AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

De Staatssecretaris Koninkrijksrelaties en Digitalisering
Postbus 20011
2500 EA Den Haag

Datum	Ons kenmerk	Uw brief van
5 december 2022	z2022-5161	29 maart 2022
	Contactpersoon	Uw kenmerk
	[illegible]	2022-0000160333

Onderwerp

Advies over het concept voor Wijziging van de Paspoortwet in verband met de invoering van een centrale voorziening voor de verwerking van de gezichtsopname, handtekening en vingerafdrukken

Geachte mevrouw Van Huffelen,

Bij brief van 29 maart 2022 is de Autoriteit Persoonsgegevens (AP) op grond van het bepaalde in artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (AVG), geraadpleegd over het concept voor Wijziging van de Paspoortwet in verband met de invoering van een centrale voorziening voor de verwerking van de gezichtsopname, handtekening en vingerafdrukken ten behoeve van reisdocumenten, het schrappen van de geslachtsvermelding op de identiteitskaart, alsmede enige andere wijzigingen (hierna: het concept).

Naar het oordeel van de AP gaat het om een ingrijpend concept-wetsvoorstel waarvan de noodzaak en evenredigheid in dat licht onvoldoende zijn gemotiveerd. Daarnaast wordt in het concept de verwerkingsverantwoordelijkheid op onduidelijke wijze geregeld, waardoor er hiaten kunnen ontstaan in de bescherming van persoonsgegevens.
De AP heeft op deze punten bezwaar tegen het concept en adviseert de procedure niet voort te zetten, tenzij het bezwaar is weggenomen.

Hoofdlijn

- Subsidiariteit en proportionaliteit van het voorstel zijn, mede gelet op de gevoeligheid van de betrokken persoonsgegevens, niet voldoende met dragende argumenten onderbouwd. Daarbij wordt – voor zover valt af te leiden uit de tekst van het concept – onvoldoende rekening gehouden met het risico op *'function creep'* en het risico dat de biometrische gegevens in verkeerde handen kunnen vallen.

- De verdeling van verwerkingsverantwoordelijkheid aan de hand van activiteiten van bevoegde autoriteiten en de minister, die niet goed aansluit bij de verwerkingen van persoonsgegevens die daadwerkelijk plaatshebben, laat onduidelijkheid bestaan over de gevallen waarin bevoegde autoriteiten of de minister voor een concrete verwerking van persoonsgegevens verwerkingsverantwoordelijke is.
- Gelet op centralisering van de gegevensopslag en -verstrekking die wordt beoogd met het concept en de beperkte rol die bevoegde autoriteiten zullen spelen bij de verwerking van persoonsgegevens, wordt geadviseerd de minister als verwerkingsverantwoordelijke aan te merken.
- In het concept dient te worden uitgewerkt welke waarborgen er zijn of worden getroffen om ervoor te zorgen dat de doorgifte van persoonsgegevens naar Caribisch Nederland in overeenstemming is met de AVG.

Strekking

Het concept is onderdeel van het programma 'Verbeteren Reisdocumentenstelsel'. In het kader van dat programma is reeds het basisregister reisdocumenten tot stand gebracht. Daarin worden centraal opgeslagen de biografische aanvraaggegevens van alle verstrekte reisdocumenten en gegevens in verband met het gebruik van de Nederlandse identiteitskaart als publiek identificatiemiddel. Het concept strekt tot aanvulling van het centrale basisregister met gegevens over de voortgang van een aanvraag voor een reisdocument en gegevens over vermiste, gestolen of van rechtswege vervallen documenten.

Met het concept wordt tevens beoogd een tweede centrale voorziening in te richten waarin de overige aanvraaggegevens ten behoeve van reisdocumenten worden opgeslagen. Het gaat dan om de gezichtsopname, handtekening en twee vingerafdrukken van de betrokkene. Deze gegevens worden vooralsnog decentraal opgeslagen in een systeem bij tot uitreiking bevoegde autoriteiten, zoals gemeenten. Volgens het concept zullen de autoriteiten deze gegevens in de centrale voorziening moeten vastleggen. Tot uitgifte bevoegde autoriteiten zullen toegang hebben tot deze centraal opgeslagen persoonsgegevens op aanvraagnummer en documentnummer. Zij kunnen tevens via de centrale voorziening gezichtsopnamen doen verstrekken om een overgelegde gezichtsopname te vergelijken met die van een eerdere aanvraag van een reisdocument. Uitgevende instanties beslissen daarnaast over verstrekking van de door hen in de centrale voorziening opgenomen gezichtsopnamen en handtekeningen aan in de wet genoemde derden onder de in wet gestelde voorwaarden.

Ook zal het concept de Paspoortwet aanpassen zodat de Nederlandse identiteitskaart het geslacht van de betrokkene niet meer vermeldt.

AUTORITEIT
PERSOONSGEGEVENS

Datum
5 december 2022

Ons kenmerk
z2022-5161

Advies

1. Subsidiariteit en proportionaliteit

Op de voet van het Handvest van de grondrechten van de Europese Unie en de AVG moet vastgesteld worden dat :

1) het concept geschikt is om de nagestreefde doelstelling van algemeen belang te verwezenlijken (geschiktheid);
2) de inmenging in het recht op bescherming van persoonsgegevens beperkt blijft tot het strikt noodzakelijke, in die zin dat het doel niet redelijkerwijs even doeltreffend kan worden bereikt op een andere wijze, die de grondrechten van de betrokkenen minder aantast (subsidiariteit);
3) de inmenging niet onevenredig is aan dat doel, wat met name een afweging impliceert van het belang van het doel en de ernst van de inmenging (proportionaliteit);
4) het concept duidelijke en nauwkeurige regels over de reikwijdte en de toepassing bevat die waarborgen dat verwerking tot het noodzakelijke beperkt blijft en dat betrokkenen over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik (duidelijkheid en waarborgen).

De AP is van oordeel dat de onderbouwing van de subsidiariteit (punt 2) en de proportionaliteit (punt 3) tekortschieten.

In de toelichting op het concept wordt aangestipt **wat het doel** is van de invoering van een centrale voorziening en wordt aangegeven dat niet meer persoonsgegevens worden verwerkt dan nodig om dat doel te bereiken.[1] Daarnaast wordt aangestipt dat de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd.[2] Uit de toelichting volgt echter niet op overtuigende wijze hoe de centrale voorziening bijdraagt aan de bestrijding van fraude. Daarnaast worden het grondrecht op bescherming van persoonsgegevens en het doeleinde van de maatregel niet uitdrukkelijk afgewogen. Volgens de AP zou daarbij in het bijzonder ook aandacht moeten zijn voor het gevoelige karakter van een permanente centrale database met de biometrische gegevens van vrijwel de gehele bevolking; de huidige wetgever kan immers niet voorkomen dat de wetgever – eventueel in de verre toekomst, eventueel onder een ander politiek gesternte – nieuwe doelstellingen voor een dergelijke feitelijk dan bestaande database vaststelt, zodat '*function creep*' als risico meegewogen dient te worden. Los daarvan mist de AP aandacht voor het risico dat centraal opgeslagen gegevens onverhoopt in verkeerde handen vallen.

Vereist is tevens dat er geen minder ingrijpende maatregelen zijn waarmee het doel van het bewerkstelligen van een consistent, betrouwbaar en frauderesistent reisdocumentenstelsel kan worden bewerkstelligd (subsidiariteit). Als alternatief voor een centrale voorziening wordt in de toelichting genoemd de voortzetting van de huidige verwerking op decentraal niveau, waarbij de uitwisseling van gegevens tussen de decentrale systemen wordt verbeterd. Dat alternatief wordt in de toelichting buiten de

[1] Toelichting op het concept, p. 18.
[2] Toelichting op het concept, p. 18.

kaders van het gegevensbeschermingsrecht besproken.[3] De nadelen van het alternatief worden aangestipt, maar niet toegelicht en ook niet uitdrukkelijk in verband gebracht met de gevolgen voor de bescherming van persoonsgegevens. Een nadeel dat wordt genoemd, en dat relevant kan zijn met het oog op de bescherming van persoonsgegevens, is dat er met een verbeterde decentrale voorziening meer gegevensstromen tussen instanties wordt gegenereerd dan met een centrale voorziening. Daartegenover staat dat het aantal gegevensstromen als zodanig niet afneemt omdat de instanties steeds gegevens zullen uitwisselen met de centrale voorziening. Dat aspect wordt echter niet betrokken in de toelichting.

Elders in de toelichting, in het kader van de proportionaliteit en de subsidiariteit, worden hoofdzakelijk de voordelen van de centrale voorziening ten opzichte van het huidige decentrale systemen genoemd.[4] De nadelen die kleven aan een centrale voorziening worden echter niet uitdrukkelijk betrokken in de toelichting. Het ontbreekt daar aan een systematische analyse van de geïdentificeerde risico's en een beschrijving van hoe die specifieke risico's zullen worden geadresseerd, met daarbij ook aandacht voor het bijzondere karakter van de centraal opgeslagen persoonsgegevens. Zonder een dergelijke analyse is niet te bepalen of de te treffen maatregelen afdoende zullen zijn. Een verwijzing naar de DPIA – die niet openbaar is – is in dat verband niet voldoende.

In de risicoanalyse zou in ieder aandacht besteed moeten worden aan de risico's die samenhangen met de centrale opslag van gevoelige gegevens, zoals de grotere impact die een datalek kan hebben doordat het datalek de persoonsgegevens van een grotere groep mensen betreft, bijvoorbeeld als ongeautoriseerde toegang plaatsheeft. Ook de eventuele toekomstige inzet van technische middelen voor de beoordeling en vergelijking van gezichtsopnamen, die ingrijpend is en waarover de toelichting rept in het kader van de voordelen van een centrale voorziening, legt gewicht in de schaal.[5] Rekenschap dient ook te worden gegeven van het feit dat met de centrale voorziening in wezen een landelijke databank met identificerende gegevens wordt aangelegd die in de toekomst ook gebruikt kan worden voor andere doeleinden dan waarvoor de voorziening nu in het leven zou worden geroepen. Uiteraard dienen nieuwe toepassingen van de centrale voorziening hun grondslag te vinden in wettelijke bepalingen die voldoen aan de eisen die de AVG en andere (hogere) regelgeving daaraan stellen. Desalniettemin brengt feitelijke beschikbaarheid van de centrale voorziening nieuwe toepassingen dichterbij in zowel praktische zin (de gegevens en technologische voorzieningen zijn reeds beschikbaar) als bestuurlijke zin (de politieke 'hobbel' van een centrale biometrische databank is reeds genomen). Wetgeving is uiteraard een belangrijke waarborg, maar weerspiegelt ook de machtsverhoudingen en inzichten op een bepaald moment; er is geen zekerheid dat de huidige opvattingen over het doel van de voorziening en zelfs het belang van bescherming van persoonsgegevens in de wat verdere toekomst niet substantieel anders zouden kunnen zijn. Het enkele bestaan van een database als deze kan dan een groot risico blijken te zijn.

Tot slot wordt in het concept en de toelichting daarop geen onderscheid gemaakt tussen de opslag van gezichtsopnamen en vingerafdrukken. Ingevolge het concept zal gelden dat vingerafdrukken worden

[3] Toelichting op het concept, p. 12.
[4] Toelichting op het concept, p. 18-19.
[5] Toelichting op het concept, p. 11. Uiteraard geldt dat als deze ondersteuningsmiddelen worden ingezet, voor de daarmee samenhangende verwerkingen ook een verwerkingsgrondslag gevonden zal moeten worden.

opgeslagen tot – kortgezegd – het reisdocument is uitgereikt.[6] Deze persoonsgegevens mogen volgens het concept alleen maar worden verwerkt ten behoeve van de verstrekking en de uitreiking van het reisdocument. Van verstrekking aan andere uitgevende instanties of derden zal daarom geen sprake zijn. Het opslaan en raadpleegbaar maken van vingerafdrukken in een centrale voorziening zal ten aanzien van dat aspect dan waarschijnlijk ook niets toevoegen. De te maken afweging in het kader van de proportionaliteit en subsidiariteit met betrekking tot de verwerking van vingerafdrukken dient daarom afzonderlijk plaats te hebben.

De AP adviseert om in de toelichting met dragende argumenten te motiveren hoe met de invoering van een centrale voorziening wordt voldaan aan het subsidiariteitsvereiste en het proportionaliteitsvereiste. Daarbij dient in ieder geval ingegaan te worden op de risico's in verband met het gevoelige karakter van een omvattende centrale opslag van biometrische gegevens de mogelijke (grote) gevolgen van ongeautoriseerde toegang, en voorzienbare nieuwe toepassingen van de voorziening in de nabije en verdere toekomst.

2. Verwerkingsverantwoordelijkheid

Het concept van verwerkingsverantwoordelijkheid is van cruciaal belang omdat daarmee wordt bepaald wie verantwoordelijk is voor de naleving van de regels in de AVG en jegens wie betrokkenen hun rechten in de praktijk kunnen uitoefenen.[7] Juist waar veel partijen in onderlinge samenhang persoonsgegevens verwerken is van groot belang dat eenduidig vaststaat wie voor welke verwerking verantwoordelijk is.

Verwerkingsverantwoordelijkheid kan, in gevallen zoals in voorliggend advies, uit wetgeving worden afgeleid maar ook expliciet in wetgeving worden toebedeeld. Daarbij laat de AVG de wetgever de nodige ruimte om verwerkingsverantwoordelijken verplichtingen op te leggen met betrekking tot de verwerking.[8] Ook is het mogelijk dat verschillende partijen als verwerkingsverantwoordelijke moeten worden aangemerkt voor verschillende verwerkingen in een keten van verwerkingen De verantwoordelijkheid voor één bepaalde concrete verwerking kan echter niet tussen partijen worden verdeeld, althans niet buiten de constructie van gezamenlijke verwerkingsverantwoordelijkheid (zie hierna). Verwerkingsverantwoordelijkheid is dus niet '*á la carte*' deelbaar; verantwoordelijkheid voor een bepaalde verwerking komt met alle verplichtingen die de AVG daaraan verbindt. Het is, met andere woorden, niet mogelijk om voor een bepaalde verwerking de een verantwoordelijk te houden voor nakoming van de rechten van betrokkenen en de ander voor de juistheid of de beveiliging van de gegevens of het uitvoeren van een gegevensbeschermingseffectbeoordeling.[9] Zo wordt voorkomen dat onduidelijkheid ontstaat in de verantwoordelijkheidsverdeling waardoor organisaties zich achter elkaar zouden kunnen verschuilen en betrokkenen de door de AVG aan hen verstrekte rechten niet of moeilijker daadwerkelijk zouden kunnen uitoefenen.

---

[6] Artikel 4f, vijfde lid, van het concept.
[7] Artikel 5, tweede lid, van de AVG. Zie tevens artikel 24, eerste lid, van de AVG. Zie tevens: Europees Comité voor gegevensbescherming, Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, p. 8.
[8] Artikel 6, tweede en derde lid, van de AVG ('specifieke voorschriften voor de verwerking' resp. en 'specifieke bepalingen (...) verwerkingsactiviteiten en –procedures).
[9] Zie artikelen 32, 35 en 5, eerste lid, onder d, van de AVG.

Met inachtneming van artikel 26 AVG kunnen meerdere verwerkingsverantwoordelijken komen tot een vorm van gezamenlijke verwerkingsverantwoordelijkheid voor één bepaalde verwerking. Gezamenlijk verwerkingsverantwoordelijken kunnen de taken en de rollen die voortvloeien uit de gezamenlijke verantwoordelijkheid voor die verwerking onderling verdelen. Niet uitgesloten lijkt dat de wetgever in bijzondere gevallen tot een vorm van gezamenlijke verantwoordelijkheid komt, maar het ligt voor de hand dat dan ook sprake moet zijn van gezamenlijk bepaalde doelen en middelen en een vorm van gestructureerde gezamenlijke besluitvorming daarover.[10] De AVG verzekert daarbij de positie van de betrokkene wiens gegevens gezamenlijk worden verwerkt door te bepalen dat deze zich aan de onderlinge verdeling van verantwoordelijkheden niets gelegen hoeft te laten liggen en zijn rechten tegen elke deelnemer aan de gezamenlijke verwerking kan uitoefenen.[11]

In het concept wordt bepaald dat tot uitreiking bevoegde autoriteiten verantwoordelijk zijn voor de verwerking van de gegevens in de centrale voorziening ten behoeve van de aanvraag, verstrekking en uitreiking van reisdocumenten.[12] De Minister van Binnenlandse Zaken zal ingevolge het concept verantwoordelijk zijn voor enerzijds de verwerkingen die plaatshebben voor de vervaardiging van reisdocumenten en anderzijds verantwoordelijk zijn voor het beheer en de beveiliging van de centrale voorziening.[13] In de toelichting wordt opgemerkt dat het daarbij niet gaat om 'een en dezelfde (gezamenlijk uitgevoerde) verwerking, waarvoor twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen bepalen.'[14] Volgens de toelichting zijn de minister en de tot uitreiking bevoegde autoriteiten in geen geval als gezamenlijk verwerkingsverantwoordelijken aan te merken. De verwerkingen van persoonsgegevens worden in toelichting als volgt onderscheiden: 'de verwerking ten behoeve van de aanvraag, verstrekking en uitreiking van reisdocumenten, alsmede voor de verstrekking aan derden onder verantwoordelijkheid van tot uitreiking bevoegde autoriteiten enerzijds en de verwerking ten behoeve van de vervaardiging van het reisdocument door de leverancier onder verantwoordelijkheid van de Minister anderzijds.'

De AP kan volgen dat gezamenlijke verwerkingsverantwoordelijkheid hier niet aan de orde is. Het eenvoudige onderscheid in de toelichting naar activiteiten van enerzijds bevoegde autoriteiten en anderzijds de minister doet volgens de AP echter geen recht aan de diverse verwerkingen van persoonsgegevens van bevoegde autoriteiten en de minister die plaatshebben in het kader van de centrale voorziening. Voor elk van de voornoemde activiteiten zullen verschillende verwerkingen van persoonsgegevens plaatshebben, zoals het verzamelen, vastleggen, ordenen, opslaan, wijzigen, raadplegen, verstrekken, en wissen van gezichtsopnamen, handtekeningen en – in voorkomend geval – vingerafdrukken. Voor sommige van deze verwerkingen van persoonsgegevens, bijvoorbeeld de wijziging of het wissen van persoonsgegevens, is niet duidelijk of het daarbij gaat om verwerkingen die worden verricht in het kader van het beheer van de centrale voorziening. Ook kunnen er vragen ontstaan over de

[10] Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker", p. 13.
[11] Artikel 26, derde lid, van de AVG.
[12] Toelichting op het concept, p. 21.
[13] Artikel 4f, zesde lid, van het concept.
[14] Toelichting op het concept, p. 32.

verantwoordelijkheid voor de beveiliging van verwerkingen die in feite door bevoegde autoriteiten worden verricht, zoals de verstrekkingen van persoonsgegevens om die persoonsgegevens te doen opslaan in de centrale voorziening. Het concept stelt daarom een verantwoordelijkheidsverdeling voor die niet goed aansluit bij de verschillende verwerkingen van persoonsgegevens in het kader van de centrale voorziening en die daarom vragen kan oproepen over wie verantwoordelijk is voor bijvoorbeeld de beveiliging van persoonsgegevens met betrekking tot een bepaalde verwerking.

Deze onduidelijke verantwoordelijkheidsverdeling in het concept lijkt terug te voeren op enerzijds de wens om één centrale voorziening te treffen ten behoeve van de opslag, raadpleging en verstrekking van de persoonsgegevens, en anderzijds de wens om vast te willen houden aan de rol en verantwoordelijkheden die bevoegde autoriteiten hebben in het huidige decentrale voorziening met gekoppelde systemen en onderlinge uitwisseling van persoonsgegevens. Op grond van het concept zal echter niet alleen de opslag van persoonsgegevens plaatshebben 'bij' de minister, maar ook de voorziening waarmee bevoegde autoriteiten persoonsgegevens op afstand kunnen raadplegen zal in beheer zijn van de minister. En hoewel bevoegde autoriteiten in het concept beslissen over de verstrekking van persoonsgegevens aan andere bevoegde autoriteiten, zal er in de regel van een daadwerkelijke inhoudelijke afweging door hen mogelijk geen sprake zijn en is het de centrale voorziening van waaruit de persoonsgegevens aan de andere bevoegde autoriteit ter beschikking worden gesteld.

Gelet op het vorenstaande, en gegeven de beoogde centralisering van de verwerkingen van persoonsgegevens, adviseert de AP om de minister als verwerkingsverantwoordelijke aan te merken voor het geheel van verwerkingen van persoonsgegevens die plaatshebben in het kader van de centrale voorziening met uitzondering van de verstrekking door de decentrale overheid. Decentrale overheden verstrekken dan de persoonsgegevens aan de minister die ze opslaat en zo nodig 'terugverstrekt'. Zo wordt voorkomen dat de nakoming van de verplichtingen in de AVG en de doeltreffende en volledige bescherming van de persoonsgegevens in gevaar komt. Het voorgaande hoeft overigens niet te betekenen dat bevoegde autoriteiten geen rol kunnen spelen ten aanzien van het beheer van de persoonsgegevens die centraal worden opgeslagen. Zo ligt het voor de hand dat gemeenten een rol spelen met betrekking tot de juistheid van gegevens en het eventueel laten corrigeren daarvan. Het concept kan daarvoor de basis bieden door autoriteiten te verplichten eventuele correcties aan te (laten) brengen in de centraal opgeslagen persoonsgegevens. Ook de inhoudelijke beslissing over verstrekking kan aan derden aan bevoegde autoriteiten worden overgelaten door te bepalen dat de minister uitsluitend op verzoek, met instemming of gehoord die autoriteiten verstrekt.

De AP adviseert om de minister als verwerkingsverantwoordelijke aan te merken voor de verwerkingen van persoonsgegevens in en door middel van de centrale voorziening en de verantwoordelijkheden van bevoegde autoriteiten met betrekking tot de verwerking van persoonsgegevens in het concept nader uit te werken.

3. Doorgifte van persoonsgegevens naar Caribisch Nederland

In de toelichting bij het concept wordt verwezen naar artikel 46, eerste lid, van de AVG, dat bepaalt dat persoonsgegevens, bij het ontbreken van een adequaatheidsbesluit, naar een derde land mogen worden

doorgegeven mits de verwerkingsverantwoordelijke of een verwerker passende waarborgen bieden en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Dergelijke waarborgen kunnen worden geboden, zonder dat daarvoor toestemming nodig is van de Autoriteit Persoonsgegevens, door de in artikel 46, tweede lid, van de AVG, opgesomde instrumenten.

Met betrekking tot de doorgifte aan derde landen wordt in de toelichting slechts verwezen naar de Wet bescherming persoonsgegevens BES en relevante Landsverordeningen van Aruba, Curaçao en Sint Maarten. Opgemerkt wordt dat 'deze regelgeving die grotendeels is ontleend aan de inmiddels ingetrokken Wet bescherming persoonsgegevens en bevat [sic] dwingende voorschriften voor de beoogde ontvangers (zoals de bevoegde autoriteiten) van gegevens uit decentrale voorziening.'[15] Deze enkele verwijzing naar wetgeving die geldt in Caribisch Nederland is niet voldoende om aan te tonen dat er sprake is van waarborgen die ervoor zorgen dat de doorgifte van (bijzondere) persoonsgegevens door middel van de centrale voorziening in overeenstemming is met de AVG. Daarvoor is een toelichting vereist op de maatregelen die door de verschillende overheden zijn of worden getroffen om ervoor te zorgen dat de bescherming van persoonsgegevens op orde is.

De AP adviseert om toe te lichten welke specifieke waarborgen er worden getroffen ten aanzien van de doorgifte van persoonsgegevens naar Caribisch Nederland.

Openbaarmaking van het advies

De AP is voornemens dit advies niet eerder dan na vier weken openbaar te maken op de website www.autoriteitpersoonsgegevens.nl. Behoudens tegenbericht gaat zij ervan uit dat hiertegen geen bezwaar bestaat.

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter

[15] Toelichting op het concept, p. 23