MEMORIE VAN ANTWOORD
NAV HET VOORLOPIG VERSLAG
WETSVOORSTEL DIGITALE OVERHEID
(34 972)

Inhoudsopgave

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR BINNENLANDSE ZAKEN EN DE HOGE COLLEGES VAN STAAT/ALGEMENE ZAKEN EN HUIS VAN DE KONING

Vastgesteld: 29 september 2020

1. Inleiding

*De leden van de **FVD**-fractie hebben het wetsvoorstel met belangstelling gelezen.*
Zij wensen nog een aantal vragen te stellen.

*De leden van de fractie van **GroenLinks** hebben van het wetsvoorstel kennisgenomen. Zij hebben nog een aantal vragen.*

*De leden van de **D66**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en van de antwoorden van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties naar aanleiding van de commissiebrief van 10 juli 2020. Deze leden staan in beginsel niet afwijzend tegenover de inzet van de regering om een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op de verschillende niveaus te vormen. Toch hebben deze leden hierover nog een aantal zorgen, nadere vragen en opmerkingen naar aanleiding van de beantwoording van de staatssecretaris op 31 augustus jl.*[1]

Op 30 juni 2020 heeft de vaste Kamercommissie voor Binnenlandse Zaken een deskundigenbijeenkomst in de Eerste Kamer georganiseerd. De regering is blijkens de brief van de staatssecretaris van 31 augustus 2020 op de hoogte van wat de deskundigen aan kanttekeningen met betrekking tot het wetsvoorstel naar voren brachten. De leden van de D66-fractie zouden het op prijs stellen als de regering per deskundige op de geleverde kritiek zou willen reageren. Is zij daartoe bereid?

*De leden van de **PvdA**-fractie hebben kennisgenomen van het wetsvoorstel digitale overheid. Zij maken zich grote zorgen om de bescherming van de digitale identiteit van burgers en benadrukken het belang van de toegankelijkheid van nieuwe systemen ook voor mensen met minder doenvermogen. Zij hebben daarover verschillende vragen.*

*De leden van de **PVV**-fractie hebben van het wetsvoorstel kennisgenomen. Zij hebben een aantal vragen.*

*De leden van de **SP**-fractie danken de staatssecretaris voor de reactie op de commissiebrief rondom de invoering van de Wet digitale overheid. Zij zijn echter verbaasd over de antwoorden. Zij menen een grote discrepantie te zien in de antwoorden van de staatssecretaris ten opzichte van het huidige kabinetsbeleid.*

*De leden van de fractie van de **ChristenUnie** hebben met interesse kennisgenomen van het voorstel voor de Wet digitale overheid. Zij hebben hierover enkele vragen.*

Graag bedank ik de fracties voor hun bijdrage en ga ik in op de gestelde vragen.
Bij de beantwoording zijn de indeling en volgorde van het verslag zoveel mogelijk aangehouden, met dien verstande dat vergelijkbare vragen zijn geclusterd. Om recht te doen aan de door de fracties aangesneden thema's, zijn bovendien enkele vragen vanuit verschillende invalshoeken beantwoord, waardoor de beantwoording dubbelingen bevat. Bij gelegenheid van de beantwoording wordt tevens ingegaan op de tijdens de bijeenkomst in de Eerste Kamer op 30 juni jl. door de deskundigen ingebrachte kanttekeningen met betrekking tot het wetsvoorstel, die terugkomen in de door de fracties gestelde vragen. Aan de vraag van de leden van de D66-fractie om te reageren op de inbreng van de deskundigen wordt op deze wijze gehoor gegeven.

[1] Kamerstukken I 2019/20, 34 972, I.

2. De Wet digitale overheid als Kaderwet

Regulering van de toegang tot de digitale overheid is een nieuw en dynamisch terrein. Sprake is van voortdurende (ICT-)technische, organisatorische en procesmatige innovatie, tegen de achtergrond van internationale en Europese ontwikkelingen. Wet- en regelgeving heeft in dat verband een instrumentele en faciliterende functie, maar moet ook waarborgen, rechtszekerheid en rechtsbescherming bieden. Er dienen geboden, verboden, taken en verantwoordelijkheden te worden verankerd, maar tegelijkertijd dient er ruimte en flexibiliteit te worden geboden om de dynamiek en praktische ontwikkelingen te kunnen 'opvangen', innovatie mogelijk te maken en een zekere wendbaarheid in de uitvoering te bewerkstelligen zonder dat dit risicovol is. Er dient, kortom, bij het ontwerpen van het *geheel* aan regels een verantwoord en werkbaar evenwicht te worden gerealiseerd, waarbij bovendien recht wordt gedaan aan democratische legitimiteit.

Om hierin te voorzien bevat de Wet digitale overheid de hoofdnormen die nodig zijn om duidelijkheid en rechtszekerheid voor burgers en bedrijven te verankeren, terwijl de uitwerking is gedelegeerd naar algemene maatregelen van bestuur en ministeriële regelingen. Dit is conform het algemeen wetgevingsbeleid, zoals hierna aan de orde komt. Los van het onderhavige wetsvoorstel is een aantal waarborgen neergelegd in de AVG, die rechtstreekse werking heeft, en in de Algemene wet bestuursrecht.

In het onderstaande ga ik in op de uitgangspunten bij het ontwerpen van 'wetgevingsarchitectuur' in het algemeen en bij wetgeving inzake de toegang tot de digitale overheid in het bijzonder. Hierbij worden de vragen van de fracties van **GroenLinks,** de **SP** en de **ChristenUnie** eveneens beantwoord.

Uitgangspunten voor wetgeving; algemeen

Bij het ontwerpen van wet- en regelgeving is, zoals ook door enkele fracties opgemerkt, het *primaat van de wetgever* leidend. Dit principe is vervat in de Aanwijzingen voor de regelgeving, en luidt als volgt:

> **Aanwijzing 2.19 Primaat van de wetgever**
>
> Bij verdeling van de elementen van een regeling over de wet en algemeen verbindende voorschriften van lager niveau bevat de wet tenminste de hoofdelementen van de regeling. Bij de keuze welke elementen in de wet zelf regeling moeten vinden en ter zake van welke elementen delegatie is toegestaan, dient het primaat van de wetgever als richtsnoer.
>
> **Toelichting**
>
> **Betrokkenheid parlement.** Het primaat van de wetgever dient niet aldus te worden verstaan dat het parlement bij alle onderdelen van een regeling rechtstreeks moet worden betrokken. Lang niet alle onderdelen van een regeling zijn van die betekenis dat directe parlementaire invloed op de vaststelling daarvan in de rede ligt. De mogelijkheid die het parlement heeft het regeringsbeleid achteraf te controleren, is dan voldoende.
> Gelet op het vorenstaande dient voor de keuze welke elementen van een regeling in de wet moeten worden geregeld en ter zake van welke elementen delegatie toelaatbaar is, steeds te worden onderzocht welke elementen van een regeling zo gewichtig zijn dat de volksvertegenwoordiging rechtstreeks bij de vaststelling moet worden betrokken. Aldus moeten ten minste de hoofdelementen van een regeling in de wet worden opgenomen.
>
> **Hoofdelementen van de regeling.** Hoofdelementen zijn in ieder geval de reikwijdte en de structurele elementen van de regeling. Veelal zullen daartoe ook de voornaamste duurzame normen behoren. Het kan echter uit een oogpunt van toegankelijke regelgeving

beter zijn om in de wet over een bepaald onderwerp geen materiële normen op te nemen, maar aan de lagere wetgever over te laten een integrale materiële regeling tot stand te brengen.

Uit het bovenstaande volgt dat *niet alle normen* in een *formele* wet hoeven te worden opgenomen of zelfs zouden moeten worden opgenomen. Alleen de hoofdelementen behoeven in beginsel opname in de wet. Wat onder reikwijdte en structurele elementen moet worden verstaan is eveneens vervat in Aanwijzingen voor de regelgeving:

Aanwijzing 2.21 Bij wet vast te stellen voorschriften

Zoveel mogelijk worden in de wet opgenomen voorschriften:

a. die de grondslag vormen voor een stelsel van vergunningen of een stelsel waarbij anderszins de toelaatbaarheid van handelingen afhankelijk wordt gesteld van toestemming van de overheid;
b. die andere overheden in medebewind roepen;
c. waarbij bestuursorganen in het leven worden geroepen;
d. betreffende rechtsbescherming;
e. inzake sancties van bestuursrechtelijke of civielrechtelijke aard;
f. waarbij toezichts- of opsporingsbevoegdheden worden toegekend;
g. omtrent rechten en verplichtingen van burgers jegens elkaar;
h. die beogen aan de burger procedurele waarborgen te bieden ten aanzien van het gebruik van bevoegdheden door de overheid.

Voor zover het niet gaat om de bovenstaande voorschriften ("hoofdelementen"), is derhalve delegatie van regelgevende bevoegdheid toegestaan en in bepaalde gevallen ook aangewezen, bijvoorbeeld indien wendbaarheid nodig is gelet op technologische ontwikkelingen. Ook hiervoor voorzien de Aanwijzingen voor de regelgeving in uitgangspunten. Delegatie dient in de delegerende regeling zo concreet en nauwkeurig mogelijk worden begrensd, waarbij kan worden gedacht aan het concretiseren van de omstandigheden waarin van de gedelegeerde bevoegdheid gebruik mag worden gemaakt, van de te regelen onderwerpen en van de doeleinden waartoe zij mag worden gebruikt (Ar 2.23).

Voorts verdient het, indien delegatie plaatsvindt, de voorkeur dat de bevoegdheid wordt toegekend bij algemene maatregel van bestuur (AMvB) regels te stellen. Slechts in bepaalde gevallen is delegatie aan een minister passend. Dit wordt beperkt tot voorschriften van administratieve aard, uitwerking van de details van een regeling, voorschriften die dikwijls wijziging behoeven en voorschriften waarvan te voorzien is dat zij mogelijk met grote spoed moeten worden vastgesteld. Delegatie 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 (Ar 2.24).

Tot slot geschiedt delegatie aan een minister, indien mogelijk, rechtstreeks in de wet. Indien bij het formuleren van een wet reeds vaststaat dat bepaalde voorschriften bij ministeriële regeling moeten worden gegeven, dient, indien dit wetgevingstechnisch niet tot problemen leidt, het stellen van die regels in de wet rechtstreeks aan de betrokken minister te worden gedelegeerd. Er wordt dan niet gekozen voor delegatie aan de regering (dus: gebruik van een AMvB), die op haar beurt dan weer aan de minister delegeert. Voor dat laatste is bijvoorbeeld reden als ten tijde van het formuleren van de wet voorzienbaar is dat er onderwerpen zullen zijn die voor opneming in een ministeriële regeling in aanmerking komen (volgens de criteria van Ar 2.24), maar nog onvoldoende duidelijk is in welke mate de meer wezenlijke aspecten van die onderwerpen in een algemene maatregel van bestuur een plaats behoren te krijgen (Ar 2.25).

Uitgangspunten voor wetgeving; het wetsvoorstel

De hiervoor aangegeven uitgangspunten zijn essentieel voor de regulering van de toegang tot de digitale overheid en zijn onverkort toegepast om een afgewogen geheel aan wet- en regelgeving tot stand te brengen. Ten eerste door de hoofdelementen (kaders) in de formele wet op te nemen, functioneel en techniekonafhankelijk – maar niet abstract of open – te formuleren. Ten tweede door nauwkeurig begrensde delegatiegrondslagen te hanteren, waar mogelijk en nodig te delegeren naar (aan het parlement voor te leggen) AMvB's. En ten derde door de uitwerking van (technische en administratieve en aan wijziging onderhevige) details in ministeriële regelingen te vervatten. Zo wordt een wettelijk stelsel gerealiseerd dat, in onderlinge samenhang bezien, recht doen aan de rechtstatelijke en democratische waarborgen.

Meer concreet, en in aansluiting op de hierna vermelde vragen die hierover worden gesteld door de fracties van **GroenLinks**, de **SP** en de **ChristenUnie**, leidt dit voor wat betreft het wetsvoorstel tot het volgende beeld.

HOOFDSTUK 1. ALGEMEEN

Artikel 1. Definities
Betreft de reikwijdte en de structurele elementen van de regeling (conform Ar 2.19).

Artikel 2. Reikwijdte
Betreft de reikwijdte van de regeling (conform Ar 2.19).

HOOFDSTUK 2. ALGEMENE REGELS

Artikel 3. Standaarden
Betreft reikwijdte en structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), delegatie naar AMvB (Ar 2.24).

HOOFDSTUK 3. DE GENERIEKE DIGITALE INFRASTRUCTUUR

Artikel 4. Informatieveiligheid
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), primair naar AMvB (Ar 2.24), te weten het voorgenomen Besluit digitale overheid.

Artikel 5. Verantwoordelijkheid voor het beheer
Betreft de reikwijdte en structurele elementen van de regeling (conform Ar 2.19), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23).

*De fracties van de **SP** en de **ChristenUnie** hebben in dit verband, refererend aan het advies van de Afdeling Advisering van de Raad van State bij het wetsvoorstel, gevraagd om in de wet zelf de centrale onderdelen van de gdi op te nemen. In het bijzonder verzoekt de fractie van de ChristenUnie om de uitgifte van publieke identificatiemiddelen wettelijk te regelen en niet in lagere regelgeving.*

Beide fracties lijken van mening dat de regering het advies van de Afdeling Advisering van de Raad van State ter zake niet heeft opgevolgd. Dit is echter wel het geval, zoals ook is aangegeven in het nader rapport in reactie op het advies. Het wetsvoorstel bevat namelijk de taken, verantwoordelijkheden en functionaliteiten met betrekking tot een aantal belangrijke voorzieningen van de generieke digitale infrastructuur (de centrale onderdelen), waarbij concretisering en uitwerking bij lagere regelgeving plaatsvindt. De grondslagen hiervoor worden in artikel 5 van het wetsvoorstel ingekaderd en begrensd. Zo is de taak van de minister van BZK voor de uitgifte van publieke identificatiemiddelen wettelijk verankerd in het eerste lid, onder a, van het wetsvoorstel

en nader uitgewerkt in twee voorgenomen AMvB's, te weten het Besluit digitale overheid (voor wat betreft de bescherming van persoonsgegevens) en het Besluit identificatiemiddelen voor natuurlijke personen WDO (voor wat betreft de eisen waaraan publieke middelen moeten voldoen). Anders dan de fracties lijken te menen, zit er derhalve geen licht tussen de zienswijze van de Afdeling Advisering van de Raad van State en die van de regering en voorziet het wetsvoorstel in de verankering van de elementen die de fracties van de SP en de ChristenUnie voorstaan.

HOOFDSTUK 4. TOEGANG TOT ELEKTRONISCHE DIENSTVERLENING

§ 4.1 Algemeen

Artikel 6. Betrouwbaarheidsniveaus
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25), te weten de voorgenomen Regeling authenticatieniveaus elektronische dienstverlening.

§ 4.2 Elektronische dienstverlening aan burgers

Artikel 7. Acceptatie burgermiddelen
Betreft reikwijdte en structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

Artikel 8. Gebruik in publieke domein
Betreft reikwijdte en structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

Artikel 9. Toelating identificatiemiddelen en diensten/ grondslag stelsel erkenningen
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), naar AMvB, in dit geval het Besluit identificatiemiddelen voor natuurlijke personen WDO, en subdelegatie naar ministeriële regeling (Ar 2.24).

Het kernelement van het wettelijke systeem, een toelatingsprocedure die afhankelijk is van een erkenning of een aanwijzing, wordt in de wet vastgelegd. Ten aanzien van de criteria voor toetsing en de regels over de toetsingsprocedure vindt gecontroleerde delegatie en voor zover nodig subdelegatie plaats. Daarmee wordt geborgd dat het parlement betrokken is bij de inhoud van gestelde eisen en het toetsingsproces en dat het in de gelegenheid is om te controleren of subdelegatie voldoende begrensd en goed gemotiveerd plaatsvindt.

Artikel 10. Regels ten aanzien van gebruik
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

§ 4.3 Elektronische dienstverlening aan bedrijven

Artikel 11. Erkenning bedrijfs- en organisatiemiddel en diensten
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), naar AMvB, zoals uitgewerkt in het conceptbesluit bedrijfs- en organisatiemiddelen WDO en subdelegatie naar ministeriële regeling (Ar 2.24).

Het kernelement van het wettelijke systeem, een toelatingsprocedure die afhankelijk is van een erkenning, wordt in de wet vastgelegd. Ten aanzien van de criteria voor toetsing en de regels over de toetsingsprocedure vindt gecontroleerde delegatie en voor zover nodig subdelegatie plaats. Daarmee wordt geborgd dat het parlement betrokken is bij de inhoud van gestelde eisen en het

toetsingsproces en dat het in de gelegenheid is om te controleren of subdelegatie voldoende begrensd en goed gemotiveerd plaatsvindt.

Artikel 12. Aanwijzing van attributen
Betreft structureel element van de regeling (conform Ar 2.19), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

Artikel 13. Rechten en plichten voor erkende diensten
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), naar AMvB, zoals uitgewerkt in het conceptbesluit bedrijfs- en organisatiemiddelen WDO en subdelegatie naar ministeriële regeling (Ar 2.24).

Artikel 14. Intrekking en overdracht van erkenning
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), naar AMvB, zoals uitgewerkt in het conceptbesluit bedrijfs- en organisatiemiddelen WDO en subdelegatie naar ministeriële regeling (Ar 2.24).

Artikel 15. Acceptatie bedrijfs- en organisatiemiddelen
Betreft reikwijdte en structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

HOOFDSTUK 5. BESCHERMING VAN PERSOONSGEGEVENS

Artikel 16. Bescherming persoonsgegevens
Betreft reikwijdte en structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar AMvB, zoals uitgewerkt in het conceptbesluit digitale overheid (Ar 2.24).

*In dit verband refereert de fractie van **GroenLinks** aan p. 24 van de memorie van toelichting bij het wetsvoorstel, waar als reden voor het regelen van de verwerking van persoonsgegevens bij algemene maatregel van bestuur staat, dat het voorstel het karakter heeft van een kaderwet. Dat is volgens voornoemde leden een toelichting die, samengevat, er een is van "het is een kaderwet omdat het een kaderwet is". De leden vragen hierop te reageren.*

Zoals hierboven uiteengezet, is het primaat van de wetgever het leidende principe bij het ontwerpen van dit wetsvoorstel. Door de hoofdelementen (kaders) in de wet zelf op te nemen, nauwkeurig begrensde delegatiegrondslagen te hanteren, waar mogelijk en nodig te delegeren naar AMvB's en de uitwerking van details in ministeriële regelingen te vervatten, wordt *een geheel* aan regels gerealiseerd waarmee een verantwoord en werkbaar evenwicht is gevonden tussen rechtstatelijke en democratische waarborgen en flexibiliteit.

Privacybescherming vormt een belangrijk onderdeel van het wetsvoorstel. Artikel 16 van de wet biedt grondslagen voor verwerking van persoonsgegevens door genoemde normadressaten *voorzover* dat noodzakelijk is voor de uitvoering en het verlenen van veilige toegang tot elektronische dienstverlening en het voorkomen van misbruik of oneigenlijk gebruik van de toegang. Daarmee verankert het wetsvoorstel de principes van de AVG en kadert het specifiek in welke publieke of private organisatie voor welke taak persoonsgegevens mag verwerken. Artikel 16 bevat daarmee de hoofdelementen van privacybescherming bij de toegang tot elektronische dienstverlening; uitwerking dient te geschieden bij AMvB. De omstandigheden waarin van de gedelegeerde bevoegdheid gebruik mag worden gemaakt zijn geconcretiseerd, alsmede de te regelen onderwerpen en doelen. Uitwerking geschiedt in het conceptbesluit digitale overheid, zoals bij uw Kamer voorgehangen. Hierin wordt per type verwerking en normadressaat uitputtend vastgelegd welke persoonsgegevens mogen worden verwerkt, aan wie deze mogen worden verstrekt en hoe lang deze mogen worden bewaard. In de Nota van toelichting bij het

conceptbesluit wordt toegelicht op welke wijze hiermee tegemoet wordt komen aan de waarborgen van de AVG, waaronder de beginselen van proportionaliteit en subsidiariteit. De regels lenen zich door hun mate van detaillering niet voor opname in de wet; dat is niet problematisch omdat het Besluit nauwkeurig is begrensd door artikel 16 van de wet. Overigens sluit deze wijze van reguleren aan bij de reeds bestaande systematiek van de huidige regelgeving op het gebied van de verwerking van persoonsgegevens ter zake van GDI-voorzieningen, te weten het Besluit verwerking persoonsgegevens GDI. Het Besluit digitale overheid beoogt (ingrijpende, namelijk ter zake van gegevensverwerking uitputtender) wijziging van voornoemd Besluit.

Ten aanzien van privacybescherming hecht ik eraan nog het volgende op te merken. Ik ben het met de leden eens dat privacybescherming goed geregeld moet worden. Echter: privacybescherming is meer dan het in wet- en regelgeving verankeren van verwerkingen van persoonsgegevens. Daadwerkelijke privacybescherming is – ook in het eID-stelsel – vooral een continue verantwoordelijkheid, om te zorgen dat in de praktijk getroffen maatregelen up to date blijven en er snel ingespeeld kan worden op de digitale wereld, waarin parallel aan de beschermingsmogelijkheden ook de digitale dreigingen zich snel ontwikkelen. Flexibiliteit is daarbij essentieel.

HOOFDSTUK 6. NALEVING

Artikel 17. Toezicht en handhaving
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), aanwijzingsgrondslag is nauwkeurig begrensd (conform Ar 2.23), naar ministerieel besluit (Ar 2.24).

Artikel 18. Bijzondere bevoegdheden
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21). Geen delegatie van regelgevende bevoegdheid.

Artikel 19. Informatieverstrekking
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21). Geen delegatie van regelgevende bevoegdheid.

HOOFDSTUK 7. FINANCIËLE BEPALINGEN

Artikel 20. Leges voor verstrekking publiek identificatiemiddel
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

Artikel 21. Doorberekening kosten
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23) en naar ministeriële regeling (Ar 2.24 en 2.25).

Artikel 22. Doorberekening aanvraag erkenning en toezicht op naleving erkenningseisen
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), naar AMvB, zoals uitgewerkt in het conceptbesluit identificatiemiddelen voor natuurlijke personen WDO en het conceptbesluit bedrijfs- en organisatiemiddelen WDO en subdelegatie naar ministeriële regeling (Ar 2.24).

Artikel 23. Evaluatie
Betreft – gelet op de specifieke uitwerking – structureel element van de regeling (conform Ar 2.19 en 2.21), maar wenselijk om in wet op te nemen. Geen delegatie van regelgevende bevoegdheid.

Artikel 24. Overgangsrecht bedrijfs- en organisatiemiddel
Betreft structureel element van de regeling (conform Ar 2.19 en 2.21). Geen delegatie van regelgevende bevoegdheid.

Art. 25. Parlementaire betrokkenheid bij gedelegeerde regelgeving
Betreft geen structureel element van de regeling (conform Ar 2.19 en 2.21), maar wenselijk om in wet op te nemen. Wanneer gebruik wordt gemaakt van regelgevende bevoegdheid wordt een concept van de belangrijkste AMvB's voorgehangen. Dit zijn: het Besluit digitale overheid, het Besluit bedrijfs- en organisatiemiddel WDO en het Besluit identificatiemiddelen voor natuurlijke personen WDO.

Art. 26 Innovatie
Betreft structureel element van de regeling (conform Ar 2.19), delegatiegrondslag is nauwkeurig begrensd (conform Ar 2.23), naar AMvB (Ar 2.24), waarbij voorzien is in parlementaire betrokkenheid.

Het bovenstaande overziend kan geconcludeerd worden, dat in casu een geheel aan regels wordt gerealiseerd waarmee aan de rechtstatelijke en democratische waarborgen wordt voldaan. In reactie op de vraag hierover van de leden van de fractie van de ChristenUnie, merk ik dan ook op, dat voor wat dit wetsvoorstel betreft geen sprake is van het verschuiven van de wetgevende macht van parlement naar regering of een afzonderlijke minister; de wetgever verliest niet aan betekenis. De Wet digitale overheid is een kaderwet in die zin, dat de hoofdelementen van de te regelen materie in de wet staan – overigens zonder daarbij open normen te hanteren – en de uitwerking daarvan op onderdelen aan de regering of de minister wordt overgelaten.

Het geheel moet in samenhang worden bezien en is, zoals hierboven toegelicht, ingericht en vormgegeven volgens de uitgangspunten van delegatie van regelgevende bevoegdheden. Hiermee wordt een wendbaar en efficiënt wettelijk kader gecreëerd dat recht doet aan het primaat van de wetgever zoals dat in het Nederlandse staatsbestel wordt gehanteerd en gewaardeerd.

De heer van Lochem concludeerde tijdens de deskundigenbijeenkomst van 30 juni jl. dat bij dit type wetgeving, dat op het terrein ligt van technologie en innovatie, de argumenten om daarin behoorlijk wat te delegeren, voor minstens een flink deel wel valide zijn. Hij adviseerde uw Kamer er minder op aan te dringen om toch nog zoveel mogelijk in de wet onder te brengen, maar wat meer dan normaal mee te kijken met de uitvoerende regelgeving en als Kamer vinger aan de pols te houden. In aansluiting daarop merk ik op, dat om die reden het wetsvoorstel voorziet in (zware) voorhang bij het parlement, waardoor van gecontroleerde delegatie sprake is.

Voor de volledigheid wijs ik op het overzicht dat in reactie op een vraag van de leden van de GroenLinks-fractie van de Tweede Kamer eveneens aan uw Kamer is toegezonden bij de beantwoording van de vragen over het (voorgehangen) conceptbesluit digitale overheid. Het betreft een overzicht van alle onderliggende regelgeving bij dit wetsvoorstel – algemene maatregelen van bestuur en ministeriële regelingen –, de onderwerpen die hierin worden geregeld alsmede de wettelijke grondslag ter zake (kamerstuk nr. 46).

Overige vragen

In de inleiding is aangegeven, dat bij de beantwoording zoveel mogelijk de indeling en volgorde van het verslag zijn aangehouden. In dat verband ga ik op deze plek in op een aantal elders in het verslag gestelde vragen, die (tevens) betrekking hebben het onderwerp van dit hoofdstuk, "De Wet digitale overheid als kaderwet".

*De leden van de **SP-fractie** stellen dat de voorliggende wet de identiteit van onze burgers gaat digitaliseren en daar de kaders voor geeft. Zij stellen dat niet alleen mensen met goede ideeën, maar ook partijen die in essentie andere belangen hebben dan die van het Nederlandse volk een product zullen willen aanbieden en dus toegang willen tot de basisregistratie. De leden van de SP-fractie schromen niet om deze partijen bij naam te noemen. Onder andere Facebook en Google moeten keer op keer hun koers bijstellen omdat ze over de grenzen van de wetgeving zijn gegaan.*

De leden menen dat een karige kaderwet bij lange na niet voldoende is om dit te borgen en de verwijzingen naar de AVG in de eerdere beantwoording van de vragen van de commissie laten zien dat er geen oog is geweest voor het grensoverschrijdende gedrag van deze partijen. Deze zeer machtige partijen kunnen met veel middelen lange juridische procedures voeren, zijn buiten Europa gevestigd en kunnen daarmee de bescherming van de gegevens van de Nederlandse burgers in gevaar brengen. Om dit te borgen vragen de leden van de SP-fractie twee essentiële zaken op te nemen in deze kaderwet en niet over te laten aan de keuze van de aanbieder of een algemene maatregel van bestuur: open source en decentrale opslag.

*Ook de leden van de fractie van de **ChristenUnie** vragen, refererend aan het memo 'Onze digitale identiteit staat op het spel' van Waag Technology & Society waarin wordt gezegd dat open source, dataminimalisatie en lokale opslag in de wet zouden moeten staan, waarom het pleidooi van deze deskundigen niet is gevolgd.*

In reactie op het bovenstaande merk ik op dat, zoals hierna bij hoofdstuk 3 nader zal worden toegelicht, de aspecten open source en decentrale opslag niet onder uitsluiting van closed source en centrale opslag zijn gereguleerd, omdat dit voor adequate privacybescherming niet nodig is, en dit bovendien onnodig belemmerend zou zijn voor het realiseren van andere belangrijke waarborgen en privacybeschermende maatregelen. Uitgangspunten bij de inrichting van het geheel aan wet- en regelgeving inzake toegang tot de digitale overheid zijn privacybescherming, veiligheid en betrouwbaarheid; daaraan worden, op basis van de wet en aansluitend bij de AVG en de eIDAS-verordening, eisen gesteld aan alle betrokken publieke en private partijen. Het is niet nodig, niet doelmatig en niet doeltreffend om daarbij ook specifieke eisen te stellen aan de wijze van opslag en de gebruikte software. Zoals ik aanstipte zijn dergelijke specifieke eisen niet de enige maatregelen die de bescherming van persoonsgegevens kunnen borgen. Opname van deze specifieke eisen in de wet zou andere beschermende maatregelen en oplossingen uitsluiten; daarmee zou de uitvoeringspraktijk de mogelijkheid worden ontnomen om te reageren op wijzigende dreigingen. Kortom, privacybescherming is een continu proces, dat op wetsniveau ingekaderd, maar niet dichtgeregeld moet worden. Voorts moet worden bedacht, dat als het wetsvoorstel zou voorschrijven dat oplossingen open source en decentraal moeten zijn, ook grote techbedrijven – die niet specifiek gericht zijn op het leveren van privacybeschermende inlogmiddelen, maar in theorie kunnen overwegen deze te gaan aanbieden – open source en decentrale oplossingen zouden kunnen leveren. Dit zou dus niet voorzien in hetgeen de aan het woord zijnde Kamerleden beogen. Waar het om gaat is dat de partijen, wie dat ook zijn, vooraf strikt worden gecontroleerd op hun specifieke oplossingen (die een combinatie van software en hardware zullen zijn) aan de hand van de toepasselijke eisen en daarop tijdens hun dienstverlening worden gecontroleerd. Daarin voorziet het wetsvoorstel. Hierna wordt daarop nader ingegaan.

Voor wat betreft het principe van dataminimalisatie wordt opgemerkt dat dit principe verankerd is in de – in de lidstaten van de EU rechtstreeks toepasselijke – AVG en artikel 16 van het wetsvoorstel en is uitgewerkt in het Besluit digitale overheid. Hierin wordt per type verwerking en (publieke of private) normadressaat uitputtend vastgelegd welke persoonsgegevens mogen worden verwerkt, aan wie deze mogen worden verstrekt en hoe lang deze mogen worden bewaard. De verwerking van de in het Besluit opgesomde persoonsgegevens is nodig en toereikend voor het verlenen van veilige toegang tot elektronische dienstverlening en het voorkomen van misbruik of oneigenlijk gebruik van de toegang, zodat burgers die in de problemen komen kunnen worden geholpen. Aldus wordt geborgd dat er niet meer persoonsgegevens worden verwerkt dan noodzakelijk.

*De leden van de fractie van de **ChristenUnie** lezen in de memorie van toelichting dat de overheid mee moet gaan in de 'digitale vaart der volkeren' om steeds meer diensten online te leveren. In haar visie vormt de Wet digitale overheid een eerste tranche van wetgeving ten behoeve van een verdere digitalisering van de overheid op verschillende niveaus. De memorie van toelichting stelt dat de onderhavige wet de meest urgente onderwerpen van regelgeving bevat (p. 1):*

- *de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid;*
- *het stellen van regels over informatieveiligheid;*
- *de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI);*
- *de digitale toegang tot publieke dienstverlening voor burgers (natuurlijke personen) en bedrijven (rechtspersonen en ondernemingen).*

De memorie van toelichting spreekt over een 'eerste tranche'. De leden vragen aan te geven welke tranches nog meer gaan volgen, hoe de verschillende tranches zich ten opzichte van elkaar verhouden en of de leden van de Eerste Kamer deze wet wel goed kunnen beoordelen als zij de andere tranches nog niet kennen.

In reactie op het bovenstaande merk ik op dat met dit wetsvoorstel de basis wordt gelegd waarop de digitale overheid zich de komende jaren ontwikkelt. In de voorliggende eerste tranche worden de zaken geregeld die nu nodig zijn. Dit wetsvoorstel, met bijbehorende uitvoeringsregelgeving, is daartoe afgebakend en zelfstandig bruikbaar en te beoordelen. Ondertussen staat het denken niet stil en oriënteren we ons op nieuwe ontwikkelingen en nut en noodzaak om op termijn nieuwe wet- en regelgeving voor te bereiden. In volgende tranches zullen verdere stappen worden gezet in de ontwikkeling van de digitale overheid. Dat geschiedt vanuit bepaalde waarden en uitgangspunten. Vanuit NL DIGIbeter zijn dat gebruiksvriendelijkheid, privacybescherming, veiligheid en betrouwbaarheid. Het is op dit moment niet te zeggen hoeveel tranches van de wet nog zullen volgen, wat deze zullen regelen en wat de planning hiervan is. Dit hangt af van de aard van de ontwikkelingen, alsmede van nut en noodzaak van verankering in wet- en regelgeving. Zaken waaraan voor een volgende tranche wordt gedacht zijn de verbetering van de persoonlijke informatiepositie van burgers (regie op gegevens), een door de overheid gevalideerde online identiteit die breed bruikbaar is – dat wil zeggen voor het afnemen van diensten bij publieke *en* private (commerciële) organisaties –, het verder integreren van het burger- en bedrijvendomein, bredere toepassing van standaarden voor digitale dienstverlening en machtigen. Over deze onderwerpen vindt de gedachtenvorming momenteel volop plaats.

*De leden van de **ChristenUnie-fractie** vragen of de Wet digitale overheid wel noodzakelijk is. Je kunt betogen, zo stelt de fractie, dat de wet niet noodzakelijk is in het licht van de AVG en de Europese eIDAS-regeling voor elektronische identiteiten. Vanuit dit perspectief kun je ook betogen, zo stelt de fractie, dat de wet name nodig is om private partijen de mogelijkheid te geven om via een centrale architectuur inlogmiddelen te ontwikkelen.*

In reactie op het bovenstaande merk ik op, dat het belangrijkste onderwerp dat opname in een wet rechtvaardigt, de verplichtingen zijn voor (semi-)overheden om hun diensten in te delen naar betrouwbaarheidsniveau en ter zake alleen toegelaten (erkende) inlogmiddelen te accepteren. Dit zijn dermate essentiële normen, mede gelet op de aanspraken die daaruit voor burgers en bedrijven voortvloeien, dat opname daarvan in een wet vanuit een oogpunt van rechtszekerheid en rechtsbescherming nodig is. Voorts, en in samenhang met het voorgaande, is het wetsvoorstel nodig om de toelating (erkenning) van inlogmiddelen en –diensten van private partijen te reguleren. Immers: voorschriften die de grondslag vormen voor een stelsel van vergunningen of een stelsel waarbij anderszins de toelaatbaarheid van handelingen afhankelijk wordt gesteld van toestemming van de overheid dienen – eendachtig het primaat van de wetgever – zoveel mogelijk in de wet zelf te worden opgenomen (Ar 2.21). Ook van andere "hoofdelementen" van de materie ligt wettelijke verankering in de rede, zoals hiervoor reeds artikelsgewijs is uiteengezet. Zo is – ook ingevolge de AVG – een nationaal-wettelijke grondslag nodig om mogelijk te maken dat private partijen het burgerservicenummer kunnen verwerken.

*De fractie van de **ChristenUnie** vraagt naar de situatie in andere landen. Hebben die ook WDO-achtige wetten? Welke keuzen worden daar gemaakt met betrekking tot de software (centraal, decentraal, open source, closed source, etc.)?*

In reactie op deze vraag merk ik op, dat meerdere EU-lidstaten een eID-stelsel kennen, waarin naast publieke inlogmiddelen tevens - via een open stelsel toegelaten - private inlogmiddelen functioneren. Enkele lidstaten, zoals België, kennen WDO-achtige wetten. De gemaakte keuzes verschillen per lidstaat en zijn afhankelijk van reeds bestaande nationale stelsels op het punt van identificatie, informatiebeveiliging en privacybescherming. Dit houdt verband met het feit, dat de bovenliggende Europese regels en uitgangspunten (waaronder de AVG, de eIDAS-verordening en de richtlijn inzake open data) aan de lidstaten de ruimte laten om eigen keuzes te maken, mits aan bepaalde minimumeisen wordt voldaan.

3. Privacybescherming

In dit hoofdstuk worden de door de fracties gestelde vragen beantwoord over gegevensverwerking door private partijen, waaronder profiling, pseudonimisering, privacy en security by design, gebruik van (veiligheids-)standaarden, open source software en de wijze van gegevensopslag. De vragen die de leden hebben gesteld adresseren vanuit verschillende nuances privacybescherming, maar hebben als gemene deler dat ze wijzen op het grote belang van bescherming van persoonsgegevens en de zorg die de leden daarover hebben. Teneinde nog beter tegemoet te komen aan de geuite vragen en zorgen, ben ik voornemens een wetswijziging in te dienen waarbij het verhandelverbod inzake gegevens, privacy by design en open source als hoofdelementen van de te regelen materie wettelijk worden verankerd. Dit voornemen wordt bij de desbetreffende onderdelen in dit hoofdstuk toegelicht.

Laat ik om te beginnen stellen dat ik het grote belang van privacybescherming ten volle onderschrijf en de zorgen daarover begrijp. Ik beschouw het als mijn verantwoordelijkheid om dat belang te bewaken. Dit is de essentie van het wetsvoorstel en daarom worden de vragen over privacybescherming vanuit die invalshoek beantwoord. In dat verband zeg ik uw Kamer toe het commercieel uitnutten van gegevens door private partijen te verbieden, privacy bij design te verplichten en open source te verankeren.

Ik hecht er aan te benadrukken, dat privacybescherming, veiligheid en betrouwbaarheid de kernprincipes zijn die ten grondslag liggen aan dit wetsvoorstel. Hieraan worden geen concessies gedaan. Wel worden met in achtneming van deze principes keuzes gemaakt. Daarbij gaat het er om de verwerking van persoonsgegevens – waar mogelijk met technische maatregelen – tot een minimum te beperken. Tegelijkertijd moet ervoor gezorgd worden dat burgers, die in de problemen komen als zij bijvoorbeeld een inlogmiddel kwijt zijn of er door anderen misbruik van hun inlogmiddel wordt gemaakt, geholpen kunnen worden zodat onjuist gebruik van persoonsgegevens kan worden hersteld en schade kan worden voorkomen. Ook dat vormt een essentieel onderdeel van privacybescherming, en voor dat doel is het nodig om over een zekere mate van herleidbaarheid te kunnen beschikken. Want hoe goed ook beschermende maatregelen worden getroffen in systemen, of dat nou eID of andere systemen zijn: absolute veiligheid is nooit te garanderen. Daarom is het van essentieel belang om daarop voorbereid te zijn en hier rekening mee te houden.

De keuzes die ik maak om een goede balans te bieden in de bescherming van persoonsgegevens licht ik in het onderstaande toe. Dit doe ik aan de hand van een aantal (deel)thema's, waarbinnen de gestelde vragen zoveel mogelijk zijn geclusterd. Daarbij geldt dat de eisen aan de toelating van inlogmiddelen, waaronder de eisen die richting private partijen worden gehanteerd met betrekking tot gebruikte software, niet-verhandelbaarheid en standaarden, nader worden uitgewerkt in lagere regelgeving. De AMvB's bij het wetsvoorstel zijn aan Uw Kamer voorgelegd. In de beantwoording wordt hiernaar verwezen.

Middels het geheel aan ge- en verboden, toezicht en handhaving tezamen met uitvoering in (ICT-) systemen en voorzieningen, wordt de adequate veiligheid, betrouwbaarheid en privacybescherming geboden die de regering voorstaat en die tegemoetkomt aan de wensen van uw Kamer.

In het navolgende zal ik, gegroepeerd naar onderwerp, de door de leden gestelde vragen beantwoorden.

Gegevensverwerking door private partijen

*De leden van de **GroenLinks-fractie** vragen of de regering de grote Amerikaanse techbedrijven voldoende integer en vertrouwelijk acht en de informatieveiligheid (beschikbaarheid, integriteit en vertrouwelijkheid ("BIV-vereisten) kunnen bieden.*

Voorop staat dat alle bedrijven die inlogmiddelen willen aanbieden de BIV- en alle overige vereisten die ik stel aantoonbaar moeten naleven. Zij worden daarop vooraf bij de toelating gecontroleerd en met regelmaat gedurende hun dienstverlening. Dat is waar het om gaat en dat staat los van de beleving en van de achtergrond of vestigingsland van het bedrijf. Als onderdeel van de toelating van private partijen kan een Bibob-toets worden uitgevoerd. Bovendien heb ik de mogelijkheid om ingeval van cyberdreigingen of dreigingen tegen de staatsveiligheid een toelating te weigeren of in te trekken. Ten aanzien van persoonsgegevens zal, ter voorkoming van commerciële uitnutting van gegevens die partijen verkrijgen, wettelijk worden vastgelegd dat zij die niet mogen verwerken voor andere doeleinden dan vervaardiging en werking van het inlogmiddel. Profilering of verkoop van gegevens mag dus niet. Partijen worden daarop voorafgaand aan de toelating gecontroleerd; ook gedurende hun dienstverlening worden ze hierop met regelmaat gecontroleerd. Bij overtreding kan uitsluiting van de dienstverlening volgen of een omzetgerelateerde boete.

*De leden van de fractie van **GroenLinks** merken op dat de DigiD-aanbieder Logius verschillende maatregelen heeft getroffen om het gebruik van profielen te voorkomen. De leden constateren dat in het huidige wetsvoorstel regels om zulke maatregelen voor private eID's te verplichten ontbreken. Zij vragen waarom de regering dit niet minimaal zo stevig, of eigenlijk nog steviger door de groei van data heeft verankerd.*

In reactie op deze vraag zeg ik u toe dat in het Besluit identificatiemiddelen voor natuurlijke personen WDO, een AMvB bij het wetsvoorstel die bij het parlement is voorgehangen, wordt verboden dat persoonsgegevens worden gebruikt voor het aanmaken van profielen. Het besluit zal voor publieke voorzieningen en private partijen tevens een verplichting tot gescheiden opslag van gebruiks- en gebruikersgegevens bevatten, waardoor koppeling van loggegevens aan personen niet mogelijk is (paragraaf 4.1.3). Het combineren van deze gegevenssets wordt slechts toegestaan wanneer dat noodzakelijk is om misbruik of incidenten te herkennen, te herstellen en gebruikers op de hoogte te stellen en te helpen. Voor dit proces zullen extra regels worden opgenomen (paragraaf 4.1.3 besluit). Om te benadrukken dat het verhandelen van persoonsgegevens niet is toegestaan, zal bovendien aan het wetsvoorstel worden toegevoegd dat een erkenning (toelating) slechts aan een private partij wordt verleend indien zijn verdienmodel betrekking heeft op het identificatiemiddel waarop de aanvraag ziet. Dat betekent dat door mij wordt getoetst op het bestaan van een directie relatie tussen de vergoeding en geleverde dienst, alsmede of diensten niet door andere organisatieonderdelen worden gefinancierd.

*De leden van de **GroenLinks-fractie** vragen of de regering zicht heeft op de toekomstige verdienmodellen en of er op enigerlei wijze geld verdiend mag worden met de data. Voor het publieke domein is verkoop van data niet toegestaan. Hoe kan de regering hier toezicht op houden of gaat zij simpelweg uit van vertrouwen?*

In reactie hierop zij benadrukt, dat het toekomstige verdienmodel gehaald zal moeten worden uit de uitgifte van inlogmiddelen. Er mag, zoals eerder aangegeven, door private partijen geen geld worden verdiend aan het op enigerlei wijze commercieel uitnutten van (persoons)gegevens die in

het kader van eID beschikbaar zijn. Het wetsvoorstel staat dit niet toe; dit zal bij wetswijziging nader worden aangevuld. Hierop wordt toezicht gehouden. De eisen in en op basis van het wetsvoorstel zullen daarom naar verwachting juist een positieve prikkel vormen voor partijen die zich professioneel toeleggen op veilige inlogmethoden, en niet voor partijen die op andere wijze geld willen verdienen aan persoonsgegevens. Bovendien wordt mensen daarmee de mogelijkheid geboden om te kiezen voor een inlogmiddel van een aanbieder waarbij zij niet indirect met hun persoonsgegevens en dus niet met hun privacy betalen.

*De leden van de **GroenLinks-fractie** merken op dat ook profilering niet is toegestaan, maar zonder inzicht in de broncodes niet controleerbaar. Is de regering het hiermee eens? Hoe denkt de regering adequaat toezicht te kunnen houden of bijvoorbeeld op kredietwaardigheid wordt geprofileerd? Het Agentschap Telecom en de Autoriteit Persoonsgegevens zullen immers niet in de systemen van bijvoorbeeld Google mogen kijken.*

In reactie hierop merk ik op dat ik de conclusie niet deel dat controleerbaarheid alleen mogelijk is indien de broncode van software beschikbaar is. Zoals ik eerder heb aangeven dienen partijen bij toelating, zowel in het ontwerp als inzake de functionele werking, aan te tonen dat aan de gestelde vereisten wordt voldaan. Dat vergt dat partijen ter zake inzicht bieden in hun systemen. Indien Google een verzoek tot toelating zou doen, geldt dat voor Google onverkort. Met andere woorden: als zij niet voldoen, dan worden zij niet toegelaten. Met het Besluit identificatiemiddelen voor natuurlijke personen WDO zal worden verboden dat persoonsgegevens worden gebruikt voor het aanmaken van profielen. Het besluit voorziet in een verplichting tot gescheiden opslag van gebruiks- en gebruikersgegevens waardoor koppeling van loggegevens aan personen niet mogelijk is. Een uitzondering hierop is wanneer het combineren van gegevens noodzakelijk is om misbruik of incidenten te herkennen, te herstellen en gebruikers op de hoogte te stellen. Voor dit proces zullen extra regels worden opgenomen (paragraaf 4.1.3). Op overtreding hiervan staat in ultimo intrekking van de erkenning of een omzetgerelateerde boete. Ik deel uw gezichtspunt dat de handelwijze van private partijen nadrukkelijk aandacht behoeft en ik zal daarom met het AT afspraken maken over het door hen te houden toezicht op het verbod van commerciële uitnutting.

*De leden van de fractie van de **ChristenUnie** merken op dat deze inloggegevens vervolgens door private partijen kunnen worden gebruikt voor het ontwikkelen van hun eigen business. Hoe kijkt de regering aan tegen dit dreigende gevaar, mede in het licht van kritische vragen over en onderzoeken naar de handel en wandel van grote techbedrijven?*

In reactie op het bovenstaande zeg ik u toe, dat het verhandelen van persoonsgegevens bij wet zal worden verboden. Het is in strijd met de AVG, met in het wetsvoorstel vastgelegde en in uitvoeringsregelgeving nader uit te werken regels, waaronder het verbod om gegevens te gebruiken voor anderen doeleinden. Profilering en verkoop van gegevens mag dus niet. Dit staat overigens los van het feit, dat aanbieders van inlogmiddelen over deze gegevens mogen en zelfs moeten beschikken om burgers die slachtoffer worden van misbruik te kunnen helpen.

*De leden van de fractie van de **ChristenUnie** merken op dat private partijen voor dit soort inlogmiddelen twee typen verdienmodellen zullen kunnen ontwikkelen. Het eerste verdienmodel is het laten betalen door de gebruiker, het tweede is gerelateerd aan alle persoonsgegevens die private partijen verzamelen om een nieuwe business te ontwikkelen. In dit model kan sprake zijn van het 'verkopen van gegevens' maar ook het gebruiken van deze gegevens voor profilering en micro-targeting. De leden van de fractie van de ChristenUnie vragen de regering of zij overleg heeft gehad met private partijen over hun verdienmodel en wat daar uit gekomen is. Ook vragen zij of de huidige Wet digitale overheid het tweede verdienmodel volledig onmogelijk maakt. Indien het antwoord 'ja' is, dan is de vraag hoe goed dit gehandhaafd kan worden met het oog op (machtige) private partijen. Een andere vraag is waarom private partijen eigenlijk dit soort inlogmiddelen zouden moeten aanbieden. Heeft het geen voorkeur alleen een of enkele publieke partijen toe te laten?*

In reactie op het bovenstaande benadruk ik mijn toezegging dat het verdienmodel voor private partijen niet gebaseerd mag zijn op het op het verhandelen van persoonsgegevens. Andere (commerciële) uitnutting van gegevens is verboden. Daar zal door mij, het AT en de AP nadrukkelijk op worden toegezien en gehandhaafd. Het is wenselijk naast publieke middelen ook private middelen toe te laten, om voor gebruikers brede beschikbaarheid en een terugvaloptie te realiseren. Ik hecht eraan om in dit verband op te merken dat marktwerking of het bieden van marktkansen geen doel op zich is. Echter, een marktmechanisme brengt ook vitaliteit met zich mee waarbij doorlopend wordt gestreefd naar betere en in dit verband dus veiligere producten met nieuwe beschermingsmethoden. Daarvan wil ik, binnen de strenge privacygrenzen die ik stel, gebruikmaken zodat het kan leiden tot betere bescherming van de burger.

*De leden van de fractie **van de ChristenUnie** merken op dat in de deskundigenbijeenkomst van 30 juni 2020 veel deskundigen hebben gewezen op de gevaren van de huidige Wet digitale overheid. Zo waarschuwde de heer Wolfsen van de Autoriteit Persoonsgegeven voor het feit dat deze wet onze 'democratische rechtsstaat kwetsbaar kan maken'. De heer Böhre van Privacy First waarschuwde voor de enorme risico's voor de privacy van burger gezien de 'commerciële aard van de nieuwe eID-aanbieders, waaronder techbedrijven met dubieuze businessmodellen en schimmige profileringspraktijken'. Zou de regering op deze mogelijke gevolgen kunnen reflecteren? Hoeveel garanties kan zij geven dat internationale ICT-giganten – die door hun omvang veel macht hebben – zich ook aan de regels gaan houden bij het aanbieden van inlogmiddelen in Nederland? Wat zou dat kunnen betekenen voor de Wet digitale overheid?*

In reactie herhaal ik de gedane toezegging dat commerciële uitnutting van persoonsgegevens anders dan voor de inlogdienstverlening categorisch zal worden verboden. Er zal vanzelfsprekend ook op worden gecontroleerd: voorafgaand aan de toelating (erkenning) en met regelmaat tijdens de dienstverlening. Het AT en de AP houden toezicht. Bij overtreding is het mogelijk om de partij uit het eID-stelsel te zetten en om een omzetgerelateerde boete op te leggen.

*De leden van de **D66**-fractie geven aan het zeer onwenselijk te vinden wanneer er een mogelijkheid is voor commerciële partijen om gevoelige data te vergaren door inloggegevens te koppelen. De staatssecretaris geeft in zijn brief aan dat er doelbinding, onder meer in relatie tot private partijen, wordt opgenomen. Dit zou moeten voorkomen dat commerciële partijen inloggegevens kunnen misbruiken.*

In reactie op het bovenstaande benadruk ik, dat binnen het eID-stelsel gegevens te allen tijde in overeenstemming met de AVG moeten worden verwerkt en de noodzaak van verwerking moet bestaan. Het verhandelen van persoonsgegevens wordt wettelijk verboden. In het concept Besluit digitale overheid, dat op 17 maart 2020 bij uw Kamer is voorgehangen, zijn voorts strenge regels opgenomen betreffende het verwerken van persoonsgegevens in de voorzieningen in het eID-stelsel. De identificatiemiddelen functioneren hiermee in samenhang; ook functioneren ze conform de bepalingen in het Besluit digitale overheid over de verwerking van persoonsgegevens door private partijen (artt. 5b, 5e, 9b, 14b). Doelbinding wordt eveneens opgenomen in het Besluit identificatiemiddelen voor natuurlijke personen WDO (art. 4, onder b). Daarnaast geldt dat dit besluit zal voorzien in een verplichting tot gescheiden opslag van gebruiks- en gebruikersgegevens waardoor koppeling van loggegevens aan personen niet mogelijk is (artikel 3, lid 1, onder f). Een uitzondering hierop is wanneer het combineren van gegevens noodzakelijk is om misbruik of incidenten te herkennen, te herstellen en gebruikers op de hoogte te stellen. Voor dit proces zijn extra regels opgenomen (paragraaf 4.1.3). Bovendien voorziet dit besluit in een verbod voor partijen om gegevens op basis van toestemming van de gebruiker te verhandelen. Daarmee doe ik mijn toezegging gestand te verzekeren dat gegevens van burgers niet commercieel worden uitgenut door bijvoorbeeld profiling of verkoop ervan (paragraaf 4.1.3). In ditzelfde besluit wordt tevens opgenomen dat de identificatiemiddelen functioneren overeenkomstig de hen betreffende artikelen in het Besluit digitale overheid, waarin onder andere de bewaartermijnen van de te verwerken gegevens is opgenomen (artt. 5b, 5e, 9b en 14b). Voldoet een middel niet aan deze eisen, dan wordt het niet toegelaten.

*De **D66-fractie** vraagt voorts wie er verantwoordelijk is voor het vernietigen van onder meer inloggegevens als ze niet meer nodig zijn voor het doel, en hoe wordt gecontroleerd dat dit ook daadwerkelijk gebeurt.*

In reactie hierop merk ik op, dat in het Besluit digitale overheid gedetailleerde bewaartermijnen zijn opgenomen voor (soorten) gegevens. Partijen zijn hiervoor in eerste instantie zelf verantwoordelijk. Voorafgaand aan de toelating en tijdens hun dienstverlening worden zij op de naleving van deze regels gecontroleerd, en zal indien nodig worden gehandhaafd.

*De **D66-fractie** constateert dat er mogelijk verdienmodellen aan verkeerd gebruik van data gekoppeld kunnen worden. Graag verzoeken de leden van de D66-fractie een reflectie van de regering op mogelijke verdienmodellen die gestoeld zijn op deze data.*

Zoals eerder betoogd, zeg ik u toe dat voor verdienmodellen anders dan voor inloggen geen plaats is. Commerciële uitnutting van gegevens voor overige doelen dan eID zal bij wet worden verboden, zoals gewenst door uw fractie.

*De leden van de **PVV-**fractie vragen, refererend aan het schriftelijke verslag en de deskundigenbijeenkomst, of de regering nader uiteen kan zetten in hoeverre in voorliggend wetsvoorstel voorkomen wordt dat er met gegevens geld wordt verdiend, anders dan het enkel verkopen van gegevens als 'handelswaar'. Kan de regering tevens aangeven hoe daar toezicht op wordt gehouden en in hoeverre dit toezicht kan worden geëffectueerd bij grote techbedrijven, indien deze diensten gaan aanbieden? Kan de regering ook aangeven hoe voorkomen wordt dat er sprake kan zijn van koppeling van gegevens bij het inloggen (en daarmee het risico op profilering)? En kan de regering aangeven waarom niet expliciet wordt gekozen voor een decentraal systeem om daarmee profilering zoveel mogelijk te voorkomen? Graag ontvangen de aan het woord zijnde leden ook een toelichting hoe burgers effectief controle kunnen houden op de uitwisseling van gegevens.*

Zoals toegezegd, zal middels voorschriften in het wetsvoorstel en in de uitvoeringsregelgeving worden voorkomen dat aan eID-gegevens geld wordt verdiend. Zo wordt, in lijn met de AVG, voorgeschreven dat gegevens alleen mogen worden verwerkt voor zover dat noodzakelijk is voor het in de WDO beschreven doel, te weten de taak om burgers veilig te laten inloggen. Daarbij is bepaald dat het verboden is om gegevens voor andere doeleinden te verwerken, ook niet met toestemming van de gebruiker. Bij wetswijziging zal daaraan worden toegevoegd dat verhandelen van gegevens niet is toegestaan. Dit betekent dat met de gegevens niet mag worden geprofileerd, en dat de gegevens niet mogen worden verkocht. Daarnaast zal worden bepaald dat gebruikers en gebruiksgegevens gescheiden moeten worden opgeslagen, en niet geautomatiseerd mogen worden gekoppeld. Dit zorgt er voor dat gegevens ook niet kunnen worden ingezet voor de genoemde acties.

Om te zorgen dat de regels ook daadwerkelijk worden nageleefd zal hierop voorafgaand aan de dienstverlening, bij de toelating, maar ook met regelmaat gedurende de dienstverlening controle plaatsvinden. Bedrijven dienen daartoe openheid en inzage te geven in de functionele werking van hun oplossingen. Niet alleen hoe zij het op papier hebben voorzien, maar ook in de wijze waarop het feitelijk werkt. Dat geldt voor grote techbedrijven, maar ook voor andere bedrijven. Als zij geen volledige openheid kunnen of willen geven in de wijze waarop hun oplossing werkt en hoe zij voldoen aan de gestelde eisen, dan kunnen en zullen zij niet worden toegelaten.

Ten aanzien van de vraag waarom niet expliciet wordt gekozen voor een decentraal systeem merk ik op, dat er ten aanzien van het aspect doelbinding c.q. het verbod op verhandeling geen verschil is tussen centrale of decentrale oplossingen. Risico's zijn niet gelegen in de opslag van attributen, maar in de gegevens die worden gegeneerd door de werking van het systeem, ongeacht of dit centraal of decentraal is. Zoals ik eerder aangaf, worden ook bij als decentraal bekend staande

oplossingen loggegevens bijgehouden. Dit gebeurt om goede redenen, namelijk om gebruikers te kunnen helpen indien zij problemen ondervinden als zij bijvoorbeeld slachtoffer worden van misbruik of diefstal van hun inlogmiddel. Om deze reden dienen de maatregelen zich te richten op het voorkomen van ongewenst gebruik van loggegevens, in plaats van op het categorisch vermijden van deze gegevens. Gegevens kunnen in geval van problemen immers juist ten dienste staan van gebruikers.

In reactie op de vraag, hoe burgers controle kunnen houden op hun eigen gegevens, merk ik het volgende op. Om te zorgen dat burgers weten welke middelen zij hebben aangevraagd, draag ik zorg voor een register waarin een overzicht van hun middelen beschikbaar is. Daarnaast kunnen burgers zich richten tot de aanbieder van inlogmiddelen om inzage in hun gegevens te verkrijgen. Dat kan op basis van het inzagerecht ingevolge de AVG. Het is belangrijk dat burgers deze controle kunnen hebben en kunnen zien met wie de gegevens zijn uitgewisseld. Alleen zo kunnen zij daartegen bezwaar maken of aan te bel trekken als zij merken dat hun gegevens zijn gebruikt zonder dat zij dat wisten, hetgeen kan duiden op misbruik of identiteitsfraude.

*De fractie van de **PVV** vraagt of de regering kan aangeven in hoeverre binnen het kader van deze wet voorkomen wordt dat (private) partijen gegevens opslaan op buitenlandse servers, wat gevolgen kan hebben voor de controleerbaarheid van (de omgang met) deze gegevens, waaronder zeer privacygevoelige gegevens zoals BSN en medische gegevens. In hoeverre acht de regering het risico aanwezig de regie te verliezen over de eigen digitale infrastructuur?*

In reactie op het bovenstaande merk ik op, dat bij het toelaten van inlogmiddelen controle plaatsvindt op grond van de gestelde eisen. Het doel daarvan is om de belangen – dat kunnen privacybelangen zijn, maar ook belangen rond cyber- of staatsveiligheid - te verzekeren. Dat kan ertoe leiden dat gegevens niet in bepaalde landen mogen worden opgeslagen, of dat aanvullende waarborgen gerealiseerd moeten worden. De eisen vloeien onder meer voort uit de eIDAS-verordening en de AVG. Op basis van de AVG moeten gegevens niet worden verwerkt in landen waar geen passend, met de AVG vergelijkbaar beschermingsniveau geldt. Daarnaast zullen inlogmiddelen niet toegelaten worden indien zwaarwegende redenen ten aanzien van cyber- en staatsveiligheid in het geding zijn en zich daartegen verzetten. Dat is vastgelegd in artikel 9, zesde lid, van het wetsvoorstel. Hierop zal, in lijn met uw wens, specifiek worden toegezien. Van een dergelijke reden zou sprake kunnen zijn als gegevensverwerking plaatsvindt in landen waar dat op enig moment, gelet op bepaalde aanwijzingen of digitale dreigingen, niet verantwoord wordt geacht. In die zin is het dus mogelijk om te voorkomen dat gegevens op bepaalde buitenlandse servers worden verwerkt. Echter, het doel is niet om per definitie verwerking op buitenlandse servers te voorkomen, maar om te zorgen dat de belangen van burgers en het publieke belang te allen tijde verzekerd zijn, en regie kan worden gehouden over de eigen digitale infrastructuur.

Veiligheid, privacy - en security by design

*De leden van de **GroenLinks-fractie** stellen vast dat informatiebeveiliging traditioneel wordt bekeken vanuit de BIV-driehoek: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Zij vragen of het vanuit deze benadering überhaupt wel wenselijk is om private partijen nieuwe ruimte te geven in dit domein.*

In reactie op deze vraag merk ik op, dat het primair van belang is dat de BIV vereisten aantoonbaar worden nageleefd. Het draait om de vraag, of een organisatie daar feitelijk en professioneel toe in staat is. Of een organisatie publiek of privaat van karakter is, staat daar los van.

*De leden van de **GroenLinks-fractie** vragen of de regering het eens is met de leden, dat concepten als open source van broncodes en privacy by design niet aantrekkelijk zijn voor private aanbieders. Ook vragen zij wat het gevolg is dat privacy by design niet als voorwaarde is opgenomen in de wet.*

In reactie merk ik op, dat de eerste vraag wordt beantwoord in het cluster open source - closed source. In reactie op de tweede vraag merk ik op dat de, rechtstreeks in de EU-lidstaten toepasselijke, AVG, verwerkingsverantwoordelijken verplicht om te werken volgens de principes van privacy by design en privacy by default. Dat betekent dat er bijvoorbeeld bij het ontwerpen van een informatiesysteem of nieuw product rekening moet worden gehouden met privacy (by design). Ook moet ervoor gezorgd worden dat er standaard zo min mogelijk persoonsgegevens worden verwerkt (by default). Ingevolge art. 25 AVG moeten er door het hele proces van het verwerken van persoonsgegevens technische en organisatorische maatregelen genomen worden om aan deze beginselen te voldoen. Nationaal-wettelijke verankering van deze principes is, vanwege het 'overschrijfverbod' ter zake van EU-verordeningen, niet nodig en zelfs niet toegestaan. De principes gelden reeds door de rechtstreekse toepasselijkheid. Dit betekent dat zowel voor mij als bevoegd gezag, als voor partijen die toegelaten (erkend) willen worden, de plicht geldt tot het hanteren van privacy by design; in de techniek en de uitvoering is dit principe leidend. Hoewel de toepassing van en toetsing aan privacy by design dus reeds is 'afgedekt', geeft de door de fracties geuite zorg mij aanleiding om dit principe te verankeren in het wetsvoorstel. Hiertoe zal een wetswijziging worden ingediend die om redenen van duidelijkheid en rechtszekerheid ertoe strekt bij de toelating van inlogmiddelen een extra nationaal-wettelijk criterium te hanteren. Door privacy by design toe te voegen wordt geëxpliciteerd dat een aanvraag kan worden afgewezen wanneer niet aan het beginsel wordt voldaan.

*De fractie van **Groen Links** vraagt of de regering bereid is om het gebruik van pseudoniemen voor burgers toe te staan. Waarom heeft de regering hier niet louter voor gekozen?*

In reactie op deze vraag merk ik op, dat uitgangspunt bij de eisen die aan inlogmiddelen worden gesteld is dat er waarborgen gelden ten aanzien van betrouwbaarheid, veiligheid en privacy. Dit kan op meerdere manieren ingevuld worden. In het Besluit identificatiemiddelen voor natuurlijke personen, dat wordt voorgelegd aan uw Kamer, worden daarom doelvoorschriften gesteld, waarbij het belangrijk is dat de waarborgen worden ingevuld. Een manier waarop dit kan is door het gebruik van pseudoniemen. Het Besluit identificatiemiddelen voor natuurlijke personen maakt het mogelijk om bij ministeriële regeling voor te schrijven dat met pseudoniemen gewerkt wordt (zie artikel 5 Besluit). Daarvoor kan worden gekozen indien een verantwoord evenwicht kan worden gevonden tussen het gebruik van pseudoniemen en herstelvermogen.

*De leden van de fractie **van de ChristenUnie** merken op dat de VNG in het onderzoek Technische Analyse Digitale Identiteit een uitvoerig onderzoek heeft gedaan naar protocollen en oplossingen die relevante functionaliteiten mogelijk maken en die alle veiligheidsrisico's mitigeren. De conclusie van de VNG is dat protocollen zoals IRMA, Sovrin en Trustchain het meest kansrijk zijn. De leden van de fractie van de ChristenUnie vragen of de regering bekend is met dit onderzoek, of zij de conclusie van dit onderzoek deelt en welke conclusies zij daar met betrekking tot de Wet digitale overheid uit zou willen trekken. Daar komt het volgende bij. Een initiatief als IRMA is van Nederlandse bodem en betreft een niet-commercieel initiatief. Hoe kijkt de regering naar dit initiatief? Zou dit een publiek alternatief kunnen zijn? En wat denkt zij van Sovrin en Trustchain? De leden verzoeken mij om te reflecteren op bestaande initiatieven.*

In reactie merk ik op dat het bedoelde document niet goedgekeurd is door de VNG en dat het daarmee geen VNG-publicatie betreft, maar slechts een interne technische verkenning naar invullingen van inlogoplossingen. Zoals ik eerder heb opgemerkt, zijn er meerdere aspecten van belang dan de vragen in het onderzoek. Ik benadruk nogmaals dat ik geen van dergelijke initiatieven uitsluit – de WDO biedt ruimte aan dit initiatief en soortgelijke initiatieven – maar dat bepalend is of de initiatieven voldoen aan de aan inlogmiddelen gestelde eisen, waaronder de Europese regels voor inlogmiddelen (eIDAS) en of deze adequate bescherming van persoonsgegevens bieden op basis van de AVG en overige privacyregels.

*De leden van de **FVD-fractie** vragen of de regering kan garanderen dat deze Wet digitale overheid en het toelatingskader voor private middelen voorkomen dat data van personen via centrale verwerkers lekken, gestolen worden, dan wel oneigenlijk worden gebruikt. In dit verband geven leden van de fractie van **GroenLinks** aan dat de informatiebeveiliging bij de overheid vaak nog te wensen overlaat en dat slechte beveiliging kan leiden tot datalekken, die bij de overheid meer impactvol kunnen zijn vanwege de veel aanwezige bijzondere of gevoelige persoonsgegevens. Deze leden vragen welke mechanismen de overheid heeft ingebouwd om datalekken te voorkomen, welke lessen zijn getrokken uit het verleden en of hier documentatie over beschikbaar is.*

In reactie op de vragen van de leden van de FVD-fractie en de GroenLinks fractie merk ik in de eerste plaats op dat datalekken - of er nu met centrale of decentrale systemen wordt gewerkt - nooit volledig kunnen worden voorkomen. Datalekken vinden immers plaats vanwege meerdere factoren, technische maar ook menselijke. Zij kunnen nooit volledig worden voorkomen, maar als het gebeurt moet er alles aan gedaan kunnen worden om de gevolgschade zo klein mogelijk te houden. Juist daarom zeg ik u toe in het toetsingskader stringente eisen op te nemen om het risico te beperken dat gegevens die bij een datalek vrijkomen, bruikbaar zijn voor kwaadwillende partijen. Een van de maatregelen die genomen moet worden is het gescheiden opslaan van gebruikersgegevens en gebruiksgegevens. Het Besluit identificatiemiddelen voor natuurlijke personen zal het voorts mogelijk maken om regels te stellen die tegengaan dat gebruikers worden omgeleid naar een andere website dan waar zij denken in te loggen (paragraaf 4.1.3 Besluit). Voorts voorziet het wetsvoorstel in herstelvermogen, dat ervoor zorgt dat burgers die in de knel komen, snel en adequaat geholpen kunnen worden, en eventuele schade zo veel mogelijk kan worden voorkomen of hersteld. Als er onverhoopt toch een datalek plaatsvindt, gelden er procedures om deze zo snel mogelijk te ontdekken, maatregelen te nemen om verder lekken en schade te voorkomen, burgers te informeren en eventueel een melding te doen bij de AP.

In reactie op de vraag van GroenLinks merk ik op dat de overheid haar toevertrouwde informatie beveiligt in overeenstemming met de daarvoor gangbare praktijk, zoals door toepassing van de ISO 27002 in de Baseline Informatiebeveiliging Overheid. Verder is de overheid gebonden aan de beveiligingsvereisten van de AVG, waar de omgang met bijzondere persoonsgegevens een plaats heeft. Voor specifieke overheidssystemen en –processen bestaat eigen wet- en regelgeving waarin eveneens informatiebeveiligingseisen staan en waar doorgaans ook een specifieke toezichtssystematiek is opgenomen. Verder investeert de overheid in de borging van haar digitale weerbaarheid door te oefenen met incidentsituaties. Het trekken van lessen van specifieke feitelijke incidenten bij organisaties is onderdeel van de informatiebeveiligingscyclus en wordt in deze organisaties zelf opgevolgd. Over incidenten met overheidsbrede effecten zoals Diginotar of Citrix is uw Kamer geïnformeerd, evenals over de acties die hiervan het gevolg zijn.

*De leden van de fractie van **GroenLinks** vragen voorts waarom de regering niet heeft gekozen om meer in te zetten op dataminimalisatie, privacy by design en privacy-attributed based identity.*

In reactie benadruk ik dat privacy by design uitgangspunt is bij implementatie van privacybescherming binnen het eID stelsel. Zoals hierboven aangegeven, zal ik een wetswijziging indienen waarmee privacy by design als toelatingscriterium in de wet wordt geëxpliciteerd. Hiermee wordt verduidelijkt dat een aanvraag voor een toelating van een inlogmiddel kan worden afgewezen wanneer niet aan het beginsel wordt voldaan.

De wijze waarop privacybescherming systematisch wordt aangepakt is beschreven in de Privacyvisie eID zoals ik deze in januari 2019 aan het parlement heb gezonden. Daarbij spelen dataminimalisatie, maar ook andere AVG-beginselen een belangrijke rol. Attribuutgebaseerde inlogmethoden kunnen, mits zij voldoen aan de eisen, een - maar niet de enige - oplossing vormen.

*De leden van de fractie van **GroenLinks** vragen of de regering garandeert dat wordt gewerkt met de allerlaatste veiligheidsstandaarden en dat deze continu up-to-date worden gehouden.*

In de eisen die worden gesteld aan aanbieders van inlogmiddelen spelen beveiligingseisen, waaronder de zorg voor het continu up-to-date houden van de beveiliging, een belangrijke rol. In reactie op de vraag merk ik op, dat de systematiek van open toelating erop is gericht om zo breed mogelijk gebruik te maken van nieuwe en innovatieve beschermingstechnieken. Dus niet alleen bestaande maatregelen up-to-date houden, maar zo mogelijk ook steeds veiliger maken. Dat is een belangrijke reden om niet specifieke oplossingen voor te schrijven of uit te sluiten.

De leden van de fractie van **GroenLinks** merken op dat het koppelen van bestanden en het voorkomen van schending van het beginsel van 'doelbinding' een belangrijke voorwaarde is binnen de AVG, net als dataminimalisatie. Welke bestanden gaat de overheid koppelen en op welke wijze gaat dit gebeuren? Kan de regering hiervan een lijst geven? Het verzamelen van data moet tot een minimum beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Hoe heeft de regering daar binnen de verschillende facetten binnen de Wet digitale overheid rekening mee gehouden? Kan zij hiervan een exhaustieve lijst opsommen en tevens uitleggen hoe zij kan garanderen dat de private aanbieders dit ook zullen doen?

In reactie op deze vraag merk ik op dat uiteraard geldt dat gegevens in overeenstemming met de AVG worden verwerkt en de noodzaak van verwerking moet bestaan. In het concept Besluit digitale overheid dat op 17 maart 2020 bij uw Kamer is voorgehangen, zijn regels opgenomen betreffende het verwerken van persoonsgegevens in de voorzieningen in de generieke digitale infrastructuur. In dit conceptbesluit zijn alle gegevensverwerkingen die in verband met het eID stelsel onder mijn verantwoordelijkheid plaatsvinden opgenomen.

Wat betreft het koppelen van bestanden merk ik op, dat het primair van belang is dat het verwerken van persoonsgegevens geschiedt in overeenstemming met de in het wetsvoorstel en uitvoeringsregelgeving (onder meer het concept-Besluit digitale overheid) vastgelegde doelen, waardoor ervoor wordt gezorgd dat gegevens niet voor andere doelen dan voor inloggen bij de overheid en het herstellen van problemen van burgers worden gebruikt. Dat is stringent geregeld. Private aanbieders worden hierop, voorafgaand aan de toelating, en tijdens de dienstverlening bij herhaling gecontroleerd.

In het Besluit identificatiemiddelen voor natuurlijke personen, dat aan het parlement wordt voorgelegd, worden de eisen in artikel 5b en 5e van het Besluit digitale overheid verder geëxpliciteerd. Dit besluit zal, aansluitend op de wens van uw fractie, voorzien in een verplichting tot gescheiden opslag van gebruiks- en gebruikersgegevens waardoor koppeling van loggegevens aan personen niet mogelijk is (paragraaf 4.1.3). Uitzondering hierop is wanneer het combineren van gegevens noodzakelijk is om misbruik of incidenten te herkennen, te herstellen en gebruikers op de hoogte te stellen. Voor dit proces zijn extra regels opgenomen (paragraaf 4.1.3).

*De leden van de fractie van **GroenLinks** merken op dat privacy by design en security by design heel erg in elkaars verlengde liggen, omdat data die je niet hebt ook niet kunnen lekken. Is de regering het met de leden van de fractie van GroenLinks eens dat een dergelijk model meer in de geest van de AVG is dan de huidige wetgeving, gelet op dataminimalisatie en privacy by design?*

In reactie op het voorgaande merk ik op, dat ik het met de leden eens ben dat deze begrippen in elkaars verlengde liggen. De vraag is echter of het "niet hebben van gegevens", zeker in een context waarin burgers erop moeten kunnen vertrouwen dat zij worden geholpen op het moment dat zij in de problemen komen, altijd beter is. Op het moment dat daarvoor geen gegevens beschikbaar zijn, zal de burger op zichzelf aangewezen zijn. Het is meer opportuun om (een minimale set) gegevens beschikbaar te hebben en deze conform de AVG te verwerken en beveiligen.

*De **D66-fractie** merkt op, dat een mogelijkheid om verkeerd gebruik van data aan de voorkant te voorkomen is het verplichten van privacy by design, waardoor data niet verwerkt hoeven te*

worden. Waarom kiest de regering niet voor het verplichten van privacy by design? De leden van de D66-fractie missen in de brief de onderbouwing hiervoor.

Zoals hiervoor betoogd in reactie op vragen van de fractie van GroenLinks, wordt in het eID-stelsel wel degelijk gekozen voor privacy by design. Dat is uit hoofde van de AVG verplicht en zal worden geëxpliciteerd in de wet. Hiertoe zal ik een wetswijziging indienen.

*Refererend aan het schriftelijke verslag en de deskundigenbijeenkomst vraagt de fractie van de **PVV** of de regering kan aangeven in hoeverre naast privacy by design ook security by design bij dit wetsvoorstel wordt toegepast.*

Zoals bij eerdere vragen opgemerkt, geldt het uitgangspunt van privacy by design op grond van de AVG en zal dit worden geëxpliciteerd in het wetsvoorstel. Ik zal hiertoe een wetswijziging indienen waarmee privacy by design als criterium wordt opgenomen bij de toelating van een inlogmiddel. Beveiliging van persoonsgegevens maakt daarvan integraal onderdeel uit. De wijze waarop dat gebeurt heb ik beschreven in de Privacyvisie eID, die in begin 2019 aan het parlement is gezonden. De zorg voor privacy en security by design is niet alleen een kwestie van wettelijke verankering, maar tevens van het in de praktijk treffen van maatregelen en zorgen dat deze up-to-date blijven. Het is een verantwoordelijkheid die continu aandacht behoeft.

*De leden van de fractie van **GroenLinks** merken op dat attributen zich minder goed lenen voor grootschalige hacks of heimelijke toegang, massale datalekken en function creep, oftewel sluipende doelverschuiving.*

In reactie merk ik op dat ook attributen (gegevens) kunnen worden gehackt, ongeacht of deze centraal of decentraal staan opgeslagen. Zo kunnen attributen die op een telefoon staan opgeslagen worden gehackt. Dat kan ook grootschalig op telefoons van meerdere gebruikers als een app 'lek' is, of als gebruikers onderliggende software zelf niet tijdig updaten.

*De leden van de fractie van de **ChristenUnie** vragen hoe vertrouwenwekkend toetsing is zonder transparantie. Daarnaast vragen zij of het niet mogelijk is om vooraf ten tijde van toelating de toezichthouder te laten toetsen op de naleving van de in de Algemene verordening gegevensbescherming gestelde eisen, waaronder privacy by design. Dit is nu al gebruikelijk in de systematiek van toelating en toezicht onder de eIDAS-verordening.*

In reactie op het bovenstaande merk ik op dat het toetsen van middelen ook vooraf gebeurt; hierbij is de toezichthouder betrokken. Naleving van privacy by design is daar een onderdeel van.

Open source - closed source

*De leden van de **FVD-fractie** vragen waarom de regering er bewust voor kiest aanvullende zekerheden niet op te nemen in het kader, zoals open source, waar zij zelf een richtlijn op heeft voor overheidssoftware. Of decentraliteit, waarmee in ieder geval gegarandeerd is dat er geen centrale databases beheerd worden met gevoelige persoonsgegevens die onderhevig zijn aan lekken, diefstal, verlies of oneigenlijke aanwending van persoonsgegevens.*

In reactie hierop merk ik op, dat de richtlijn over overheidssoftware gaat over het feit, dat door of in opdracht van de overheid ontwikkelde software in principe open source ter beschikking wordt gesteld, vanuit de gedachte dat met gemeenschapsgeld wordt gewerkt en de maatschappij hiervan moet kunnen profiteren. In het verband van het onderhavige wetsvoorstel betreft het evenwel het stellen van eisen aan producten met software-oplossingen die worden ingekocht en ingezet door de overheid. In het navolgende cluster wordt nader ingegaan op het thema centrale-decentrale opslag.

*De leden van de **GroenLinks-fractie** vragen hoe de regering de grote techbedrijven denkt te controleren zonder broncodes en open standaarden.*

In reactie hierop merk ik op, dat partijen voorafgaand aan de toelating gedocumenteerd moeten aantonen hoe 'hun' inlogmiddelen functioneel werken. De gebruikte (open source of closed source) software maakt daarvan onderdeel uit. Tevens dient de operationele werking aangetoond te worden voordat inlogmiddelen worden toegelaten. Deze toetsing zorgt ervoor dat voorafgaand aan de toelating een helder beeld ontstaat van de werking van de middelen en de achterliggende processen. De aan de orde zijnde wet- en regelgeving biedt voldoende grondslagen om een aanvraag af te wijzen of een toelating in te trekken, wanneer bijvoorbeeld onvoldoende is geborgd dat zorgvuldig wordt omgegaan met gegevens.

*De leden van de **GroenLinks-fractie** vragen of de regering het eens is met de leden, dat concepten als open source van broncodes en privacy by design niet aantrekkelijk zijn voor private aanbieders. Ook vragen zij wat het gevolg is dat privacy by design niet als voorwaarde is opgenomen in de wet.*

Mijn reactie op de eerste vraag is ontkennend. Er zijn veel voorbeelden van private partijen die producten open source aanbieden. Het feit dat software open source is, betekent niet dat de dienst ook gratis is. Het betekent ook niet dat open source commercieel niet interessant is. Partijen kunnen zich als verdienmodel richten op organisatiespecifiek maatwerk en onderhoud van de software. Dat gebeurt in de praktijk ook. Of privacy by design niet aantrekkelijk is voor private aanbieders, is minder relevant, aangezien zij op grond van de AVG en de voorgenomen wetswijziging verplicht zullen worden dit (inrichtings-)principe toe te passen. Private partijen overtreden de regels als zij dit niet doen. De vraag inzake privacy by design wordt in het betreffende cluster nader beantwoord.

*De leden van de **GroenLinks-fractie** vragen hoe de regering het risico beoordeelt voor burgers die bij één partij een inlogmiddel voor alle diensten gaan gebruiken met alle persoonsgegevens van de desbetreffende persoon. Ook vragen ze of de regering bereid is in de wet op te nemen dat voor toelating van een inlogmiddel vereist is dat dit gebruik maakt van open source voor alle verwerking van persoonsgegevens en gebaseerd is op een decentrale structuur. De leden vragen voorts of open source van broncodes niet de eenvoudigste eis is om adequaat toezicht te garanderen. Dit probleem doet zich niet voor bij decentrale systemen. Gaat de overheid actief uitdragen dat burgers hiervoor kunnen kiezen? De **D66 fractie** constateert dat de regering te kennen heeft gegeven dat het van groot belang is dat de werking van processen transparant is, zodat deze controleerbaar zijn. Desalniettemin kiest zij niet voor het verplichten van open source software. Waarom wil de regering niet in alle gevallen gebruikmaken van de kennis en kunde van een samenleving die meekijkt op de kwaliteit van de code en suggesties kan doen voor verbetering en de code kan aanpassen? De leden van de **D66-fractie** constateren dat wanneer de broncode inzichtelijk is, de waarborging van privacy, veiligheid en andere aspecten niet alleen afhangt van de toezichthouder. Hoe zorgt de regering voor transparantie in het geval van closed source software? En vindt de regering dat dit transparant moet zijn voor het publiek?*

In reactie op de bovenstaande vragen merk ik in de eerste plaats op, dat elke partij die gegevens verwerkt aan de strenge (privacy- en veiligheids-)regels moet voldoen die gesteld worden bij en krachtens het onderhavige wetsvoorstel, mede tegen de achtergrond van de AVG. Uitgangspunt bij dit wetsvoorstel is dat persoonsgegevens aantoonbaar adequaat beschermd moeten zijn. Hierdoor is het risico voor burgers zeer beperkt. Met betrekking tot de wijze waarop dit doel wordt bereikt, merk ik op dat open source software en een decentrale architectuur kunnen worden ingezet. Open source software geeft een eigenschap van de software aan, namelijk dat de broncode openbaar is. Het concept 'decentraal' ziet op de wijze of locatie waar gegevens worden opgeslagen. Het zijn verschillende begrippen die elkaar niet uitsluiten. Zo kan een decentraal systeem werken met closed source en een centraal systeem met open source software. Overigens ben ik van mening dat een systeem dat adequate privacybescherming biedt zowel centrale als decentrale elementen zal

bevatten. In het navolgende cluster wordt nader ingegaan op het thema centrale-decentrale opslag.

Met betrekking tot open source merk ik op dat ik graag gebruik maak van de kennis en kunde die de hele samenleving te bieden heeft. Waar het om gaat is dat aan het doel van veiligheid en betrouwbaarheid wordt voldaan. De openbaarheid van de broncode – door het 'meer-ogen-principe' – kan bijdragen aan veiligheid. Door dit principe kunnen meer mensen kijken of de software werkt zoals bedoeld, en of er geen veiligheidsproblemen in zitten. De kracht of sterkte van open source is echter primair afhankelijk van de sterkte en activiteit van omvang van de gemeenschap en ontwikkelaars die dit 'dragen'. De eigenschap open source als zodanig biedt niet de garantie voor transparantie en veiligheid. Om het principe te laten gelden zal een voldoende omvangrijke en actieve gemeenschap moeten bestaan en in stand worden gehouden.

Naast de voordelen moeten wij niet de ogen sluiten voor de aandachtspunten. De veiligheid – en daarmee ook de privacybescherming - kan namelijk door de openbaarheid verzwakt worden. Het kan leiden tot veiligheidsproblemen omdat veiligheidslekken makkelijker kunnen worden uitgenut doordat kwaadwillenden deze kunnen opmerken en benutten, in plaats van dichten. Zo lang andere ontwikkelaars het lek niet ontdekken, heeft een kwaadwillende vrij spel. Daarbij zij opgemerkt, dat voor kwaadwillenden de 'baten' van het zoeken naar, en benutten van lekken aanzienlijk kunnen zijn. De 'businesscase' kan voor hen aldus aantrekkelijk zijn. Het risico wordt bovendien vergroot op het moment dat de software draait in omgevingen die buiten de invloedsfeer staan van de ontwikkelaars zelf, en de veiligheid afhankelijk wordt van het samenspel van de software met andere soft- en hardware onderdelen van een oplossing. In dergelijke situaties kan het voor de veiligheid voordelen hebben om software gesloten(er) te maken. Gezien vanuit dit gezichtspunt wordt de veiligheid van closed software beoogd door de werking van de software niet breed bekend te maken. Het kan vanuit het oogpunt van veiligheid verstandig zijn om die keuze te maken. Echter uiteraard moet dan wel – nadrukkelijk door anderen dan de leverancier zelf - worden vastgesteld dat de software werkt zoals beschreven en dat deze veilig is.

In de met dit wetsvoorstel geregelde toelatingssystematiek worden beoordelingen van alle onderdelen van de inlogmiddelen voorzien, waaronder de gebruikte software. Daarnaast wordt beoogd om testen uit te voeren om de bestandheid van software tegen binnendringen te beproeven (zogeheten penetratietesten). Tenslotte wordt de werking in het gehele productiesysteem getoetst, dat wil zeggen de veiligheid van het samenstel van hard- en softwarecomponenten die samen de oplossing (het inlogmiddel) vormen. Want dat bepaalt uiteindelijk of de totale oplossing veilig is.

De door de fracties gestelde vragen geven mij aanleiding om in het wetsvoorstel inzake de toelating van inlogmiddelen open source te verankeren. Hiertoe zal ik een wetswijziging indienen. Dit heeft tot gevolg dat door mij aan open source zal worden getoetst bij het behandelen van de aanvraag om een toelating; ook zal hierop worden toegezien door AT.

Essentieel bij open source is dat de sterkte van de achterliggende open source gemeenschap voldoende is om ook op termijn veilige en betrouwbare inlog te kunnen garanderen. Transparantie mag nooit ten koste gaan van de veiligheid en de mate waarin de burger daadwerkelijk beschermd wordt. Dit kan er in voorkomend geval op neerkomen dat de inzet van open source niet in de rede ligt en dat (op onderdelen) voor closed source kan – en moet - worden gekozen omdat veiligheid met open source niet gegarandeerd kan worden.

Met verankering van open source wordt een ontwikkeling in gang gezet naar een nieuw toelatingscriterium voor markt- en overheidspartijen op dit punt. Dit betreft een beweging met aanzienlijke gevolgen voor de huidige aanbieders van inlogmiddelen. Bij de toelating moet immers het ontwerp dan wel de motivatie van de keuze van de gebruikte software tegen het licht worden gehouden, hetgeen tijd en moeite van betrokkenen vergt. Dat is op zichzelf geen belemmerende overweging, maar wel een die in potentie raakt aan de continuïteit van de nu en in de nabije

toekomst beschikbare inlogmiddelen om veilig bij de overheid te kunnen inloggen. Het waarborgen daarvan is voor mij essentieel en leidend. De ontwikkeling naar open source behelst daarom een transitieproces en noopt tot zorgvuldige inrichting waarbij, gelet op de uitvoeringsconsequenties, in overleg met partijen die inlogmiddelen reeds aanbieden of in de nabije toekomst gaan aanbieden, zal worden bezien binnen welke termijn dit redelijkerwijs haalbaar en verantwoord is, opdat burgers en bedrijven niet zonder veilige inlogmogelijkheid komen te zitten.

*De leden van de **D66-fractie** vragen of, en zo ja, welke onderdelen van closed source software door de aanbieders wel transparant aangeboden kunnen worden.*

In reactie hierop merk ik op, dat dat niet op voorhand te zeggen valt omdat nu nog niet bekend is welke aanbieders zich zullen melden en derhalve ook niet op welke wijze zij hun inlogmiddel – dat meer is dan software alleen – zullen vormgeven. Mogelijk zullen aanbieders een samenstelling van open en closed source willen hanteren. Het principe van open source zal worden vastgelegd; hiertoe wordt het wetsvoorstel aangepast.

*De leden van de **PvdA**-fractie merken op dat de digitale bescherming van persoonlijke (inlog)gegevens volgens experts het beste is gediend met open source en decentrale opslag. Wat is het oordeel van de regering over de volgende conclusie in het VNG-rapport Technische Analyse Digitale Identiteit van 11 september 2020, p. 31:*

> *"Wat wel duidelijk is, is dat protocollen …die voortkomen uit het meest recente paradigma van digitale identiteiten (het paradigma van de self sovereign identity), technisch gezien het meest kansrijk zijn om de beleidsdoelen te behalen, omdat deze protocollen de gebruiker centraal stellen en uitgaan van security by design."*

Deelt de regering deze conclusie? Zo nee, waarom niet? Zo ja, waarom hanteert zij deze niet als uitgangspunt bij de vormgeving van de Wet digitale overheid?

In reactie op het bovenstaande merk ik op dat het bedoelde document niet goedgekeurd is door de VNG en dat het daarmee geen VNG-publicatie betreft, maar slechts een interne technische verkenning naar invullingen van inlogoplossingen. Het document kiest een technische invalshoek, met daarbij horende technische maatregelen. Het scala aan mogelijke privacybeschermende maatregelen is breder dan de genoemde maatregelen. De regering kiest voor de bescherming van persoonsgegevens, niet voor - of tegen - specifieke maatregelen. In het navolgende cluster wordt nader ingegaan op het thema centrale-decentrale opslag.

*De leden van de **PvdA-fractie** wijzen erop dat in de beantwoording van de vragen de commissie de regering zegt dat open source een mogelijkheid is, maar dat transparantie en veiligheid ook via closed source geborgd zijn door middel van afspraken met de leveranciers. De leden vragen waarom niet gekozen is voor verplichte open source. De stelling in de brief van de regering dat open source mogelijk blijft, maar closed source ook kan, is geen antwoord op deze vraag. Volgens experts is open source veruit de beste garantie voor de bescherming van digitale identiteit van burgers. Zoals deskundige Marleen Stikker in een recente open brief aan de Eerste Kamer stelt: "Open source is een absolute voorwaarde. Bedrijven kunnen zo geen achterdeuren inbouwen en het is mogelijk voor een grote diversiteit van maatschappelijke actoren om daarop toe te zien." Is de regering het met deze stelling eens? Zo nee, kan de regering uitleggen waarom volgens haar Marleen Stikker ongelijk heeft en open source geen absolute voorwaarde is? Zo ja, is de regering dan bereid in het toelatingskader voor private eID-middelen de verplichting op te nemen dat toetreding als aanbieder alleen mogelijk is indien de volledige broncode van alle applicatiesoftware die met persoonsgegevens omgaat gepubliceerd is en voor eenieder toegankelijk is om te beoordelen en te onderzoeken?*

In reactie op het bovenstaande merk ik op dat essentieel is, dat de bescherming van de (persoons)gegevens van burgers goed geborgd is. De wijze waarop deze borging gerealiseerd

wordt, is verwoord in de aan het parlement gezonden Privacyvisie eID, waaraan bij eerdere vragen en ook tijdens het deskundigenoverleg is gerefereerd. Hierin wordt toegelicht hoe ik als verwerkingsverantwoordelijke bij de inrichting van het eID-stelsel zorg draag voor de juiste naleving van de AVG en andere privacyregelgeving. Er is een verschil tussen zaken die wettelijk geregeld moeten worden, zoals grondslagen voor de verwerking van persoonsgegevens, en het treffen van maatregelen om de bescherming van persoonsgegevens in (technische) systemen en processen te implementeren.

Ik deel het uitgangspunt van de fractieleden dat het belangrijk is dat de verwerking van persoonsgegevens transparant plaatsvindt en controleerbaar is. Om dat doel te bereiken zijn, wat betreft de in te zetten software, meerdere middelen denkbaar, namelijk de inzet van open source software of closed source software. De eigenschap open of closed source *sec* biedt geen garantie en is geen synoniem voor "transparant en veilig".

Een inlogmiddel zal in praktijk naar verwachting niet uitsluitend bestaan uit een softwareproduct. Inlogmiddelen bestaan veelal tevens uit een ondersteunende infrastructuur, inclusief processen voor administratie, beveiliging (bijvoorbeeld om de privacy te borgen), versiebeheer, contractmanagement, ondersteuningsdienstverlening, etc. Bij de aanvraag tot toelating moet inzicht worden gegeven in de huidige inrichting van het middel, maar ook in de manier waarop met wijzigende omstandigheden zal worden omgegaan. Voor de inrichting van de ondersteunende processen is voorts software nodig.

Ik herhaal in dat verband de gedane toezegging dat ik het gebruik van open source wettelijk zal bevorderen door het principe als toelatingscriterium te verankeren. Ik zal hiertoe een wetswijziging indienen.

*De leden van de **PVV-fractie** vragen, refererend aan de deskundigenbijeenkomst en het verslag van het schriftelijk overleg, of de regering kan aangeven waarom afspraken met leveranciers van closed source software over het borgen van de veiligheid niet zouden kunnen worden gemaakt met leveranciers van open source software.*

In reactie op deze vraag zij er op gewezen, dat in de beantwoording van de commissiebrief niet staat dat afspraken niet mogelijk zijn. Er wordt aangegeven dat open source op zich, zonder achterliggende waarborgen en garanties, niet per definitie meerwaarde oplevert. Die meerwaarde is gelegen in de mate waarin de open source software gemeenschap actief ondersteund en onderhouden wordt. Niet als zodanig in het feit dat software open source is. Open source software die niet actief ondersteund en onderhouden wordt kan dan zelfs een veiligheids*risico* worden in plaats van een veiligheids*maatregel*.

*De leden van de **PVV-fractie** constateren dat in de deskundigenbijeenkomst verschillende experts hebben aangegeven dat voor de bescherming van de privacy van burgers het gebruik van open source de beste optie is en dit als harde eis zou moeten worden toegevoegd voor de toelating van eID-middelen.[2] Kan de regering uitleggen waarom niet gekozen wordt voor open source met toezicht vóóraf (door het Agentschap Telecom) in plaats van toezicht achteraf (door de Autoriteit Persoonsgegevens), waardoor het risico ontstaat van "dweilen met de kraan open"?*

In reactie op het bovenstaande merk ik op dat er sprake is van toezicht vooraf, namelijk toelating (erkenning), waarbij het AT een grote rol heeft bij de toetsing vooraf, dus voordat een aanbieder diensten mag verlenen. Zoals ik eerder opgemerkt heb, is een inlogmiddel meer dan een stuk software alleen. Het inlogmiddel wordt als totaal bezien: de werking van de software in de technische omgeving, eventueel gebruikte hardware, etc. Het AT toetst daarnaast ook tussentijds. Dit laat de toezichthoudende rol van de AP waar het gaat om de bescherming van

[2] Zie bijv. de opmerkingen van de heer Böhre (Privacy First) op p. 6, de heer Van Boheemen (Rathenau Instituut) op p. 14 en de opmerkingen van mevrouw Moerel (Tilburg University/Cyber Security Raad) op p. 25 van het verslag van de deskundigenbijeenkomst (Kamerstukken I 2019/20, 34 972, G).

persoonsgegevens overigens onverlet. Het is dus geen toezicht vooraf of achteraf, maar beide. Zoals hiervoor aangegeven, zeg ik u toe dat ik het gebruik van open source zal bevorderen door het principe in het wetsvoorstel te verankeren.

*De leden van de **PVV-fractie** vragen voorts of de regering kan aangeven of zij bereid is om open source alsnog als enige standaard vast te leggen indien aanbieders van een open source pakket wél (aanvullende) garanties op kwaliteit, zekerheid en een transparant servicepakket kunnen leveren.*

Zoals ik hiervoor heb aangegeven, ben ik bereid het principe van open source wettelijk te verankeren. Ik zal hiertoe een wetswijziging indienen.

*De **SP-fractie** merkt op dat in de beantwoording van de staatssecretaris wordt gesteld dat closed source even veilig kan zijn als open source. Natuurlijk kan een gesloten oplossing net zo veilig zijn, alleen moeten we dan de aanbieder op zijn blauwe ogen geloven. Bij open source kunnen we dit zelf controleren.*

In reactie hierop merk ik op dat ook bij closed source kan worden gecontroleerd; de aanbieder wordt niet zonder meer vertrouwd.

*De **SP-fractie** merkt voorts op dat het ministerie zelf een beleidsnota heeft gepresenteerd waarin het stelt dat open source de norm moet zijn. Als er ergens ooit een wetsvoorstel is geweest waar dit voor geldt, dan is het wel dit wetsvoorstel. Hoe ziet de regering dit? Wil de regering vastleggen dat de aangeboden oplossingen open source moeten zijn?*

In reactie op de bovenstaande vraag, merk ik op dat de betreffende beleidsnota betrekking heeft op een andere situatie dan waar het wetsvoorstel over gaat. De beleidsnota handelt over software die onder verantwoordelijkheid dan wel in opdracht van de overheid is ontwikkeld. Uitgangspunt is dat van producten, die door de overheid zijn ontwikkeld, de markt moet kunnen meeprofiteren en de software wordt 'teruggegeven' ten behoeve van maatschappelijk voordeel. Daarbij is het inderdaad de norm om open source ter beschikking te stellen. De toezegging die ik u eerder deed in verband van het onderhavige wetsvoorstel sluit hierbij aan.

*De leden van de fractie van de **ChristenUnie** constateren dat sommige deskundigen, vooral vanuit het bedrijfsleven, er op wijzen dat de openbaarheid van de software ook kan leiden tot een verzwakking van de veiligheid. Bijvoorbeeld wanneer ze geïnstalleerd worden op telefoons die (iets) verouderd zijn waardoor de open source software niet in een veilige omgeving kan opereren. Zij wijzen erop dat in dit soort situaties het verstandiger is als de software gesloten is. De leden vragen om hoeveel telefoons het gaat. Pleit het bedrijfsleven voor gesloten software omdat er sprake is van een terechte zorg of om inzicht in het eigen handelen en functioneren te vermijden? Deze leden vragen de regering ook of in die situaties waarin open source niet wenselijk is, toch geborgd kan worden dat de software van deze partijen, die onder de Wet digitale overheid vergund zijn, op orde is. Bijvoorbeeld door audits van onafhankelijke partijen. Welke mogelijkheden ziet de regering daarvoor?*

In reactie op het bovenstaande merk ik om veilig te kunnen werken, het van belang is dat niet alleen de specifieke software van het middel zelf, maar ook de onderliggende software (bijvoorbeeld van het besturingssysteem) of onderliggende hardware adequaat en veilig is. In zijn algemeenheid hebben zowel hard- als software een bepaalde levensduur. Na verloop van tijd zullen zij ook niet meer (kunnen) worden onderhouden. Om hoeveel telefoons het gaat is niet eenduidig te zeggen, omdat dit afhankelijk is van de combinatie telefoon met verschillende soorten softwarecomponenten. De leden lijken een pleidooi te houden voor het werken met soft- en hardware die up to date is.

Zoals eerder aangegeven, zeg ik u toe dat ik het gebruik van open source zal bevorderen door het principe wettelijk te verankeren. Dit heeft tot gevolg dat hieraan door mij zal worden getoetst bij het behandelen van de aanvraag van een partij; ook zal hierop worden toegezien door AT. Bij de toetsing wordt gekeken naar alle componenten van het inlogmiddel, inclusief de gebruikte software. Daarbij gaat het er niet alleen om dat in de opzet de middelen veilig zijn; ook worden er praktijktoetsen gehouden.

Samengevat biedt zowel open source als closed source software risico's en kansen. De kracht en de veiligheid die wordt geboden ligt in de mensen erachter die de software maken en de context waarin de software wordt ingezet. Alles afwegend en in aansluiting op de wens van meerdere fracties, kies ik ervoor de beweging naar open source in te zetten. Ik zeg u toe dat ik ervoor zorg dat door het stellen van strenge eisen aan onder meer privacy, veiligheid en transparantie in combinatie met een strenge doorlopende controle, de aangeboden oplossingen op hun merites worden beoordeeld. Het gaat er uiteindelijk om of de te beschermen belangen geborgd blijven. Transparantie mag nooit ten koste gaan van de veiligheid en de mate waarin de burger daadwerkelijk beschermd wordt.

Centrale - en decentrale opslag van gegevens

*De leden van de **GroenLinks-fractie** vragen of het klopt dat bij de gecentraliseerde infrastructuur, zoals bij het eID, bedrijven die certificaten uitgeven precies kunnen zien waar mensen inloggen en welke documenten zij ondertekenen. Zij vragen of de regering dit wenselijk acht en of de regering het met deze leden eens is dat dit een inbreuk vormt op de privacy, zeker bij gevoelige transacties.*

Graag beantwoord ik deze vraag als volgt. Het kan voor de werking van systemen nodig zijn dat minimale herleidbaarheid beschikbaar is om in het geval van problemen of misbruik te kunnen reproduceren en de gebruiker te helpen. Dit is echter iets anders dan dat uitgevende bedrijven kunnen zien welke documenten worden ondertekend.

Ik acht het wenselijk dat dit herstelvermogen bij alle toegelaten identificatiemiddelen beschikbaar is. In de uitvoeringsregels voor het toelatingsproces is daarom de beschikbaarheid van dergelijke logging voorgeschreven (met andere woorden geldt het als toelatingseis). Ook zijn de doelen waarvoor logging gebruikt mag worden nauw omschreven. Zoals ik hiervoor ook heb betoogd is het feit, dat bepaalde gegevens beschikbaar zijn, niet hetgeen voorkomen moet worden. Immers dat kan ook dienstbaar zijn om gebruikers die in de problemen zijn gekomen te helpen. Wat wel voorkomen moet worden is dat gegevens voor andere doeleinden gebruikt worden, zoals verkoop en verhandelen. En daar tref ik dan ook stringente maatregelen voor, zoals in het voorgaande is toegelicht.

*De leden van de **D66**-fractie vragen de regering of zij meer duidelijkheid over de uitgangspunten omtrent de vraagstelling centraal-decentraal wil geven. Verschillende sprekers hebben op de deskundigenbijeenkomst in verband met privacy en security gepleit voor een decentraal systeem en voor het werken met attributen. De regering sluit het gebruik van een decentraal systeem en het werken met attributen niet uit. De leden willen graag weten hoe de regering zorgt voor eenduidigheid. Ook de **PvdA**-fractie vraagt, refererend aan de eerdere commissiebrief, om uitleg ter zake. De **PvdA**-fractie en de fractie van de **ChristenUnie** vragen mede in relatie tot de coronamelder naar de architectuur binnen de WDO. De leden van de **SP-fractie** vragen of de regering wil kiezen voor decentrale opslag, omdat zij van mening zijn dat er weliswaar bij decentrale opslag ook gehackt kan worden, maar het leed dan wel te overzien is.*

In reactie op het bovenstaande merk ik het volgende op. Het wetsvoorstel beoogt adequate privacybescherming. Dat betekent dat bij implementatie moet worden voldaan aan de AVG, waarbij een set maatregelen moet worden getroffen die de resultante vormt van de afweging tussen dataminimalisatie, kwaliteitsborging van gegevens en bewaartermijnen. Of privacybescherming

afdoende is, wordt niet door de aanbieder zelf bepaald. Om dit te borgen richt ik toelating, toezicht en controle in.

Bij de implementatie zijn een centrale, maar ook een decentrale opzet mogelijk; beiden zijn geen doel op zich. Waar het om gaat is de mate van privacybescherming van de oplossing die een aanbieder van een inlogmiddel realiseert. Een keuze voor centrale of decentrale opslag van gegevens acht ik daarom niet opportuun.

In feite werken de inlogmiddelen binnen de overheid op dit moment met een (enkel) attribuut: het BSN. Overheden herkennen burgers namelijk aan de hand van hun BSN als het gaat om dienstverlening waarvoor identiteitsvaststelling noodzakelijk is. Een middel dat decentraal werkt zal op enigerlei wijze het BSN moeten aanleveren bij de overheid. Een als decentraal gekenschetste oplossing als IRMA doet dat eveneens, door de gebruiker zijn BSN te laten leveren.

Overigens wordt middels het wetsvoorstel de mogelijkheid geboden in de huidige systematiek, die door de pleitbezorgers van decentraal als centraal bestempeld wordt, met pseudonimisering te gaan werken. Hierdoor is ook het ene attribuut (BSN) voor de aanbieders van inlogmiddelen niet meer zichtbaar. Voor de volledigheid benadruk ik op deze plaats dat het wetsvoorstel er niet tot leidt dat het BSN centraal moet worden opgeslagen, anders dan nu reeds gebeurt op basis van andere wetgeving.

De leden van de **D66** fractie krijgen sterk de indruk dat er aparte afspraken met de diverse aanbieders worden gemaakt over decentraal-centraal. Het gebrek aan eenduidigheid vraagt om meer toezicht. Hoe zorgt de regering ervoor dat de toezichthouder niet op verschillende obstakels stuit bij de controle op privacy, veiligheid en andere aspecten? En hoe gaat de regering om met een datalek als dit zich voordoet bij een centraal systeem?

In reactie op het bovenstaande merk ik op, dat het primair van belang is dat de AVG en andere privacyregels worden nageleefd, waarbij centrale en decentrale oplossingen mogelijk zijn. In het wetsvoorstel is geen voorkeur verankerd; ik heb derhalve niet de behoefte om daar afspraken met wie dan ook over te maken. Op het moment dat zich een datalek voordoet in een centraal systeem zal, evenals bij een datalek in een decentraal systeem, bezien moeten worden of er gegevens zijn gelekt, wat de gevolgen daarvan zijn voor betrokkenen en of de schade kan worden beperkt. Het beperken en voorkomen van verdere schade heeft de primaire aandacht, waarbij zonodig melding wordt gedaan bij de Autoriteit Persoonsgegevens.

*De leden van de fractie van de **ChristenUnie** merken op dat de Wet digitale overheid uit gaat van een centraal model waarbij inloggegevens (inclusief BSN) kunnen worden opgeslagen in de computersystemen van de leveranciers van de inlogmiddelen.*

In reactie daarop benadruk ik dat de veronderstelling, dat de WDO uitgaat van een centraal model, niet juist is. Onduidelijk is waarop deze aanname is gebaseerd; dit blijkt niet uit de tekst van het wetsvoorstel, noch uit de Memorie van toelichting en de uitvoeringsregelgeving. Wel voorziet de wet er in dat – bij de controle of een BSN daadwerkelijk toebehoort aan de persoon die een middel aanvraagt – in het vervolg gebruik gemaakt kan worden van pseudoniemen. De wet gaat er derhalve niet vanuit dat een BSN – of andere attributen – bij een leverancier van inlogmiddelen worden opgeslagen.

*De fractie van de **PVV** merkt op dat volgens de heer Böhre een decentrale opzet meer zou passen bij het idee van informationele zelfbeschikking conform de slogan "Regie op Gegevens" van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Kan de regering aangeven hoe de mogelijkheid voor een centrale opzet zich tot het "Regie op Gegevens"-concept van het ministerie verhoudt?*

In reactie op deze vraag merk ik op, dat 'regie op gegevens' erop ziet dat burgers weten welke gegevens over hen verwerkt worden, daar zelf indien nodig correctie op kunnen (laten) plegen en hun gegevens zelf kunnen delen met anderen indien zij dat wensen. Dit vraagstuk is overigens wezenlijk anders dan een inrichtingskeuze voor specifieke privacymaatregelen in systemen, waarover het bij eID gaat. De burger wordt niet verplicht om regie op zijn gegevens te nemen. Mensen die dat niet willen hoeven dat niet te doen. Wel is het zo, dat ik op dit moment onderzoek hoe ik burgers die dat wel willen, kan ondersteunen om dit op een veilige wijze te doen. Er wordt niet beoogd om de burger een nieuwe of aanvullende rol te geven in lopende overheidsprocessen, bijvoorbeeld dat hij voor elke stap zou moeten instemmen met verwerking van zijn gegevens. Uitgangspunt is dat de burger niet steeds zijn gegevens hoeft aan te leveren (hergebruik; de overheid vraagt niet naar de bekende weg) en dat de burger mag verwachten dat de overheid zaken voor hem regelt zonder hem onnodig (administratief) te belasten. Daarmee wordt ook voorkomen dat gegevens op meerdere plekken worden opgeslagen. Ook zal de burger meer zicht krijgen op wat er met zijn gegevens gebeurt. Dit aanvullend op de reeds geldende mogelijkheden om inzage te bieden in de verwerking van gegevens.

In het laatste cluster van dit hoofdstuk wordt nader ingegaan op het thema 'regie op gegevens'.

*De leden van de fractie van de **PVV** geven aan dat de regering stelt dat de gegevens goed worden beschermd omdat de AVG van toepassing is. Zij vragen of de regering kan aangeven in hoeverre ook aan de 'voorkant' wordt getoetst of aan de eisen van deze verordening wordt voldaan of dat dit toezicht alleen achteraf plaatsvindt. En kan de regering aangeven waarom er toch ingezet wordt op de mogelijkheid van een centrale opzet, terwijl juist volgens de moderne privacyvereisten op het gebied van privacy by design een decentrale architectuur meer voor de hand ligt, waarbij de kans op grootschalige hacks, heimelijke toegang, massale datalekken en sluipende doelverschuiving ook kleiner is?*

In reactie op het bovenstaande merk ik op dat de eisen die aan inlogmiddelen worden gesteld gebaseerd zijn op de eIDAS verordening en de AVG. Op deze eisen wordt zowel voorafgaand aan de toelating, als tijdens de dienstverlening gecontroleerd.

Ten aanzien van decentrale opzet benadruk ik, dat dat één van de manieren, dus niet de enige manier, is waarop adequate privacybescherming kan worden gerealiseerd. Ook in een centrale architectuur is het niet per definitie zo dat attributen op meer plaatsen centraal worden opgeslagen dan nu het geval is. Het wetsvoorstel faciliteert centrale en decentrale oplossingen. De WDO maakt voorts het werken met pseudoniemen mogelijk, waardoor attributen (gegevens) in het geheel niet beschikbaar zijn voor aanbieders van inlogmiddelen en daarmee de genoemde risico's worden ondervangen. Iets anders is de beschikbaarheid van loggegevens. Zoals eerder aangegeven, zijn deze beschikbaar bij zowel decentraal als centraal bekend staande aanbieders. Ik vind dat van belang omdat logging ten dienste kan zijn van burgers die in de knel komen. Waar het om gaat is dat ongewenst gebruik van gegevens onmogelijk wordt gemaakt en verboden wordt; dat gebeurt ook. De AP houdt, als toezichthouder op de bescherming van persoonsgegevens, aanvullend toezicht.

Samengevat biedt zowel een decentrale als een centrale opzet risico's en kansen. Het één is niet per definitie beter dan het andere. Ik kies daarom niet voor of tegen een specifieke opzet, omdat ik daarmee voor de burger goede oplossingen zou uitsluiten. Als decentraal te boek staande oplossingen zijn daarom mogelijk. Overigens ben ik van mening dat voor een goede oplossing er elementen van beide nodig zijn, die elkaar bovendien kunnen versterken. De kracht en de bescherming die wordt geboden ligt in het samenstel van deze elementen, waarbij een oplossing controleert aan een bronregister om te zorgen dat de identiteit van de burger juist gekoppeld wordt, ernaar wordt gestreefd zo min mogelijk gegevens op te slaan en er ook voor gezorgd wordt dat de burger geholpen kan worden wanneer deze met problemen bij de overheid aanklopt. Daarbij zorg ik ervoor dat door het stellen van strenge eisen aan de bescherming van persoonsgegevens, in combinatie met een strenge doorlopende controle, aangeboden oplossingen op hun merites

worden beoordeeld. Het gaat er uiteindelijk om of de te beschermen belangen geborgd blijven, niet met welke oplossingsrichting dat gebeurt.

Regie op gegevens

*De leden van de fractie van **GroenLinks** vragen of de regering het met ze eens is, dat juist de laatste jaren er in gevoelige domeinen een duidelijke verschuiving heeft plaatsgevonden van centrale naar decentrale infrastructuren, bijvoorbeeld op het terrein van biometrie en persoonsgegevens als het BSN. Hoe kan de regering garanderen dat er maximale standaardinzage, correctierecht en verwijderingsrecht worden verankerd, waarbij bij aanpassingen en verwijderingen deze in de gehele keten worden aangepast?*

In reactie merk ik op dat ik deze verschuiving niet waarneem. Ik wijs erop dat er momenteel wordt gewerkt aan 'regie op gegevens'. Het gaat daarbij niet om het verankeren van de door de leden gememoreerde rechten – deze bestaan immers al, onder meer ingevolge de AVG – maar het zorgen dat deze rechten ook daadwerkelijk door burgers geeffectueerd kunnen worden.

*De leden van de fractie van **GroenLinks** vragen naar een reactie inzake het idee van informationele zelfbeschikking en de slogan "Regie op Gegevens" van het ministerie van Binnenlandse Zaken.*

In reactie op deze vraag merk ik op, dat ik informationele zelfbeschikking van belang vind. Zoals hiervoor opgemerkt moet 'regie op gegevens', waaraan op dit moment wordt gewerkt, moet ervoor zorgen dat de burger de op hem betrekking hebbende gegevens snel en laagdrempelig ter beschikking kan hebben en veilig met andere organisaties kan delen indien hij dat wenst. Dat staat los van de inrichting van eID en inlogmiddelen. Het voornemen bestaat om het onderwerp verbetering van de persoonlijke informatiepositie van burgers (regie op gegevens) in de volgende tranche van de WDO een plek te geven, zoals ook in hoofdstuk 2 is aangegeven.

4. Elektronische identificatie (eID)

In dit hoofdstuk worden de door de fracties gestelde vragen beantwoord over innovatie, attributen, de rol van de overheid en van private partijen bij elektronische identificatie, alsmede wordt ingegaan op inclusiviteit.

*De fractie van **FVD** hecht aan de Nederlandse voorloperspositie op het gebied van technologische innovatie: van de eerste internetverbinding in 1988 tot het ontwikkelen van bluetoothtechnologie. De fractie vraagt of de regering aan kan geven op welke wijze zij de Nederlandse concurrentiepositie en Nederlandse initiatieven en marktpartijen bij het ontwikkelen van vertrouwensdiensten ondersteunt, alsmede welke rol de Wet digitale overheid hierbij speelt.*

In reactie hierop merk ik op, dat vertrouwensdiensten ingevolge de definitie van de eIDAS-verordening (artikel 3, onder 16) diensten zijn voor het aanmaken, verifiëren en valideren van elektronische handtekeningen, zegels of tijdstempels of certificaten voor authenticatie van websites. Vertrouwensdiensten worden niet gereguleerd door het onderhavige wetsvoorstel. De uitvoering van dit onderdeel van de eIDAS-verordening is gerealiseerd middels de wet van 21 december 2016 tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (Stb. 2017,13).

Nederland ondersteunt innovatie en digitalisering, waaronder elektronische vertrouwensdiensten, door de randvoorwaarden hiervoor op orde te hebben en door digitalisering in diverse domeinen te stimuleren. In de Nederlandse Digitaliseringsstrategie worden jaarlijks de resultaten en

doelstellingen van het kabinet voor digitalisering uiteengezet. Bij digitale transacties spelen elektronische vertrouwensdiensten een belangrijke rol als het gaat om de vertrouwelijkheid en integriteit van gegevens. Het kabinet ondersteunt verschillende datadeel-initiatieven waarbij vertrouwensdiensten ook worden gebruikt. In Europees verband werkt het kabinet aan de verdere doorontwikkeling van de eIDAS-verordening, zodat aanbieders van vertrouwensdiensten hun producten nog beter op de Europese markt kunnen aanbieden.

*De leden van de fractie van **FVD** vragen wat de noodzaak is van een middel naast DigiD, als het op eenzelfde centrale manier beheerd wordt als het DigiD-stelsel, maar dan niet onder directe sturing/controle van de overheid geëxploiteerd wordt. In dit verband vragen de leden van de **SP-fractie** waarom er niet gekozen is voor een publieke taak. Zij geven aan dat het verifiëren van iemands identiteit door middel van een check op de basisregistratie niet overgelaten moeten worden aan de markt. Als de regering hier aan vast wil houden, dan zou een verstandige keuze zijn om geen aanbieders met een winstoogmerk toe te staan. Commerciële partijen hebben namelijk andere belangen dan puur een goed werkend product aan te willen bieden. De winsten hoeven zeker niet alleen uit inkomsten uit de applicatie te bestaan, vooral omdat meer geld verdiend kan worden met data. Wanneer ervoor gekozen wordt om commerciële partijen geen onderdeel te laten zijn, dan valt een belangrijk risico weg. Hoe ziet de regering dit? De SP-fractie geeft mee dat dit iets is wat we niet aan het toeval moeten overlaten. Iedere bestuurder en passagier die in een auto stappen, gaan ervan uit dat er geen ongeluk zal gebeuren. Toch doen we de veiligheidsgordel om. Voor de leden van de SP-fractie is deze veiligheidsgordel hard nodig om goedkeuring te kunnen geven aan het wetsvoorstel.*

In reactie op het bovenstaande merk ik op, dat ervoor is gekozen om in het burgerdomein naast het publieke middel DigiD ook private middelen toe te laten. Reden hiervoor is het borgen van de continuïteit van de dienstverlening bij een eventuele uitval van DigiD. Burgers hebben daardoor een terugvaloptie. Daarnaast zorgt het mogelijk maken van de komst van private middelen voor vitaliteit in het stelsel, omdat door concurrentie – binnen het strenge publiekrechtelijke kader waarmee de overheid op veiligheid en privacy stuurt en controleert – de prikkel naar vernieuwing en daarmee de inzet van steeds betere beschermingsmethoden (innovatie) wordt aangejaagd. Bovendien zorgt de aanwezigheid van meerdere middelen gezamenlijk voor het sneller bereiken van een grotere dekkingsgraad van middelen met een hogere betrouwbaarheid. In dit verband wordt, anders dan de SP-fractie lijkt te menen, de verificatie van iemands identiteit niet overgelaten aan de markt, maar wordt dit gerealiseerd door een generieke digitale voorziening (het BSN-koppelregister), zoals voorzien in art. 5, eerste lid onder d, van het wetsvoorstel.

Of een dergelijk privaat middel op een centrale of decentrale manier beheerd wordt, is als zodanig niet van belang zolang er voldaan wordt aan de wettelijke veiligheids- en betrouwbaarheidseisen, die bij AMvB en ministeriële regeling nader worden ingevuld. Op conformiteit met deze eisen, waaronder het verbod op verhandelen van gegevens, wordt door mij voorafgaand aan de toelating (erkenning) getoetst, alsmede gedurende de dienstverlening; toezicht ter zake wordt opgedragen aan het AT. Er is dus sprake van toetsing en controle door de overheid. In het vorige hoofdstuk heb ik aangegeven welke waarborgen in dit verband opgenomen zijn; de AMvB's bij het wetsvoorstel worden aan het parlement voorgelegd zodat ook daarop democratische controle kan worden uitgeoefend.

*De leden van de **GroenLinks-fractie** merken op, dat de regering verwacht dat door private aanbieders toe te laten de weerbaarheid en beschikbaarheid worden vergroot. De leden vragen of er niet voor wordt gevreesd, dat er slechts enkele grote aanbieders zullen overblijven, zoals we bijvoorbeeld ook zien in de telecomsector en sociale media.*

In reactie hierop merk ik op, dat het moeilijk te voorspellen is hoe de markt zich gaat ontwikkelen. In de gesprekken die tijdens marktconsultaties met private partijen worden gevoerd, blijkt dat er op dit moment een grote variëteit bestaat aan aanbieders, waarbij het vooral kleinere innovatieve bedrijven zijn die zich toeleggen op het aanbieden van betrouwbare authenticatie, en dat derhalve

niet als een bijproduct, maar als 'core business' zien. Het toelaten en streng inkaderen van inlogmiddelen die te gebruiken zijn in het publieke domein, en het onmogelijk maken van verdienmodellen waarin persoonsgegevens commercieel worden uitgenut, zie ik in die zin ook als een manier om bedrijven in de Nederlandse markt, die zich professioneel toeleggen op 'inloggen' als hun primaire business, de kans te bieden en te beschermen (en daarmee ook burgers) tegen grote techbedrijven die deze dienstverlening als een bijproduct zien voor de uitnutting van persoonsgegevens.

Doordat burgers deze middelen ook breder kunnen gebruiken dan alleen voor toegang tot de overheid worden zij ook in breder verband beter beschermd. Buiten het publieke domein – inloggen bij commerciële bedrijven zoals webwinkels - worden nu in aanzienlijke en toenemende mate inlogmethoden gebruikt van grote (tech)bedrijven. Die ontwikkeling is gaande en staat los van de WDO. Reden voor het als 'bijproduct' aanbieden van inlogmiddelen is veelal om zoveel mogelijk mensen een zo volledig mogelijk pakket digitale diensten te bieden. Dergelijke klantenbinding is op zichzelf gerechtvaardigd. Door burgers de keus te bieden en in staat te stellen om gebruik te maken van een door de overheid toegelaten (en derhalve op basis van de WDO goedgekeurd en gecontroleerd) inlogmiddel, kunnen zij kiezen voor een middel gebaseerd op overheidsvertrouwen, en zijn zij niet aangewezen op of afhankelijk van een 'big tech' inlogmiddel. Afgeleid van de WDO wordt op die manier aan burgers de mogelijkheid geboden om, breder dan bij de overheid alleen, te kiezen voor een alternatief.

*De leden van de **GroenLinks-fractie** vragen of het zogenoemde 'aanvalsoppervlak' niet vele malen groter wordt door het toelaten van private partijen en of de regering overwogen heeft om zelf meerdere systemen te ontwikkelen.*

Zoals eerder opgemerkt worden alle partijen voorafgaand aan de toelating onderworpen aan strenge controles. Meer partijen biedt een voordeel voor wat betreft beschikbaarheid en het hebben van een terugvaloptie. Dat is een belangrijke reden geweest om te kiezen voor een open stelsel, waarbij meerdere middelen kunnen worden toegelaten, waaronder private. Daarnaast worden – en dat behoort tot mijn verantwoordelijkheid – publieke middelen ontwikkeld. Het is van belang dat private inlogmiddelen hiervoor een volwaardig, even veilig en betrouwbaar alternatief vormen, middels gescheiden systemen, organisaties en methoden.

De leden van de **GroenLinks-fractie** vragen of de keus voor private aanbieders er niet voor zorgt dat de overheid meer onderhoud en toezicht moet verzorgen.

In reactie hierop merk ik op, dat dat inderdaad de consequentie is. Echter, gelet op de genoemde voordelen van de gekozen systematiek, ben ik van mening dat deze extra inspanningen gerechtvaardigd zijn, zeker ook vanwege de werking die zich met private middelen niet alleen uitstrekt tot het overheidsdomein maar voor burgers ook profijt kan bieden voor inloggen in het commerciële domein.

*De fractie van **Groen Links** merkt op dat de wet uitgaat van een centraal systeem en juist attributen voor inlogmiddelen voor individuen er niet in staan. Waarom is in 2017 het systeem van attributen losgelaten? Is de regering bereid, gelet op het lange voortraject van deze wet en de aanwezigheid, in tegenstelling tot 2017, van nieuwe attributenaanbieders, dit te heroverwegen? Is daardoor de wet niet feitelijk ingehaald door de tijd? Is de regering bijvoorbeeld bereid om in artikel 1 een zin toe te voegen waarin alsnog een definitie van een attributendienst wordt opgenomen, in artikel 5 de dienst als onderdeel van de generieke digitale infrastructuur toe te voegen aan het eerste lid en als laatste in artikel 9 op te nemen dat attributendiensten worden toegelaten door verlening van een erkenning door de minister.*

Zoals in het vorige hoofdstuk is toegelicht, gaat de wet niet uit van een centraal systeem. De wet stelt de adequate bescherming van persoonsgegevens centraal, en biedt ruimte voor zowel centrale als decentrale oplossingen. Voorts merk ik het volgende op. Een attributendienst is een partij die

een verklaring afgeeft over de kenmerken en gegevens van een natuurlijke persoon of rechtspersoon. Aanvankelijk was de gedachte deze diensten afzonderlijk toe te laten tot het eID-stelsel. Na de (internet)consultatie is de systematiek van het wetsvoorstel gewijzigd, waarna attributendiensten als zodanig niet langer in het wetsvoorstel zijn gedefinieerd of onderworpen aan een erkenning. Reden daarvoor is dat het afgeven van authenticatieverklaringen - die gebaseerd zijn op persoonsidentificatiegegevens, oftewel attributen (zie artikel 1 wetsvoorstel) - en de uitgifte van inlogmiddelen worden beslagen door de regels voor authenticatiediensten en middelenuitgevers.

In het wetsvoorstel wordt geregeld dat die partijen aan strenge eisen moeten voldoen, willen ze voor erkenning (toelating) in aanmerking komen. Ook worden aan de erkenning voorschriften en beperkingen verbonden. Deze eisen en voorschriften, die onder meer betrekking hebben op de werking, beveiliging en betrouwbaarheid van inlogmiddelen op verschillende betrouwbaarheidsniveaus, zijn gebaseerd op de eIDAS-verordening en bijbehorende uitvoeringsverordeningen, en zijn uitgewerkt bij en krachtens AMvB. Gedacht moet bijvoorbeeld worden aan eisen met betrekking tot de wijze waarop de identiteit van de aanvrager van het middel wordt bewezen en geverifieerd, de kenmerken van het middel, uitgifte, uitreiking en intrekking van het middel en controle van de juistheid van voor het authenticatieproces gebruikte gegevens.

Attributenaanbieders behoeven dus geen afzonderlijke regulering, aangezien zij als zodanig geen authenticatieverklaring of inlogmiddel uitgeven; validatie en gebruik van attributen wordt reeds, namelijk over de band van authenticatiediensten en middelenuitgevers, geregeld. Het systeem van attributen is niet losgelaten, maar wordt op een andere wijze geregeld. Indien hier, op basis van opgedane ervaringen of nieuwe inzichten, aanleiding toe bestaat, zal de attributendienst als zodanig in de volgende tranche van het wetsvoorstel worden verankerd.

*De leden van de **PVV-fractie** constateren dat de staatssecretaris in het verslag van het schriftelijk overleg stelt: "In dit verband wordt binnen het eID-stelsel ook de mogelijkheid geboden om met attributen (gegevenssets, zie artikel 1 van het wetsvoorstel) te werken."[3] De leden vragen of de regering kan aangeven waarom attributen slechts als 'mogelijkheid' worden geboden in plaats als vaste standaard.*

In reactie hierop – en in aanvulling op mijn reactie op de hierboven gestelde vragen van de GroenLinks fractie - merk ik op, dat de reden hiervoor is dat er naast oplossingen die met attributen werken ook andere oplossingen mogelijk (kunnen) zijn die aan de vereisten van het wetsvoorstel, de uitvoeringsregelgeving, de eIDAS-verordening en de AVG voldoen.

*De leden van de fractie van de **ChristenUnie** merken op dat de afgelopen jaren de noodzaak van het gebruik van betrouwbare en veilige digitale identificatiemiddelen steeds urgenter is geworden. Ondanks verschillende aanpassingen, zoals twee-factor-authenticatie en inloggen middels een applicatie, is het middel DigiD dringend aan vervanging toe. Ontwikkelingen in de markt nopen hier ook toe: consumenten willen steeds meer online zakendoen (in 2019 is de omzet van online winkelen met 7% gestegen). Tegelijkertijd is er geen zicht op een inlogmiddel vanuit de overheid en is het aanbod van digitale inlogmiddelen in de markt beperkt. Kan de regering aangeven welke rol de Wet digitale overheid speelt in het oplossen van dit urgente vraagstuk?*

In reactie op het bovenstaande merk ik op, dat dit wetsvoorstel de taken en verantwoordelijkheden ten behoeve van de werking van de infrastructuur voor identificatie en authenticatie in het publieke domein door burgers en bedrijven verankert. In dat verband draag ik zorg voor de ontwikkeling van inlogmiddelen voor burgers op een hoger betrouwbaarheidsniveau dan het huidige DigiD, zodat diensten die een hoge of zeer hoge mate van betrouwbaarheid vereisen ook digitaal kunnen worden verleend. Het wetsvoorstel verplicht daarnaast bestuursorganen en aangewezen

[3] Kamerstukken I 2019/20, 34 972, I, p. 7.

organisaties, vanwege het feit dat een groot deel ervan een publieke taak uitoefent voor hun elektronische diensten waarvoor, gelet op de aard ervan veilige toegang in de rede ligt, het betrouwbaarheidsniveau 'substantieel' of 'hoog' te gebruiken. De verplichtingen gelden ook voor daartoe (in de bijlage bij de wet) aangewezen private organisaties, die elektronische diensten verlenen aan burgers of bedrijven waarvoor een veilige en betrouwbare authenticatie essentieel is, zoals bij zorgverzekeraars en pensioenuitvoerders. Dit wetsvoorstel strekt er tevens toe dat de digitale toegang tot dienstverlening van bestuursorganen en aangewezen organisaties generiek wordt ingericht zodat burgers en bedrijven met één of meer generieke identificatiemiddelen overheidsbreed en op een passend betrouwbaarheidsniveau toegang kunnen krijgen tot elektronische diensten.

Op dit moment is DigiD op betrouwbaarheidsniveau 'substantieel 'beschikbaar en vanaf 1 januari 2021 is de eNIK beschikbaar. Het eRijbewijs volgt vanaf inwerkingtreding van onderhavig wetsvoorstel. Tegelijkertijd wordt het publieke inlogmiddel continu doorontwikkeld op basis van gebruikerservaringen en nieuwe beschikbare technieken.

Naast publieke inlogmiddelen voorziet het wetsvoorstel erin om, middels de systematiek van erkenning, private burgermiddelen op niveau substantieel en hoog toe te laten. In die zin is de inwerkingtreding van deze wet randvoorwaardelijk voor een brede beschikbaarheid van inlogmiddelen op een hoger betrouwbaarheidsniveau.

*De leden van de fractie van **GroenLinks** vragen hoe de regering verklaart dat Wet digitale overheid leunt op een site die verouderde informatie en standaarden bevat en waarvan het lijkt dat deze niet (voldoende) actueel gehouden wordt terwijl dat essentieel is.*

In reactie op deze vraag merk ik op dat mogelijk gedoeld wordt op de website www.digitaleoverheid.nl. Deze website wordt continu door een redactie in samenspraak met de dossierhouders bijgewerkt. Dank voor uw signaal dat de website mogelijk verouderde informatie bevat. Ik zal er zorg voor dragen dat de informatie op actualiteit wordt gecheckt.

*De leden van de fractie van de **ChristenUnie** hebben ook vragen over de ethische aspecten van de COVID-app. De minister van VWS heeft een aantal deskundigen gevraagd om een ethische analyse daarvan te geven en op basis van die analyse enkele aanbevelingen te doen. Hun rapport 'Ethische analyse van de COVID-19 notificatie-app' identificeert tien kernwaarden. Deze leden vragen de regering welke kernwaarden ook van belang voor zijn de Wet digitale overheid, en in hoeverre die waarden in het onderliggende wetsvoorstel gerealiseerd zijn.*

In reactie op het bovenstaande merk ik op dat het rapport 'Ethische analyse van de COVID-19 notificatie-app tien kernwaarden noemt die leidend zijn bij het ontwerp, de invoering en het gebruik van de COVID-19 notificatie-app. Deze zijn: vrijwilligheid, effectiviteit, privacy, rechtvaardigheid, inclusiviteit, procedurele rechtvaardigheid, verantwoordelijkheid, voorkomen van oneigenlijk gebruik, borgen burgerlijke vrijheden, noodzakelijkheid en proportionaliteit. Middels het onderhavige wetsvoorstel kunnen burgers (natuurlijke personen) en bedrijven (rechtspersonen en ondernemingen) effectief digitale toegang krijgen tot de publieke dienstverlening van de overheid; dit is vanzelfsprekend een ander doel dan het ontwerp van een app.

De genoemde kernwaarden zijn niettemin wel terug te vinden; in het wetsvoorstel zelf en in de uitvoeringsregelgeving. Zo kent het wetsvoorstel artikelen die betrekking hebben op privacybescherming (art. 16 WDO), de toelating van publieke- en private identificatiemiddelen (art. 9 WDO: vrijwilligheid private partijen), verantwoordelijkheid van de minister van BZK voor het beheer van de generieke digitale infrastructuur (art. 5 WDO), het voorkomen van oneigenlijk gebruik (art. 10 WDO) en de zorg voor een machtigingsvoorziening (art. 5(1)(b) WDO: inclusiviteit).

De kernwaarden worden nader uitgewerkt in lagere regelgeving. Privacybescherming wordt nader uitgewerkt in het Besluit Digitale Overheid; hierin worden regels gesteld betreffende de verwerking van persoonsgegevens in de voorzieningen voor de generieke digitale infrastructuur DigiD, DigiD Machtigen, MijnOverheid, BSN-koppelregister, routeringsvoorziening, privaat identificatiemiddel en – diensten, bedrijfs- en organisatiemiddel en – diensten en eIDAS-voorziening. Ingevolge het Besluit identificatiemiddelen voor natuurlijke personen en het Besluit bedrijfs- en organisatiemiddelen worden nadere eisen gesteld aan de toelating van inlogmiddelen. Kernwaarden als privacy, het voorkomen van oneigenlijk gebruik en inclusiviteit (toegankelijkheid, gebruiksvriendelijkheid) komen hierin naar voren. Zo mogen de persoonsgegevens enkel gebruikt worden ter aanvraag van het middel, mag het identificatiemiddel enkel gebruikt worden door de houder van het middel en zorgt het systeem van open toelating ervoor dat een breed scala aan middelen specifiek toegespitst op bepaalde doelgroepen toegelaten kan worden.

*De leden van de fractie van de **ChristenUnie** wijzen op de dynamiek tussen innovatie enerzijds en ethische principes anderzijds. De vraag is: bepaalt innovatie de inhoud van ethische principes of geven ethische principes (mede) vorm aan innovatie? In de ethiek van de techniek wordt in het algemeen de opvatting gehuldigd dat ethische principes mede richting zouden moeten geven aan innovaties. Is de regering het met deze opvatting eens? Zo ja, wat zou dat betekenen voor de Wet digitale overheid in relatie tot kernwaarden in het voornoemde rapport?*

In reactie op het bovenstaande merk ik op dat het kabinet van mening is dat fundamentele rechten en publieke waarden centraal moeten staan bij innovaties die impact hebben op mens en samenleving. Techniek dient de mens en niet andersom. De fundamentele rechten en publieke waarden zijn deels verankerd in wet- en regelgeving, deels in ethische kaders waarvan het kabinet het wenselijk acht dat die gevolgd worden. Wet- en regelgeving voorzien in (juridisch afdwingbare) waarborgen; niet wordt voorgeschreven hoe de innovaties eruit komen te zien. De normstelling in en op basis van dit wetsvoorstel is zoveel mogelijk functioneel en techniekonafhankelijk van karakter om ruimte te bieden aan maatwerk en om specifieke maatschappelijke knelpunten op een innovatieve wijze op te lossen. Alleen waar noodzakelijk – bijvoorbeeld voor de borging van interoperabiliteit – is in meer specifieke normstelling voorzien. Dit is ook conform de wens van de Tweede Kamer. De ervaringen die worden opgedaan kunnen ertoe leiden dat in de toekomst bepaalde normen worden aangescherpt en waar wenselijk zelfs tot formele wet worden verheven.

*De fractie van **Groen Links** merkt op dat burgers voorheen met de overheid per brief konden communiceren. Met name ouderen, laagopgeleiden en laaggeletterden hechten hier veel waarde aan. In de digitale variant kan dat niet. De leden hebben een aantal vragen. Is de regering bereid na te denken om middels tweezijdig verkeer de mogelijkheid te openen om zowel via een fysiek loket als digitaal direct met een overheid te kunnen communiceren? Hoe kijkt de regering aan tegen een chatfunctie, zoals je bij veel bedrijven en zorgverzekeraars al ziet? Is de regering bereid toe te zeggen dat er een fatsoenlijke klachtbehandeling wordt verankerd in de wet, waarbij met name ouderen, laagopgeleiden en laaggeletterden meer worden ontzorgd? Is de regering bereid om financieel kwetsbare burgers tegemoet te komen in de kosten?*

*De leden van de **ChristenUnie** fractie wijzen in dit verband op Het rapport-Remkes (rapport van de Staatscommissie parlementair stelsel) dat benadrukt dat de overheid nabij de burger moet zijn. In tijden van digitalisering is dit met name belangrijk voor burgers die moeite hebben met lezen en schrijven. De leden vragen de regering wat deze wet bijdraagt aan de nabijheid van de digitale overheid. Draagt deze wet bij aan een overheid die dichter bij haar burgers staat? Draagt deze wet bij aan het verminderen van de kloof tussen digitaal vaardige en niet digitaal vaardige burgers? In de deskundigenbijeenkomst kwamen twee aandachtspunten aan de orde: de klachtenregeling en machtigingsregeling. Hoe kijkt de regering naar deze onderwerpen? Is verbetering noodzakelijk? Zo ja, hoe gaat de regering dat vormgeven?*

*Ook de leden van de **PvdA** vragen of de regering kan aangeven hoe dit wetsvoorstel voorziet in een goede toegankelijkheid van de voorzieningen voor mensen met minder doenvermogen.*

*De leden van de fractie van de **PVV** vragen, refererend aan het gestelde tijdens de deskundigenbijeenkomst, of de regering kan aangeven in hoeverre de namens de Stichting Lezen en Schrijven geschetste risico's voor de betreffende doelgroepen worden ondervangen. Het betreft het feit dat er voor laaggeletterden meerdere keuzemogelijkheden komen, het feit dat er extra handelingen nodig zijn wat voor grotere drempels zorgt, alsmede het feit dat kosten minimaal moeten zijn.*

In reactie op het bovenstaande merk ik in de eerste plaats op, dat het wetsvoorstel niet verplicht tot digitale communicatie met de overheid; het geeft slechts regels voor het geval er digitaal met de overheid wordt gecommuniceerd. De papieren weg blijft open. Dat volgt niet uit de WDO, maar (sinds 2004) uit de Algemene wet bestuursrecht (Awb). Afdeling 2.3 van de Awb, inzake elektronisch bestuurlijk verkeer, wordt momenteel gemoderniseerd. Hiertoe is wetvoorstel bij de Tweede Kamer nr. 35 261 ingediend. In dit Awb-wetsvoorstel wordt de gelijkschakeling van de papieren en digitale weg gehandhaafd; de burger kan kiezen of hij digitaal of op papier met de overheid communiceert. Het Awb-wetsvoorstel introduceert nieuwe waarborgen (rechtsbescherming) voor het geval de burger de digitale weg kiest, zoals een notificatieplicht voor het bevoegd gezag, de digitale ontvangstbevestiging en verlengde termijnen bij storing. Ook bevat het wetsvoorstel, los van digitalisering, een zorgplicht voor het bevoegd gezag tot passende ondersteuning bij bestuurlijk verkeer. Het bevoegd gezag moet ervoor zorgen dat de doelgroep waarop een dienst zich richt, normaal gesproken deze dienst kan afnemen, mede gelet op de beschikbare maatschappelijke voorzieningen en de eigen verantwoordelijkheid om aan bepaalde kwalificaties te voldoen. De vorm waarin de ondersteuning wordt geleverd wordt aan het bevoegd gezag overgelaten en is afhankelijk van de aard van de dienstverlening en betreffende doelgroep(en). Het gaat hierbij om het geven van voorlichting en het beantwoorden van vragen op een manier die aansluit bij de doelgroep, zoals via een helpdesk of chatfunctie.

Overigens hecht ik eraan om in zijn algemeenheid op te merken, dat digitalisering niet per se leidt tot uitsluiting en het groter worden van de groep die niet digitaal zaken doet, integendeel. Door op een goede manier gebruik te maken van de mogelijkheden van digitalisering, en door dat samen met verschillende partijen te doen, kunnen juist meer mensen aan de maatschappij deelnemen. In dit verband voorziet het inclusiebeleid van de regering er bijvoorbeeld in, dat in gemeenten fysieke Informatiepunten Digitale Overheid worden ingericht. Middels een landelijk dekkend netwerk – de informatiepunten worden veelal in bibliotheken en gemeentehuizen gehuisvest - wordt mensen (gratis) praktische hulp geboden bij het leggen van digitaal contact met de overheid en worden ze bijvoorbeeld geholpen met vragen over zorg- en huurtoeslag, het betalen van verkeersboetes en het gebruik van DigiD. Iedereen moet immers mee kunnen doen in de digitale samenleving. Het voorgaande sluit nauw aan bij hetgeen door de vertegenwoordigers van de Stichting Lezen en Schrijven is opgemerkt tijdens de deskundigenbijeenkomst van 30 juni jl.

Voorts wijs ik erop, dat klachtbehandeling in (hoofdstuk 9 van) de Awb verankerd is en dat art. 2.1 Awb erin voorziet dat een ieder zich ter behartiging van zijn belangen in het verkeer met bestuursorganen kan laten bijstaan of door een gemachtigde laten vertegenwoordigen. De digitale machtigingsvoorziening wordt geregeld in het wetsvoorstel Digitale overheid.

Bij de voorbereiding van het eID-stelsel is rekening gehouden met de vraag of de regeling doenlijk is voor burgers. In verband met de ontwikkeling van DigiD substantieel en hoog zijn gedurende het gehele proces gebruiksvriendelijkheid, toegankelijkheid (inclusie) en brede bruikbaarheid mede uitgangspunten. Hieraan wordt onder meer via onderzoek en gebruikerspanels getoetst. De uitkomsten hiervan werken ook door in de regelgeving. Ook zijn er, naast generieke oplossingen voor het grootste deel van de burgers, ook meer specifieke op doelgroepen gerichte oplossingen mogelijk. Bij de technisch-organisatorische inrichting en vormgeving van het eID-stelsel is een evenwicht gevonden tussen betrouwbaarheid en veiligheid – waardoor inderdaad meer handelingen nodig zijn - en het burgerperspectief. DigiD is zo eenvoudig uitvoerbaar als mogelijk is, gelet op de veiligheid en betrouwbaarheid. Overigens

betreft het een continu ontwikkelproces; op basis van opgedane ervaringen en nieuwe inzichten zullen de komende jaren verdere verbeteringen worden doorgevoerd.

5. Toezicht en handhaving

*De leden van de **FVD-fractie** merken op dat het goed lijkt als het duidelijk is dat marktpartijen die gespecialiseerd zijn in veilig online handelen beschikbaar zijn voor burgers om zaken te doen met overheden en bedrijfsleven. Juist als deze partijen zich richten op het veilig houden van de informatie voor de burger los van de partijen waar zij zaken mee doen versterkt dit de positie van de burger. Want er kan natuurlijk ook een belangentegenstelling zijn tussen de burger en de overheid. Wat dan wel geborgd moet zijn, is dat deze partijen gedwongen zijn zich te houden aan strenge regelgeving (standaarden) en goed toezicht. De leden vragen in hoeverre de Wet digitale overheid toeziet op het handhaven van de hoogste veiligheids- en privacy-standaarden. Dit mag niet ondermijnd worden doordat sommige lidstaten een ander idee hebben over kwaliteit en handhaving. Kan de regering toelichten op welke basis, naast de Algemene verordening gegevensbescherming, kan worden gehandhaafd? Welke rol speelt hierbij de eIDAS-verordening? Worden er ook andere standaarden gewogen bij het toelaten van dit soort (vertrouwens)diensten in Nederland? Tot slot, hoe ziet de regering de rol van het Agentschap Telecom bij het implementeren van deze wet en of deze wet er inderdaad voor gaat zorgen dat de kracht van de normen in Nederland overeind blijft?*

In reactie op het bovenstaande merk ik op dat ingevolge dit wetsvoorstel strenge privacy- en beveiligingseisen worden gesteld, waaraan vooraf (dat wil zeggen bij de aanvraag om toelating/erkenning) en tijdens de dienstverlening door het Agentschap Telecom (AT) wordt getoetst. Het gaat daarbij over inlogdiensten. Vertrouwensdiensten, een andersoortige dienstverlening, valt niet binnen de werkingssfeer van de Wet digitale overheid. Overigens is AT hier ook de toezichthouder. Zie hierover hetgeen in reactie op een vraag van de leden van de FVD-fractie is opgemerkt in hoofdstuk 4. Overigens is het goed om op te merken dat de eIDAS-verordening uitgaat van het beginsel van wederzijdse erkenning. Een inlogmiddel dat in een andere lidstaat is toegelaten, moet in Nederland geaccepteerd worden voor de toegang tot overheidsdienstverlening. Dit staat los van het onderhavige wetsvoorstel.

*De leden van de fractie van **GroenLinks** vragen zich af in welk licht de regering de huidige tekorten bij de Autoriteit Persoonsgegevens ziet, gelet op de Wet digitale overheid. Acht zij de Autoriteit in staat om op voldoende adequate wijze haar taak uit te voeren op het gebied van toezicht van de digitale overheid? Is zij bereid de Autoriteit beter te faciliteren, mocht de wet in deze vorm worden aangenomen?*

In reactie op deze vragen merk ik op dat de Autoriteit Persoonsgegevens (AP) een onafhankelijke toezichthouder is, belast met het toezicht op de naleving van wettelijke regels voor bescherming van persoonsgegevens. In die rol zal de AP ook toezicht houden op het naleven van de regelgeving in relatie tot dit wetsvoorstel. Het spreekt voor zich dat ik de AP zal faciliteren indien hier in het kader van een onderzoek om gevraagd wordt. Over de wijze waarop de AP haar taken uitvoert en hoe met de beschikbare capaciteit wordt omgegaan, kan ik echter geen uitspraken doen. De AP bepaalt zelf haar prioriteiten en de daaraan gekoppelde inzet van toegekende middelen. Het toezicht van de AP heeft een eigen positie naast het toezicht wat is belegd bij het Agentschap Telecom (AT). Beide toezichthouders zullen hierin de afstemming vinden.

*De leden van de fractie van **GroenLinks** vragen voorts hoe de regering de governance gaat vormgeven en hoe de informatie-uitwisseling met de toezichthouder tot stand zal worden gebracht. Waarom heeft de regering gekozen voor een verschillend normenstelsel voor bedrijven en burgers? Maakt dit het niet onnodig ingewikkeld voor de toezichthouder?*

In reactie op het bovenstaande merk ik op dat het bestaan van twee regimes voortvloeit uit de bestaande praktijk in beide domeinen. Het naar elkaar toegroeien van deze domeinen, hetgeen voor de toekomst is voorzien, zal op enkele punten complexiteit met zich mee brengen. Echter, het is ook belangrijk om de domeinen geleidelijk en beheerst te laten samengroeien. Te abrupte wijziging heeft in beide domeinen het risico van discontinuïteit in zich. Het normenkader in het burger- en bedrijvendomein zijn overigens, mede vanwege hun oorsprong in de eIDAS-verordening, reeds deels eenduidig. Dit komt tot uitdrukking in de uitvoeringsregelgeving. Hierdoor is materieel al een eerste stap gezet in de richting van samenvoeging. De toezichthouder AT heeft aangegeven dat harmonisatie vanuit oogpunt van uitvoerbaarheid en handhaafbaarheid wenselijk is, maar acht de geschetste verschillen, gezien het voorziene toegroeien naar elkaar, op dit moment werkbaar.

*De leden van de fractie van **GroenLinks** merken op dat het Agentschap Telecom is aangewezen als toezichthouder. Overweegt de regering de toelating door een andere partij te laten doen of is het Agentschap Telecom hiervoor de meest logische partij? Hoe gaat de regering adequate handhaving vormgeven? Welke bevoegdheden gaat zij bij welke partijen beleggen, zoals bijvoorbeeld intrekking van toelating?*

In reactie op het bovenstaande merk ik op dat het AT de taak krijgt de toelating (erkenning) namens de minister uit te voeren. Ik acht het wenselijk dat de partij, die toezicht gaat houden op de naleving van de toelatingseisen, tevens betrokken is bij de toelating. Vanzelfsprekend blijf ik als bevoegd gezag verantwoordelijk voor besluiten tot toelating van een partij en intrekking of opschorting daarvan, waarbij ik in het bijzonder de cyber- en staatsveiligheid zal bezien. De taken van AT, informatieverstrekking, uitvoeringsinstructies en dergelijke zullen worden vastgelegd in een mandaatbesluit.

*De leden van de **D66-fractie** constateren dat de Raad van State heeft gewezen op de noodzaak van voldoende ICT-expertise bij de overheid. Kan de regering aangeven op welke manier dit advies van de Raad van State is overgenomen? Hoe wordt het kennisniveau ook op de lange termijn gegarandeerd? En kan de regering aangeven in hoeverre de aanbevelingen van de tijdelijke commissie ICT uit de Tweede kamer onder leiding van voormalig Kamerlid Ton Elias zijn uitgevoerd?*

In reactie op de vraag van de leden van de fractie van D66 merk ik op dat nut en noodzaak van voldoende ICT-expertise bij de overheid vanaf de vorige kabinetsperiode op de agenda staat. Het is vanuit mijn verantwoordelijkheid een belangrijk onderdeel van de Strategische I-Agenda voor de Rijksdienst. De aanbevelingen op dit gebied van de Tijdelijke commissie ICT zijn destijds grotendeels overgenomen. Zo is er een IT-traineeprogramma opgezet dat inmiddels succesvol is uitgebouwd naar drie tracks (IT, Data, Cyber). Ook is de pool van ICT project- en programmamanagers (I-Interim Rijk) fors uitgebreid en is het curriculum voor CIO-adviseurs geprofessionaliseerd. Dit is terug te lezen in de kabinetsreactie en voortgangsrapportages die destijds zijn opgesteld. Recentelijk zijn initiatieven die een impuls geven aan (actuele) ICT-expertise geïntensiveerd. Vanuit een rijksbreed onderzoek naar knelpunten is in 2018 het programma Versterking HR ICT Rijksdienst opgezet met diverse initiatieven voor het aantrekken, ontwikkelen en behouden van ICT-expertise. Onderdeel daarvan is een I-Partnerschap tussen de Rijksdienst en het Hoger Onderwijs om meer structureel in beeld te komen bij een jonge doelgroep, maar ook om eigen IT-expertise actueel te houden. Ook wordt met de Rijksacademie voor Digitalisering en Informatisering Overheid (RADIO) een impuls gegeven aan digitaliseringskennis van niet IT-ers, zoals beleidsmedewerkers en de ABD topmanagement groep, die veelal een opdrachtgeversrol hebben. Naast deze rijksbrede activiteiten worden vanzelfsprekend ook door afzonderlijke departementen en lagere overheden initiatieven ontplooid om ICT-expertise op peil te houden.

*De leden van de **PVV-fractie** vragen of de regering kan aangeven hoe van deze wet verwacht kan worden uitvoerbaar en handhaafbaar te ze zijn als deze voor de toezichthouder cruciale aspecten*

ontbreken. De leden vragen of de regering tevens kan aangeven wat de meest actuele stand van zaken is van het overleg tussen het ministerie en het Agentschap hierover en welke consequenties dit eventueel heeft voor voorliggend wetsvoorstel. Kan de regering aangeven waarom een duidelijk toelatingskader binnen de wet ontbreekt en waarom dit niet middels wetgeving geregeld wordt?

Zoals het AT ook zelf aangeeft, ben ik met hen in gesprek. Dat betreft zowel het maken van afspraken over de uitvoering van de toelating- en toezichttaken, als ook de communicatie en informatie-uitwisseling tussen het AT en mijn ministerie. Het overleg is constructief en betreft de nadere uitwerking van het wetsvoorstel in de uitvoeringsregelgeving. Het heeft geen consequenties voor het wetsvoorstel zelf.

Het toelatingskader in de wet wordt nader verankerd in twee AMvB's en een ministeriële regeling op basis van het wetsvoorstel – dus wel degelijk in regelgeving – met daarin eisen aan inlogmiddelen. Het betreft doelvoorschriften ('principle based'), wat wil zeggen dat deze nadere invulling behoeven via concreet te nemen maatregelen. De maatregelen kunnen daarbij verschillen. Hiermee wordt voorkomen dat specifieke oplossingen of technieken dichtgeregeld worden en is er ruimte voor nieuwe 'state of the art' beschermingsmethoden (innovatie). Dit is conform de wens van de Tweede Kamer, die mij verzocht dicht bij de eIDAS-vereisten te blijven. De toezichthouder geeft vervolgens zelf invulling aan de wijze waarop zij de toetsing uitvoert. Hiermee heeft AT als Rijksinspectie reeds ervaring onder bestaande wetgeving als de Telecommunicatiewet (mede in relatie tot de eIDAS-verordening) en de Wet beveiliging netwerk- en informatiesystemen.

*De leden van de fractie van de **ChristenUnie** constateren dat in de huidige voorstellen het Agentschap Telecom toezicht houdt op een deel van de Wet digitale overheid. De leden hebben daar vragen over. Wie houdt toezicht op die delen waar het Agentschap niet verantwoordelijk voor is? En wie houdt toezicht op het geheel? Krijgen de toezichthouders ook de benodigde bevoegdheden? Wat is de relatie tussen toelating versus toezicht? Hoe kan voorkomen worden dat (private) partijen toegelaten worden waarvan later blijkt dat ze niet aan de eisen van bijvoorbeeld doelbinding of bescherming van persoonsgegevens voldoen?*

In reactie op het bovenstaande merk ik op dat met het toezicht op de naleving van het bepaalde bij of krachtens de artikelen 9, 11 en 13 – toelating van publieke en private inlogmiddelen voor burgers en bedrijven – het Agentschap Telecom bij wet is aangewezen als toezichthouder. Het AT beschikt over de noodzakelijke toezichthoudende bevoegdheden op grond van de Awb. De tevens noodzakelijke handhavende bevoegdheden, zoals intrekking van een erkenning, last onder bestuursdwang, bestuurlijke boete, zal ik mandateren. Vanzelfsprekend ben ik als minister verantwoordelijk voor de veilige en betrouwbare werking van het stelsel als geheel. In dat verband wordt de inrichting van deze stelselverantwoordelijkheid door mij verder voorbereid en zal ik actief sturen op het realiseren van de maatschappelijke doelen van eID, waaronder veiligheid, betrouwbaarheid en privacy. Ten aanzien van de bescherming van persoonsgegevens wijs ik op de eerdere beantwoording ter zake.

6. Uitleiding

In de bovenstaande beantwoording heb ik toegelicht dat het geheel aan voorgenomen regels, toezicht en handhaving tezamen met uitvoering in (ICT-) systemen en voorzieningen, adequate veiligheid, betrouwbaarheid en privacybescherming biedt. Het geheel moet in onderlinge samenhang worden bezien en is ingericht en vormgegeven volgens de uitgangspunten van delegatie van regelgevende bevoegdheden. Hiermee wordt een efficiënt wettelijk kader gecreëerd dat recht doet aan het primaat van de wetgever zoals dat in het Nederlandse staatsbestel wordt gehanteerd.

Er is een verantwoord evenwicht gevonden tussen sturing op hoofdlijnen, grip op de uitwerking, flexibiliteit en rechtszekerheid. Zonder onnodig belemmerend te zijn, wordt de betrouwbaarheid en privacybescherming geboden die de regering voorstaat en die tegemoetkomt aan de wensen van uw Kamer. Dit wetsvoorstel is nodig en wenselijk om veilig inloggen mogelijk te maken, brede beschikbaarheid van inlogmiddelen te realiseren en private partijen aan strenge eisen te onderwerpen.

In het bijzonder heb ik uw Kamer toegezegd het commercieel uitnutten van gegevens door private partijen bij wet te verbieden. In deze in te dienen wetswijziging zullen tevens privacy by design en open source als hoofdelementen van de te regelen materie wettelijk worden verankerd.

Tot slot verzoek ik uw Kamer, gelet op het grote belang van voortgang, in te stemmen met het aanbieden van het voorgehangen Besluit digitale overheid, het Besluit bedrijfs- en organisatiemiddelen en het Besluit identificatiemiddelen voor natuurlijke personen voor advies aan de Afdeling advisering van de Raad van State.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops