]). Dit omvat (maar is niet beperkt tot) bijvoorbeeld redenen voor een vertraging die niet aan de betrokken partij kunnen worden toegerekend (d.w.z. situaties waarop de klager geen invloed heeft, bijvoorbeeld wanneer hij of zij niet in kennis is gesteld van het verzamelen van zijn of haar persoonsinformatie) of overmacht (bv. een natuurramp, oorlog).

Tot slot kunnen personen ook een grondwettelijke klacht indienen bij het Grondwettelijk Hof ([175]). Op basis van de Wet op het Grondwettelijk Hof kan elke persoon wiens door de grondwet gewaarborgde rechten zijn geschonden als gevolg van de uitoefening of niet-uitoefening van een overheidsbevoegdheid (met uitzondering van uitspraken van de rechtbanken) verzoeken om de behandeling van een grondwettelijke klacht. Indien andere verhaalsmogelijkheden beschikbaar zijn, moeten deze eerst worden uitgeput. Volgens de jurisprudentie van het Grondwettelijk Hof kunnen buitenlandse onderdanen een grondwettelijke klacht indienen voor zover hun basisrechten worden erkend in de Koreaanse grondwet (zie de uitleg in punt 1.1) ([176]). Grondwettelijke klachten moeten worden ingediend binnen negentig dagen nadat de betrokkene kennis heeft gekregen van de inbreuk, en binnen één jaar nadat deze zich heeft voorgedaan. Aangezien de procedure van de Wet administratieve procesvoering wordt toegepast op geschillen op grond van de Wet op het Grondwettelijk Hof ([177]), is een klacht nog steeds ontvankelijk wanneer sprake is van "gerechtvaardigde redenen", zoals uitgelegd volgens de hierboven beschreven rechtspraak van het Hooggerechtshof.

Indien eerst andere rechtsmiddelen moeten worden uitgeput, moet een grondwettelijke klacht worden ingediend binnen dertig dagen na de definitieve beslissing over een dergelijk rechtsmiddel ([178]). Het Grondwettelijk Hof kan de uitoefening van de overheidsbevoegdheid die de inbreuk heeft veroorzaakt ongeldig verklaren of bevestigen dat een bepaald nalaten ongrondwettelijk is ([179]). In dat geval is de betrokken overheid verplicht maatregelen te nemen om zich naar de beslissing van het Hof te voegen.

3. TOEGANG DOOR DE OVERHEID TEN BEHOEVE VAN DE NATIONALE VEILIGHEID

3.1. Bevoegde overheidsinstanties op het gebied van de nationale veiligheid

De Republiek Korea beschikt over twee speciale inlichtingendiensten: de Nationale Inlichtingendienst (NIS) en het Commando ondersteuning defensie en veiligheid. Daarnaast mogen ook de politie en het Openbaar Ministerie persoonsinformatie verzamelen met het oog op de nationale veiligheid.

De NIS is opgericht bij de Wet op de Nationale Inlichtingendienst (*NIS-wet*) en werkt direct onder de bevoegdheid en het toezicht van de president ([180]). De NIS verzamelt, bundelt en verspreidt met name informatie over andere landen (waaronder Noord-Korea) ([181]), inlichtingen in verband met het tegengaan van spionage (waaronder militaire en industriële spionage), terrorisme en de activiteiten van internationale criminele organisaties, inlichtingen over bepaalde soorten misdrijven tegen de openbare en nationale veiligheid (bv. binnenlands oproer, buitenlandse agressie) en inlichtingen in verband met de taak om de cyberveiligheid te waarborgen en cyberaanvallen en -dreigingen te voorkomen en te bestrijden ([182]). De NIS-wet, waarbij de NIS is opgericht en waarin haar taken uiteen zijn gezet, bevat ook algemene beginselen die een kader vormen voor al haar activiteiten. Als algemeen beginsel geldt dat de NIS politiek neutraal moet blijven en de vrijheden en rechten van natuurlijke personen moet beschermen ([183]). De voorzitter van de NIS heeft als taak algemene richtsnoeren te ontwikkelen waarin de beginselen, het toepassingsgebied en de procedures worden uiteengezet voor de uitvoering van de taken van de NIS in verband met de verzameling en het gebruik van informatie, en hij moet de Nationale Vergadering hiervan in kennis stellen ([184]). De Nationale Vergadering kan (via haar Inlichtingencommissie) vereisen dat de richtsnoeren worden gecorrigeerd of aangevuld wanneer zij van mening is dat deze onwettig of onrechtvaardig zijn. Meer in het algemeen mogen de directeur en het personeel van de NIS bij de uitvoering van hun taken instellingen, organisaties of personen er niet toe dwingen dingen te doen waartoe zij niet verplicht zijn en mogen zij de uitoefening van rechten door personen niet belemmeren door misbruik te maken van hun officiële bevoegdheid ([185]). Daarnaast moet een eventuele censuur van post, onderschepping van telecommunicatie, verzameling van locatiegegevens en verzameling van communicatiebevestigende gegevens of het eventuele opnemen of afluisteren

([173]) Artikel 20 van de Wet administratieve procesvoering. Deze uiterste termijn is ook van toepassing op verzoeken om de onwettigheid van nalaten te bevestigen, zie artikel 38, lid 2, van de Wet administratieve procesvoering.
([174]) Beslissing nr. 90Nu6521 van het Hooggerechtshof van 28 juni 1991.
([175]) Artikel 68, lid 1, van de Wet op het Grondwettelijk Hof.
([176]) Beslissing nr. 99HeonMa194 van het Grondwettelijk Hof van 29 november 2001.
([177]) Artikel 40 van de Wet op het Grondwettelijk Hof.
([178]) Artikel 69 van de Wet op het Grondwettelijk Hof.
([179]) Artikel 75, lid 3, van de Wet op het Grondwettelijk Hof.
([180]) Artikel 2 en artikel 4, lid 2, van de NIS-wet.
([181]) Hieronder valt geen informatie over natuurlijke personen, maar wel algemene informatie over andere landen (trends, ontwikkelingen) en over de activiteiten van overheidsactoren van derde landen.
([182]) Artikel 3, lid 1, van de NIS-wet.
([183]) Artikel 3, lid 1, artikel 6, lid 2, en de artikelen 11 en 21. Zie ook de regels in verband met belangenconflicten, met name de artikelen 10 en 12.
([184]) Artikel 4, lid 2, van de NIS-wet.
([185]) Artikel 13 van de NIS-wet.

van privécommunicatie door de NIS in overeenstemming zijn met de CPPA, de Wet locatiegegevens of het CPA ([186]). Voor misbruik van bevoegdheden of het in strijd met deze wetten verzamelen van informatie gelden strafrechtelijke sancties ([187]).

Het Commando ondersteuning defensie en veiligheid is een militaire inlichtingendienst die is opgericht onder auspiciën van het ministerie van Defensie. Het is verantwoordelijk voor veiligheidskwesties binnen het leger, militaire strafrechtelijke onderzoeken (die vallen onder de Wet op de militaire rechtbank) en militaire inlichtingen. Het Commando ondersteuning defensie en veiligheid surveilleert over het algemeen geen burgers, tenzij dit noodzakelijk is voor de uitvoering van zijn militaire taken. Personen die kunnen worden onderzocht zijn militair personeel, civiele werknemers van de krijgsmacht, personen in militaire opleiding, personen in militaire reserve- of rekruteringsdienst en krijgsgevangenen ([188]). Bij het verzamelen van communicatiegegevens met het oog op de nationale veiligheid moet het Commando ondersteuning defensie en veiligheid zich houden aan de beperkingen en waarborgen die zijn vastgelegd in de CPPA en het bijbehorende uitvoeringsdecreet.

3.2. **Rechtsgrondslagen en beperkingen**

In de CPPA, de Wet inzake terrorismebestrijding ter bescherming van burgers en de openbare veiligheid (hierna de "Wet terrorismebestrijding" genoemd) en de TBA is voorzien in rechtsgrondslagen voor de verzameling van persoonsinformatie met het oog op de nationale veiligheid en zijn de toepasselijke beperkingen en waarborgen uiteengezet ([189]). Deze beperkingen en waarborgen, zoals beschreven in de volgende punten, zorgen ervoor dat de verzameling en verwerking van informatie wordt beperkt tot wat strikt noodzakelijk is om een wettige doelstelling te verwezenlijken. Dit sluit het massaal en ongedifferentieerd verzamelen van persoonsinformatie om redenen van nationale veiligheid uit.

3.2.1. *Verzameling van communicatiegegevens*

3.2.1.1. Verzameling van communicatiegegevens door inlichtingendiensten

3.2.1.1.1. Rechtsgrondslag

De CPPA biedt inlichtingendiensten de bevoegdheid om communicatiegegevens te verzamelen en vereist dat aanbieders van communicatiediensten met deze diensten samenwerken wanneer zij een verzoek ontvangen ([190]). Zoals beschreven in punt 2.2.2.1 wordt in de CPPA onderscheid gemaakt tussen de verzameling van de inhoud van communicatie (d.w.z. "*communicatiebeperkende maatregelen*", zoals "*aftapping*" of "*censuur*" ([191])) en de verzameling van "*communicatiebevestigende gegevens*" ([192]).

De drempel voor het verzamelen van deze twee soorten informatie verschilt, maar de toepasselijke procedures en waarborgen zijn grotendeels gelijk ([193]). Het verzamelen van communicatiebevestigende gegevens (of metagegevens) kan plaatsvinden om bedreigingen voor de nationale veiligheid te voorkomen ([194]). Voor het uitvoeren van communicatiebeperkende maatregelen (d.w.z. het verzamelen van de inhoud van communicatie) geldt een hogere drempel en deze maatregelen mogen slechts worden genomen wanneer de nationale veiligheid naar verwachting ernstig in gevaar zal worden gebracht en de verzameling van de inlichtingen noodzakelijk is om een dergelijk gevaar te voorkomen (d.w.z. wanneer er een ernstig risico voor de nationale veiligheid bestaat en de verzameling noodzakelijk is om dit te voorkomen) ([195]). Het inzien van de inhoud van communicatie is bovendien alleen toegestaan als laatste redmiddel om de nationale veiligheid te waarborgen en er moeten inspanningen worden geleverd om de schending van de communicatieprivacy tot een minimum te beperken ([196]). Zelfs wanneer de passende goedkeuring/toestemming is verkregen, moeten dergelijke maatregelen onmiddellijk worden stopgezet zodra zij niet langer noodzakelijk zijn, zodat ervoor wordt gezorgd dat een inbreuk op het communicatiegeheim van personen tot een minimum wordt beperkt ([197]).

3.2.1.1.2. Beperkingen en waarborgen die van toepassing zijn op de verzameling van communicatiegegevens waarbij ten minste één Koreaans onderdaan betrokken is

Het verzamelen van communicatiegegevens (zowel inhoud als metagegevens), waarbij één of beide betrokkenen bij de communicatie Koreaans onderdaan zijn, mag slechts plaatsvinden met toestemming van een opperrechter van het

([186]) Artikel 14 van de NIS-wet.
([187]) Artikelen 22 en 23 van de NIS-wet.
([188]) Artikel 1 van de Wet op de militaire rechtbank.
([189]) Bij het onderzoeken van misdrijven in verband met de nationale veiligheid handelen de politie en de NIS op basis van het CPA, terwijl het Commando ondersteuning defensie en veiligheid onder de Wet op de militaire rechtbank valt.
([190]) Artikel 15-2 CPPA.
([191]) Artikel 2, leden 6 en 7, CPPA.
([192]) Artikel 2, lid 11, CPPA.
([193]) Zie ook artikel 13-4, lid 2, CPPA en artikel 37, lid 4, van het CPPA-uitvoeringsdecreet, waarin is bepaald dat de procedures die gelden voor de verzameling van de inhoud van communicatie mutatis mutandis van toepassing zijn op de verzameling van communicatiebevestigende gegevens.
([194]) Artikel 13-4 CPPA.
([195]) Artikel 7, lid 1, CPPA.
([196]) Artikel 3, lid 2, CPPA.
([197]) Artikel 2 van het CPPA-uitvoeringsdecreet.

Hof ([198]). Het verzoek van de inlichtingendienst moet schriftelijk worden ingediend bij een aanklager of bij het Bureau van de procureur-generaal ([199]). In het verzoek moeten de redenen voor de verzameling worden vermeld (d.w.z. dat de nationale veiligheid naar verwachting ernstig in gevaar zal worden gebracht of dat de verzameling noodzakelijk is om een bedreiging van de nationale veiligheid te voorkomen), evenals materiaal ter ondersteuning van deze redenen en waaruit een kennelijke reden voor de zaak blijkt en de details van het verzoek (d.w.z. de doelstellingen, de persoon/personen op wie het betrekking heeft, de reikwijdte, de daadwerkelijke periode van verzameling en de manier waarop en waar de verzameling zal plaatsvinden) ([200]). Vervolgens verzoekt de aanklager/het Bureau van de procureur-generaal een hooggeplaatste rechter van het Hof om toestemming ([201]). Die hooggeplaatste rechter mag slechts schriftelijke toestemming geven wanneer hij/zij van mening is dat het verzoek gegrond is en wijst het verzoek af wanneer hij/zij het ongegrond acht ([202]). In het bevel worden het soort, de doelstelling, het voorwerp, de reikwijdte en de daadwerkelijke periode van de verzameling gespecificeerd, evenals de manier waarop en waar deze zal plaatsvinden ([203]).

Er gelden specifieke regels wanneer de maatregel gericht is op het onderzoeken van een samenzwering die een bedreiging vormt voor de nationale veiligheid en er een noodsituatie bestaat waardoor het onmogelijk is de bovengenoemde procedures te volgen ([204]). Indien aan deze voorwaarden is voldaan, mogen inlichtingendiensten surveillancemaatregelen uitvoeren zonder voorafgaande goedkeuring van de rechter ([205]). De inlichtingendienst moet de rechter echter onmiddellijk na de uitvoering van de noodmaatregelen om toestemming verzoeken. Wanneer de toestemming niet is verkregen binnen 36 uur na het ogenblik waarop de maatregelen zijn genomen, moeten deze onmiddellijk worden stopgezet ([206]). Het verzamelen van informatie in noodsituaties moet altijd plaatsvinden in overeenstemming met een "verklaring inzake censuur/aftapping in noodsituaties" en de inlichtingendienst die de informatie verzamelt, moet een register bijhouden van alle noodmaatregelen ([207]).

In gevallen waarin de surveillance binnen korte tijd wordt beëindigd, waardoor geen toestemming van de rechter kan worden gevraagd, moet het hoofd van het bevoegde Bureau van de procureur-generaal een door de inlichtingendienst opgestelde kennisgeving van noodmaatregelen sturen aan het hoofd van de bevoegde rechtbank, die het register van noodmaatregelen bijhoudt ([208]). Zo kan de rechter de wettigheid van de verzameling toetsen.

3.2.1.1.3. Beperkingen en waarborgen die van toepassing zijn op de verzameling van communicatiegegevens waarbij uitsluitend niet-Koreaanse onderdanen betrokken zijn

Voor het verzamelen van informatie over communicatie tussen niet-Koreaanse onderdanen moeten inlichtingendiensten vooraf schriftelijke goedkeuring van de president verkrijgen ([209]). Dergelijke communicatie wordt alleen met het oog op de nationale veiligheid verzameld wanneer deze valt onder één van verschillende gespecificeerde categorieën, namelijk communicatie tussen ambtenaren of andere personen van landen die de Republiek Korea vijandig gezind zijn, buitenlandse agentschappen, groepen of onderdanen die worden verdacht van activiteiten tegen Korea ([210]) of leden van groepen op het Koreaanse schiereiland die effectief niet onder de jurisdictie van de Republiek Korea vallen en hun overkoepelende groepen in derde landen ([211]). Als één partij bij de communicatie een Koreaans onderdaan is en de andere partij niet, is echter goedkeuring van de rechter vereist overeenkomstig de in punt 3.2.1.1.2 beschreven procedure.

Het hoofd van een inlichtingendienst moet een plan voor de beoogde maatregelen indienen bij de directeur van de NIS ([212]). De directeur van de NIS evalueert of dit plan passend is en dient het plan, wanneer dit het geval is, ter goedkeuring in bij de president ([213]). De informatie die in het plan moet worden opgenomen, is dezelfde als de informatie die vereist is voor een verzoek om rechterlijke toestemming voor het verzamelen van informatie over Koreaanse onderdanen (zoals hierboven beschreven) ([214]). In het verzoek moeten met name de redenen voor de verzameling worden vermeld (d.w.z. dat de nationale veiligheid naar verwachting ernstig in gevaar zal worden gebracht of dat de verzameling noodzakelijk is om een bedreiging van de nationale veiligheid te voorkomen), evenals de

([198]) Artikel 7, lid 1, punt 1, CPPA. De bevoegde rechter is het Hof dat bevoegd is voor de verblijfplaats of locatie van de vestiging van één of beide partijen die worden gesurveilleerd.
([199]) Artikel 7, lid 3, van het CPPA-uitvoeringsdecreet.
([200]) Artikel 7, lid 3, en artikel 6, lid 4, CPPA.
([201]) Artikel 7, lid 4, van het CPPA-uitvoeringsdecreet. In het verzoek dat de aanklager richt tot de rechter moeten de belangrijkste redenen voor de verdenking worden uiteengezet en, voor zover om meerdere toestemmingen tegelijk wordt verzocht, de rechtvaardiging hiervan (zie artikel 4 van het CPPA-uitvoeringsdecreet).
([202]) Artikel 7, lid 3, en artikel 6, leden 5 en 9, CPPA.
([203]) Artikel 7, lid 3, en artikel 6, lid 6, CPPA.
([204]) Artikel 8 CPPA.
([205]) Artikel 8, lid 1, CPPA.
([206]) Artikel 8, lid 2, CPPA.
([207]) Artikel 8, lid 4, CPPA. Zie punt 2.2.2.2 hierboven voor noodmaatregelen in het kader van de rechtshandhaving.
([208]) Artikel 8, leden 5 en 7, CPPA. In de kennisgeving moeten het doel, het voorwerp, de reikwijdte, de periode, de plaats van uitvoering en de methode van surveillance worden aangegeven, alsmede de redenen waarom geen verzoek om toestemming is ingediend voordat de maatregel werd genomen (artikel 8, lid 6, CPPA).
([209]) Artikel 7, lid 1, punt 2, CPPA.
([210]) Hiermee wordt verwezen naar activiteiten die een bedreiging vormen voor het bestaan en de veiligheid van de natie, de democratische orde of het voortbestaan en de vrijheid van het volk.
([211]) Als één partij een persoon is zoals beschreven in artikel 7, lid 1, punt 2, CPPA en de andere partij onbekend is of niet kan worden gespecificeerd, is bovendien de procedure van artikel 7, lid 1, punt 2, van toepassing.
([212]) Artikel 8, lid 1, van het CPPA-uitvoeringsdecreet. De directeur van de NIS wordt benoemd door de president na bevestiging van het parlement (artikel 7 van de NIS-wet).
([213]) Artikel 8, lid 2, van het CPPA-uitvoeringsdecreet.
([214]) Artikel 8, lid 3, van het CPPA-uitvoeringsdecreet juncto artikel 6, lid 4, CPPA.

belangrijkste redenen voor de verdenking, materiaal ter ondersteuning van deze redenen en waaruit een kennelijke reden voor de zaak blijkt en de details van het verzoek (d.w.z. de doelstellingen, de persoon/personen op wie het betrekking heeft, de reikwijdte, de daadwerkelijke periode van verzameling en de manier waarop en waar de verzameling zal plaatsvinden). Wanneer meerdere verzoeken om toestemming tegelijk worden ingediend, moeten de strekking en redenen daarvan worden vermeld ([215]).

In noodsituaties ([216]) moet een voorafgaande goedkeuring worden verkregen van de minister onder wie de desbetreffende inlichtingendienst valt. In dit geval moet de inlichtingendienst onmiddellijk na het nemen van de noodmaatregelen echter om goedkeuring van de president verzoeken. Wanneer een inlichtingendienst niet binnen 36 uur na indiening van het verzoek goedkeuring verkrijgt, moet de verzameling onmiddellijk worden stopgezet ([217]). In dergelijke gevallen wordt de verzamelde informatie altijd vernietigd.

3.2.1.1.4. Algemene beperkingen en waarborgen

Wanneer zij verzoeken om de samenwerking van particuliere entiteiten, moeten inlichtingendiensten deze entiteiten het rechterlijk bevel/de presidentiële toestemming of een kopie van de omslag van een verklaring van censuur in noodsituaties overleggen, die de betreffende entiteit in haar dossiers moet bewaren ([218]). Entiteiten die worden verzocht informatie te verstrekken aan inlichtingendiensten op basis van de CPPA mogen dit weigeren wanneer de toestemming of de verklaring inzake de censuur in noodsituaties betrekking heeft op de verkeerde identificator (bv. een telefoonnummer dat aan een andere persoon toebehoort dan de geïdentificeerde persoon). Bovendien mogen wachtwoorden die voor communicatie worden gebruikt in geen enkel geval worden bekendgemaakt ([219]).

Inlichtingendiensten mogen de uitvoering van communicatiebeperkende maatregelen of de verzameling van communicatiebevestigende informatie toevertrouwen aan een postkantoor of aanbieder van telecommunicatiediensten (zoals gedefinieerd in de Wet op de telecommunicatieactiviteiten) ([220]). Zowel de betrokken inlichtingendienst als de aanbieder die een verzoek om samenwerking ontvangt, moet gedurende drie jaar een register bijhouden waarin het doel van het verzoek om de maatregelen, de datum van uitvoering of samenwerking en het voorwerp van de maatregelen (bv. post, telefoon of e-mail) worden vermeld ([221]). Aanbieders van telecommunicatiediensten die communicatiebevestigende gegevens verstrekken, moeten gedurende een periode van zeven jaar in hun dossiers informatie bijhouden over de frequentie van de verzameling en tweemaal per jaar verslag uitbrengen aan de minister van Wetenschap en ICT ([222]).

Inlichtingendiensten moeten bij de directeur van de NIS verslag uitbrengen over de informatie die zij hebben verzameld en over het resultaat van de surveillance ([223]). Met betrekking tot de verzameling van communicatiebevestigende gegevens moeten registers worden bijgehouden van het feit dat een verzoek om dergelijke gegevens is ingediend, alsook van het schriftelijke verzoek zelf en de instelling die hiervan gebruik heeft gemaakt ([224]).

Het verzamelen van zowel de inhoud van de communicatie als de communicatiebevestigende gegevens mag slechts hoogstens vier maanden worden voortgezet en moet onmiddellijk worden stopgezet wanneer het nagestreefde doel eerder wordt bereikt ([225]). Wanneer de voorwaarden voor de toestemming blijven bestaan, kan de periode met maximaal vier maanden worden verlengd, met toestemming van de rechter of goedkeuring van de president. Het verzoek om toestemming voor verlenging van de surveillancemaatregelen moet schriftelijk worden ingediend, met opgave van de redenen waarom verlenging wordt verzocht en met overlegging van ondersteunend materiaal ([226]).

Afhankelijk van de rechtsgrondslag voor de verzameling worden de betrokkenen over het algemeen in kennis gesteld wanneer hun communicatie wordt verzameld. Meer bepaald moet het hoofd van de inlichtingendienst de betrokkene binnen dertig dagen na afloop van de surveillance schriftelijk in kennis stellen, ongeacht of de verzamelde informatie de inhoud van de communicatie dan wel de communicatiebevestigende gegevens betreft en ongeacht of de informatie werd verkregen in het kader van de gewone procedure of in een noodsituatie ([227]). In de kennisgeving moet het volgende

([215]) Artikel 8, lid 3, en artikel 4 van het CPPA-uitvoeringsdecreet.
([216]) Dat wil zeggen, in gevallen waarin de maatregel gericht is op een samenzwering die de nationale veiligheid bedreigt, er onvoldoende tijd is om de goedkeuring van de president te verkrijgen en het niet nemen van noodmaatregelen de nationale veiligheid kan schaden (artikel 8, lid 8, CPPA).
([217]) Artikel 8, lid 9, CPPA.
([218]) Artikel 9, lid 2, CPPA en artikel 12 van het CPPA-uitvoeringsdecreet.
([219]) Artikel 9, lid 4, CPPA.
([220]) Artikel 13 van het CPPA-uitvoeringsdecreet.
([221]) Artikel 9, lid 3, CPPA en artikel 17, lid 2, van het CPPA-uitvoeringsdecreet. Deze periode geldt niet voor communicatiebevestigende gegevens (zie artikel 39 van het CPPA-uitvoeringsdecreet).
([222]) Artikel 13, lid 7, CPPA en artikel 39 van het CPPA-uitvoeringsdecreet.
([223]) Artikel 18, lid 3, van het CPPA-uitvoeringsdecreet.
([224]) Artikel 13, lid 5, en artikel 13-4, lid 3, CPPA.
([225]) Artikel 7, lid 2, CPPA.
([226]) Artikel 7, lid 2, CPPA en artikel 5 van het CPPA-uitvoeringsdecreet.
([227]) Artikel 9-2, lid 3, CPPA. Overeenkomstig artikel 13-4 CPPA geldt dit voor de verzameling van zowel de inhoud van de communicatie als de communicatiebevestigende gegevens.

worden vermeld: 1) het feit dat de informatie is verzameld, 2) de uitvoerende instantie en 3) de uitvoeringsperiode. De kennisgeving kan echter worden uitgesteld wanneer het waarschijnlijk is dat deze de nationale veiligheid in gevaar zou brengen of het leven en de fysieke veiligheid van mensen zou schaden ([228]). De kennisgeving moet worden gedaan binnen dertig dagen nadat de redenen voor het uitstel niet langer bestaan ([229]).

Deze kennisgevingsvereiste geldt echter alleen voor de verzameling van informatie waarbij ten minste een van de partijen een Koreaans onderdaan is. Niet-Koreaanse onderdanen worden bijgevolg alleen in kennis gesteld wanneer hun communicatie met Koreaanse onderdanen wordt verzameld. Er is dus geen kennisgevingsvereiste voor de verzameling van communicatie tussen uitsluitend niet-Koreaanse onderdanen.

De inhoud van de communicatie en de communicatiebevestigende gegevens die door middel van surveillance zijn verkregen op basis van de CPPA mogen alleen worden gebruikt 1) voor het onderzoeken, vervolgen of voorkomen van bepaalde misdrijven, 2) voor tuchtrechtelijke procedures, 3) voor gerechtelijke procedures waarin een partij die betrokken is bij de communicatie deze gebruikt in een vordering tot schadevergoeding of 4) op basis van andere wetten ([230]).

3.2.1.2. Verzameling van communicatiegegevens door de politie/aanklagers met het oog op de nationale veiligheid

De politie/aanklager mag communicatiegegevens (zowel de inhoud van de communicatie als de communicatiebevestigende gegevens) verzamelen met het oog op de nationale veiligheid, onder dezelfde voorwaarden als beschreven in punt 3.2.1.1. Wanneer wordt opgetreden in een noodsituatie ([231]) is de procedure van toepassing die hierboven is beschreven met betrekking tot de verzameling van de inhoud van de communicatie met het oog op de rechtshandhaving in noodsituaties (d.w.z. artikel 8 CPPA).

3.2.2. *Verzameling van informatie over terreurverdachten*

3.2.2.1. Rechtsgrondslag

De Wet terrorismebestrijding verleent de directeur van de NIS de bevoegdheid om informatie over terreurverdachten te verzamelen ([232]). Een "*terreurverdachte*" wordt gedefinieerd als een lid van een terroristische groepering ([233]), een persoon die een terroristische groepering heeft gepropageerd (door ideeën of tactieken van een terroristische groepering te bevorderen of te verspreiden), of die middelen heeft ingezameld voor of bijgedragen heeft aan terrorisme ([234]) of een persoon die betrokken is bij andere activiteiten in verband met het voorbereiden, samenzweren, propageren of aanzetten tot terrorisme of een persoon ten aanzien van wie goede redenen bestaan om aan te nemen dat hij dergelijke activiteiten heeft uitgevoerd ([235]). Als algemene regel moet een ambtenaar die de Wet terrorismebestrijding handhaaft de basisrechten eerbiedigen die zijn verankerd in de Koreaanse grondwet ([236]).

In de Wet terrorismebestrijding op zich zijn geen specifieke bevoegdheden, beperkingen en waarborgen uiteengezet voor de verzameling van informatie over terreurverdachten, maar wordt in plaats daarvan verwezen naar de procedures van andere wetten. Op basis van de Wet terrorismebestrijding mag de directeur van de NIS informatie verzamelen over 1) het binnenkomen in en het verlaten van de Republiek Korea, 2) financiële transacties en 3) communicatie. Afhankelijk van het soort informatie dat nodig is, zijn de relevante procedurele vereisten vastgesteld in respectievelijk de Wet inzake immigratie en douane, de ARUSFTI of de CPPA ([237]). Voor de verzameling van informatie over het binnenkomen in en het verlaten van Korea is in de Wet terrorismebestrijding verwezen naar de in de Wet inzake immigratie en douane

([228]) Artikel 9-2, lid 4, CPPA.
([229]) Artikel 13-4, lid 2, en artikel 9-2, lid 6, CPPA.
([230]) Artikel 5, leden 1 en 2, artikel 12 en artikel 13-5 CPPA.
([231]) Dat wil zeggen wanneer de maatregel gericht is op een samenzwering die de nationale veiligheid in gevaar brengt en er sprake is van een noodgeval waardoor het niet mogelijk is om de gewone goedkeuringsprocedure te volgen (artikel 8, lid 1, CPPA).
([232]) Artikel 9 van de Wet terrorismebestrijding.
([233]) Een "*terroristische groepering*" is gedefinieerd als een groep terroristen zoals aangeduid door de Verenigde Naties (artikel 2, lid 2, van de Wet terrorismebestrijding).
([234]) "*Terrorisme*" wordt in artikel 2, lid 1, van de Wet terrorismebestrijding gedefinieerd als gedrag dat erop is gericht om de uitoefening van het gezag van de staat, een lokale overheid of een buitenlandse overheid (met inbegrip van lokale overheden en internationale organisaties) te belemmeren, of om deze tot actie te dwingen zonder dat daartoe een wettelijke verplichting bestaat, of om het publiek te bedreigen. Dit omvat a) het doden van een persoon of het leven van een persoon in gevaar brengen door die persoon lichamelijk letsel toe te brengen, gevangen te nemen, op te sluiten, te ontvoeren of te gijzelen; b) bepaalde soorten gedrag gericht op een vliegtuig (bv. het doen neerstorten, kapen of beschadigen van een vliegtuig in de lucht); c) bepaalde soorten gedrag in verband met een schip (bv. het kapen van een schip of mariene structuur dat/die in bedrijf is, het vernielen van een schip of mariene structuur dat/die in bedrijf is of het zodanig beschadigen ervan dat de veiligheid hierdoor in gevaar komt, waaronder het beschadigen van de lading op een schip of mariene structuur dat/die in bedrijf is); d) het plaatsen, ontsteken of op andere wijze gebruiken van een biochemisch, explosief of brandwapen of -apparaat met het oogmerk de dood, ernstig letsel of ernstige materiële schade te veroorzaken of met een dergelijk gevolg voor bepaalde soorten voertuigen of voorzieningen (bv. treinen, trams, motorvoertuigen, openbare parken en stations, de elektriciteits- en gasvoorzieningen, telecommunicatie-infrastructuur enz.); e) bepaalde soorten gedrag in verband met nucleair materiaal, radioactief materiaal of nucleaire installaties (bv. toebrengen van schade aan het leven, het lichaam of de eigendom van mensen of het op andere wijze verstoren van de openbare veiligheid door een kernreactor te vernietigen of radioactief materiaal op onrechtmatige wijze te manipuleren enz.).
([235]) Artikel 2, lid 3, van de Wet terrorismebestrijding.
([236]) Artikel 3, lid 3, van de Wet terrorismebestrijding.
([237]) Artikel 9, lid 1, van de Wet terrorismebestrijding.

uiteengezette procedures. Deze wetten voorzien momenteel echter niet in dergelijke bevoegdheden. Met betrekking tot het verzamelen van informatie over communicatie en financiële transacties verwijst de antiterrorismewet naar de beperkingen en waarborgen in het CPPA (die hieronder nader worden toegelicht) en de ARUSFTI (die, zoals uiteengezet in punt 2.1, niet relevant is voor de beoordeling van het adequaatheidsbesluit).

Daarnaast is in artikel 9, lid 3, van de Wet terrorismebestrijding bepaald dat de directeur van de NIS een verantwoordelijke voor de verwerking van persoonsinformatie ([238]) of een aanbieder van locatiegegevens ([239]) mag verzoeken om persoonsinformatie of locatiegegevens van een terreurverdachte. Deze mogelijkheid is beperkt tot verzoeken om vrijwillige verstrekking, waarop verantwoordelijken voor de verwerking van persoonsinformatie en aanbieders van locatiegegevens niet hoeven te antwoorden en dit in ieder geval alleen in overeenstemming met de PIPA en de Wet locatiegegevens mogen doen (zie punt 3.2.2.2 hieronder).

3.2.2.2. Beperkingen en waarborgen die van toepassing zijn op de vrijwillige verstrekking op grond van de PIPA en de Wet locatiegegevens

Verzoeken om vrijwillige samenwerking op grond van de Wet terrorismebestrijding moeten beperkt zijn tot informatie over terreurverdachten (zie punt 3.2.2.1 hierboven). Een dergelijk verzoek van de NIS moet in overeenstemming zijn met de beginselen van wettigheid, noodzakelijkheid en evenredigheid die voortvloeien uit de Koreaanse grondwet (artikel 12, lid 1, en artikel 37, lid 2) ([240]) en met de vereisten van de PIPA voor de verzameling van persoonsinformatie (artikel 3, lid 1, PIPA, zie punt 1.2 hierboven). In de NIS-wet is bovendien bepaald dat de NIS een instelling, organisatie of persoon niet mag dwingen iets te doen waartoe zij niet verplicht zijn, noch de uitoefening van de rechten van een persoon mag belemmeren door misbruik te maken van haar officiële bevoegdheid ([241]). Voor een schending van dit verbod kunnen strafrechtelijke sancties worden opgelegd ([242]).

Verantwoordelijken voor de verwerking van persoonsinformatie en aanbieders van locatiegegevens die verzoeken van de NIS ontvangen op basis van de Wet terrorismebestrijding zijn niet verplicht daarop in te gaan. Zij kunnen dat vrijwillig doen, maar dan uitsluitend overeenkomstig de PIPA en de Wet locatiegegevens.. Wat de naleving van de PIPA betreft, moet de verwerkingsverantwoordelijke met name rekening houden met de belangen van de betrokkene en mag hij geen informatie verstrekken wanneer dit waarschijnlijk op oneerlijke wijze inbreuk zou maken op de belangen van de betrokkene of van derden ([243]). Daarnaast moet de betrokkene overeenkomstig Kennisgeving nr. 2021-1 over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie op de hoogte worden gesteld van het verstrekken van de informatie. Een dergelijke kennisgeving mag in uitzonderlijke gevallen worden vertraagd, met name indien en zolang de kennisgeving een lopend strafrechtelijk onderzoek in gevaar zou brengen, of het leven of de lichamelijke integriteit van een andere persoon zou kunnen schaden, wanneer deze rechten of belangen duidelijk zwaarder wegen dan de rechten van de betrokkene ([244]).

3.2.2.3. Beperkingen en waarborgen op grond van de CPPA

Op basis van de Wet terrorismebestrijding mogen inlichtingendiensten slechts communicatiegegevens (zowel de inhoud van de communicatie als de communicatiebevestigende gegevens) verzamelen wanneer dit noodzakelijk is in verband met activiteiten voor terrorismebestrijding, dat wil zeggen activiteiten die verband houden met het voorkomen van en het nemen van maatregelen tegen terrorisme. De procedures van de CPPA die in punt 3.2.1 zijn beschreven, zijn van toepassing op de verzameling van communicatiegegevens met het oog op de terrorismebestrijding.

3.2.3. *Vrijwillige verstrekking door telecommunicatie-exploitanten*

Telecommunicatie-exploitanten mogen op grond van de TBA voldoen aan een verzoek om het verstrekken van "communicatiegegevens" van een inlichtingendienst die de informatie wil verzamelen om een bedreiging van de nationale veiligheid te voorkomen ([245]). Een dergelijk verzoek moet in overeenstemming zijn met de beginselen van wettigheid, noodzakelijkheid en evenredigheid die voortvloeien uit de Koreaanse grondwet (artikel 12, lid 1, en artikel 37, lid 2) ([246]) en met de vereisten van de PIPA voor de verzameling van persoonsinformatie (artikel 3, lid 1, PIPA, zie punt 1.2 hierboven). Bovendien gelden dezelfde beperkingen en waarborgen als in verband met vrijwillige verstrekkingen met het oog op de rechtshandhaving (zie punt 2.2.3) ([247]).

([238]) Zoals bepaald in artikel 2 PIPA, namelijk een overheidsinstantie, rechtspersoon, organisatie, individu enz. die/dat persoonsinformatie direct of indirect verwerkt om bestanden met persoonsinformatie te gebruiken voor officiële of zakelijke doeleinden.
([239]) Zoals bepaald in artikel 5 van de Wet inzake de bescherming, het gebruik enz. van locatiegegevens (hierna "Wet locatiegegevens" genoemd), d.w.z. iedereen die van de Koreaanse Communicatiecommissie toestemming heeft verkregen om zakelijke activiteiten in verband met locatiegegevens te verrichten.
([240]) Zie ook artikel 3, leden 2 en 3, van de Wet terrorismebestrijding.
([241]) Artikel 11, lid 1, van de NIS-wet.
([242]) Artikel 19 van de NIS-wet.
([243]) Artikel 18, lid 2, PIPA.
([244]) Kennisgeving nr. 2021-1 van de PIPC over aanvullende voorschriften voor de uitlegging en toepassing van de Wet bescherming persoonsinformatie, deel III, 2, punt iii).
([245]) Artikel 83, lid 3, TBA.
([246]) Zie ook artikel 3, leden 2 en 3, van de Wet terrorismebestrijding.
([247]) Meer bepaald moet het verzoek schriftelijk zijn en de redenen voor het verzoek vermelden, evenals het verband met de desbetreffende gebruiker en de omvang van de informatie waarom wordt verzocht en moet de aanbieder van telecommunicatie een register bijhouden en tweemaal per jaar verslag uitbrengen aan de minister van Wetenschap en ICT.

Telecommunicatie-exploitanten zijn niet verplicht op een verzoek in te gaan; zij mogen dit vrijwillig doen, maar wel uitsluitend overeenkomstig de PIPA. In dit verband gelden dezelfde verplichtingen, ook met betrekking tot de kennisgeving aan de betrokkene, voor exploitanten van telecommunicatiebedrijven als wanneer zij verzoeken van strafrechtelijke handhavingsinstanties ontvangen, zoals nader toegelicht in punt 2.2.3.

3.3. **Toezicht**

Verschillende organen houden toezicht op de activiteiten van de Koreaanse inlichtingendiensten. Het toezicht op het Commando ondersteuning defensie en veiligheid wordt uitgeoefend door het ministerie van Nationale Defensie, overeenkomstig de richtlijn van het ministerie inzake de uitvoering van interne controles. Het toezicht op de NIS wordt uitgeoefend door de uitvoerende macht, de Nationale Vergadering en andere onafhankelijke organen, zoals hieronder nader toegelicht.

3.3.1. *De mensenrechtenfunctionaris*

Voor gevallen waarin inlichtingendiensten informatie over terreurverdachten verzamelen, voorziet de Wet terrorismebestrijding in toezicht door de Commissie terrorismebestrijding en de mensenrechtenfunctionaris ([248]).

De Commissie terrorismebestrijding ontwikkelt onder meer beleid in verband met activiteiten voor terrorismebestrijding en houdt toezicht op de uitvoering van maatregelen voor terrorismebestrijding, alsook op de activiteiten van de verschillende bevoegde autoriteiten op het gebied van terrorismebestrijding ([249]). De commissie wordt voorgezeten door de premier en bestaat uit verschillende ministers en hoofden van overheidsinstanties, waaronder de minister van Buitenlandse Zaken, de minister van Justitie, de minister van Nationale Defensie, de minister van Binnenlandse Zaken en Veiligheid, de directeur van de NIS, de commissaris-generaal van de Nationale Politie en de voorzitter van de Commissie financiële diensten ([250]). Bij het verrichten van onderzoek ter bestrijding van terrorisme en het opsporen van terreurverdachten om informatie of materiaal te verzamelen dat nodig is voor de terrorismebestrijding moet de directeur van de NIS verslag uitbrengen aan de voorzitter van de Commissie terrorismebestrijding (d.w.z. de premier) ([251]).

Bij de Wet terrorismebestrijding is bovendien de mensenrechtenfunctionaris ingesteld om de basisrechten van personen te beschermen tegen inbreuken als gevolg van activiteiten voor terrorismebestrijding ([252]). De mensenrechtenfunctionaris wordt door de voorzitter van de Commissie terrorismebestrijding benoemd uit personen die voldoen aan de in het Uitvoeringsdecreet van de Wet terrorismebestrijding opgenomen kwalificaties (d.w.z. een persoon die gekwalificeerd advocaat met ten minste tien jaar werkervaring is, of die beschikt over deskundigheid op het gebied van mensenrechten en tien jaar als (ten minste) universitair hoofddocent werkzaam is of is geweest, of die als hooggeplaatst ambtenaar werkzaam is geweest bij de staatsoverheid of bij plaatselijke overheden, of die ten minste tien jaar werkervaring heeft op het gebied van mensenrechten, bijvoorbeeld bij een niet-gouvernementele organisatie) ([253]). De mensenrechtenfunctionaris wordt benoemd voor een periode van twee jaar (die kan worden verlengd) en mag alleen uit zijn/haar functie worden ontheven om specifieke, beperkte en gegronde redenen, bijvoorbeeld wanneer hij/zij in staat van beschuldiging wordt gesteld in een strafzaak die verband houdt met zijn/haar functie, wanneer hij/zij vertrouwelijke informatie openbaar maakt of wegens langdurige geestelijke of lichamelijke ongeschiktheid ([254]).

Wat de bevoegdheden betreft, kan de mensenrechtenfunctionaris aanbevelingen doen voor een betere bescherming van de mensenrechten door instanties die betrokken zijn bij activiteiten voor terrorismebestrijding en kan hij/zij verzoeken van burgers behandelen (zie punt 3.4.3) ([255]). Wanneer redelijkerwijs kan worden vastgesteld dat sprake is van een inbreuk op de mensenrechten bij de uitvoering van officiële taken, kan de mensenrechtenfunctionaris het hoofd van de verantwoordelijke instantie aanbevelen die inbreuk te corrigeren ([256]). De verantwoordelijke instantie moet de mensenrechtenfunctionaris vervolgens op de hoogte stellen van de genomen maatregelen om die aanbeveling uit te voeren ([257]). Indien een instantie een aanbeveling van de mensenrechtenfunctionaris niet uitvoert, wordt de zaak doorgestuurd naar de Mensenrechtencommissie, met inbegrip van haar voorzitter, de premier. Tot dusver hebben er zich nog geen gevallen voorgedaan waarin aanbevelingen van de mensenrechtenfunctionaris niet zijn uitgevoerd.

3.3.2. *De Nationale Vergadering*

Zoals beschreven in punt 2.3.2 kan de Nationale Vergadering overheidsinstanties onderzoeken en inspecteren en in dat verband verzoeken om de openbaarmaking van documenten en getuigen verplichten te verschijnen. Met betrekking tot zaken die vallen onder de jurisdictie van de NIS wordt dit parlementaire toezicht uitgeoefend door de Inlichtingencommissie van de Nationale Vergadering ([258]). De directeur van de NIS, die toezicht houdt op de uitvoering van de taken

([248]) Artikel 7 van de Wet terrorismebestrijding.
([249]) Artikel 5, lid 3, van de Wet terrorismebestrijding.
([250]) Artikel 3, lid 1, van het Uitvoeringsdecreet van de Wet terrorismebestrijding.
([251]) Artikel 9, lid 4, van de Wet terrorismebestrijding.
([252]) Artikel 7 van de Wet terrorismebestrijding.
([253]) Artikel 7, lid 1, van het Uitvoeringsdecreet van de Wet terrorismebestrijding.
([254]) Artikel 7, lid 3, van het Uitvoeringsdecreet van de Wet terrorismebestrijding.
([255]) Artikel 8, lid 1, van het uitvoeringsdecreet van de Wet terrorismebestrijding.
([256]) Artikel 9, lid 1, van het Uitvoeringsdecreet van de Wet terrorismebestrijding. De mensenrechtenfunctionaris beslist autonoom over het al dan niet vaststellen van aanbevelingen, maar is verplicht deze aanbevelingen te melden aan de voorzitter van de Commissie terrorismebestrijding.
([257]) Artikel 9, lid 2, van het Uitvoeringsdecreet van de Wet terrorismebestrijding.
([258]) Artikel 36 en artikel 37, lid 1, punt 16, van de Wet inzake de Nationale Vergadering.

door die dienst, brengt verslag uit aan de Inlichtingencommissie (en aan de president) ([259]). De Inlichtingencommissie zelf mag ook verzoeken om een verslag over een specifieke zaak. De directeur van de NIS moet hierop onverwijld antwoorden ([260]). Hij/zij mag slechts weigeren te antwoorden of voor de Inlichtingencommissie te getuigen met betrekking tot staatsgeheimen betreffende militaire of diplomatieke kwesties of kwesties in verband met Noord-Korea, waarvan publieke kennis ernstige gevolgen kan hebben voor de nationale lotsbestemming ([261]). In dit geval kan de Inlichtingencommissie de premier om uitleg vragen. Wanneer die uitleg niet binnen zeven dagen na het verzoek wordt gegeven, mag het antwoord of de getuigenverklaring niet langer worden geweigerd.

Wanneer de Nationale Vergadering vaststelt dat onwettige of ongepaste activiteiten hebben plaatsgevonden, kan zij de betrokken overheidsinstantie verzoeken corrigerende maatregelen te nemen, met inbegrip van de toekenning van een schadevergoeding, het nemen van tuchtmaatregelen en het verbeteren van de interne procedures ([262]). Naar aanleiding van een dergelijk verzoek moet de instantie onverwijld handelen en aan de Nationale Vergadering verslag uitbrengen over de resultaten. Er bestaan specifieke regels voor het parlementair toezicht met betrekking tot het gebruik van communicatiebeperkende maatregelen (d.w.z. de verzameling van de inhoud van communicatie) op grond van de CPPA ([263]). Wat het laatste betreft kan de Nationale Vergadering de hoofden van inlichtingendiensten vragen om een verslag over specifieke communicatiebeperkende maatregelen. Daarnaast kan zij inspecties ter plaatse van afluisterapparatuur verrichten. Tot slot moeten inlichtingendiensten die informatie over inhoud hebben verzameld en exploitanten die deze hebben verstrekt met het oog op de nationale veiligheid op verzoek van de Nationale Vergadering over die verstrekking verslag uitbrengen.

3.3.3. *De Controle- en Inspectieraad*

De BAI verricht dezelfde toezichtstaken met betrekking tot inlichtingendiensten als op het gebied van de strafrechtelijke rechtshandhaving (zie punt 2.3.2) ([264]).

3.3.4. *De Commissie bescherming persoonsinformatie*

Wat betreft de gegevensverwerking met het oog op de nationale veiligheid, met inbegrip van de verzameling, wordt aanvullend toezicht gehouden door de PIPC. Zoals nader uitgelegd in punt 1.2 omvat dit de algemene beginselen en verplichtingen zoals uiteengezet in artikel 3 en artikel 58, lid 4, PIPA, evenals de uitoefening van de individuele rechten die worden gewaarborgd door artikel 4 PIPA. Het toezicht van de PIPC heeft op grond van artikel 7-8, leden 3 en 4, en artikel 7-9, lid 5, PIPA ook betrekking op mogelijke inbreuken op de in specifieke wetten opgenomen regels tot vaststelling van de beperkingen en waarborgen in verband met de verzameling van persoonsinformatie, zoals de CPPA, de Wet terrorismebestrijding en de TBA. Gezien de vereisten van artikel 3, lid 1, PIPA in verband met de rechtmatige en behoorlijke verzameling van persoonsinformatie vormt een schending van deze wetten een schending van de PIPA. De PIPC is dus bevoegd om schendingen te onderzoeken ([265]) van de wetten waarin de toegang tot gegevens met het oog op de nationale veiligheid wordt geregeld, alsook van de verwerkingsvoorschriften in de PIPA en om advies te verlenen voor de verbetering, corrigerende maatregelen op te leggen, tuchtmaatregelen aan te bevelen en mogelijke inbreuken door te sturen naar de desbetreffende onderzoeksautoriteiten ([266]).

3.3.5. *Nationale Mensenrechtencommissie*

Het toezicht van de NHRC is op dezelfde wijze van toepassing op inlichtingendiensten als op andere overheidsinstanties (zie punt 2.3.2).

3.4. **Individueel verhaal**

3.4.1. *Verhaal voor de mensenrechtenfunctionaris*

Met betrekking tot de verzameling van persoonsinformatie in het kader van terrorismebestrijding is voorzien in een specifieke verhaalsmogelijkheid door de mensenrechtenfunctionaris, die onder de auspiciën van de Commissie terrorismebestrijding is ingesteld. De mensenrechtenfunctionaris behandelt verzoeken van burgers in verband met inbreuken op de mensenrechten als gevolg van activiteiten in het kader van terrorismebestrijding ([267]). Hij/zij kan corrigerende maatregelen aanbevelen en de desbetreffende instantie moet verslag uitbrengen aan de functionaris over eventuele maatregelen die zijn genomen om die aanbevelingen uit te voeren. Er zijn geen vaste eisen voor personen om een klacht bij de mensenrechtenfunctionaris in te dienen. De mensenrechtenfunctionaris handelt daarom alle klachten af, zelfs wanneer de betrokkene tijdens het ontvankelijkheidsonderzoek niet kan aantonen dat hij/zij daadwerkelijk is benadeeld.

([259]) Artikel 18 van de NIS-wet.
([260]) Artikel 15, lid 2, van de NIS-wet.
([261]) Artikel 17, lid 2, van de NIS-wet. "Staatsgeheimen" zijn gedefinieerd als feiten, goederen of kennis aangemerkt als staatsgeheim waartoe slechts een beperkt aantal personen toegang heeft en die niet mogen worden bekendgemaakt aan andere landen of organisaties om ernstig nadeel voor de nationale veiligheid te voorkomen, zie artikel 13, lid 4, van de NIS-wet.
([262]) Artikel 16, lid 2 van de Wet inzake de inspectie en het onderzoek van de overheidsadministratie.
([263]) Artikel 15 CPPA.
([264]) Net zoals met betrekking tot de Inlichtingencommissie van de Nationale Vergadering, mag de directeur van de NIS slechts weigeren de BAI te antwoorden in verband met zaken die staatsgeheimen vormen en wanneer publieke kennis ernstige gevolgen voor de nationale veiligheid zou hebben (artikel 13, lid 1, van de NIS-wet).
([265]) Artikel 63 PIPA.
([266]) Artikel 61, lid 2, artikel 65, leden 1 en 2, en artikel 64, lid 4, PIPA.
([267]) Artikel 8, lid 1, punt 2, van het Uitvoeringsdecreet van de Wet terrorismebestrijding.

3.4.2. *Op grond van de PIPA beschikbare verhaalsmechanismen*

Natuurlijke personen kunnen hun rechten op toegang, correctie, verwijdering en opschorting uit hoofde van de PIPA uitoefenen in verband met persoonsinformatie die wordt verwerkt met het oog op de nationale veiligheid ([268]). Verzoeken om deze rechten uit te oefenen kunnen rechtstreeks bij de inlichtingendienst worden ingediend, of indirect via de PIPC. De inlichtingendienst kan de uitoefening van dit recht vertragen, beperken of ontzeggen voor zover en zolang dit noodzakelijk en evenredig is voor de bescherming van een belangrijke doelstelling van openbaar belang (bv. voor zover en zolang als de verlening van het recht een lopend onderzoek in gevaar zou brengen of de nationale veiligheid zou bedreigen), of wanneer de verlening van het recht schade kan toebrengen aan het leven of de lichamelijke integriteit van een derde. Wanneer het verzoek wordt afgewezen of beperkt, moet de betrokkene onverwijld in kennis worden gesteld van de redenen daarvoor.

Op grond van artikel 58, lid 4, PIPA (vereiste ter waarborging van de passende afhandeling van individuele klachten) en artikel 4, lid 5, PIPA (recht op een passende rechtsmiddel in verband met schade die voortvloeit uit de verwerking van persoonsinformatie via een snelle en eerlijke procedure) hebben betrokkenen personen bovendien het recht om verhaal te halen. Dit omvat het recht om een vermeende schending te melden bij het Privacy Call Centre, dat wordt beheerd door het Koreaans Agentschap voor internet en veiligheid, en om een klacht in te dienen bij de PIPC ([269]). Deze verhaalsmiddelen zijn zowel beschikbaar voor mogelijke inbreuken op de voorschriften die zijn opgenomen in specifieke wetten waarin de beperkingen en waarborgen in verband met de verzameling van persoonsinformatie met het oog op de nationale veiligheid zijn vastgesteld als voor mogelijke inbreuken op de PIPA. Zoals uitgelegd in Kennisgeving nr. 2021-1, kan een EU-burger bij de PIPC een klacht indienen via zijn/haar nationale gegevensbeschermingsautoriteit. In dat geval zal de PIPC de betrokkene via de nationale gegevensbeschermingsautoriteit op de hoogte brengen zodra het onderzoek is afgesloten (en, in voorkomend geval, informatie verstrekken over de opgelegde corrigerende maatregelen). Tegen beslissingen of het uitblijven van maatregelen van de PIPC kan verder beroep worden aangetekend voor de Koreaanse rechter op grond van de Wet administratieve procesvoering.

3.4.3. *Verhaal voor de Nationale Mensenrechtencommissie*

De mogelijkheid om individueel verhaal te halen voor de NHRC is op dezelfde wijze van toepassing op inlichtingendiensten als op andere overheidsinstanties (zie punt 2.4.2).

3.4.4. *Gerechtelijk beroep*

Zoals het geval is met betrekking tot de activiteiten van strafrechtelijke handhavingsinstanties kunnen natuurlijke personen op verschillende manieren gerechtelijk beroep instellen tegen inlichtingendiensten met betrekking tot schendingen van de bovengenoemde beperkingen en waarborgen.

Ten eerste kunnen betrokkenen een schadevergoeding verkrijgen op grond van de Wet inzake overheidscompensatie. In één zaak werd bijvoorbeeld een schadevergoeding toegekend met betrekking tot onrechtmatige surveillance door het Commando ondersteuning defensie (de voorganger van het Commando ondersteuning defensie en veiligheid) ([270]).

Ten tweede biedt de Wet administratieve procesvoering personen de mogelijkheid beslissingen en nalatigheden van bestuursinstanties, met inbegrip van inlichtingendiensten, aan te vechten ([271]).

Tot slot kunnen personen op basis van de Wet op het Grondwettelijk Hof een grondwettelijke klacht indienen bij het Grondwettelijk Hof tegen maatregelen van inlichtingendiensten.

([268]) Artikel 3, lid 5, en artikel 4, leden 1, 3 en 4, PIPA.
([269]) Artikel 62 en artikel 63, lid 2, PIPA.
([270]) Beslissing nr. 96Da42789 van het Hooggerechtshof van 24 juli 1998.
([271]) Artikelen 3 en 4 van de Wet administratieve procesvoering.