Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

34 972 Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 46

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 14 mei 2020

De vaste commissie voor Binnenlandse Zaken heeft enkele vragen en opmerkingen voorgelegd aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over de brief van 17 maart 2020 over het ontwerpbesluit digitale overheid (Kamerstuk 34 972, nr. 45).

De vragen en opmerkingen zijn op 7 april 2020 aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 13 mei 2020 zijn de vragen door de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties beantwoord.

De voorzitter van de commissie,
Ziengs

De adjunct-griffier van de commissie,
Hendrickx

kst-34972-46
ISSN 0921 - 7371
's-Gravenhage 2020

Vragen en opmerkingen vanuit de fracties en reactie van de Staatssecretaris

Inhoudsopgave **blz.**

I. Algemeen **2**

1. Inleiding 2
2. Hoofdlijnen 3
3. Verhouding tot andere regelgeving 4
4. Inhoud 5
5. Privacy en verhouding tot algemene verordening gegevensbescherming 10
6. Consultatie 11
7. Evaluatie 11

II Artikelsgewijze toelichting **12**

Nota Bene; aanvulling Besluit **14**

I. Algemeen

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het ontwerpbesluit Digitale overheid. Dit is de eerste uitvoeringsregelgeving op basis van de Wet digitale overheid. Dat wetsvoorstel is onlangs door de Tweede Kamer aanvaard. Graag willen de leden van de VVD-fractie de regering een aantal vragen voorleggen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het ontwerpbesluit houdende wijziging van het Besluit verwerking persoons-gegevens generieke digitale infrastructuur in verband met het stellen van de kaders voor informatieveiligheid en persoonsgegevensverwerking (Besluit digitale overheid). Deze leden hebben daarover enkele vragen.

De leden van de D66-fractie hebben kennisgenomen van het genoemde ont-werpbesluit en willen de regering nog enkele vragen voorleggen. Voor de leden van de D66-fractie is het van groot belang dat informatieveiligheid bij publieke dienstverleners gewaarborgd is.

De leden van de GroenLinks-fractie hebben kennisgenomen van het ontwerpbesluit digitale overheid. Zij hebben hierover een aantal vragen aan de rege-ring. Allereerst begrijpen deze leden dat er niet één AMvB of Ministeriële regeling komt waarin de Wet digitale overheid nader in wordt uitgewerkt. Het voorliggende Ontwerpbesluit is één van de onderliggende regelgevende documenten. Kan de regering in een schematisch overzicht alle onderliggende regelgevende documenten – die voortvloeien uit artikel 4 en artikel 16 van de Wet digitale overheid – weergeven met daarbij wat deze regelingen in hoofdzaak regelen?

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van het Ontwerpbesluit digitale overheid. Zij hebben behoefte aan het stellen van een beperkt aantal vragen.

Graag bedank ik de fracties voor hun bijdrage en ga ik in op de gestelde vragen. Bij de beantwoording is de indeling en volgorde van het verslag aangehouden, met dien verstande dat vergelijkbare vragen zijn samenge-

nomen. U wordt tevens verzocht kennis te nemen van de ingevoegde Nota Bene, waarin wordt ingegaan op een aanvulling van het ontwerpbesluit.

Dit voorstel wijzigt het Besluit verwerking persoonsgegevens gdi, met het oog op de uitwerking van enkele bepalingen van het wetsvoorstel digitale overheid (WDO). De uitwerking betreft de artikelen 4 en 16 WDO, inzake informatiebeveiliging respectievelijk persoonsgegevensverwerking. Ingevolge artikel 25 van het wetsvoorstel wordt het onderhavige besluit aan het parlement voorgelegd.

In reactie op een vraag van de leden van de GroenLinks-fractie is in de bijlage[1] bij dit verslag een overzicht opgenomen van alle onderliggende regelgeving – algemene maatregelen van bestuur en ministeriële regelingen –, de onderwerpen die hierin worden geregeld alsmede de wettelijke grondslag terzake.

2. Hoofdlijnen

De leden van de GroenLinks-fractie vinden het van groot belang dat erkende private partijen effectief worden gecontroleerd aangezien zij potentieel privacygevoelige informatie van burgers in handen kunnen krijgen. De leden hebben gevraagd om nader in te gaan op de vraag hoe controle en handhaving plaatsvindt en of er volgende capaciteit is om effectieve naleving van de wet en onderliggende regels te waarborgen. De leden vragen om daarbij om specifiek in te gaan op de capaciteit van het ministerie en de Autoriteit Persoonsgegevens.

Het belang van een goede omgang met privacygevoelige informatie en effectieve controle daarop deel ik volledig. Ik maak hierover een aantal opmerkingen op hoofdlijnen. De onderhavige AMvB regelt dat de private aanbieders van inlogmiddelen, mits toegelaten/erkend, over de verwerkingsgrondslagen beschikken om de middelen te kunnen aanbieden. De eisen die worden gesteld aan de private aanbieders van inlogmiddelen, inclusief de inrichting van de controle daarop, is onderwerp van separate AMvB's; een AMvB voor de regulering van inlogmiddelen voor burgers (natuurlijke personen) en een AMvB voor inlogmiddelen voor bedrijven (rechtspersonen). Deze AMvB's kennen eveneens een voorhangprocedure en zullen u later dit jaar worden gezonden. Omdat de genoemde vragen zien op de inhoud van die AMvB's ga ik daarop in het onderstaande in algemene zin in.

Voordat partijen worden toegelaten/erkend, wordt getoetst of de door hen aangeboden middelen voldoen aan de eisen voor toelating. Partijen moeten met hun aanvraag aantonen dat zij aan deze eisen voldoen. Onderdeel van het proces is een beoordeling van de wijze waarop het middel in de praktijk functioneert. Daarbij zal worden gewerkt met een systeem van certificering. Partijen die een erkenning aanvragen moeten bij hun aanvraag een conformiteitsbeoordeling van een geaccrediteerde certificerende instelling overleggen. Deze verklaring ondersteunt het erkenningsproces, doordat deze een extra waarborg biedt bij de beoordeling van de aanvraag. De Minister van BZK baseert zich voor het besluit tot erkenning op deze beoordelingen. Wanneer uit de toetsing blijkt dat een partij niet voldoet aan de gestelde eisen, dan wordt deze niet erkend en kan deze geen diensten verlenen. En hoewel controle aan de poort belangrijk is, is het van even groot belang dat erkende aanbieders zich gedurende hun dienstverlening aan de eisen blijven conformeren en daarop gecontroleerd worden. Daarom wordt voorzien in onafhankelijk

[1] Raadpleegbaar via www.tweedekamer.nl.

toezicht, waarbij periodieke controle plaatsvindt. Dit wordt zowel voor burger- als bedrijvenmiddelen belegd bij het Agentschap Telecom (AT), conform de wens van Uw Kamer, zoals verwoord in het amendement terzake bij de behandeling van het bovenliggende wetsvoorstel. Daartoe zullen met AT afspraken worden gemaakt over de benodigde capaciteit. Ook in de toezichtfase wordt gebruik gemaakt van de voordelen die certificering biedt voor het efficiënt inzetten van de beschikbare capaciteit. Voorts is de Autoriteit Persoonsgegevens (AP) belast met toezicht op verwerkingen van persoonsgegevens in het algemeen. De AP is een zelfstandig bestuursorgaan en stelt zelf haar beleidsprioriteiten vast op basis van de haar toegekende capaciteit. De wijze waarop zij die capaciteit inzet en zich specifiek richt op het toezicht op de verwerkingen zoals die plaatsvinden op grond van de onderhavige AMvB bepaalt de AP derhalve zelf.

De leden vroegen voorts op welke wijze burgers straks actief geïnformeerd worden over hun rechten en hoe en of zij eventueel misbruik van hun gegevens kunnen melden en tegengaan. De leden vragen of er wellicht een mogelijkheid is om bij ieder privaat digitaal inlogmiddel een duidelijke disclaimer verplicht in beeld te laten brengen met daarin heldere informatie over hoe omgegaan wordt met de gegevens van de burger en de rechten die deze burger heeft (bijvoorbeeld het recht op inzage van het gebruik van zijn/haar gegevens) die gebruik maakt van het inlogmiddel.

Aanbieders van inlogmiddelen voor burgers dienen te voldoen aan strenge eisen, die worden vastgesteld in de AMvB voor burgermiddelen, waaraan ik eerder refereerde, en de nadere uitvoeringsregeling. Daarin zal onder meer worden opgenomen dat aanbieders, in lijn met de geldende verplichtingen op grond van de AVG en de eIDAS-verordening, burgers moeten informeren over hun inzagerechten, maar ook over de werking van de middelen, de voorwaarden voor het gebruik en aanbevolen veiligheidsmaatregelen. Er zullen specifieke regels worden gesteld aan aanbieders van inlogmiddelen om te zorgen dat misbruik van inlogmiddelen kan worden gemeld, herkend en de eventuele gevolgen ervan kunnen worden hersteld.

3. Verhouding tot andere regelgeving

De leden van de GroenLinks-fractie hebben nog twee vragen n.a.v. moties ingediend bij de behandeling van de Wet digitale overheid. Allereerst vernemen zij graag of, en zo ja hoe, gewerkt wordt aan het waarborgen dat bij (private) authenticatiediensten zoveel mogelijk gebruik wordt gemaakt van open source?

De werking van processen moet transparant zijn zodat deze controleerbaar zijn. Daarnaast dient de veiligheid van de middelen te worden geborgd. Dat is uiteindelijk het doel. Een manier om transparantie te bewerkstelligen, is het gebruik maken van open source. Transparantie kan echter ook worden gerealiseerd met gesloten software. Ten aanzien van het veiligheidsaspect zitten aan beide voor- en nadelen; open source software wordt beveiligd door openheid, closed source software door bescherming. Ten aanzien van de veiligheid van closed source zullen met leveranciers afspraken gemaakt moeten worden over het borgen van de veiligheid.

Daarnaast vernemen de leden van de GroenLinks-fractie graag een actuele stand van zaken over het vraagstuk rondom het feit dat ondernemers problemen ervaren met het doen van aangiften (eHerkenningsproblemen en de kosten voor het doen van belastingaangiften).

Per brief van 3 maart jl. (Kamerstuk 34 972, nr. 44) bent u geïnformeerd over de laatste stand van zaken aangaande de organisaties die niet staan ingeschreven in het Handelsregister in relatie tot het doen van aangifte voor de loonheffing, vennootschapsbelasting en omzetbelasting. Het kabinet streeft ernaar om uw Kamer in mei nader te informeren over de kosten voor het inlogmiddel bij het doen van aangifte door bedrijven en organisaties. Daarbij wordt ook de actuele stand aangaande de organisaties, die nog geen eHerkenning kunnen aanschaffen, betrokken.

4. Inhoud

4.1 Verwerking persoonsgegevens

De leden van de D66-fractie vragen zich af of de regering voorbeelden kan schetsen waarin het wenselijk zou zijn dat artikel 5b, lid 3 en artikel 5c, lid 3 het mogelijk maken om ook gegevens over de gezondheid in niet versleutelde vorm te verwerken?

De onder deze artikelen opgenomen gezondheidsgegevens hebben betrekking op de gegevens van een dienstverlener en de dienst die geleverd wordt (bijvoorbeeld de trombosedienst van een ziekenhuis). Deze gegevens krijgen authenticatiediensten (publieke en private) aangeleverd bij een authenticatieverzoek. Een authenticatiedienst heeft deze gegevens nodig om een gebruiker te vragen of hij of zij zich inderdaad voor deze betreffende dienst wil authenticeren. Ook worden deze gegevens gebruikt om een gebruiker adequaat te kunnen informeren over het gebruik van zijn middel en om in geval van misbruik een gebruiker te helpen. Een authenticatiedienst kan deze gegevens daarom (onversleuteld) zien, maar ziet uiteraard niet wat de gebruiker na authenticatie verder doet op het portaal van de dienstverlener (het concrete gebruik). Er worden eisen gesteld aan het gescheiden opslaan van gebruikersgegevens en gebruiksgegevens zodat de gebruiker en de kenmerken van zijn gebruik niet zomaar gecombineerd kunnen worden.

In het bedrijvendomein kan een zgn eHerkenningsmakelaar (een private ontsluitende dienst) wel zien bij welke dienstverlener en dienst een gebruiker inlogt, maar kan deze private dienst niet zien wie de gebruiker is (anders dan in de vorige alinea). Echter, kenmerken van het gebruik van een bedrijvenmiddel zullen geen zorgaanbieders betreffen. Het afnemen van diensten in de zorg zullen gebruikers (natuurlijke personen) doorgaans namelijk met het eigen authenticatiemiddel afhandelen en niet met een middel van de werkgever. Om evenwel de theoretische mogelijkheid niet uit te sluiten dat een werknemer, directeur-grootaandeelhouder of zzp'er zijn bedrijfsmiddel gebruikt om zich te authenticeren voor de arbodienst, de aanvraag van een subsidieregeling voor gehandicapten of om in te loggen bij een bedrijfsarts, is de mogelijkheid om medische gegevens te verwerken opgenomen.

Uiteraard geldt voor alle gegevensverwerkingen dat gegevens in overeenstemming met de AVG worden verwerkt en de noodzaak voor de verwerking moet bestaan.

De leden van de D66 fractie horen voorts graag van de regering hoe kan worden voorkomen dat gegevens, conform artikel 5e, op basis van andere verwerkings-gronden dan de goede werking van identificatiemiddelen en de goede en veilige toegang met die middelen of via machtiging tot elektronische dienstverlening worden gebruikt.

Zoals ik eerder heb opgemerkt geldt er een strenge controle op de dienstverlening van aanbieders van inlogmiddelen, zowel vooraf, bij de toelating, als gedurende de dienstverlening. Deze controle ziet ook op een juist c.q. rechtmatig gebruik van persoonsgegevens. In de regeling is niet alleen bepaald dat gegevens enkel en alleen mogen worden gebruikt voor de goede werking van de dienstverlening (doelbinding), maar is daarbij eveneens expliciet verboden dat de gegevens voor andere doelen worden ingezet. Ten slotte geldt dat de waarborgen niet alleen in deze juridische grondslagen zijn opgenomen, maar dat ook operationele maatregelen, zoals de gescheiden opslag van gebruiks- en gebruikersgegevens wordt verlangd, waardoor ook feitelijk wordt voorkomen dat gegevens voor andere doeleinden worden ingezet.

De leden van deze fractie zouden graag horen wat wordt verstaan onder «overige gegevens die bij het account horen» in artikel 5b sub c.

Onder accountgegevens worden gegevens verstaan die bij een account van een gebruiker horen. Denk hierbij aan de inlognaam en contactgegevens als het mobiele nummer of e-mailadres, maar ook bijvoorbeeld het soort document dat gebruikt wordt voor elektronische identificatie. Voor de nog toe te laten private middelen is zoveel mogelijk aangesloten bij de (account)gegevens die het publieke middel DigiD nu verwerkt. Echter, aangezien het nog niet duidelijk is welke precieze accountgegevens de te erkennen private partijen nodig hebben voor de werking van hun middel, zijn deze gegevens hier niet uitputtend opgenomen. Uitgangspunt voor de verwerking is dat de gegevensverwerking noodzakelijk is en in overeenstemming met de AVG plaatsvindt. Deze gegevensset vormt een onderdeel van de eisen voor toelating/erkenning van middelen en zal bijgevolg worden opgenomen in de ministeriële regeling bij de AMvB's inzake het burgermiddel resp. het bedrijvenmiddel.

De leden van de D66-fractie vragen zich af waarom de eis tot het scheiden van de opslag van gegevens over de gebruiker van het private identificatiemiddel enerzijds, en de gegevens over het gebruik van het middel anderzijds niet wordt vastgelegd in artikel 5e.

Het is van groot belang dat gegevens die van burgers worden verkregen bij het inloggen bij de overheid niet als handelswaar worden behandeld. De regels waarmee dit wordt voorkomen staan in het onderhavige besluit en in het Besluit identificatiemiddelen voor burgers Wdo. Artikel 5e van het onderhavige besluit bevat het verbod om persoonsgegevens te gebruiken voor een ander doel dan het doel waarvoor deze zijn verstrekt (doelbinding). Dat verbod staat in de weg aan het verkopen van de gegevens. Verder wordt het verplicht om gegevens over gebruikers en gebruik gescheiden op te slaan. Daardoor is een nadere handeling nodig om het gebruik van een burger in te zien. Deze eis zal worden opgenomen in het Besluit identificatiemiddelen voor burgers Wdo. Hiervoor is gekozen om redenen van wetsystematische aard. Beide regels gelden niettemin voor aanbieders van private burgermiddelen; zij moeten de gegevens over gebruiker en gebruik gescheiden opslaan en mogen deze niet doorverkopen.

De leden van de D66-fractie ontvangen graag een nadere toelichting over hoe met de genoemde specifieke, zichtbare en toegankelijke verklaring voldoende uitvoering wordt gegeven aan het recht van inzage en rectificatie van per-soonsgegevens.

Een burger heeft op grond van artikel 15 AVG het recht om te weten welke persoonsgegevens door de verantwoordelijke worden verwerkt, onder meer voor welke doeleinden en aan welke personen of instanties deze

gegevens zijn verstrekt. Op grond van de artikelen 16 tot en met 18 AVG heeft hij het recht de verantwoordelijke te verzoeken hem betreffende gegevens te rectificeren, gegevens te wissen, of de verwerking te beperken. De wijze waarop uitvoering wordt gegeven aan deze rechten zal, wat betreft de voorzieningen in dit besluit onder de verantwoordelijkheid van de Minister van BZK, worden vastgelegd in op te stellen privacyverklaringen die op de betrokken websites zullen worden geplaatst. Daar waar een voorziening geen eigen website heeft (zoals de routeringsvoorziening of het BSNk) zal deze informatie in de privacyverklaring op website van de publieke authenticatiedienst (DigiD) en MijnOverheid worden geplaatst zodat het inzichtelijk is voor een gebruiker hoe zijn of haar gegevens door de hele keten gebruikt worden. Private partijen moeten deze informatie op hun eigen website opnemen.

De leden van de D66-fractie ontvangen graag een nadere toelichting waarom in paragraaf 4.1.2. van de nota van toelichting wordt gekozen voor een opt-out mechanisme en niet een opt-in mechanisme om automatisch berichten te ontvangen.

Het ongevraagd toezenden van elektronische berichten vergt, gelet op artikel 2:14 Awb, een wettelijke grondslag. Daartoe wordt in artikel 20 van de Bekendmakingswet aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties de bevoegdheid gegeven om periodiek elektronische berichten te zenden over bekendmakingen en mededelingen (Wetsvoorstel elektronische publicaties, 35 218). Deze bepaling biedt ook de grondslag voor de het opslaan en verwerken van persoonsgegevens uit de BRP en MijnOverheid waarmee een woonadres aan een e-mailadres kan worden gekoppeld. Het verwerken van deze persoonsgegevens is gerechtvaardigd gelet op het belang om burgers te informeren over voor hen relevante algemene bekendmakingen, mededelingen en kennisgevingen. De opslag is noodzakelijk om de beoogde verwerking te kunnen verrichten. Hierbij weegt mee dat de burger zich kan afmelden voor de attendering. Op basis van uitgevoerd onderzoek kan geconcludeerd worden, dat met een medium dat gedistribueerd wordt op basis van het zelf moeten nemen van een abonnement (opt-in) bij lange na niet het bereik kan worden gerealiseerd van een medium dat ongevraagd verspreid wordt (opt-out). Gelet op het grote belang van kenbaarheid en toegankelijkheid van overheidspublicaties is de ongevraagde attendering (met de mogelijkheid van afmelding) aanvaardbaar. Dit sluit ook aan bij het advies van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) «Weten is nog geen doen; een realistisch perspectief op zelfredzaamheid». De WRR beveelt hierin aan om in het beleid in te spelen op beperkingen in het vermogen van burgers om keuzes te maken en uit te voeren door de keuzearchitectuur aan te passen, bijvoorbeeld door gebruik te maken van een opt-outstelsel.

4.1.3 Persoonsgegevens toegelaten privaat middel voor burgers
De leden van D66 hebben de regering gevraagd om nader toe te lichten waarom ook private identificatiemiddelen worden toegelaten voor overheidsdienstverlening.

Op dit moment is toegang voor burgers tot elektronische diensten van publieke dienstverleners slechts mogelijk met DigiD, het publiek uitgegeven inlogmiddel. Dat betekent dat als DigiD onverhoopt uitvalt, de elektronische dienstverlening van de hele overheid stilvalt. Toelating van private middelen moet de afhankelijkheid van een enkel inlogmiddel terugdringen; burgers en overheden krijgen de beschikking over meerdere (terugval)opties, waarbij burgers zelf de keuze krijgen. Tevens wordt beoogd om innovatie vanuit de markt meer ruimte te bieden, waardoor beschermingstechnieken sneller kunnen worden ingezet en kunnen

meegroeien met veranderende dreigingen. Dit leidt tot een grotere robuustheid van het systeem voor identificatiemiddelen als geheel, waarvan zowel burgers, bedrijven als overheden profijt hebben. Daarbij leidt het toelaten van private middelen naar verwachting tot een hogere beschikbaarheidsgraad van identificatiemiddelen onder burgers op de betrouwbaarheidsniveaus substantieel en hoog. Om genoemde redenen is een systeem van erkenning van private partijen opgenomen in het wetsvoorstel, dat door Uw Kamer is aangenomen en dat momenteel in de Eerste Kamer wordt behandeld.

De leden vroegen tevens of de toelating van private middelen extra risico's met zich meebrengt op het gebied van *phishing* en hoe wordt voorkomen dat data, gerelateerd aan overheidsdienstverlening, door een private partij voor commerciële doeleinden worden gebruikt.

Het risico van *phishing* verschilt niet bij het gebruik van private middelen of publieke middelen. Het is en blijft in alle gevallen, naast de (technische) veiligheidsmaatregelen die aanbieders zelf treffen om *phishing* (het ontfutselen van gegevens door derden) tegen te gaan, van groot belang om gebruikers bewust en alert (controleren van het «slotje» op websites) te maken op de dreigingen die zich in een digitale omgeving voordoen. Benadrukt zij, zoals ook bij de behandeling van het wetsvoorstel aan de orde was, dat identiteit geen handelswaar is. Om privacy te beschermen wordt de verwerking van persoonsgegevens door publieke en private partijen streng gereguleerd. Verwerking is op grond van dit besluit alleen toegestaan voor zover die strikt noodzakelijk is om veilig bij publieke dienstverleners in te loggen en een eventueel opgetreden probleem te kunnen herstellen. Dat volgt uit de onderhavige AMvB. Zie ook hierboven bij 4.1. Elk ander gebruik van persoonsgegevens wordt expliciet verboden om te voorkomen dat partijen gegevens voor andere (commerciële) doeleinden gebruiken. De bescherming wordt niet alleen geboden door regels te stellen, maar er worden ook eisen gesteld aan de feitelijke (technische) inrichting, waardoor, zoals eerder opgemerkt, koppeling van gegevens door partijen feitelijk niet meer mogelijk wordt. Bedrijven kunnen niet verdienen aan het verhandelen van de verkregen gegevens. Zij zullen hun verdienmodel moeten baseren op de inkomsten uit het aanbieden van inlogmiddelen. Voor de volledigheid wijs ik op de doorlopende controle (toezicht) zoals ik eerder heb toegelicht, en die wordt uitgevoerd om te verzekeren dat partijen zich aan de regels houden. Het spreekt voor zich, dat tegen partijen die op dit punt de regels overtreden, maatregelen worden genomen, daaronder begrepen dat de toelating van partijen wordt beëindigd of dat een boete wordt opgelegd.

De leden vroegen voorts hoe de risico's worden ondervangen en kan worden voorkomen dat statelijke actoren misbruik maken door private aanbieders toe te staan.

De eisen zoals hierboven besproken, gelden onverkort voor buitenlandse leveranciers. Daarbij geldt dat ook de eIDAS-verordening en AVG eisen aan middelen stellen. Deze vormen een essentiële drempel. Voorts heb ik de mogelijkheid om voor bedrijven die middelen willen aanbieden een Bibob-toets te laten uitvoeren, teneinde na te gaan of bedrijven geen relatie met criminaliteit hebben. Bovendien kan ik bij zwaarwegende redenen partijen hun erkenning ontnemen. Zij kunnen dan geen middelen meer aanbieden. Dat kan bijvoorbeeld bij gevaar voor cyberveiligheid of nationale veiligheid.

4.1.4. Persoonsgegevens bedrijfs- en organisatiemiddel
De leden van de VVD-fractie begrijpen dat de algemene maatregel van bestuur (AMvB) ook betrekking heeft op bedrijfs- en organisatiemiddelen. Zijn er op basis van deze AMvB gevolgen voor de huidige bedrijfs- en organisatiemiddelen (e-herkenning)? Zo ja, welke zijn dat?

In deze AMvB zijn de gegevens opgenomen die de bedrijfs- en organisatiemiddelen (bijvoorbeeld eHerkenning) verwerken zover dit noodzakelijk is voor de werking van het middel en de goede en veilige toegang met dat middel tot elektronische dienstverlening binnen het eID- stelsel en op grond van de eIDAS-verordening. Deze AMvB heeft daarom geen gevolgen voor de bedrijfs- en organisatiemiddelen. Buiten de reikwijdte van deze AMvB vallen de gegevens die nu of later aanvullend door private partijen verwerkt worden voor de werking van hun inlogmiddel en die per partij kunnen verschillen. Denk bijvoorbeeld aan persoonsgegevens die nodig zijn voor identificatie op afstand. De verwerking van deze persoonsgegevens valt onder de verantwoordelijkheid van de private partijen zelf en – omdat dergelijke verwerking niet nodig is voor de werking van eID-stelsel – niet onder de verantwoordelijkheid van de Minister van BZK en buiten de werkingssfeer van deze AMvB. Uiteraard geldt voor aanvullende verwerking door private partijen dat deze conform de AVG dient te zijn.

4.1.5. Persoonsgegevens BSN-K
De leden van de VVD-fractie lezen dat de afgeleide vorm van het BSN in het private domein wordt gebruikt bij diensten waarvoor geen BSN verwerkt mag worden. De afgeleide vorm bevat geen BSN. Graag krijgen deze leden een verduidelijking van deze passage, want deze AMvB heeft toch geen betrekking op de private sector, met uitzondering van die delen die het BSN moeten gebruiken, zoals zorgverzekeraars?

Het klopt dat deze AMvB alleen betrekking heeft op het (semi-)publieke domein. Toegelaten private partijen kunnen middelen leveren waarmee ingelogd kan worden bij BSN-gerechtigde organisaties in het (semi-) publieke domein en bij niet BSN-gerechtigde organisaties. Het BSNk verwerkt de versleutelde vorm van het BSN om in te loggen bij een BSN-gerechtigde organisatie (die hieruit een BSN kan herleiden) en de afgeleide vorm van het BSN om in te loggen bij een niet-BSN gerechtigde organisaties (hieruit kan geen BSN herleid worden). Juist om die reden is de inrichting van het BSNk zodanig, dat waar het private en het publieke domein elkaar in potentie raken, te weten bij de aanbieder van een privaat middel, deze geen koppeling kan maken tussen het BSN en de afgeleide vorm daarvan. De afgeleide vorm van het BSN wordt daarnaast door het BSNk verwerkt voor de BSNkfunctie waarmee de gebruiker inzage kan krijgen in welke middelen aan hem zijn of waren gekoppeld en de status van die middelen.

De VVD-fractie vraagt zich voorts af, wat de gevolgen zijn van het «zoveel mogelijk werken met pseudonomisering en polymorfe identiteiten» voor de uitwerking van de motie van het lid Middendorp over het gebruik van identificatiemiddelen in niet-publieke overige sectoren? (Kamerstuk 34 972, nr. 29).

Conform deze motie zal ik onderzoeken of, en zo ja, hoe publieke middelen buiten de overheid gebruikt zouden kunnen worden. Het is daarbij van belang veilig en betrouwbaar te werk te gaan; pseudonimisering is in dit verband behulpzaam. Het BSN, een belangrijk persoonsgegeven dat ten grondslag ligt aan publieke middelen, mag immers niet in niet-publieke sectoren gebruikt worden.

De leden van de CDA-fractie hebben gevraagd wat precies de functie is van het BSN-Koppelregister in de rollen die de Wet digitale overheid heeft gedefinieerd en op grond waarvan de voorziening tot stand komt. De leden constateren dat het BSN-Koppelregister niet wordt genoemd in de definities van de Wet digitale overheid.

Het klopt dat het BSNk niet wordt genoemd in de definitiebepaling in de wet. Reden hiervoor is dat ervoor is gekozen om in (artikel 5 van) de wet functionele beschrijvingen te hanteren. Dit past in een techniek-onafhankelijke wet; het zou onwenselijk zijn om bij een nieuwe voorziening voor eenzelfde functionaliteit steeds de wet te moeten aanpassen. Wel wordt het BSNk in de onderhavige AMvB uitgewerkt, waarbij geldt dat deze de functionaliteit vervult zoals aangegeven in artikel 5, eerste lid, onder d, van de wet. In de artikelsgewijze toelichting bij het wetsvoorstel wordt dit ook nader toegelicht.

De leden hebben gevraagd of deze voorziening een centrale rol heeft in het stelsel, en of alle middelen via deze voorziening communiceren. Voorts vroegen de leden of deze voorziening dan niet in strijd is met het doel van de Wet digitale overheid, namelijk ervoor zorgen dat wij op het gebied van online identificatie en authenticatie niet afhankelijk zijn van unieke voorzieningen.
Het BSNk zorgt ervoor dat burgers kunnen inloggen zonder dat daarvoor iedere keer het BSN verwerkt hoeft te worden. En dat betrokken dienstverleners en partijen op basis van pseudoniemen met elkaar kunnen samenwerken. Door het versleutelingsmechanisme verschillen deze pseudoniemen per organisatie («polymorf»).
Het inloggen bij een publieke dienstverlener is echter niet afhankelijk van het BSNk. Het BSNk speelt enkel een rol op het moment dat een burger een inlogmiddel voor het eerst in het publieke domein wil gaan gebruiken. Dan vindt éénmalig een controle plaats of het BSN correspondeert met de door een gebruiker opgegeven gegevens in de BRP. Bij een positieve controle wordt vervolgens een pseudoniem gegenereerd. Dit verloopt via het BSNk. Bij het daadwerkelijk gebruik van het inlogmiddel (de authenticatie) is er vervolgens geen tussenkomst meer nodig van het BSNk.

Ten slotte vragen de leden van de CDA-fractie wat de noodzaak is van het gebruik van pseudonieme identiteiten in het BSN-domein.

Het gebruik van polymorfe identiteiten is een privacymaatregel, bedoeld om het BSN te beschermen door de verwerking ervan te beperken. Dit staat er overigens niet aan in de weg dat private aanbieders van inlogmiddelen op andere wijze hun middel kunnen vormgeven en privacybescherming in lijn met de AVG kunnen inrichten.

5. Privacy en verhouding tot algemene verordening gegevensbescherming

De leden van de GroenLinks-fractie hebben gevraagd naar de uit de AVG voortvloeiende verplichte dataminimalisatie. Zij refereren daarbij aan de behandeling van de Wet digitale overheid, waarbij de leden zorgen hebben gewisseld over de mogelijkheid van private organisaties om een digitaal identificatiemiddel in te stellen. De leden vragen de regering – zo mogelijk met een concreet voorbeeld van een fictief bedrijf – om aan te geven hoe de dataminimalisatie moet worden bereikt en hoe dit door zowel de overheid als voor burgers te controleren is of aan de AVG wordt voldaan.

Gewezen zij op de antwoorden op eerdere vragen over de controle op private aanbieders en de beantwoording van de vragen over maatregelen om commercieel gebruik van gegevens door private organisaties te voorkomen. Voorts is het zo, dat dataminimalisatie als privacybeginsel van groot belang is. Echter, effectieve naleving van de AVG wordt niet bereikt door focus op één van de in de AVG opgenomen beginselen. Naleving betreft een afweging tussen de AVG-beginselen, waaronder ook doelbinding, transparantie voor gebruikers en kwaliteitsborging door herstelvermogen. Daarbij merk ik op dat adequate naleving van privacywetgeving niet statisch is, maar een doorlopende activiteit. Dat betekent dat door de tijd maatregelen die getroffen worden om bescherming van persoonsgegevens te realiseren kunnen wijzigen, bijvoorbeeld door voortschrijdende beveiligingstechnieken, maar ook door veranderende dreigingen.

6. Consultatie

De leden van de ChristenUnie-fractie vinden het van belang dat het nieuwe besluit ook voor zorgpartijen goed uitvoerbaar is en tot zo min mogelijk meerkosten leidt. Op welke manier kan de terughoudendheid van zorgpartijen verder worden weggenomen ten aanzien van de zorgen die zij hebben ten gevolge van dit besluit? Hoe wordt ook bij het toelaten van identificatiemiddelen rekening gehouden met de uitvoerbaarheid voor zorgpartijen en overige aangewezen organisaties om de eigen systemen op de verschillende soorten identificatiemiddelen af te stemmen? Hoe gaat er rekening worden gehouden met door zorginstellingen reeds gehanteerde methodieken? Is de regering bereid om zorginstellingen actief te betrekken bij de nadere uitwerking van het besluit? De leden lezen dat «Uitgangspunt is evenwel alle dienstverleners op eenduidige wijze te (kunnen) beoordelen; hierdoor is de ruimte voor eigen vormgeving van audits en rapportage beperkt.» Is hierin het gemak voor het Ministerie leidend, of is het streven om waar dat kan maximaal ruimte te bieden aan zorgpartijen om regelarm te kunnen rapporteren?

De WDO en onderliggende regelgeving vergen het nodige van dienstverleners. Het is daarom wenselijk een verantwoord evenwicht te vinden tussen veiligheid en uitvoerbaarheid. Dit is ook het uitgangspunt bij het onderhavige besluit. De regels inzake informatieveiligheid hebben op dit moment de status van beleidsregels of richtsnoeren en zijn vrijblijvend van aard. Met dit besluit is sprake van stroomlijning en codificering van in de praktijk reeds gehanteerde documenten zoals de Baseline Informatiebeveiliging rijksoverheid (BIR), Baseline Informatiebeveiling Gemeenten (BIG), de aansluitvoorwaarden inzake diverse gdi-voorzieningen (o.a. DigiD) en de ICT-beveiligingsrichtlijnen van de NCSC. Materieel gaan er voor wat betreft informatiebeveiliging niet of nauwelijks aanvullende verplichtingen gelden. Voor specifiek de zorgsector geldt dat dit besluit niets wijzigt aan de door de zorg reeds gehanteerde methodieken.

7. Evaluatie

De leden van de VVD-fractie nemen aan dat de toelichting met betrekking tot de evaluatiebepaling nog wordt aangepast in verband met het aangenomen amendement Middendorp en Van der Molen (Kamerstuk 34 972, nr. 21) waardoor de termijn voor de evaluatie van vijf jaar is veranderd in drie jaar. Ook is vastgelegd dat de toegankelijkheid van elektronische dienstverlening voor mensen die digitaal minder vaardig zijn nadrukkelijk bij de evaluatie wordt meegenomen. Ook de leden van de CDA-fractie constateren dat in artikel 23 van het wetsvoorstel sprake is van een termijn van drie jaar.

Paragraaf 8 van de nota van toelichting bij het Besluit zal op het punt van de evaluatietermijn worden geactualiseerd.

II Artikelsgewijze toelichting

Artikel I

Onderdeel F

Artikelen 5 en 5b

De leden van de VVD-fractie constateren dat de onderhavige AMvB een grotere dataset definieert dan de minimale dataset van de eIDAS-Verordening en vragen zich af waarom hiervoor is gekozen. Zou hier niet moeten worden verwezen naar de Verordening zelf? Ook de leden van de CDA-fractie constateren dit, en vragen hoe dit zich verhoudt tot het uitgangspunt van de regering om geen aanvullende eisen te stellen aan bestaande Europese regels en principes, zoals de Minister tijdens de plenaire behandeling van het wetsvoorstel stelde.

Uitgangspunt is dat zoveel mogelijk wordt aangesloten bij de eIDAS-eisen, zoals ik ook bij de parlementaire behandeling heb aangegeven. Aard en strekking van de Verordening brengen mee dat aanvullende eisen, mits noodzakelijk, proportioneel en non-discriminatoir, geoorloofd zijn. Om redenen van veiligheid en betrouwbaarheid wordt op onderdelen een grotere dataset gedefinieerd ter zake waarvan bij verwerking een grondslag nodig is. Daartoe dient dit Besluit. Om redenen van duidelijkheid en eenduidigheid is ervoor gekozen om voor de privacyeisen niet (tevens) te verwijzen naar de Verordening, maar deze bij elkaar in een en dezelfde AMvB op te nemen. Het voorgaande laat onverlet, dat genotificeerde inlogmiddelen uit andere lidstaten – ook als zij alleen voldoen aan de minimale dataset van de eIDAS-Verordening – door Nederlandse dienstverleners moeten worden geaccepteerd (wederzijdse erkenning). Dit volgt uit de eIDAS-Verordening alsmede uit de WDO.

Verder vragen de leden van de VVD-fractie naar de rolverdeling bij het aanleveren van die data. Zijn middelenleveranciers bijvoorbeeld wel in staat om het IP-adres en sessie-gegevens, waaronder cookies, van gebruikers aan te leveren? Hoe verhoudt dit zich tot de principes van dataminimalisatie?

De erkende partijen in artikel 5c verwerken persoonsgegevens zover dit noodzakelijk is voor de werking van het bedrijfs- en organisatiemiddel en goede en veilige toegang met dat middel tot elektronische dienstverlening. Het geformuleerde pakket wordt door de keten heen verwerkt; partijen verwerken bepaalde gegevens naar gelang hun rol/plek en de omstandigheden van het geval. Het is dus niet zo dat alle partijen alle gegevens moeten verwerken. Omdat alle partijen, zoals gezegd, onderdeel zijn van de eigen keten van het bedrijfs- en organisatiemiddel is ervoor gekozen om de verschillende partijen niet apart te behandelen.

Artikel 5d

De leden van de VVD-fractie merken op dat artikel 5d de term «eIDAS-voorziening» introduceert en vragen zich af, of dit een andere benaming is voor het «eIDAS-koppelpunt». Waarom wordt in deze AmvB niet duidelijker aangesloten bij de bestaande terminologie, diensten en begrippen uit de eIDAS-verordening zelf?

De term eIDAS-voorziening vloeit voort uit het bovenliggende wetsvoorstel, waarin in artikel 5 de verantwoordelijkheid van de Minister van BZK is neergelegd voor (voorzieningen van) de generieke infrastructuur. Onderdeel hiervan is de voorziening genoemd in het tweede lid, waarin, onder a en b, functioneel wordt omschreven wat deze behelst: mogelijk maken dat elektronische identificatiemiddelen voor burgers en bedrijven uit andere EU-lidstaten ontsloten worden voor gebruik in Nederland en vice versa (wederzijdse erkenning). Het begrip eIDAS-voorziening is om wetsystematische redenen gekozen. In de uitvoeringspraktijk wordt in dit verband ook wel de term «eIDAS-koppelpunt» gebruikt, om aan te geven dat sprake is van een schakel tussen Nederland en andere EU-lidstaten.

Meer in het algemeen wordt in de WDO en onderliggende regelgeving om redenen van uitvoerbaarheid en werkbaarheid binnen de Nederlandse context op onderdelen aangesloten bij (bestaande) nationale begrippen en wetsystematiek, en worden onduidelijke of ongebruikelijke begrippen of voorschriften uitgewerkt («vertaald»). Vanzelfsprekend geschiedt dit alleen waar dit echt nodig is.

Onderdelen K, L, M, N en O

Bij een aantal onderdelen, zoals K, L, M, N en O, zo stellen de leden van de VVD-fractie vast, is er sprake van een bewaartermijn van persoonsgegevens van vijf jaar. Waarop is de periode van vijf jaar gebaseerd? In hoeverre is de termijn van vijf jaar noodzakelijk? Graag krijgen de leden van de VVD-fractie een reactie van de regering.

Deze periode komt voort uit en is thans opgenomen in het geldende Besluit verwerking persoonsgegevens GDI, waar dit besluit de actualisering van vormt. Deze bewaartermijn is in de nota van toelichting bij dat besluit gemotiveerd en houdt verband met het kunnen bieden van herstelvermogen. Samengevat: met de verdere maatschappelijke integratie van de digitale overheid raken de voorzieningen voor de toegang tot die digitale overheid meer vervlochten. Het aantal gebruikers neemt daarbij in intensiteit, diversiteit en in (financieel) belang verder toe. De voorzieningen vormen steeds vaker een essentiële schakel in de keten, waarbij afnemers en vaak ook burgers gehouden zijn gegevens over de onderlinge contacten voor langere tijd te bewaren. Bewaartermijnen van enige jaren zijn daarbij geen uitzondering. De onderhavige voorzieningen vormen bovendien steeds meer onderdeel van de processen zoals die zich tussen burgers en afnemers (overheden) voltrekken en het gebruik ervan zal direct van invloed zijn op de gelding van onderlinge rechten en verplichtingen.

De praktijk laat ook een tendens zien waarbij burgers zich vaker met vragen om hun gegevens tot de voorzieningen wenden. Vaak gaat het om vragen in verband met bewijsvoering in juridische geschillen of procedures. Veel burgers verwachten van de overheid dat zij de gevraagde informatie voor hen beschikbaar heeft.

Het gebruik van de voorzieningen wordt voor veel burgers het enige punt waar zij nog op kunnen terugvallen en geholpen kunnen worden als zij problemen ondervinden. Bijvoorbeeld bij fiscale problemen, waarbij de mogelijkheid bestaat om tot in ieder geval 5 jaar jaren terug met afhandeling van bijvoorbeeld aangifte inkomstenbelasting of toeslagen bezig te zijn, kan het van belang zijn om gebruiksgegevens van de voorzieningen over die periode ter beschikking te hebben. Daarnaast is het in de praktijk voorgekomen dat slachtoffers van misbruik of oneigenlijk gebruikt niet adequaat konden worden ondersteund, omdat het misbruik zich uitstrekte

over een langere periode dan waarvan de gebruiksgegevens nog beschikbaar waren. Ook voor dit soort situaties draagt een langere bewaartermijn bij aan adequatere ondersteuning en bescherming van burgers.

De geschetste praktijk en de verwachte ontwikkelingen in de vraag naar informatie over de verwerking van met name gebruiksgegevens vraagt om een nieuwe afweging tussen het belang van de gebruiker om geholpen (en beschermd) te worden en het belang van de gebruiker dat zijn gegevens niet onnodig lang worden bewaard. Gelet op de op mij rustende zorg voor de beveiliging en betrouwbaarheid van de voorzieningen en gelet op het belang dat de burger en de afnemers/overheden daarbij hebben – een betrouwbare voorziening kan informatie leveren aan gebruikers en afnemers; een veilige voorziening voorkomt of bestrijdt misbruik ervan –, is een bewaartermijn van 5 jaar voor bepaalde gegevens in het licht van de geschetste praktijk en verwachte ontwikkelingen gerechtvaardigd.

De leden van de D66-fractie vragen een toelichting of de bewaartermijnen in het kader van misbruikbestrijding van 5 jaar, zoals genoemd in artikel 14e, bovenop de genoemde bewaartermijnen van de in artikel 11 tot en met 14d genoemde bewaartermijnen van 5 jaar komt.

Artikel 14e stelt dat de bewaartermijn van de gegevens die in het kader van misbruikbestrijding zijn verwerkt, maximaal 5 jaar na die verwerking kunnen worden bewaard. Deze termijn is dus aanvullend op de in de artikelen 11 tot en met 14d genoemde bewaartermijnen. De bedoelde gegevens worden verwerkt in het kader van onderzoek naar mogelijk misbruik of oneigenlijk gebruik van de diverse voorzieningen en middelen in het authenticatieproces.

Artikel 18 en 24

De leden van de D66-fractie vragen zich af waarom onder artikel 18 wel fysieke- en personele beveiligingseisen worden gesteld aan het informatie-veiligheidsbeleid, maar dat fysieke- en personele beveiliging volgens artikel 24 vervolgens niet onderdeel uitmaken van de vereiste audit voor dienstverleners.

Bij de audit ligt de focus op (technische) ICT-voorzieningen en de bijbehorende beheersprocessen en niet op fysieke en personele beveiliging. Reden hiervoor is dat het op dit moment niet wenselijk is om de auditlast van dienstverleners te verzwaren. De WDO en onderliggende regelgeving vergen het nodige van dienstverleners; het is in dat verband wenselijk een verantwoord evenwicht te vinden tussen veiligheid en uitvoerbaarheid. Op basis van opgedane ervaringen – ingevolge artikel 23 WDO wordt binnen 3 jaar geëvalueerd, in het bijzonder ten aanzien van onder meer de getroffen maatregelen op het gebied van beveiliging – zal worden bezien of een brede en meer integrale audit verplicht moet worden gesteld.

Nota Bene: aanvulling Besluit

Van de gelegenheid wordt gebruik gemaakt om het voorgenomen Besluit aan te vullen op het punt van het op aanvraag met dienstverleners delen van informatie over machtigingsrelaties. Aanleiding hiervoor is de tijdens de Corona-crisis gebleken behoefte van dienstverleners om bij machtiging betrokken burgers en organisaties (vertegenwoordigden en gemachtigden) te informeren over een specifieke dienst, zoals de mogelijkheid tot

uitstel van belastingaangifte. Artikel 7, onderdeel b, van het onderhavige Besluit (verstrekkingen DigiD machtigen) maakt het thans niet expliciet mogelijk om als dienstverlener bij de Minister van BZK een dienstgericht overzicht op te vragen van de machtigingsaanvragen en -registraties die voor diensten van de betreffende dienstverlener zijn afgegeven. Er is dus op dit moment geen juridische basis om dit overzicht op te vragen, terwijl toepassing van deze verstrekking zeer wenselijk is. Om deze leemte zo kort mogelijk te laten duren, wordt artikel 7 onderdeel b aangevuld met het bepaalde, dat op verzoek van de afnemer een persoonsgericht of dienstgerelateerd overzicht kan worden verstrekt van alle machtigingsaanvragen en machtigingsregistraties die voor diensten van de betreffende afnemer zijn afgegeven. In de Nota van toelichting zal worden opgenomen dat deze aanvulling specificeert dat aan dienstverleners persoonsgericht of dienstgerelateerd inzicht kan worden geven in de machtigingsaanvragen en -registraties teneinde de goede werking van de machtigingsvoorziening te realiseren, waaronder begrepen serviceverlening en informatieverschaffing door de betreffende afnemer aan gemachtigden over een specifieke dienst.