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

De Staatssecretaris van Binnenlandse Zaken en
Koninkrijksrelaties
De heer drs. R.W. Knops
Turfmarkt 147
2511 DP Den Haag

Datum	Ons kenmerk	Uw brief van
15 oktober 2020		9 juli 2020
	Contactpersoon	Uw kenmerk

Onderwerp
Advies over de consultatieversie van de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening

Geachte heer Knops,

Bij brief van 9 juli 2020 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 de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (hierna: het concept). De AP heeft de volgende opmerkingen bij het concept en adviseert daarmee rekening te houden.

Samenvatting advies

Het concept schrijft voor hoe dienstverleners de betrouwbaarheid van hun diensten dienen in te schalen gelet op de risico's die aan de diensten zijn verbonden. De belangrijkste opmerkingen bij het concept:

- Het concept houdt het midden tussen een plicht voor dienstverleners om een bepaald betrouwbaarheidsniveau te gebruiken en een richtsnoer dat veel minder strikt is. Doordat wordt voorzien in ruime mogelijkheden voor dienstverleners om van de voorgestelde regels af te wijken, bestaat het risico dat het doel van de ontwerpregeling - een veiligere toegang tot dienstverlening - in gevaar komt. Gelet op de eis uit de AVG van een passende beveiliging van persoonsgegevens, adviseert de AP zo nodig het concept aan te passen.
- Voor persoonsgegevens die vallen onder het betrouwbaarheidsniveau 'hoog' zijn de voorgestelde criteria in het licht van de overwegingen uit de AVG over een 'hoog risico' te streng, onvolledig en onduidelijk. De AP adviseert de criteria aan te passen.
- De noodzaak van het toestaan van het 'naastlagere' niveau voor een termijn van twee jaar is niet voldoende onderbouwd. Bovendien kent de bepaling geen inhoudelijke voorwaarde of beperking. Hierdoor kan een veilige toegang tot de dienst in gevaar komen. De AP adviseert de noodzaak van

de mogelijkheid tot afwijking voor een termijn van twee jaar nader te motiveren en te voorzien in een voorwaarde of beperking.

Strekking van het concept

In de Wet digitale overheid (hierna: de Wdo) is gekozen om de vaststelling van de mate van toegangscontrole en de keuze voor het toegangsmiddel niet meer vrijblijvend te laten zijn, maar daar op basis van de wet een verplichtend karakter aan te geven.[1] Doelstelling is een veiligere toegang tot overheidsdienstverlening en meer eenduidigheid in inlogniveaus voor gelijksoortige dienstverlening bij verschillende overheden.[2]

Het concept werkt artikel 6 van het voorstel voor de Wdo uit, dat voorschrijft dat bestuursorganen en aangewezen organisaties (hierna: dienstverleners) bepalen welk authenticatie[3] betrouwbaarheidsniveau op een door hen aangeboden dienst van toepassing is, alsmede dat hiertoe regels worden gesteld.[4]

Het concept schrijft voor hoe dienstverleners de betrouwbaarheid van hun diensten moeten inschalen, gelet op de risico's die aan de diensten zijn verbonden.[5]

Voor de inschaling kiest het concept voor eenzelfde inschaling met de betrouwbaarheidsniveaus laag, substantieel en hoog, zoals die in eIDAS-verordening worden gehanteerd.[6] Voor niveau 'laag' volstaat een middel met éénfactorauthenticatie, zoals een combinatie van een gebruikersnaam en wachtwoord.[7] Voor

[1] Het voorstel voor de wet Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid) is in behandeling in de Eerste Kamer (Kamerstukken 34 972).
[2] Toelichting, blz. 7.
[3] Authenticatiemiddelen zorgen ervoor dat de overheden weten met welke burger of welk bedrijf ze van doen hebben. Deze middelen zijn er op verschillende betrouwbaarheidsniveaus. Het niveau hangt met name af van de aard van de (gegevens)transactie en de gevolgen ervan (zoals financieel of juridisch). Er zijn veel verschillende digitale overheidsdiensten. Het is niet mogelijk om voor al die diensten één uniforme oplossing vast te stellen voor identificatie, authenticatie en autorisatie. Zo is een standaardoplossing met een zeer hoog betrouwbaarheidsniveau in veel gevallen te duur of simpelweg niet nodig. Bovendien wordt dan het gebruik van e-diensten onnodig beperkt. Maar een standaardoplossing met een laag betrouwbaarheidsniveau werkt ook niet. Die kan namelijk aanzienlijke veiligheidsrisico's met zich mee brengen. Vgl. Forum Standaardisatie, Een handreiking voor Overheidsorganisaties Forum Standaardisatie, Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, april 2017 blz. 8.
[4] Het voorstel voor de Wet digitale overheid vormt een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op verschillende niveaus en is in behandeling in de Eerste Kamer (Kamerstukken 34 972).
[5] Toelichting, blz. 8.
[6] Vgl. met name artikel 8 van Verordening 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en Uitvoeringsverordening 2015/1502 van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014. In artikel 2 van het concept en de bijlage daarbij wordt bepaald welk betrouwbaarheidsniveau voor een dienst van toepassing is, gelet op onder meer de aard van de persoonsgegevens.
[7] Aldus: Forum Standaardisatie, Een handreiking voor Overheidsorganisaties Forum Standaardisatie, Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, april 2017, blz. 24. Volgens https://www.digitaleoverheid.nl/nieuws/expert-opinion-publieke-authenticatie/ vallen DigiD Basis als DigiD Midden binnen eIDAS Laag, terwijl veeltransacties bij de overheid het niveau Substantieel vragen. Vgl. voorts de Privacy-visie van het ministerie van BZK van 10 december 2018, blz. 16, alsmede https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=176620999.

niveau 'substantieel' is tweefactorauthenticatie vereist en er moet sprake zijn van dynamische authenticatie: de cryptografische gegevens voor de authenticatie veranderen bij ieder gebruik, zoals bij tokens van banken. Voor niveau 'hoog' gelden de eisen voor substantieel en bovendien moet het middel goed beschermd zijn tegen misbruik door anderen, zoals een cryptografisch token, dat ook nog een PIN-code vereist.[8]

Advies

1. Hybride karakter

Volgens de toelichting is de voorgestelde regeling 'normatiever dan de – veeleer adviserende – Handreiking betrouwbaarheidsniveaus en daarmee een meer dwingende opvolger van de Handreiking betrouwbaarheidsniveaus voor digitale dienstverlening.'[9] Hiervoor is gekozen omdat met de bovenliggende wet wordt toegewerkt naar harmonisatie en standaardisatie van het veilig en betrouwbaar inloggen bij de overheid.

Het concept bevat een bijlage met een afwegingskader. De factoren, op basis waarvan het betrouwbaarheidsniveau moet worden bepaald, vormen volgens de toelichting houvast waarmee dienstverleners hun weg moeten vinden. Het concept bevat geen afvinklijst, maar richtsnoeren waarmee de desbetreffende organisatie aan de slag kan om de eigen diensten te classificeren naar betrouwbaarheidsniveau, aldus de toelichting. Van belang daarbij is dat een beredeneerde afweging wordt gemaakt. Een dergelijke ruimte voor eigen inschatting is bijvoorbeeld nodig, omdat in de praktijk bij het gebruik van open tekstvakken niet altijd op voorhand duidelijk is welke gegevens door de gebruiker worden ingegeven, aldus de toelichting.[10]

De AP merkt op dat het concept een hybride karakter heeft: enerzijds normatief en dwingend en anderzijds een kader voor dienstverleners zelf voor het maken van een beredeneerde afweging. Enerzijds schrijft artikel 2 voor dat een dienstverlener bepaalt dat voor een elektronische dienst authenticatie op betrouwbaarheidsniveau 'hoog' vereist is ´indien één van de in bijlage 2 bij deze regeling genoemde criteria in de kolom hoog op die dienst van toepassing is. Anders dan in de toelichting is gesteld, heeft deze bepaling bij uitstek het karakter van een afvinklijst.

Volgens de Privacy-visie van 10 december 2018 van de minister van BZK dient in de komende jaren DigiD te worden verbreed, waarbij de strategie is om de groep rechthebbenden op DigiD te verbreden en ervoor te zorgen dat meer mensen DigiD op het betrouwbaarheidsniveau 'substantieel' gaan gebruiken. Ook zal DigiD op betrouwbaarheidsniveau 'hoog' worden aange

[8] Bovendien moet de gebruiker bij de identiteitsverificatie bij niveau 'hoog' in aanvulling op de eisen bij niveau 'substantieel' ten minste eenmaal fysiek verschijnen. Vgl. Forum Standaardisatie, Een handreiking voor Overheidsorganisaties Forum Standaardisatie, Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, april 2017 blz. 24.

[9] Een handreiking voor Overheidsorganisaties Forum Standaardisatie, Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, april 2017, zie https://www.forumstandaardisatie.nl/nieuws/nieuwe-versie-handreikingbetrouwbaarheidsniveaus, voor de laatste versie.

[10] Toelichting, blz. 8.

Anderzijds voorzien de artikelen 3 en 4 in risicoverlagende factoren[11] en risicoverhogende factoren. De factoren op grond waarvan in artikel 2 tot een lager niveau kan worden gekomen, zijn daarbij zodanig ruim omschreven dat de vraag is of daarmee een veiliger toegang en meer eenduidigheid wordt bewerkstelligd zoals de regeling beoogt. Zo kan voor een lager niveau worden gekozen 'indien het bestuursorgaan of de aangewezen organisatie later in het proces herstelmaatregelen neemt of indien bij het inloggen alleen informatie aan de instelling beschikbaar wordt gesteld.'

De AVG schrijft voor dat een passend beveiligingsniveau voor het verwerken van persoonsgegevens moet worden gewaarborgd.[12] Gelet op het voorgaande adviseert de AP in de toelichting nader in te gaan op het hybride karakter van het concept in het licht van de doelstellingen van de ontwerpregeling en de ervaringen met de huidige handreiking, dan wel, zo nodig het concept aan te passen. Tevens adviseert de AP daarbij te voorzien in adequate advisering over de regeling van dienstverleners bij het maken van de afweging tot classificatie van de eigen diensten.[13]

2. Persoonsgegevens die vallen binnen het betrouwbaarheidsniveau 'hoog'

Volgens het concept gaat het hierbij om persoonsgegevens die stigmatiserend kunnen werken, reputatieschade kunnen opleveren, schade kunnen opleveren aan de gezondheid, of chanteerbaarheid kunnen opleveren of gegevens die onder het medisch beroepsgeheim vallen.[14] De toelichting stelt over het betrouwbaarheidsniveau 'hoog':[15]

'In deze categorie gaat het om persoonsgegevens of persoonsgegevens die bijzonder van aard kunnen zijn en een hoog risico vormen voor de persoon in kwestie indien deze gegevens in verkeerde handen vallen. Dit kan stigmatiserend werken, uitsluiting en/of reputatieschade opleveren, schade opleveren aan de gezondheid, (identiteits)fraude bewerkstelligen, ernstig misbruik of oneigenlijk gebruik van de betreffende dienst opleveren of de betrokkene chantabel maken. Strafrechtelijke gegevens met een dergelijk hoog risico vallen hieronder, alsmede gegevens over werkprestaties of relatieproblemen.
Om te bepalen of iets stigmatiserend kan zijn of reputatieschade oplevert, kan als maatstaf worden gebruikt dat deze categorie is voorbehouden aan de gevallen waarin het afbreukrisico zo groot is voor de betrokkene(n) dat deelname aan de maatschappij bijna onmogelijk is. Te denken valt aan de volgende voorbeelden:

[11] Artikel 3 (risicoverlagende factoren) luidt: Onverminderd de toepasselijkheid van wettelijke voorschriften kan, in afwijking van artikel 2, tweede en derde lid, een bestuursorgaan of aangewezen organisatie voor een elektronische dienst authenticatie op een naastlager betrouwbaarheidsniveau vaststellen, indien: a. het proces van toegangsverlening voorziet in een adequate aanvullende technische of fysieke controle op de authenticiteit van de gebruiker van het identificatiemiddel na het moment waarop daarmee voor de eerste keer voor de desbetreffende dienst een authenticatie is uitgevoerd, b. bij het inloggen slechts informatie aan het bestuursorgaan of de aangewezen organisatie ter beschikking wordt gesteld, of c. het bestuursorgaan of de aangewezen organisatie later in het proces herstelmaatregelen neemt.
[12] Artikel 5, eerste lid, onder f, bepaalt dat persoonsgegevens door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").
[13] Vgl. toelichting, blz. 9 en bijv. de 'regelhulp' bij de huidige handreiking https://regelhulpenvoorbedrijven.nl/betrouwbaarheiddigitaledienstverlening/.
[14] Zie de bijlage bij artikel 2 van het concept.
[15] Toelichting, blz. 13.

Bijzondere gegevens: gegevens over geestelijke gezondheidszorg, gokverslaving, alcoholverslaving etc. Strafrechtelijke gegevens: zaken zoals zedenmisdrijven, of gevallen waarin het identificatie van een dader betreft.´

In het licht van het beginsel uit de AVG dat een passend beveiligingsniveau voor het verwerken van persoonsgegevens moet worden gewaarborgd,[16] heeft de AP de volgende opmerkingen bij het classificeren van de voorgestelde persoonsgegevens onder betrouwbaarheidsniveau 'hoog'.

a. Te strenge en onvolledige maatstaf

De AP acht de in de toelichting voorgestelde maatstaf voor stigmatisering of reputatieschade, dat 'voor betrokkene deelname aan de maatschappij bijna onmogelijk is', te streng. In overwegingen 75 tot en met 78 van de AVG wordt nader ingegaan op het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen dat kan voortvloeien uit persoonsgegevensverwerking.[17] Daarbij wordt onder meer reputatieschade genoemd, maar niet een risico op zodanige schade dat 'voor betrokkene deelname aan de maatschappij nagenoeg onmogelijk is'.

Reputatieschade kan zich namelijk in verschillende gradaties voordoen en het niveau 'hoog' kan zijn gerechtvaardigd in gevallen zonder een zodanig afbreukrisico voor betrokkene dat 'deelname aan de maatschappij nagenoeg onmogelijk' is. Welbeschouwd is er nooit een andere keuze voor betrokkene dan deelname aan de maatschappij, waardoor het niveau 'hoog' nagenoeg nooit wordt bereikt. Dat zou betekenen dat bijna nooit sprake zal zijn van persoonsgegevens die vallen onder het niveau 'hoog' terwijl er daarbij wel een kans op reputatieschade bestaat. In zoverre is de voorgestelde maatstaf te streng. Daarnaast is het risico op stigmatisering of reputatieschade mede afhankelijk van de taak en

[16] Artikel 5, eerste lid, onder f, bepaalt dat persoonsgegevens door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

[17] Overweging 75 luidt: Het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen kan voortvloeien uit persoonsgegevensverwerking die kan resulteren in ernstige lichamelijke, materiële of immateriële schade, met name: waar de verwerking kan leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, ongeoorloofde ongedaanmaking van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel; wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen; wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen; wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken; wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen. Overweging 76 luidt: De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking. Het risico moet worden bepaald op basis van een objectieve beoordeling en vastgesteld moet worden of de verwerking gepaard gaat met een risico of een hoog risico.

maatschappelijke positie van betrokkene, zoals de status van een publiek figuur.[18] Niet blijkt dat hiermee in voorkomende gevallen rekening wordt gehouden.[19]

Verder wordt in de bijlage gesproken over 'ernstig misbruik of oneigenlijk gebruik van de overheidsdienst'. Afgezien van de vraag wanneer daarvan sprake is, sluit het risico van oneigenlijk gebruik *van de overheidsdienst* niet goed aan op de maatstaf van het risico dat deelname aan de maatschappij voor *betrokkene* nagenoeg onmogelijk wordt en bij de risico's *voor natuurlijke personen* uit de AVG.

Bovendien is in de overwegingen bij de AVG *de omvang* van de verwerking van bijzondere persoonsgegevens relevant voor aanname van een 'hoog risico'. Het verwerken van bijzondere persoonsgegevens (onder het regime 'substantieel') kan zodoende toch als 'hoog' moeten worden aangemerkt vanwege het grote aantal persoonsgegevens van een persoon waartoe toegang wordt verkregen, zoals een compleet medisch dossier, of vanwege de toegang tot slechts enkele persoonsgegevens maar van heel veel verschillende personen.[20] In het concept is de grootschalige omvang wel uitdrukkelijk opgenomen bij betrouwbaarheidsniveau 'substantieel', maar niet bij 'hoog'. Bovendien wordt niet uitgelegd waarop de grootschalige omvang betrekking heeft.[21]

Ten slotte worden in de genoemde overwegingen bij de AVG nog een aantal andere aspecten genoemd voor aanname van een hoog risico die relevant kunnen zijn, met name de omstandigheid dat het gaat om kwetsbare personen als kinderen of wanneer personen rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen. Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, bijv. een rechtsgevolg betreffen, is ook de impact van verlies of onrechtmatige verwerking groter.[22] Het doel van de verwerking, de impact voor de rechten en vrijheden van betrokkene en de kwetsbare positie van betrokkene zijn echter als zodanig niet uitdrukkelijk meegenomen in het voorgestelde artikel 2 en de bijlage.[23]

Gelet op het voorgaande adviseert de AP het concept zo mogelijk aan te passen op basis van overwegingen 75 en 76 bij de AVG, voor zover relevant.

b. Onduidelijke onderscheiden

[18] Enerzijds mag van publieke figuren, zoals bekende politici, volgens het Hof voor de Rechten van de Mens worden verwacht dat zij zich meer laten welgevallen dan een gemiddelde burger. Anderzijds is het afbreukrisico voor publieke figuren zoals politici ook groot, vanuit het adagium 'hoge bomen vangen veel wind'.
[19] Weliswaar bevat artikel 4 van het concept de mogelijkheid van risico verhogende factoren, maar die hebben betrekking op 'de aard van de dienst', terwijl het in het voorbeeld gaat om de status van betrokkene.
[20] Vgl. Privacycare – PBLQ, Onderzoek betrouwbaarheidsniveau patiëntenauthenticatie bij elektronische gegevensuitwisseling in de zorg, mei 2016, blz. 35.
[21] De AVG bevat een aantal verplichtingen voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken. De AP vult 'grootschalige gegevensverwerking' voor de zorg nader in.
[22] Vgl. ook de handreiking voor Overheidsorganisaties Forum Standaardisatie, Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, april 2017.
[23] Weliswaar wordt in artikel 4 ´de aard van de dienst´ vermeld als risicoverhogende factor.

Daarnaast is naar het oordeel van de AP het onderscheid tussen het niveau 'hoog' en 'substantieel' onvoldoende duidelijk voor een adequate en consistente toepassing in de praktijk. De bijlage bij de conceptregeling geeft aan dat bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard onder 'substantieel' vallen.[24] Bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard kunnen naar het oordeel van de AP echter vaak leiden tot stigmatisering of uitsluiting. Dan vallen zij onder de classificatie hoog, zoals ook volgt uit de genoemde toelichting. Maar bijzondere en strafrechtelijke gegevens worden echter niet uitdrukkelijk genoemd in de bijlage bij het niveau 'hoog', in geval zij tot stigmatisering of reputatieschade kunnen leiden.

Opvallend in dit verband is dat een 'reëel risico' op 'identiteitsfraude' in het concept wordt geclassificeerd onder niveau 'substantieel', terwijl in de toelichting onder 'hoog' is vermeld 'het bewerkstelligen van identiteitsfraude als de gegevens in verkeerde handen vallen'. Bovendien is onder 'laag' opgenomen indien er 'geen of nauwelijks risico op identiteitsfraude' is.[25] In de eerste plaats is het begrip identiteitsfraude in het concept of toelichting niet omschreven, evenmin als een 'reëel risico' daarop. Fraude waarbij iemand gebruik maakt van een 'gestolen identiteit' gaat veelal gepaard met een hoge impact voor betrokkene, met name omdat betrokkene zich veel tijd en moeite moet getroosten om de zaak recht te trekken, zodat niveau 'hoog' naar het oordeel van de AP snel gerechtvaardigd zal zijn, ook al is het risico dat die fraude zich daadwerkelijk voordoet wellicht niet hoog.

Gelet op het voorgaande adviseert de AP om het criterium voor betrouwbaarheidsniveau 'hoog' te verduidelijken, primair door strafrechtelijke gegevens en bijzondere persoonsgegevens aan te merken als 'hoog' in plaats van 'substantieel'. Indien dat voor de praktijk door dienstverleners of burgers niet opportuun of haalbaar is, adviseert de AP in het concept een concreter onderscheid aan te brengen (bijvoorbeeld tussen overtredingen en misdrijven of onder de categorie 'hoog' te vatten misdrijven waarvoor voorlopige hechtenis is toegelaten of misdrijven die een 'ernstige inbreuk op de rechtsorde opleveren' in de zin van het Wetboek van Strafvordering) en in de toelichting daarbij nader in gaan op praktische voorbeelden.[26]
Daarnaast adviseert de AP een reëel risico op identiteitsfraude te verduidelijken en te classificeren onder het betrouwbaarheidsniveau ´hoog´.

[24] Gegevens die in beginsel zijn geclassificeerd op niveau 'substantieel' zijn: Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden. Bij bijzondere categorieën van persoonsgegevens worden persoonsgegevens verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Ook de verwerking van genetische gegevens, biometrische gegevens ter identificatie van een persoon alsmede gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid (art. 9 lid 1 AVG) zijn bijzondere persoonsgegevens (Toelichting, blz. 12).
[25] "De gevolgen voor degene wiens identiteit wordt misbruikt zijn weliswaar vervelend, maar leiden niet tot gedwongen aanpassing van activiteiten of welstandsniveau kan voor classificering van de dienst volstaan worden met betrouwbaarheidsniveau laag. Richtsnoer is dat de directe schade per geval voor burgers lager is dan €1000,-."
[26] Nota bene: In de huidige handreiking betrouwbaarheidsniveaus voor digitale dienstverlening is een ´aangifte van lichte delicten` geschaard onder niveau 'laag', blz. 41. Het daarin genoemde criterium van 'lichte delicten' is niet alleen onduidelijk, maar bovendien niet in overeenstemming met de eisen van het Besluit digitale stukken strafvordering dat tweefactorauthenticatie vereist voor elektronische aangifte.

c. Burgerservicenummer (hierna: BSN)

In de toelichting is opgemerkt dat het BSN in combinatie met andere persoonsgegevens kan leiden tot reputatieschade en in dat geval de classificatie 'hoog' is gerechtvaardigd. Dit blijkt echter niet uit de regeling zelf.

Zoals de AP in haar adviezen benadrukt is het BSN een uniek persoonsnummer dat gelet op de mogelijkheden van koppeling van gegevensbestanden, bijzondere risico's voor de bescherming van de persoonlijke levenssfeer meebrengt met mogelijk ernstige gevolgen voor de betrokkene.[27] Ook kan het sturen van een vervalste factuur met de vermelding van het juiste BSN van betrokkene een hogere 'betrouwbaarheid' verschaffen waardoor betrokkene sneller de factuur voldoet. Bovendien is ook in de huidige handreiking Betrouwbaarheidsniveaus voor digitale dienstverlening het BSN in combinatie met andere persoonsgegevens uitdrukkelijk als criterium opgenomen voor hoog terwijl de doelstelling is om het concept normatiever te maken dan de Handreiking.[28]

Gelet op het voorgaande adviseert de AP de inzage in het BSN in combinatie met andere persoonsgegevens die kunnen leiden tot reputatieschade in de regeling zelf te classificeren onder betrouwbaarheidsniveau 'hoog'.

3. Gegevens van strafrechtelijke aard in de zin van de Uitvoeringswet AVG

In de toelichting is gesteld:

"De persoonsgegevens inzake een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag waren in de Wet bescherming persoonsgegevens op één lijn gesteld met de andere persoonsgegevens van strafrechtelijke aard en die lijn is voortgezet in de UAVG (de AVG biedt die ruimte)."[29]

De AP wijst op het recente arrest van het Gerechtshof Den Haag waarin het Gerechtshof bepaalt dat een door een civiele rechter opgelegd contactverbod niet kan worden aangemerkt als een persoonsgegeven betreffende strafrechtelijke veroordeling en strafbare feiten in de zin van artikel 10 AVG:[30]

"Een door de civiele rechter opgelegd contactverbod kan, anders dan Appellant betoogt, niet worden aangemerkt als een persoonsgegeven betreffende strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 10 AVG. De verwijzing naar het strafrecht impliceert dat het tenminste moet gaan om maatregelen met een punitief karakter. Een

[27] Vgl. laatstelijk het advies van de AP van 19 december 2019 inzake toegang tot gegevens voor poortwachters bij het voorkomen van witwassen, met verwijzingen naar eerdere adviezen.
[28] Vgl. ook de toelichting bij het wetsvoorstel: "Naar verwachting zal dienstverlening, waarvoor het BSN wordt gebruikt, *over het algemeen op betrouwbaarheidsniveau substantieel of hoog worden geclassificeerd* aan de hand van de ministeriële regeling zoals bedoeld in artikel 6, tweede lid, van dit wetsvoorstel. In het proces van totstandkoming van deze ministeriële regeling zal duidelijker worden in welke mate er diensten, waarvoor het BSN wordt gebruikt, op betrouwbaarheidsniveau laag overblijven. " (Kamerstukken II 2017/18, 34 972, nr. 3, blz. 73) (curs, AP). De keuze in het concept spoort niet met deze te verwachten algemene regel.
[29] Toelichting, blz. 13.
[30] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2019:3539

civielrechtelijk contactverbod heeft geen punitief karakter. Het feit dat de Nederlandse wetgever in artikel 1 van de UAVG heeft bepaald dat onder het begrip persoonsgegevens van strafrechtelijke aard mede vallen persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag maakt dat niet anders. Het begrip persoonsgegeven betreffende strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 10 AVG is een Unierechtelijk begrip dat autonoom moet worden uitgelegd. De AVG geeft de lidstaten niet de mogelijkheid een eigen, ruimere invulling te geven aan dat begrip."

Gelet op voornoemd arrest adviseert de AP bovenstaande passage uit de toelichting te actualiseren.

4. Tijdelijk toestaan van het lagere niveau

Op grond van artikel 6, vierde lid, van de wet kan voor een bepaalde periode authenticatie met een aangewezen middel met een lager betrouwbaarheidsniveau worden toegestaan dan het niveau dat voor die dienst is bepaald.[31] Dit is uitgewerkt in het voorgestelde artikel 6 van het concept waarin wordt voorzien in een termijn tot twee jaar na de inwerkingtreding van de regeling.[32] Over de voorgestelde bepaling heeft de AP twee opmerkingen.

a. Termijn van twee jaar na inwerkingtreding

De toelichting op het concept stelt:

"Onzeker is of het middel tijdig door voldoende afnemers van elektronische diensten zal (kunnen) worden gebruikt. Dat is afhankelijk van de bereidheid van burgers/bedrijven om een dergelijk middel te verwerven en van het tempo waarop dienstverleners op de benodigde infrastructuur (gdi-voorzieningen) kunnen worden aangesloten. Zolang de beschikbaarheid en dekkingsgraad van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog nog niet op een adequaat niveau zijn, zal het toepassen van de in deze regeling vervatte regels over betrouwbaarheidsniveaus ertoe leiden dat toegang tot elektronische dienstverlening onevenredig wordt beperkt. Het is niet opportuun om dienstverleners te verplichten tot het hanteren van een bepaald betrouwbaarheidsniveau, als er door onvoldoende brede beschikbaarheid van inlogmiddelen eenvoudigweg niet aan kan worden voldaan."

Tevens wordt gesteld:

[31] Artikel 6, vierde lid, van het wetsvoorstel luidt: 4. Bij ministeriële regeling kunnen regels worden gesteld over het gedurende een bepaalde periode toestaan van toegang tot diensten, waarvoor volgens de krachtens het tweede lid gestelde regels authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, met gebruikmaking van door Onze Minister aangewezen identificatiemiddelen die het betrouwbaarheidsniveau laag respectievelijk substantieel hebben. Voor een identificatiemiddel op betrouwbaarheidsniveau laag geldt dat sprake moet zijn van ten minste twee authenticatiefactoren zoals bedoeld in de eIDAS-verordening.

[32] Het voorgestelde artikel 6 van het concept luidt: Onverminderd de toepasselijkheid van wettelijke voorschriften kan een bestuursorgaan of aangewezen organisatie besluiten voor een elektronische dienst, waarvoor op grond van artikel 2 authenticatie op betrouwbaarheidsniveau hoog respectievelijk substantieel benodigd is, *tot twee jaar na inwerkingtreding van deze regeling* voor toegang tot die dienst tevens het gebruik van een toegelaten of erkend middel op betrouwbaarheidsniveau substantieel respectievelijk een middel op niveau laag toe te staan.

"Het is de verwachting dat twee jaar na inwerkingtreding van deze regeling sprake zal zijn van voldoende beschikbaarheid en dekkingsgraad van (publieke en private) inlogmiddelen. Mocht dit (veel) eerder het geval zijn, dan zal worden bezien of het opportuun is om de tijdelijke uitzonderingsmogelijkheid te schrappen. Mocht dit onverhoopt later zijn, dan zal worden bezien of het opportuun is om de termijn te verlengen."[33]

De AP betwijfelt of deze termijn van twee jaar nodig en passend is gelet op de huidige stand van de techniek en vooral de snelle technische ontwikkelingen wat betreft inlogmiddelen.[34] Een onnodig ruime uitzonderingsmogelijkheid kan immers de ontwikkeling naar een veiligere toegang vertragen. Daarnaast valt op in de toelichting niet wordt vermeld wanneer sprake zal zijn van een 'adequate dekking en beschikbaarheid' en wat de actuele stand van zaken is.

Voorts valt op in de bepaling zelf geen materiële voorwaarde of beperking is aangebracht, met name de eis uit de toelichting dat geen sprake is van adequate beschikbaarheid en dekkingsgraad van identificatiemiddelen op betrouwbaarheidsniveaus 'substantieel' en 'hoog'.

De AP adviseert gelet op het voorgaande in de toelichting nader in te gaan op de noodzaak van een termijn van twee jaar en de stand van zaken en verwachtingen aangaande de eis van adequate dekking en beschikbaarheid. Daarnaast adviseert de AP om zo nodig en zo mogelijk een materiële voorwaarde of beperking in het voorgestelde artikel 6 van het concept aan te brengen.

b. Uitzonderingen op het tijdelijk toestaan van een lager niveau

In verband met het voorgaande wijst de AP met name op de memorie van toelichting bij het wetsvoorstel voor de Wdo waar is opgemerkt:

"Bij ministeriële regeling kunnen bepaalde (nieuwe) vormen van dienstverlening op niveau hoog worden uitgesloten van het overgangsrecht, bijvoorbeeld omdat dit de ontwikkeling van die diensten zou kunnen belemmeren of wegens de hoge risico's van het toelaten van identificatiemiddelen op het lagere niveau." [35]

Anders dan op grond van het bovenstaande zou worden verwacht, zijn in het concept echter niet bepaalde vormen van dienstverlening uitgesloten van de mogelijkheid van een tijdelijk lager niveau. Juist voor zover het daarbij ook gaat om bijv. de meest gevoelige gegevens, is dit waarschijnlijk niet passend.

De AP adviseert dit toe te lichten, dan wel, zo nodig het concept aan te passen.

5. Gegevensbeschermingseffectbeoordeling

[33] Toelichting. blz. 19.
[34] Vgl. de brief van de Staatssecretaris van BZK aan de Tweede Kamer van 28 september 2020, 26 643, nr. 711, en van de Minister van BZK aan de Tweede Kamer van 29 januari 2020, 26 643, nr. 663, alsmede https://tweakers.net/nieuws/162884/bijna-helft-digid-gebruikers-heeft-app-geactiveerd-om-veiliger-in-te-loggen.html en https://tweakers.net/nieuws/162884/bijna-helft-digid-gebruikers-heeft-app-geactiveerd-om-veiliger-in-te-loggen.html.
[35] Vgl. Kamerstukken II 2017/18, 34 972, nr. 3, blz. 71.

De AVG schrijft voor verwerkingsverantwoordelijken een GEB voor wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[36] Gelet op het "Model GEB Rijksdienst" moet een GEB worden uitgevoerd bij de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien en bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.[37] Bij het voorliggende concept is geen GEB uitgevoerd; dat is overigens wel het geval bij het voorstel voor de Wdo.

Naar het oordeel van de AP vloeien uit het concept verwerkingen van persoonsgegevens voort omdat de regeling ziet op eisen voor een veilige toegang tot het digitaal inzien en eventueel zelfs muteren van persoonsgegevens. Bovendien gaat het daarbij om persoonsgegevens met hoge risico's voor betrokkenen, zelfs het risico dat deelname aan de maatschappij voor betrokkene nagenoeg onmogelijk is. Voorts kunnen de privacy-risico's, mede in verband met de voortschrijdende techniek, zich in de loop van de tijd wijzigen.

Gelet op het voorgaande adviseert de AP om een GEB uit te voeren met betrekking tot de verwerkingen die uit het concept voortvloeien en deze, zo nodig, periodiek te herzien.

Openbaarmaking van het concept

De AP is voornemens dit advies openbaar te maken op de website www.autoriteitpersoonsgegevens.nl zodra de tekst van het gewijzigde concept openbaar is. De AP verneemt graag het moment waarop openbaarmaking wordt verwacht, zodra dit bekend is.

Hoogachtend,
Autoriteit Persoonsgegevens,

drs. C.E. Mur
Bestuurslid

[36] Volgens artikel 35, derde lid, AVG is een GEB, voor zover relevant, met name vereist in de volgende gevallen: a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen; b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

[37] Vgl. https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia, blz. 6.