AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
De Minister van Financiën
De heer ir. J.R.V.A. Dijsselbloem
Postbus 20201
2500 EE DEN HAAG

Datum	Ons kenmerk	Uw brief van
22 augustus 2017	z2017-04997	26 juli 2017
	Contactpersoon	Uw kenmerk
		2017-0000141125

Onderwerp
Advies wetsvoorstel Implementatiewet herziene richtlijn betaaldiensten

Geachte heer Dijsselbloem,

Bij brief van respectievelijk 1 juni 2017 en 26 juli 2017 heeft u de Autoriteit Persoonsgegevens (hierna: de AP) het initiële en gewijzigde wetsvoorstel Implementatiewet herziene richtlijn betaaldiensten (hierna: Wetsvoorstel) op haar verzoek toegezonden, alsmede de bijbehorende Memorie van Toelichting (hierna: MvT). Bij dezen brengt de AP haar advies uit over het Wetsvoorstel, indachtig haar taak als opgenomen in artikel 52, tweede lid, van de Wet bescherming persoonsgegevens (Wbp).[1] Uit hoofde van deze bepaling adviseert de AP over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens.

Inhoud wetsvoorstel

Het Wetsvoorstel voorziet in de nationale omzetting van de richtlijn (EU) 2015/2366 (hierna: Richtlijn).[2] De betreffende Richtlijn staat bekend als de tweede Payment Service Directive (hierna: PSD2) en vervangt richtlijn 2007/64/EG (PSD1). In navolging van PSD2 introduceert het Wetsvoorstel onder meer de gelegenheid voor een tweetal categorieën van nieuwe –innovatieve –betaaldienstverleners om actief te worden op de Nederlandse betaalmarkt.

[1] De Autoriteit Persoonsgegevens adviseert op eigen initiatief nu zij daartoe niet formeel door het Ministerie van Financiën is verzocht.
[2] Het Wetsvoorstel strekt tot wijziging van de Wet financieel toezicht (Wft), de Wet bekostiging financieel toezicht (Wbft), titel 7b van boek 7 van het Burgerlijk Wetboek (BW) de Wet handhaving consumentenbescherming (whc) ter implementatie van de richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG.

In de eerste plaats betreft het de 'betaalinitiatiedienst' (artikel 1:1 Wetsvoorstel). Met deze dienst kan de gebruiker een betaalopdracht desgewenst door de betaalinitiatiedienst laten inleiden bij een andere betaaldienstverlener, met betrekking tot de betaalrekening die hij bij laatstgenoemde aanhoudt. In de tweede plaats betreft het de 'rekeninginformatiedienst' (artikel 1:1 Wetsvoorstel). Oftewel, een onlinedienst ten behoeve van het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen - die de betaaldienstgebruiker bij een of meer betaaldienstverleners aanhoudt.

De betaalinitiatiedienstverlener en de rekeninginformatiedienstverlener zijn gehouden om in het bezit te zijn van een vergunning, om actief te mogen worden op de Nederlandse markt (artikel 2:3b Wetsvoorstel). Het Wetsvoorstel introduceert nadere eisen aan deze partijen en overigens ook aan andere betaaldienstverleners. De vereisten hebben blijkens de MvT onder meer betrekking op de omgang met veiligheidsincidenten en klachten, het opslaan, monitoren, traceren en beperken van toegang tot gevoelige betaalgegevens, de bedrijfscontinuïteit, de wijze waarop statistieken worden bijgehouden van transacties en fraude, het veiligheidsbeleid inclusief risicoanalyse en hoe toezicht wordt gehouden op agenten en bijkantoren.[3] Deze nadere eisen gelden voor aanvragers van een vergunning en zullen bij AMvB worden omgezet, met als delegatiegrondslag artikel 3:17 van de Wet financieel toezicht (Wft). De Nederlandsche Bank is blijkens het Wetsvoorstel belast met de uitvoering van het vergunningenstelsel, en zal in dit kader toetsen aan de vereisten uit voormelde AMvB.

Onder verwijzing naar artikel 94, tweede lid, van de Richtlijn mogen betaaldienstverleners zich toegang verschaffen tot de persoonsgegevens die noodzakelijk zijn voor het aanbieden van hun betalingsdiensten, deze verwerken en bewaren, mits de gebruiker van de betaaldienst hiervoor zijn uitdrukkelijke toestemming geeft.[4] Hoewel artikel 94, tweede lid, van de Richtlijn een centrale bepaling betreft met betrekking tot de bescherming van de persoonlijke levenssfeer van betrokkenen, is in het Wetsvoorstel niet (meer) voorzien in de implementatie van het hiervoor aangehaalde artikel 94, tweede lid, van de Richtlijn. De implementatie hiervan geschiedt eveneens bij de hiervoor aangehaalde AMvB.

De AP is voornemens om, zodra actueel, advies uit te brengen over bovengenoemde AMvB, gezien de impact die deze lagere regelgeving heeft op de verwerking van persoonsgegevens. In dat kader en bovendien gelet op de reikwijdte van het onderhavige Wetsvoorstel merkt de AP het volgende op.

Indachtig de geschetste wijzigingen van het reguleringskader in de financiële sector en de onmiskenbaar snelle ontwikkeling van de informatietechnologie, zal FinTech – de inzet van technologie op financieel gebied - de komende jaren een grote vlucht nemen. In de nabije toekomst is niet alleen voorzienbaar dat het betalingsverkeer, en daarmee de verwerking financiële gegevens, steeds vaker verloopt met tussenkomst van andere betaaldienstverleners. Ook tal van andere diensten zullen ontstaan, die door de analyses van rekeninginformatie beter op de behoeften van de burger kunnen inspelen.

[3] Zie pagina 5 van de MvT van het Wetsvoorstel.
[4] Artikel 94, tweede lid, van de Richtlijn (PSD2):"Betaaldienstaanbieders mogen alleen met de uitdrukkelijke toestemming van de betaaldienstgebruiker toegang krijgen tot persoonsgegevens die noodzakelijk zijn voor het aanbieden van hun betalingsdiensten, deze verwerken en bewaren."

De ontwikkeling van FinTech draait op financiële gegevens. Dit zijn persoonsgegevens van gevoelige aard in voorkomende gevallen. Daarmee is het maatschappelijk belang gegeven om al in de ontwerpfase, *by design*, oog te houden voor de privacy van betrokkenen; een grondrecht van de Europese burger.[5] Dit geldt niet alleen in de naleving van de wetgeving door burgers, het bedrijfsleven en de overheid. De Wetgeving *an sich* is het vertrekpunt en zal rechtszekerheid dienen te bieden over zijn toepasselijkheid, maar ook over het toezicht daarop en de handhaving daarvan. Om toekomstbestendig te zijn is een technologie neutrale formulering onontbeerlijk. Enerzijds om daadwerkelijk ruimte te geven aan nieuwe initiatieven en ontwikkelingen, anderzijds om te voorkomen dat de gecodificeerde waarborgen na verloop van tijd geen recht (meer) doen aan de bescherming van de privacy van betrokkenen. Alleen dan kan innovatie hand in hand gaan met de bescherming van de persoonlijke levenssfeer. Deze bescherming ligt aan de basis van het vertrouwen van burgers, bedrijven en overheden in nieuwe, innovatieve dienstenaanbieders, en daarmee aan het duurzaam welslagen van de kansen die FinTech Nederland biedt. In dat licht is het hierna volgende advies opgesteld.

Wettelijk kader

De AP is thans aangewezen als toezichthouder op de Wbp. De Wbp vindt zijn herkomst in richtlijn 95/46/EG (hierna: de Privacyrichtlijn). Per 25 mei 2018 zal de Algemene Verordening Gegevensbescherming (hierna: AVG) in de plaats treden van de Wbp.[6] De AP is in Nederland exclusief aangewezen als onafhankelijk toezichthouder op de AVG, en is in die rol verantwoordelijk voor het waarborgen van de coherente toepassing hiervan, mede door afstemming met andere bevoegde toezichthouders uit de overige lidstaten. Met de AVG in het vooruitzicht heeft de AP deze verordening in haar advisering betrokken, evenals de daarop gebaseerde (nationale) Uitvoeringswet Algemene verordening gegevensbescherming. Wetsvoorstellen dienen te voldoen aan de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (Handvest), artikel 16 van Verdrag betreffende de werking van de Europese Unie (VWEU), artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet.

Artikel 8 van het Handvest bepaalt onder meer dat persoonsgegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Artikel 16 VWEU bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens. Op grond van artikel 8 EVRM is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op respect voor zijn privéleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Artikel 10, eerste lid, van de

[5] Zie ook randnummer 89 van de Preambule van de Richtlijn (laatste volzin), met daarin aandacht voor het in acht nemen van *privacy by design*, evenals *privacy by default*.

[6] 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).

Grondwet bepaalt dat een ieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen. Deze principes komen mede tot uiting in de AVG.

Beoordeling

A. De verhouding tot de Algemene Verordening Gegevensbescherming

De Richtlijn uit 2007 waarvan het onderhavige Wetsvoorstel de implementatie vormt, verwijst met betrekking tot de bescherming van de persoonlijke levenssfeer naar de Privacyrichtlijn.[7] Dit wettelijk kader geldt per 25 mei 2018 niet meer vanwege de inwerkingtreding van de AVG, hetgeen ten tijde van het opstellen van de Richtlijn wellicht geen voorzienbare context is geweest. Inmiddels is het van kracht worden van de AVG realiteit, die echter onvoldoende in het Wetsvoorstel is betrokken. Dit klemt temeer nu de AVG, in tegenstelling tot de Privacyrichtlijn, een verordening betreft. Uit het Wetsvoorstel blijkt niet dat bij strijdigheid tussen de bepalingen van de Richtlijn en de AVG, voorrang toekomt aan de AVG. De AVG introduceert een nieuw uitgebalanceerd regime dat rechtstreeks doorwerkt in de nationale rechtsorde. De AVG zal met voorrang toepassing dienen te vinden, in geval van samenloop dan wel inconsistenties met wetgeving van lagere orde, waaronder het voorliggende Wetsvoorstel.

De AP adviseert om bij de totstandkoming van de wetgeving bovengenoemde werking van de AVG te betrekken en expliciet te maken in de toelichting, teneinde rechtsonzekerheid te voorkomen. Specifiek vraagt de AP daarnaast en in het licht van het bovenstaande, aandacht voor de verwijzing naar overweging 107 bij de AVG[8] in de derde alinea van het volgende onderdeel van de MvT van het Wetsvoorstel:

> *"10. Bescherming van persoonsgegevens*
> *Er zijn verschillende bepalingen in PSD II gewijd aan bescherming van persoonsgegevens. Zo moet een betaalinstelling bij de vergunningsaanvraag een beschrijving geven van het beveiligingsbeleid, waarin ook aandacht moet zijn voor de kans op fraude en illegaal gebruik van persoonsgegevens (artikel 5, eerste lid, onderdeel j, van de richtlijn). De verwerking van persoonsgegevens is voor betaaldienstverleners uitsluitend toegestaan met de uitdrukkelijke toestemming van de betaaldienstgebruiker (artikel 94, tweede lid, van de*

[7] Zie bijvoorbeeld randnummer 89 van de Richtlijn (PSD2):" Het aanbieden van betalingsdiensten door de betalingsdienstaanbieders kan de verwerking van persoonsgegevens met zich mee brengen. Richtlijn 95/46/EG van het Europees Parlement en de Raad (1), de nationale voorschriften tot omzetting van Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad (2) zijn van toepassing op de verwerking van persoonsgegevens in het kader van deze richtlijn. Met name is het noodzakelijk, wanneer voor de toepassing van deze richtlijn persoonsgegevens worden verwerkt, dat het precieze doel wordt aangegeven, dat de desbetreffende rechtsgrondslag wordt vermeld, dat de relevante beveiligingsvoorschriften van Richtlijn 95/46/EG worden nageleefd, en dat de beginselen noodzaak, evenredigheid, doelbegrenzing en een niet-buitensporige gegevensbewaarperiode in acht worden genomen. Ook moeten in alle gegevensverwerkingsystemen die in het kader van deze richtlijn worden ontwikkeld en gebruikt, de beginselen gegevensbescherming by design en gegevensbescherming by default in acht worden genomen."

[8] Overweging 107 bij de AVG: "De Commissie kan vaststellen dat een derde land, een gebied of een bepaalde verwerkingssector in een derde land, of een internationale organisatie geen passend beschermingsniveau meer waarborgt. De doorgifte van persoonsgegevens naar dat derde land of die internationale organisatie dient dan te worden verboden, tenzij aan de vereisten van deze verordening met betrekking tot doorgiften die onderworpen zijn aan passende waarborgen, met inbegrip van bindende bedrijfsvoorschriften, en afwijkingen voor specifieke situaties wordt voldaan. Er dient te worden geregeld dat er in die gevallen overleg plaatsvindt tussen de Commissie en de derde landen of internationale organisaties in kwestie. De Commissie moet het derde land of de internationale organisatie tijdig op de hoogte brengen van haar motivering en met de andere partij in overleg treden om de situatie te verhelpen."

richtlijn). Deze bepaling zal op grond van artikel 3.17 Wft worden geïmplementeerd in het Besluit prudentiële regels Wft.
Verder noemt overweging 89 van de richtlijn de beginselen noodzaak, evenredigheid, doelbegrenzing en een niet-buitensporige gegevensbewaarperiode. Ook moeten in alle gegevensverwerkingsystemen die in het kader van de richtlijn worden ontwikkeld en gebruikt, de beginselen gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen worden gehanteerd (artikel 94 en overweging 89 van de richtlijn).
Dit zijn ook uitgangspunten die in de Algemene Verordening Gegevensbescherming worden genoemd. Aan deze uitgangspunten kan door betaaldienstverleners onder meer uitvoering worden gegeven door het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens en transparantie met betrekking tot de functies en de verwerking van persoonsgegevens (vgl. overweging 107 van die verordening, waar ook nog meer voorbeelden worden genoemd). Deze voorwaarden zijn in de richtlijn en de verordening verder uitgewerkt.(..)"

De AP merkt op dat in de aangehaalde overweging bij de AVG, noch de in de MvT genoemde uitgangspunten, noch de wijze waarop hieraan uitvoering kan worden gegeven, zijn opgenomen. Het gaat om in overweging 78 bij de AVG opgenomen voorbeelden van maatregelen die de verwerkingsverantwoordelijke moet toepassen om de naleving van de verordening te kunnen aantonen. Daarom verzoekt de AP om deze passage te verwijderen, om misverstanden te voorkomen. Daarbij benadrukt de AP dat het onwenselijk is om middels een (sectorspecifiek) wetsvoorstel invulling te geven aan de AVG, nu immers de beoogde uniformiteit in de toepassing van de AVG dient te worden gerespecteerd.

B. Toezicht en handhaving

Onder verwijzing naar de hierboven geschetste contouren van het Wetsvoorstel, is De Nederlandsche Bank (DNB) belast met het toezicht op de gegevensbescherming van betaaldienstverleners in het kader van het vergunningenstelsel. DNB behandelt blijkens artikel 2:3b van het Wetsvoorstel aanvragen voor vergunningen, en houdt doorlopend toezicht op de naleving van de eisen aan vergunninghouders, waaronder inzake de gegevensbescherming.

Hoewel de concrete (nadere) eisen die gesteld worden aan betaaldienstverleners thans niet het onderwerp van implementatie vormen, zijn de kaders hiervan al kenbaar in het Wetsvoorstel. De implementatie van artikel 94 van de Richtlijn (het vereiste van uitdrukkelijke toestemming teneinde toegang te verkrijgen die noodzakelijk is voor het aanbieden van de dienst, deze te verwerken, en bewaren) zal bijvoorbeeld te zijner tijd onderdeel gaan uitmaken van het toetsingskader van artikel 3:17 van de Wft.

Indachtig artikel 11, tweede lid van de Richtlijn zal DNB te zijner tijd een vergunning verlenen indien de gegevens en bewijsstukken die bij de aanvraag gevoegd zijn, in overeenstemming zijn met alle voorschriften vastgelegd in artikel 5 van de Richtlijn. Uit hoofde van artikel 5, eerste lid, onder j van de Richtlijn dienen aanvragers van een vergunning de aanvraag vergezeld te doen gaan van "een beschrijving van het beveiligingsbeleid, met inbegrip van een gedetailleerde risicoanalyse met betrekking tot de betalingsdiensten en een beschrijving van de maatregelen op het gebied van beveiliging en risicobeperking

die worden genomen om de gebruikers van de betalingsdiensten afdoende tegen de vastgestelde beveiligingsrisico's, waaronder fraude en illegaal gebruik van gevoelige gegevens en persoonsgegevens, te beschermen". DNB onderzoekt en toetst de aanvraag, en verleent een vergunning indien zij over de hele lijn tot een positief oordeel komt. Voordat DNB een vergunning verleent, kan DNB andere relevante overheidsinstanties raadplegen (artikel 11, tweede lid van de Richtlijn).

In de MvT[9] van het Wetsvoorstel is hierover opgenomen:

> *De Nederlandsche Bank houdt toezicht op de naleving van in PSD II opgenomen regels ten aanzien van gegevensbescherming in het kader van vergunningverlening en oefent daarop het doorlopend toezicht uit. In Nederland is op grond van de Wet bescherming persoonsgegevens (Wbp) de Autoriteit Persoonsgegevens (AP) aangewezen om toezicht te houden op de naleving van deze verplichtingen, die thans nog in artikelen 8, 9 en 10 van de Wbp zijn neergelegd. Bevoegdheden bij overtreding van de verplichtingen zijn onder meer het opleggen van een dwangsom of een bestuurlijke boete. De AP kan voorts nog in het kader van effectief toezicht afspraken maken met andere toezichthouders, zoals de AFM en DNB. Zie hiervoor ook hetgeen in paragraaf 8 onder punt 3 van deze toelichting is vermeld over uitwisseling van vertrouwelijke gegevens en inlichtingen tussen de AP en andere toezichthouders.*

In het licht van de hiervoor beschreven (toekomstige) taken van DNB stipt de AP specifiek aan dat het criterium "uitdrukkelijke toestemming" is opgenomen in artikel 9 van de AVG, en derhalve valt onder haar toezicht. De AVG stelt daarnaast stringente eisen aan de beveiliging van persoonsgegevens, net als aan de te treffen maatregelen in geval van een 'datalek'. Gelet op de voorrang die toekomt aan de AVG (zie punt A. van dit advies) merkt de AP ten overvloede op dat zij nimmer gebonden kan zijn aan een rechtsoordeel van DNB over de naleving van de AVG. De AP blijft ten allen tijde bevoegd om een onafhankelijk oordeel te vormen, uitleg te geven, toezicht te houden en handhavend op te treden. De partijen die financiële persoonsgegevens verwerken betreffen veelal internationale spelers die geheel of ten dele de Europese markt willen bedienen. Voorkomen moet worden dat zij te maken krijgen met verschillende interpretaties over de AVG binnen de Lidstaten. Tevens is de AP gehouden om via in de AVG verankerde 'consistency mechanismen' de uitleg van de AVG te uniformeren, door hierover afstemming te zoeken met toezichthouders uit andere lidstaten. Dat versterkt de noodzaak om de positie van de AP te respecteren.

Ten slotte acht de AP van belang op te merken dat het verrichten van een gegevensbeschermingseffectbeoordeling (hierna: GEB) noodzakelijk kan zijn volgens artikel 35 van de AVG - voordat gestart wordt met de verwerking van persoonsgegevens.[10] Wanneer uit een GEB krachtens

[9] Zie pagina 9 MvT van het Wetsvoorstel.

[10] Zie randnummer 84 van de AVG: "Teneinde de naleving van deze verordening te verbeteren indien de verwerking waarschijnlijk gepaard gaat met hoge risico's in verband met de rechten en vrijheden van natuurlijke personen, dient de verwerkingsverantwoordelijke of de verwerker verantwoordelijk te zijn voor het verrichten van een gegevensbeschermingseffectbeoordeling om met name de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren. Met het resultaat van de beoordeling dient rekening te worden gehouden bij het bepalen van de passende maatregelen die moeten worden genomen om aan te tonen dat deze verordening bij de verwerking van persoonsgegevens wordt nageleefd. Wanneer een gegevensbeschermingseffectbeoordeling uitwijst dat verwerking gepaard gaat met een hoog risico dat de verwerkingsverantwoordelijke niet kan beperken door maatregelen die met het oog op de beschikbare technologie en de uitvoeringskosten redelijk zijn, dient vóór de verwerking een raadpleging van de toezichthoudende autoriteit plaats te vinden.

artikel 35 van de AVG blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, dan zal de verwerkingsverantwoordelijke ingevolge artikel 36 van de AVG voorafgaand aan de verwerking de AP moeten raadplegen. Het ligt in de rede om hieromtrent nadere afspraken te maken tussen de AP en de in dit Wetsvoorstel genoemde bevoegde toezichthouders. Mede opdat de uitkomsten van een GEB door DNB in zijn proces van vergunningverlening eventueel kunnen worden meegenomen.

De AP adviseert om het voorgaande te verwerken in het Wetsvoorstel, dan wel de toelichting daarop.

C. Overige bepalingen

In het Wetsvoorstel zijn daarnaast onderwerpen opgenomen waarbij ten onrechte niet wordt ingegaan op de samenloop met de AVG. De AP vindt dat het Wetsvoorstel op dit punt moet worden verhelderd, omdat er anders onduidelijkheid kan ontstaan over de eisen die voortvloeien uit het Wetvoorstel in relatie tot de AVG. Het betreft onder meer de eisen betreffende 'sterke cliëntauthenticatie' en de op te stellen (bindende) regels van de European Banking Association (EBA) omtrent de beveiliging van betaalgegevens.

In de kern komt het erop neer dat het noodzakelijk wordt geacht om in het Wetsvoorstel te laten zien hoe deze wetgeving zich verhoudt tot de Wbp en de AVG. Dit betekent dat de AP adviseert om het Wetsvoorstel aldus niet in te dienen.

De AP verneemt graag op welke wijze u gevolg geeft aan het advies. De AP is beschikbaar indien nadere toelichting is vereist.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Autoriteit persoonsgegevens,

Mr. W.B.M. Tomesen
Vicevoorzitter