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 BZK
drs. R.W. Knops
Turfmarkt 147
2511 DP Den Haag

Datum	Ons kenmerk	Uw brief van
17 september 2019	z2019-15241	26 juni 2019

Uw kenmerk
2019-0000319070

Onderwerp
Advies conceptbesluit bedrijfs- en organisatiemiddel Wdo

Geachte heer Knops,

Bij brief van 26 juni 2019 is de Autoriteit Persoonsgegevens (hierna: AP) gevraagd op grond van het bepaalde in artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (hierna: AVG) te adviseren over het conceptbesluit houdende vaststelling van regels inzake de erkenning van bedrijfs- en organisatiemiddelen en bijbehorende diensten (conceptbesluit bedrijfs- en organisatiemiddel Wdo)[1]; (hierna: het concept).
De AP heeft de volgende opmerkingen bij het concept en adviseert daarmee rekening te houden.

Strekking van het concept

Het concept geeft een nadere uitwerking aan het stelsel van 'bedrijfs- en organisatiemiddelen' op grond van het voorstel voor de Wet digitale overheid (hierna: Wdo).[2] Het gaat hierbij -kort gezegd- om identificatiemiddelen om bedrijven toegang te verlenen tot digitale dienstverlening door de overheid.[3] Het concept bevat regels over de erkenning van private partijen die deze elektronische identificatiemiddelen leveren. Opmerking verdient dat in het ontwerpbesluit digitale overheid wordt geregeld welke

[1] Terzijde: De citeertitel zal duidelijker zijn als 'Wdo' voluit wordt geschreven omdat de afkorting 'Wdo' niet voor een ieder bekend zal zijn. Vgl. ook aanwijzing 4. 25, eerste lid, van de Aanwijzingen voor de regelgeving: Een citeertitel bevat geen afkortingen tenzij dit onvermijdelijk is.
[2] Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), Kamerstukken 34 972.
[3] In artikel 5 van het voorstel voor de wet digitale overheid is een definitie van bedrijfs- en organisatiemiddel opgenomen.

persoonsgegevens door partijen in het kader van bedrijfs- en organisatiemiddelen worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard.[4]

Advies

Delegatie

Het valt de AP op dat veel wordt gedelegeerd naar een ministeriële regeling, terwijl de toelichting daarover veelal summier is. Paragraaf 7 van de nota van toelichting bevat een lijst met dertien onderwerpen die worden geregeld in een ministeriële regeling. Het gaat hierbij veelal om regels die de beveiliging van persoonsgegevens betreffen.

Als eerste is vermeld: 'artikel 2, derde lid: algemene eisen erkende dienst.' Artikel 2, derde lid, bepaalt dat een erkende dienst voldoet aan de eisen van beheer die zijn opgenomen in onderdeel 2.4 van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 en aan de bij ministeriële regeling dienaangaande gestelde regels.[5] Paragraaf 2.4. van de uitvoeringsverordening ziet op 'beheer en organisatie van de informatiebeveiliging'.

Het is de AP niet duidelijk om wat voor nadere regels het hier gaat, wat de grondslag is voor deze delegatie en waarom delegatie hier passend is.[6] Delegatie van regelgevende bevoegdheid aan een minister wordt namelijk beperkt tot voorschriften van administratieve aard, uitwerking van details van een regeling, voorschriften die dikwijls wijziging behoeven en voorschriften waarvan te voorzien is dat zij mogelijk met grote spoed moeten worden vastgesteld.[7]

Gelet op het voorgaande adviseert de AP om de keuze voor delegatie van de diverse onderwerpen, alsmede de aard van de regels en de grondslag nader te toe te lichten, dan wel om, zo nodig, het concept aan te passen.

Betrouwbaarheidsniveaus

In de nota van toelichting is gesteld dat de eisen uit de eIDAS-verordening 910/2014 en de daarop gebaseerde Uitvoeringsverordening 2015/1502[8] de basis vormen voor het concept. Deze eisen betreffen

[4] Artikel 5c van het ontwerpbesluit digitale overheid regelt welke persoonsgegevens erkende diensten verwerken voor de werking van het bedrijfs- en organisatiemiddel. Vgl. ook de Nota van toelichting bij het ontwerpbesluit digitale overheid, p. 16.
[5] Artikel 3 bepaalt dat bij ministeriële regeling aanvullende eisen kunnen worden of worden gesteld. Volgens de toelichting op deze bepaling biedt artikel 3 een grondslag voor het stellen van eisen die aanvullend zijn aan de eisen uit de Uitvoeringsverordening en de ministeriële regeling.
[6] Uitvoeringsverordening (EU) 2015/1502 lijkt wel ruimte te bieden voor aanvullende eisen nu het volgens de titel gaat om *minimale* technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, derde lid, van Verordening (EU) 910/2014. Aanvullende nationale regelgeving is bovendien noodzakelijk voor de aanvraag en uitgifte van Nederlandse publieke identificatiemiddelen.
[7] Vgl. ook Aanwijzing 2.24 van de Aanwijzingen voor de regelgeving. Delegatie van regelgevende bevoegdheid aan een minister is ook toegestaan indien het gaat om het verwerken in de Nederlandse wetgeving van internationale regelingen die de Nederlandse wetgever, behoudens op ondergeschikte punten, geen ruimte laten voor het maken van keuzen van beleidsinhoudelijke aard.
[8] eIDAS-Verordening (EU) 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties en Uitvoeringsverordening 2015/1502 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, derde lid, van Verordening 910/2014.

onder andere de betrouwbaarheid van elektronische identificatiemiddelen op de betrouwbaarheidsniveaus laag, substantieel en hoog met het oog op wederzijdse erkenning en grensoverschrijdende elektronische authenticatie. In het concept vormen de eisen benoemd voor 'betrouwbaarheidsniveau laag' de basis en deze zijn waar nodig met aanvullende eisen uitgebreid voor niveau 'substantieel' of 'hoog', aldus de nota van toelichting.[9]

De AP begrijpt dat om redenen van veiligheid, betrouwbaarheid en om grensoverschrijdend gebruik van erkende diensten mogelijk te maken de eisen uit de verordeningen de basis van het concept vormen.[10] In de memorie van toelichting bij het voorstel voor de Wet digitale overheid is evenwel gesteld dat vanwege de tendens om hogere betrouwbaarheidsniveaus te vereisen, bedrijven een inlogmiddel op het vrij hoge niveau 3 moeten aanschaffen.[11] De vraag is hoe het gekozen uitgangspunt van betrouwbaarheidsniveau 'laag' zich tot deze tendens verhoudt.

De AP adviseert in de nota van toelichting in de gaan op de verhouding van het gekozen betrouwbaarheidsniveau 'laag' als basis tot de tendens om hogere betrouwbaarheidsniveaus te eisen.

Hotspots

Volgens de nota van toelichting bestaat het stelsel van bedrijfs- en organisatiemiddelen uit een netwerk van erkende private partijen die één of meerdere diensten aanbieden ten behoeve van de goede werking van het bedrijfs- en organisatiemiddel en de goede toegang met dat middel tot elektronische dienstverlening. Deze diensten zijn de middelenuitgever, de authenticatiedienst, de machtigingsdienst en de ontsluitende dienst.
In de toelichting op het voorstel voor de Wet digitale overheid is het uitgangspunt benadrukt van het zoveel mogelijk vermijden van grote concentraties van persoonsgegevens (*hotspots*).[12] Gesteld is dat de uitvoeringsregelgeving zodanig dient te worden ingericht, dat het niet nodig of mogelijk is om identificatie en vertrouwelijke informatie bij één adressaat te beleggen.

In dit verband valt op dat het voorliggende concept het mogelijk maakt dat een erkende middelenuitgever tevens als authenticatiedienst is erkend.[13] De middelenuitgever is verantwoordelijk voor de uitgifte, het beheer en de intrekking van het bedrijfs- en organisatiemiddel waarvoor hij erkend is, alsmede voor het zorgvuldig vastleggen van alle daarvoor geregistreerde gegevens in een administratie.[14] In de toelichting is tevens gesteld dat een partij zich voor alle diensten kan laten erkennen.[15] Volgens de nota van toelichting bij het ontwerpbesluit digitale overheid worden bij overheidsdienstverlening aan bedrijven veel

[9] Toelichting op artikel 2.
[10] Toelichting, par. 1.
[11] Kamerstukken II 2017/18, 34 972, nr. 3, p. 49.
[12] Kamerstukken II 2017/18, 34 972, nr. 3, p. 23. Vgl. ook het advies van de AP van 13 oktober 2017 over het wetsvoorstel Wet generieke digitale infrastructuur, p. 9.
[13] Vgl. uitdrukkelijk artikel 4, derde lid, en artikel 5, tweede lid, van het concept. Vgl. voorts het advies van de AP van 6 juli 2018 bij het conceptbesluit digitale overheid, p. 4/5.
[14] Nota van toelichting, par. 2.
[15] Nota van toelichting, par. 6, tweede alinea.

gebruik(ers)gegevens verwerkt.[16] Een en ander kan naar het oordeel van de AP leiden tot een grote concentratie van persoonsgegevens bij erkende private partijen.[17]

Gelet hierop adviseert de AP om in de nota van toelichting in te gaan op het voorkomen van 'hotspots' van persoonsgegevens bij erkende private partijen in het kader van het concept, meer in het bijzonder op de genoemde cumulatie van erkende middeluitgever en authenticatiedienst, dan wel, zo nodig het concept aan te passen.

Vertrouwelijk behandelen

Artikel 2, onderdeel c, van het concept bevat de eis dat een erkende dienst zorg draagt dat alle gegevens vertrouwelijk worden behandeld. In de toelichting hierop is enkel gesteld dat van belang is dat organisaties hun netwerken 'voldoende beveiligen'.
De AP acht deze toelichting ontoereikend omdat 'voldoende beveiligen' weinig concreet is en te meer omdat 'beheer van de informatiebeveiliging' al onderdeel is van de eisen die zijn opgenomen in onderdeel 2.4 van de bijlage bij de Uitvoeringsverordening die eveneens als eis zijn opgenomen. Bovendien is vertrouwelijk behandelen niet hetzelfde als voldoende beveiligen.[18] Volgens artikel 32 van de AVG moeten maatregelen worden genomen om te zorgen dat op permanente basis de vertrouwelijkheid van de verwerkingssystemen kan worden gegarandeerd.

Gelet op het voorgaande adviseert de AP om in de nota van toelichting in te gaan op concrete maatregelen met het oog op het vertrouwelijk behandelen van de persoonsgegevens, dan wel, zo nodig, het concept aan te passen.

Gezamenlijke verwerkingsverantwoordelijken

In het concept is een samenwerkingsplicht opgenomen tussen en met erkende diensten.[19] Daarover is in de nota van toelichting gesteld:

> "In het geval dat er veranderingen worden doorgevoerd in het netwerk door één of meerdere erkende diensten, is het dan ook van belang dat het netwerk goed blijft werken en met andere versies of implementaties interoperabel blijft. Dat is een gezamenlijke verantwoordelijkheid van de erkende diensten.

[16] Nota van toelichting bij het ontwerpbesluit digitale overheid, p. 16.
[17] Vgl. voorts de Privacyvisie eID van 10 december 2018 van het kabinet, p. 21, waarin het kabinet wijst op het feitelijke risico bij de inzet van private partijen binnen het eID stelsel dat private partijen inzicht verkrijgen in de zaken die burgers (en bedrijven) met de overheid afwikkelen. Het kabinet wenst-voor zover mogelijk- in het ontwerp te zorgen dat partijen niet de beschikking krijgen over persoonsgegevens.
[18] Zo is in artikel 32, eerste lid, van de AVG 'vertrouwelijkheid' (onderdeel b) slechts een van de eisen in het kader van het te treffen beveiligingsniveau.
[19] In artikel 9 is de plicht opgenomen voor erkende diensten om ten behoeve van een betrouwbare toegang van ondernemingen tot elektronische dienstverlening over voorwaarden voor een betrouwbare interoperabiliteit binnen een bepaalde termijn afspraken met elkaar te maken. Deze overeenkomst wordt binnen vier weken toegezonden aan de minister (artikel 9, derde lid). Indien de erkende diensten geen overeenstemming kunnen bereiken over de voorwaarden, kan de minister op verzoek van een erkende dienst een bindende aanwijzing geven (artikel 10, eerste lid, onderdeel c).

> Daarom zal de erkenning een plicht met zich meebrengen om met de andere erkende diensten ten behoeve van de interoperabiliteit samen te werken."[20]

Deze 'gezamenlijke verantwoordelijkheid' van de erkende diensten kan naar het oordeel van de AP worden opgevat als 'gezamenlijke verwerkingsverantwoordelijken' in de zin van de AVG. Dit omdat de erkende diensten gezamenlijk de doeleinden en middelen van de verwerking bepalen.[21] Op grond van artikel 5c van het conceptbesluit digitale overheid valt namelijk aan te nemen dat de erkende diensten tevens verwerkingsverantwoordelijken zijn voor de verwerkingen van de aldaar genoemde persoonsgegevens 'voor een goede werking van het bedrijfs- en organisatiemiddel en voor een goede en veilige toegang met dat middel tot elektronische dienstverlening'.[22]
Daarnaast is de minister van Binnenlandse Zaken en Koninkrijkrelaties verwerkingsverantwoordelijke voor -kort gezegd- het digitale stelsel. Volgens artikel 5, aanhef en onderdeel e, van het voorstel voor de Wet digitale overheid draagt Onze Minister namelijk zorg voor de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur (e) waaronder infrastructuur die het mogelijk maakt het stelsel voor identificatie van ondernemingen en rechtspersonen te beheren.[23]

De AP adviseert de nota van toelichting in bovenbedoelde zin aan te vullen.

Gebruiksvoorwaarden

Artikel 3, derde lid, van het concept bevat als aanvullende eis dat bij ministeriële regeling wordt geregeld welke voorwaarden door een erkend middelenuitgever en een erkende machtigingsdienst in elk geval worden opgenomen in de gebruiksvoorwaarden die zij stellen aan afnemers van hun diensten. De voorwaarden hebben in elk geval betrekking op het voorkomen van verlies, diefstal, misbruik, of verspreiding van het bedrijfs- en organisatiemiddel, aldus artikel 3, derde lid.
Het is de AP niet duidelijk waarom deze aanvullende eis niet tevens geldt voor de overige erkende diensten. Daarnaast valt op dat de toelichting stelt dat in de gebruiksvoorwaarden in elk geval de kosten en de geldigheidsduur van het middel moeten worden opgenomen. Deze onderdelen staan echter niet uitdrukkelijk in de voorgestelde bepaling.

---

[20] Nota van toelichting, par. 4, tweede alinea.
[21] Artikel 26 AVG: Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Vgl. de recente arresten van het Hof van Justitie EU van 5 juni 2018 (Wirtschaftsakademie Schleswig Holstein C-210/16); 10 juli 2018, (Jehodan Todistajat C-25/17) en 29 juli 2019 (Fashion ID C-40/17) waarin het Hof van Justitie EU een ruime uitleg geeft aan het begrip gezamenlijke verwerkingsverantwoordelijkheid. Zo wordt niet vereist dat alle deelnemers die op grond van deze bepaling verantwoordelijk voor zijn eenzelfde verwerking, dat ieder van hen toegang heeft tot de betrokken persoonsgegevens (vgl. C-210/16, par. 69). Ook brengt het bestaan van een gezamenlijke verantwoordelijkheid niet noodzakelijkerwijs een gelijkwaardige verantwoordelijkheid met zich mee van de deelnemers voor de verwerking van persoonsgegevens. De verantwoordelijken kunnen juist in verschillende stadia en in verschillende mate bij de verwerking betrokken zijn, zodat het niveau van verantwoordelijkheid van elk van hen moet worden beoordeeld in het licht van alle relevante omstandigheden van het geval (C-210/16, par. 66).
[22] Artikel 5c van het ontwerpbesluit digitale overheid bepaalt, voor zover relevant, dat een erkende dienst verwerkt voor de werking van het bedrijfs- en organisatiemiddel en goede en veilig toegang met dat middel tot de elektronische dienstverlening de volgende gegevens.

Gelet op het voorgaande adviseert de AP om artikel 3, derde lid, en de toelichting daarop aan te passen.

Meldplicht

Volgens het voorgestelde artikel 8, eerste lid, meldt een erkende dienst onverwijld aan de minister elk incident of elke verstoring waarvan de duur en de gevolgen van zodanige aard zijn dat de betrouwbare toegang van ondernemingen of rechtspersonen tot elektronische dienstverlening op significante wijze in het geding is of dreigt te komen of de continuïteit van de betrouwbare toegang anderszins op significante wijze verstoord wordt of dreigt te worden.[24] Bij ministeriële regeling worden nadere regels gesteld over de incidenten of verstoringen die in elk geval gemeld dienen worden. In de nota van toelichting is gesteld dat een melding in elk geval aan de orde is in geval van incidenten of verstoringen met een verwachte duur van vier uur of meer of waarbij tenminste twee erkende diensten zijn betrokken.
Over deze meldplicht heeft de AP twee opmerkingen in verband met het beginsel uit de AVG om te zorgen voor een passend beveiligingsniveau:[25]

a.Niet is gemotiveerd waarom incidenten of verstoringen met een verwachte duur van minstens vier uur in elk geval moeten worden gemeld. Ook incidenten of verstoringen van een kortere (verwachte) duur dan vier uur en waarbij slechts één dienst is betrokken kunnen in voorkomende gevallen substantiële gevolgen hebben voor een betrouwbare toegang van bedrijven tot elektronische dienstverlening en voor een juiste verwerking van persoonsgegevens. Dit klemt temeer voor zover het gaat om incidenten bij betrouwbaarheidsniveau 'hoog'.

De AP adviseert om met het bovenstaande rekening te houden en hierop in de toelichting in te gaan.

b.In het voorgestelde artikel 8, vijfde lid, is bepaald dat bij ministeriële regeling nadere regels *kunnen* worden gesteld ter invulling van de meldingsplicht. In de nota van toelichting is echter herhaaldelijk gesteld dat het gaat om een plicht om nadere regels te stellen ter invulling van de meldplicht en niet om een mogelijkheid.[26] Bovendien bevat artikel 8, eerste lid, als gemeld, al een plicht om bij ministeriële regeling nadere regels te stellen.

In het licht van het voorgaande adviseert de AP om het voorgestelde artikel 8, vijfde lid, nader toe te lichten dan wel, zo nodig, aan te passen.

Openbaarmaking van het advies

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

[24] Aldus de toelichting op artikel 8, eerste lid.
[25] Vgl. artikel 5, eerste lid, onderdeel f, en artikel 32 AVG. In artikel 32, eerste lid, onderdeel c, AVG wordt gewezen op maatregelen die zien op het vermogen om bij een fysiek of technisch incident de beschikbaarheid en toegang tot de persoonsgegevens tijdig te herstellen.
[26] Vgl. de toelichting op artikel 8, laatste alinea: "Bij ministeriële regeling worden regels gesteld omtrent de in dit artikel genoemde meldingsplichten", alsmede par. 7.

Datum
17 september 2019

Ons kenmerk
z2019-15241

Hoogachtend,
Autoriteit Persoonsgegevens,

Mr. A. Wolfsen
Voorzitter