COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Prins Clauslaan 60
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl

AAN de Minister van Binnenlandse Zaken en Koninkrijksrelaties

Postbus 20011
2500 EA DEN HAAG

DATUM 3 december 2015
ONS KENMERK z2015-00766
CONTACTPERSOON

UW BRIEF VAN 21 september 2015
UW KENMERK

ONDERWERP Wetgevingsadvies Besluit verwerking persoonsgegevens DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister

Geachte ,

Bij brief van 21 september 2015 heeft u het College bescherming persoonsgegevens (hierna: het CBP) gevraagd op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (hierna: Wbp) te adviseren over het Besluit verwerking persoonsgegevens DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister (hierna: het ontwerp-Besluit).

Het voorstel voor het ontwerp-Besluit is ter consultatie opengesteld via internet van 22 september tot en met 19 oktober 2015. Na ommekomst van de consultatietermijn heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties het CBP de post-consultatieversie toegezonden. Het CBP adviseert over het ontwerp-Besluit zoals dat op 21 september 2015 aan het CBP is voorgelegd en heeft de wijzigingen zoals nadien zijn doorgevoerd naar aanleiding van de consultatie, voor zover relevant, bij haar advisering betrokken.

Achtergrond en inhoud van het ontwerp-Besluit
Op 13 oktober 2015 heeft de Eerste Kamer het wetsvoorstel elektronisch berichtenverkeer Belastingdienst (hierna: Wet EBV) aangenomen. Centraal hierin staat de verplichting dat het berichtenverkeer tussen de belastingplichtige en de Belastingdienst op digitale wijze plaatsvindt. Volgens de Nota van Toelichting bij de Wet EBV sluit deze verplichting aan bij de staande praktijk van steeds verdergaande digitalisering en de wens van het kabinet om met digitale communicatiemiddelen het contact tussen belastingplichtige en de Belastingdienst eenvoudiger, eenduidiger en informeler te laten verlopen.

In de Wet EBV is hiertoe (in artikel I) een grondslag gecreëerd waarmee het tweezijdige berichtenverkeer tussen de belasting- en ontheffingsplichtige (hierna: de belastingplichtige) en de inspecteur of het bestuur van 's Rijksbelastingen Belastingdienst (hierna: de Belastingdienst) - via een ingroeimodel - verplicht op digitale wijze zal plaatsvinden. De digitalisering van het berichtenverkeer tussen belastingplichtige en de Belastingdienst omvat hiermee niet alleen de berichten die de belastingplichtige aan de Belastingdienst verzendt, maar ook de berichten die de

Belastingdienst aan de belastingplichtige stuurt. Met de Wet EBV wordt de Berichtenbox van MijnOverheid aangewezen als verplicht kanaal voor het ontvangen van berichten van de Belastingdienst. De gegevensverwerkingen die plaatsvinden gebeuren derhalve niet langer op basis van vrijwilligheid (toestemming) van de belastingplichtigen (betrokkenen).

Daarnaast is in de Wet EBV (in artikel X) een zorgtaak voor de Minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: de Minister van BZK) geformuleerd die ziet op de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en registratie van machtigingen (hierna: de voorzieningen). Volgens de Nota van Toelichting worden hieronder ook eventuele toekomstige voorzieningen begrepen.

Wat betreft de met de uitvoering van die zorgtaak samenhangende gegevensverwerkingen is de Minister van BZK in artikel X aangemerkt als verantwoordelijke in de zin van artikel 1, aanhef en onder d, van de Wet bescherming persoonsgegevens (hierna: Wbp) en vinden de noodzakelijke gegevensverwerkingen plaats in het kader van de goede vervulling van zijn zorgtaak. In artikel X is tot slot opgenomen dat bij algemene maatregel van bestuur nader wordt bepaald welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. Het onderhavige ontwerp-Besluit ten aanzien waarvan het CBP om advies is gevraagd is daarvan het resultaat.

De artikelen I tot en met VI, VIII en X van de Wet EBV zijn op 1 november 2015 in werking getreden.

In het kader van de adviesaanvraag met betrekking tot het ontwerp-Besluit zijn twee PIA's aan het CBP voorgelegd. Eén PIA ziet specifiek op MijnOverheid, DigiD en DigiDMachtigen, de andere PIA heeft betrekking op het Introductieplateau E-IDstelsel. Het CBP heeft met interesse kennis genomen van beide PIA's. Wellicht ten overvloede wijst het CBP erop dat de PIA inzake het E-ID stelsel (nu: Idensys) betrekking heeft op de signalering van privacy-risico's bij (de verdere ontwikkeling van) dit stelsel en dus breed is ingestoken. Het CBP heeft kennis genomen van de uitgebreide aanbevelingen die relevant zijn voor de verdere ontwikkeling van Idensys. In verband met de advisering over het ontwerp-Besluit heeft het CBP alleen die aspecten uit de PIA betrokken die voor dat ontwerp-Besluit relevant zijn.

Opmerking vooraf: inbreuk artikel 8 EVRM
Voorafgaand aan de hiernavolgende beoordeling van het ontwerp-Besluit merkt het CBP het volgende op.

De Wet EBV omvat in artikel I het uitgangspunt dat het berichtenverkeer tussen belastingplichtige en de Belastingdienst uitsluitend op digitale wijze mag plaatsvinden.
In artikel X, eerste lid, van de Wet EBV is vervolgens de algemene zorgtaak van de Minister ten aanzien van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing en de

grondslag voor de daarmee samenhangende gegevensverwerkingen vastgelegd. In het derde lid van dit artikel is opgenomen dat bij algemene maatregel van bestuur zal worden bepaald welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. De noodzaak om bepaalde gegevensverwerkingen te doen dient dus in het bijzonder in het onderhavige ontwerp-Besluit te worden aangetoond.

In de Nota van Toelichting bij het ontwerp-Besluit zijn dat Besluit en de erin opgenomen gegevensverwerkingen getoetst aan artikel 8 EVRM en de daaruit voortvloeiende vereisten. Het CBP wijst erop dat de belangrijkste afweging in dat verband, namelijk de voorvraag of en in hoeverre het digitale berichtenverkeer met de Belastingdienst verplicht moet worden gesteld, niet in het ontwerp-Besluit is opgenomen maar is geregeld in de Wet EBV. Bij de beantwoording van de vraag of het ontwerp-Besluit en de daarin mogelijk gemaakte gegevensverwerkingen voldoen aan de bedoelde vereisten, dient ook de verplichtstelling van het gebruik van de voorzieningen in verband waarmee de gegevensverwerkingen plaatsvinden een rol te spelen. Voor de toetsing aan artikel 8 EVRM en de daaruit voortvloeiende vereisten kan de verplichting in de Wet EBV en wat is uitgewerkt in het ontwerp-Besluit niet los van elkaar worden gezien.

Het CBP zal, hoewel de Wet EBV op onderdelen al in werking is getreden[1] en het thans gaat om advisering ten aanzien van het ontwerp-Besluit, in het hiernavolgende dienen in te gaan op de gevolgen van de verplichtstelling van het gebruik van de voorzieningen.

Opmerking vooraf: de Berichtenbox als openbare elektronische communicatiedienst
Het CBP wijst op de mogelijkheid dat de Berichtenbox van MijnOverheid moet worden beschouwd als een openbare elektronische communicatiedienst als bedoeld in artikel 1.1, sub f, van de Telecommunicatiewet. Mocht de Minister tot de conclusie komen dat de berichtenbox als zodanig kwalificeert, dan adviseert het CBP aan de mogelijke gevolgen hiervan in hoofdstuk 8 van de Nota van Toelichting aandacht te besteden.

Samenhang met andere (toekomstige) ontwikkelingen
Zoals ook in de Nota van Toelichting bij het ontwerp-Besluit wordt opgemerkt, is de Wet EBV deel van een groter geheel aan - deels al tot stand gekomen - digitale ontwikkelingen en stelsels binnen de overheid die uiteindelijk in de thans in voorbereiding zijnde Wet generieke digitale infrastructuur (hierna: Wet GDI) vastgelegd moeten worden. Het CBP maakt in algemene zin de kanttekening dat met deze gefaseerde ontwikkeling het gevaar bestaat dat onvoldoende zicht is op, of onvoldoende rekening kan worden gehouden met, de samenhang tussen bepaalde voorzieningen en ontwikkelingen en de daarmee gepaarde gaande risico's voor de bescherming van de persoonlijke levenssfeer. Het CBP wijst bijvoorbeeld op de ontwikkeling van Idensys zoals die nu plaatsvindt en de mogelijkheid dat dit stelsel op termijn bij de Europese Commissie zal worden aangemeld als landelijk knooppunt voor grensoverschrijdende uitwisseling van

[1] Het CBP is niet om advies gevraagd ten aanzien van de Wet EBV

persoonsgegevens in het kader van bijvoorbeeld de verlening van vertrouwensdiensten door buitenlandse partijen[2].

Het CBP begrijpt dat het tot stand brengen van algemene wetgeving voor de digitale overheid een omvangrijk traject is en dat bepaalde voorzieningen zoals Idensys nog in ontwikkeling zijn. In het onderhavige ontwerp-besluit wordt ten aanzien van de ontwikkeling van Idensys een eerste stap gezet met het wettelijke vastleggen van het BSN-Koppelregister. Het feit dat het tegelijkertijd samenbrengen van dergelijke omvangrijke ontwikkelingen en wetgevingstrajecten in één wetsvoorstel complex is en veel tijd kost mag echter geen reden zijn dat relevante aspecten rondom de bescherming van de persoonlijke levenssfeer niet, niet op tijd of in onvoldoende mate bij - separate - wetgevingsprocessen en feitelijke ontwikkelingen wordt betrokken. Op termijn zou dit juist afbreuk kunnen doen aan het gewenste uitgangspunt bij het vormgeven van de digitale overheid: een veilige en betrouwbare tijds- en plaatsonafhankelijke dienstverlening van de overheid en het huidige grootschalige gebruik van de voorzieningen.

Het CBP mist een overzicht van de samenhang in deze ontwikkelingen en een standpunt van de Minister en adviseert dit alsnog in de Nota van Toelichting op te nemen.

Beoordeling van het ontwerp-Besluit
Het CBP heeft de inhoud van het ontwerp-Besluit getoetst aan de normen van *noodzakelijkheid*, *proportionaliteit* en *subsidiariteit*, afkomstig uit artikel 8 van het EVRM.

Artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: het EVRM) eist dat iedere inmenging op het recht op respect voor privéleven op een wettelijke grondslag berust. Artikel 10 van de Grondwet scherpt deze bepaling aan en verlangt voor elke beperking van het recht op eerbiediging van de persoonlijke levenssfeer een grondslag in de formele wet.

Voor een wettelijke beperking van het voornoemde grondrecht gelden ook materiële eisen. Het voorschrift zal voldoende nauwkeurig moeten zijn en adequate en effectieve waarborgen moeten bevatten tegen ongeoorloofde inbreuken. Voorts is een inmenging op het recht op respect voor privéleven slechts toegestaan indien deze in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Volgens de jurisprudentie van het Europese Hof voor de Rechten van de Mens betekent dit dat de beperking van de persoonlijke levenssfeer moet worden gerechtvaardigd door een 'pressing

[2] EU Verordening elektronische identiteiten en vertrouwensdiensten, http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32014R0910

social need' en in overeenstemming moet zijn met de beginselen van proportionaliteit (de beperking mag niet onevenredig zijn in verhouding tot het nagestreefde doel) en de subsidiariteit (het nagestreefde doel moet niet op een voor de burger minder ingrijpende wijze kunnen worden bereikt). Deze vereisten moeten in hun onderlinge samenhang gelezen worden.

1. Maatschappelijke noodzaak, 'pressing social need'
De omstandigheid dat het berichtenverkeer met de belastingplichtige verplicht op digitale wijze moet plaatsvinden, is (in beginsel) een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer. De Nota van Toelichting bij het concept-Besluit gaat hier ook vanuit. In de Nota van Toelichting bij het ontwerp-Besluit is de maatschappelijke noodzaak hiertoe onderbouwd door te wijzen op het feit dat het verplicht gebruik van de berichtenbox en de fiscale uitvoering van de wet slechts mogelijk kan worden gemaakt met de wettelijke basis zoals neergelegd in artikel X van de Wet EBV. Dit is een (wettelijke) *conditio sine qua non*, maar op zich zelf geen (nadere) onderbouwing van de maatschappelijke noodzaak, juist met het oog op de inbreuk op de bescherming van de persoonlijke levenssfeer.

Wat er zij van de wijze waarop in de Wet EBV de maatschappelijke noodzaak, *pressing social need*, inzake de verplichting om, kort gezegd langs elektronische weg met de Belastingdienst te communiceren, alsmede de wijze waarop en door middel waarvan dat dient te geschieden, wordt onderbouwd, de (maatschappelijke) noodzaak, in de zin van artikel 8 EVRM dient (ook) haar weerslag te vinden in het ontwerp Besluit.

Het CBP adviseert in de Nota van Toelichting (nader) te motiveren in hoeverre de inbreuk op de persoonlijke levenssfeer door de verplichtstelling van het digitale berichtenverkeer met de Belastingdienst en het gebruik van de voorzieningen door betrokkenen wordt gerechtvaardigd door een 'pressing social need'.

2. Proportionaliteit: bewaartermijn gebruiksgegevens en derdenverstrekking
In het ontwerp-Besluit wordt specifiek voor gebruiksgegevens een bewaartermijn van 5 jaar gehanteerd. Wat gebruiksgegevens zijn, is voor iedere functionaliteit in het ontwerp-Besluit verschillend gedefinieerd maar gemeenschappelijk kenmerk is dat het gegevens zijn over het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker is ingelogd, handelingen van de gebruiker (inloggen, aanvragen, intrekken en activeren), de afnemer waarvoor de gebruiker is gemachtigd, alsmede het tijdstip waarop dit gebeurt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik.

Tot het moment van totstandkoming van het ontwerp-Besluit was de bewaartermijn van gebruiksgegevens die in het kader van DigiD, DigiD Machtigen en MijnOverheid werden verwerkt 18 maanden. In de Nota van Toelichting is de uitbreiding van deze bewaartermijn naar 5 jaar gemotiveerd door erop te wijzen dat het aantal gebruikers is toegenomen - en nog meer zal toenemen - en dat er een tendens waarneembaar is waarbij burgers zich steeds vaker met vragen om hun gegevens tot de voorzieningen wenden.

Verder wordt met betrekking tot deze bewaartermijn van 5 jaar in relatie tot misbruik en oneigenlijk gebruik in de Nota van Toelichting het volgende opgemerkt:
'Kenmerk van misbruik en oneigenlijk gebruik is dat van tevoren niet kan worden bepaald hoe dat plaatsvindt en welke gegevensverwerking nodig is om de betrouwbaarheid te borgen en de burger in zijn belang te beschermen. '*Om die redenen kan niet op voorhand een inperking worden aangebracht in de gegevens die dienen te worden verwerkt en verstrekt. De verwerking kan daarmee in potentie ieder gegeven betreffen dat beschikbaar is binnen de voorziening' (cursivering CBP).*

De omstandigheid dat het aantal gebruikers en de intensiteit van het gebruik is toegenomen wil op zichzelf nog niet zeggen dat daarmee een bewaartermijn van 5 jaar noodzakelijk is. Dat geldt ook voor de toegenomen vraag van burgers naar hun gebruiksgegevens. Verder is het CBP van oordeel dat, hoewel het bestrijden van misbruik en oneigenlijk gebruik een gerechtvaardigd en ook noodzakelijk doel is, de hiervoor omschreven mogelijkheid dermate ruim geformuleerd is dat hiermee de overige - vaak aanzienlijk kortere - bewaartermijnen voor niet-gebruiksgegevens zinledig lijken te worden. Daarnaast is het volgens artikel 10 van het ontwerp-Besluit mogelijk dat de Minister van BZK indien dit noodzakelijk is in het kader van de borging van de beveiliging en betrouwbaarheid van de voorzieningen, zonder toestemming van betrokkenen aan derden gegevens verstrekt over een bezoeker of gebruiker van de voorzieningen.

Het CBP adviseert nader in te gaan op de noodzaak van de bewaartermijn voor gebruiksgegevens van 5 jaar. Daarbij kan specifiek aandacht worden besteed aan de vraag hoe de deze bewaartermijn zich verhoudt tot de overige in het ontwerp-Besluit opgenomen bewaartermijnen inzake andere gegevens dan gebruiksgegevens (de hiervoor weergegeven zinsnede uit de Nota van Toelichting).

3. Artikel 13 Wbp: beveiliging en de centrale rol van het BSN
In het ontwerp-Besluit is per functionaliteit (DigiD, DigiD Machtigen, MijnOverheid en het BSN-Koppelregister) aangegeven welke persoonsgegevens worden verwerkt, voor welk doel en hoe lang deze gegevens worden bewaard. Volgens de Nota van Toelichting is uitgangspunt dat de verwerking zo min mogelijk moet zijn en dat alleen die gegevens worden verwerkt die echt essentieel zijn om de voorzieningen beschikbaar te kunnen stellen, in stand te kunnen houden, te laten werken en beveiligen en betrouwbaar te houden. Daarbij wordt opgemerkt dat het BSN een centrale rol inneemt. In de voorzieningen wordt zo veel mogelijk alleen met het BSN gewerkt. Voor zover afnemers van bepaalde voorzieningen meer gegevens nodig hebben, zullen zij die via andere wegen moeten verkrijgen, bijvoorbeeld via het BRP mits zij daarvoor in aanmerking komen. Op die manier is het aantal persoonsgegevens dat wordt verwerkt grotendeels beperkt tot het BSN en bijbehorende gebruiks- en accountsgegevens. Daarbij wordt in de Nota van Toelichting ook nog aangegeven dat in het kader van de voorzieningen geen gevoelige persoonsgegevens worden verwerkt zoals bijvoorbeeld over ras, politieke opvatting of geloof.

Hoewel bestuursorganen het BSN mogen verwerken in het kader van de uitoefening van hun taak en de gegevensverwerkingen door de afnemers van de voorzieningen geen deel uitmaken van dit ontwerp-Besluit, wijst het CBP erop dat, in tegenstelling tot wat in de Nota van Toelichting is vermeld, met het BSN wel een bijzonder persoonsgegeven in de zin van paragraaf 2 (de verwerking van bijzondere persoonsgegevens) van de Wbp wordt verwerkt.
Dat schept extra verplichtingen voor zowel de afnemers van de voorzieningen die dit BSN verwerken (bestuursorganen die bijvoorbeeld DigiD afnemen), als voor de Minister van BZK als verantwoordelijke voor de beveiliging van de voorzieningen als bedoeld in artikel X, lid 1, van de Wet EBV en als verantwoordelijke voor de daarmee samenhangende gegevensverwerkingen als bedoeld in artikel X, lid 3, van de Wet EBV. In dat verband wijst het CBP er nog op dat volgens de Nota van Toelichting voor de ondersteuning van gebruikers van de voorzieningen klantcontactcentra beschikbaar zijn, die telefonisch of schriftelijk / per e-mail vragen en klachten in behandeling nemen en daarvan een registratie bijhouden. Omdat de accounts in de drie voorzieningen primair gebaseerd zijn op BSN dient dit volgens de Nota van Toelichting ook voor gebruikersondersteuning te worden verwerkt. De verwerking van BSN dient in dergelijke gevallen waarschijnlijk via bewerkersovereenkomsten geregeld te worden waarvan het aspect beveiliging een belangrijk onderdeel is.

Het CBP adviseert in de Nota van Toelichting expliciet aandacht te besteden aan de gevolgen van de verwerking van BSN door verschillende partijen en de vraag hoe de Minister een zorgvuldige verwerking door verschillende partijen verzekert.

Het CBP merkt daarnaast op dat de verplichtstelling van het digitale berichtenverkeer met de Belastingdienst inhoudt dat de berichtenbox van MijnOverheid dient te worden gebruikt. Dit betekent dat alle belastingplichtigen in Nederland gebruik dienen te maken van deze voorziening en dat bij het gebruik van die voorziening veel (gevoelige) persoonsgegevens worden verwerkt. Dat gegeven stelt hoge eisen aan de beveiliging van deze voorziening en aan de beveiliging van de voorzieningen waarvan het gebruik niet verplicht is gesteld. In de Ministeriële regeling voorzieningen digitale infrastructuur[3] is de verplichting voor de Minister geformuleerd om passende maatregelen te nemen om inbreuken op en aantastingen van de beveiliging en de processen van de voorzieningen te voorkomen en is opgenomen dat hierbij in ieder geval wordt voldaan aan de open normen en standaarden op de 'pas-toe-of-leg-uit-lijst' van het Forum Standaardisatie, de normen ICT-beveiligingsassessments DigiD, de Baseline Informatiebeveiliging Rijksdienst en de Voorschriften Informatiebeveiliging Rijksdienst.

[3] Voluit: Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, houdende regels met betrekking tot de werking, beveiliging en betrouwbaarheid van de voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen met betrekking tot de werking, beveiliging en betrouwbaarheid van de voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen.

Het CBP adviseert in de Nota van Toelichting bij het ontwerp-Besluit de inrichting van de beveiliging van de voorzieningen, in het licht van de Ministeriële regeling voorzieningen digitale infrastructuur, uiteen te zetten, alsmede zo nodig aan te passen en/of te concretiseren.

4. Subsidiariteit

In de Nota van Toelichting staat omschreven dat het ontwerp-Besluit de bestaande praktijk bij de voorzieningen vastlegt en dat niet is bekeken of een andere wijze dan de bestaande voorzieningen mogelijk minder ingrijpend zou zijn. In het kader van de totstandkoming van de Wet EBV heeft deze subsidiariteitstoets - in die zin dat de vraag of en in hoeverre verplichte gegevensverwerkingen op een andere, minder ingrijpende wijze zouden kunnen plaats vinden, wordt opgeworpen en beantwoord – evenwel niet als zodanig plaats gevonden.

Het CBP adviseert in de Nota van Toelichting het antwoord op de vraag naar de subsidiariteit (alsnog) onder ogen te zien en te onderbouwen.

5. Het BSN-Koppelregister

Het BSN-Koppelregister is een nieuwe voorziening die in het kader van de generieke digitale infrastructuur is ontwikkeld in verband met de ontwikkeling van Idensys. Het Koppelregister maakt het voor afnemers van MijnOverheid mogelijk om naast publieke ook private authenticatiemiddelen te accepteren. De kern van Idensys vormt de mogelijkheid voor gebruikers om met een privaat authenticatiemiddel in het publieke domein te kunnen inloggen. Nadat een burger met een privaat authenticatiemiddel heeft ingelogd bij een organisatie in het publieke domein, legt het Koppelregister een koppeling tussen het pseudo-ID van de gebruiker, waarmee de gebruiker is geregistreerd bij de private authenticatiedienst, en het eerder - eenmalig - door de authenticatiedienst aan het Koppelregister aangeleverde BSN van de gebruiker.

Het CBP wijst op haar brief van 7 mei 2015[4] waarin zij ten aanzien van de ontwikkeling van Idensys specifieke zorgpunten heeft geformuleerd. Een van die zorgpunten was het gebruik van BSN door private partijen, hetgeen zonder uitdrukkelijke specifieke wettelijke grondslag (en daarmee een afweging door de wetgever) voor dergelijke partijen niet is toegestaan. Ook over de optie om deze aanlevering via bewerkersovereenkomsten te regelen is het CBP in haar brief kritisch geweest.

In de Nota van Toelichting wordt enerzijds gesteld dat middels het samenstel van artikel X in de Wet EBV, het ontwerp-Besluit en de ministeriële regeling voorzieningen digitale infrastructuur is voorzien in de verankering van het gebruik van BSN in de private sector in wet- en regelgeving. Anderzijds is in de Nota van Toelichting opgenomen dat wat betreft de aanlevering van BSN private authenticatiediensten bewerkersovereenkomsten dienen te sluiten met de Minister van BZK als beheerder van het Koppelregister en verantwoordelijke in de zin van de Wbp. In die overeenkomsten moet onder meer worden opgenomen dat de authenticatiedienst na de

[4] https://www.cbpweb.nl/nl/nieuws/cbp-maakt-eerste-analyse-van-eid-stelsel

aanlevering het BSN niet bewaart.

Het CBP adviseert de Minister om te motiveren waar in dit samenstel van bepalingen de verankering van het gebruik van BSN door private partijen is geregeld en hoe dit zich verhoudt tot het uitgangspunt uit de Nota van Toelichting dat voor de verwerking van BSN bewerkersovereenkomsten dienen te worden gesloten (hetgeen op zichzelf terecht suggereert dat er geen wettelijke grondslag is voor private partijen om het BSN te verwerken).

Dictum
Het CBP adviseert u niet tot indiening van het voorstel over te gaan, dan nadat daarin met het vorenstaande rekening zal zijn gehouden.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College