Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2020–2021

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

O

NADER VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR BINNENLANDSE ZAKEN EN DE HOGE COLLEGES VAN STAAT/ ALGEMENE ZAKEN EN HUIS VAN DE KONING[1]

Vastgesteld 7 april 2021

1. Inleiding

De memorie van antwoord heeft de **commissie** aanleiding gegeven tot het gezamenlijk maken van enige opmerkingen en het stellen van enige vragen. Deze staan in de volgende paragraaf opgesomd, waarna de leden van enkele hier na te noemen fracties daarnaast of in aanvulling daarop nog opmerkingen en vragen aan de regering willen voorleggen. Deze zijn gerangschikt in aparte paragrafen.

De leden van de fractie van het **CDA**hebben kennisgenomen van de beantwoording door de regering. Zij hebben nog enkele nadere vragen en opmerkingen.

De leden van de fracties van **GroenLinks**, de **PvdA** en de **ChristenUnie** hebben kennisgenomen van de beantwoording door de regering en hebben gezamenlijk nog nadere opmerkingen en vragen.
De leden van de fractie van **D66** danken de regering voor de beantwoording en zijn blij met de toezegging om open source en privacy by design wettelijk te verankeren als toelatingscriteria. Zij hebben nog enkele aanvullende vragen.
De leden van de fractie van de **PVV** hebben kennisgenomen van de beantwoording door de regering. Zij hebben nog nadere opmerkingen en vragen.

[1] Samenstelling:
Kox (SP), Koffeman (PvdD), Ganzevoort (GL), De Boer (GL), Van Hattem (PVV), Pijlman (D66), Rombouts (CDA), Schalk (SGP), Koole (PvdA). Klip-Martin (VVD), Baay-Timmerman (50PLUS), Bezaan (VVD), Van der Burg (VVD), Crone (PvdA), Dessing (FVD), Dittrich (D66) *(voorzitter)*, Doornhof (CDA), Frentrop (FVD), Meijer (VVD), Nicolaï (PvdD) *(ondervoorzitter)*, Rietkerk (CDA), Rosenmöller (GL), Verkerk (CU), De Vries (Fractie-Otten), Keunen (VVD), Van der Linden (Fractie-Nanninga), Raven (OSF).

kst-34972-O
ISSN 0921 - 7371
's-Gravenhage 2021

De leden van de fractie van de **SP** bedanken de regering voor de uitgebreide beantwoording. Ze merken op dat de regering de zorgpunten van deze leden goed gehoord heeft. Ze waarderen de inzet van de regering om hieraan tegemoet te komen, maar vinden een aantal zaken nog onduidelijk. Daarom hebben zij nog een aantal vragen.

De leden van de fractie van de **ChristenUnie** hebben kennisgenomen van de beantwoording door de regering en hebben naast de gezamenlijke vragen nog enkele opmerkingen en vragen.

2. Vragen en opmerkingen van de commissie

De commissie dankt de regering voor de memorie van antwoord, de toezeggingen en de keuze om naar aanleiding van de vragen van de leden van de fracties van de Eerste Kamer tot een novelle over te gaan. Zou de regering kunnen aangeven op welke termijn zij verwacht deze novelle aan de Tweede Kamer aan te bieden? Kan zij op basis van de toezeggingen in de memorie van antwoord uiteenzetten hoe deze novelle eruit gaat zien? Gaat de regering in de opmaat naar de novelle nog een consultatieronde houden bij partijen die gespecialiseerd zijn in open source en privacy by design? De commissie vraagt ook hoe de open source en privacy by design uit de novelle zich tot de toekomstige tranches in het kader van de Wdo verhoudt?

Open source

Hoewel het beginsel open source nu in de wet zal worden opgenomen, roepen de antwoorden in de memorie van antwoord op pagina's 19 en 22 de vraag op hoe positief de regering hierover nu precies is.[2] Bovendien wordt in de memorie van antwoord over «open source» gesproken als «toelatingscriterium», «principe» of «hoofdelement», maar nooit expliciet als toelatingseis. Kan de regering bevestigen dat open source een vereiste is voor toelating? En om wat voor open source-licentie gaat het dan?

De regering schrijft op pagina 22 dat open source software die niet actief ondersteund en onderhouden wordt dan zelfs een veiligheidsrisico kan worden in plaats van een veiligheidsmaatregel. Hoe bedoelt de regering dit? Alle software die niet onderhouden wordt, vormt een risico; dat geldt niet alleen voor open source. Welke specifiek en uniek kenmerk van open source is onveiliger, zoals de regering lijkt te suggereren. Of ziet de commissie dat verkeerd? Is de regering het eens dat er een brede consensus is dat de openheid van open source software juist bijdraagt aan goede beveiliging?

In de memorie van antwoord wordt gesproken van «de beweging naar open source in te zetten» en over een «transitieproces».[3] Kan een closed source inlogmiddel wel aanvankelijk toegelaten worden, en dan pas na zeg 3 jaar open source worden, zo vraagt de commissie. Waarom wordt niet van begin af aan een heldere norm gesteld met een open source vereiste, zonder uitzonderingen en transitieproces van 3 jaar?

Kan de regering aangeven waarom zij een transitieperiode noodzakelijk acht? Hoewel de commissie allesbehalve overtuigd is van de noodzakelijkheid van een dergelijke periode, zou deze in ieder geval beperkt moeten zijn. Als open source verplicht wordt in de wet of onderliggende AMvB's is er geen noodzaak langer te wachten en er is ook geen transitieruimte nodig. De norm voor open source is helder en elke partij die

[2] Kamerstukken I, 2020/21, 34 972, L.
[3] Kamerstukken I, 2020/21, 34 972, L, p. 27 en 31.

aspiraties heeft om toegelaten te worden als privaat middel kan zijn broncode eenvoudig publiceren. De commissie ontvangt hierop graag een reactie.

Op p. 20 van de memorie van antwoord staat: «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.» Kan de regering uiteenzetten welke uitzonderingsmogelijkheden zij ziet onder welke omstandigheden voor de open source vereiste? Wie beslist er over of er al of niet sprake kan zijn van een uitzondering, op welke gronden? Gaat de regering de software die gebruikt wordt voor het inloggen met de DigiD app van de overheid, en voor het inloggen met een identiteitskaart (met behulp van de DigiD app), ook open source maken?

Decentraal en centraal

De regering zegt in de memorie van antwoord, onder andere op p. 25, dat zowel centrale als decentrale oplossingen binnen de Wet digitale overheid passen. Maar is de regering het met de commissie eens dat het risico van een hack op een centrale architectuur groot is? Kan zij daarom in de wet vastleggen dat centrale verwerking van persoonsgegevens minimaal is? Dat kan betekenen dat centraal alleen (logs)gebruiksgegevens worden, maar niet de gebruikersgegevens die gebruikt worden bij het inloggen zelf. Die gebruikersgegevens kunnen dan decentraal, op het inlogmiddel opgeslagen worden. Gaat de regering inzetten om gebruikersgegevens decentraal op te slaan en centraal alleen de logs? Is de regering het met de commissie eens dat als dit zo bij het ontwerp bij de GGD zo was geweest, een dergelijk datalek niet had kunnen voorkomen?

De regering geeft aan dat er nadelen kleven aan decentrale oplossingen. Het ontwerp van decentrale oplossingen zorgt ervoor dat een lek of hack zich beperkt tot een individu en niet de hele user-base. Binnen welk afwegings- en toetsingskader worden de voor- en nadelen tegen elkaar afgewogen van decentraal en centraal of een combinatie daarvan? En hoe verhoudt zich dit tot de toetsende en toezichthoudende rol van de overheid?

Wat betekent het privacy by design-vereiste voor logging, versleuteling tegen hacks en voor functiescheiding en pseudonimiseren van gebruiksgegevens? Gaat het om het bijhouden van welke gebruiker waar op welk moment inlogt, of moet daarbij door de aanbieder van een inlogmiddel ook geregistreerd worden welke gebruikersgegevens bij dat inloggen onthuld worden? Moeten deze loggegevens versleuteld worden, niet alleen als bescherming bij eventuele aanvallen, maar ook ter versterking van de vereiste functiescheiding? Moeten centraal opgeslagen gebruikersgegevens gepseudonimiseerd worden?

Kan de regering bevestigen dat de open source-vereiste niet alleen geldt voor het inlogmiddel, maar ook geldt voor de software die een aanbieder van zo'n inlogmiddel gebruikt voor logging en monitoring, net als voor andere centrale verwerkingen van persoonsgegevens? Kan de regering het privacy by design-vereiste concreet maken met een aantal voorbeelden van ontwerpen die niet aan privacy by design voldoen en dus tot niet-toelating leiden? In het bijzonder vraagt de commissie of een centrale architectuur met de bijbehorende privacy risico's aan privacy by design voldoet?

Buitenlandse wederzijds erkenning door eIDAS-verordening

Ingevolge de AVG is een nationaal-wettelijke grondslag nodig om mogelijk te maken dat private partijen bijvoorbeeld het burgerservicenummer kunnen verwerken. De eIDAS-verordening gaat uit 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. Kan de regering nader toelichten wat de gevolgen hiervan zijn voor de keuzen die de regering maakt inzake dit wetsvoorstel, waaronder de keuze van openstelling voor private aanbieders? Is een van de gevolgen van de eIDAS-verordening dat wanneer in een lidstaat een partij binnen of buiten de EU toelaat deze ook in Nederland is toegelaten? Klopt het dat de stelling van de regering dat Nederland inlogmiddelen van een andere lidstaat moet toelaten, alleen opgaat als Nederland zijn markt ook daadwerkelijk openstelt voor private aanbieders? En als wij in Nederland private aanbieders toelaten, wat zijn dan de gevolgen voor de kaderstellende, toetsende en toezichthoudende rol van Nederland? Overweegt de regering in de novelle om de keuze van drie jaar geleden voor toegang voor private aanbieders te heroverwegen, ook in het licht van de technologische ontwikkelingen in de laatste jaren op het gebied van systemen die veilige, open source, decentrale en privacy by design zijn?

3. Vragen en opmerkingen van de leden van de fractie van het CDA

Wetswijziging

De leden van de fractie van het CDA zijn positief dat de regering aangeeft dat open source de norm wordt, privacy by design extra zal worden benadrukt en het verhandelen van gegevens wordt verboden door een wetswijziging. Dit geldt ook voor de toevoeging dat bij het aanvragen van een erkenning duidelijk moet worden gemaakt dat het verdienmodel een directe relatie moet aantonen tussen de vergoeding en de geleverde dienst: het inlogmiddel. Deze leden vragen de regering welke aanpak en timing zij in deze voor ogen heeft: eerst de novelle laten goedkeuren door de Tweede Kamer en dan het voorliggende wetsvoorstel inclusief de novelle te behandelen, of het voorstel van de Wet digitale overheid met een toezegging inzake de genoemde wijzigingen in de Eerste Kamer te bespreken? En welke overwegingen liggen daaraan ten grondslag, juist tegen de achtergrond dat de leden van genoemde fractie de wijzigingen van essentieel belang achten.

Gegevensverwerking door private partijen

In de memorie van antwoord wordt aangegeven dat de partijen, die toegelaten zijn om een inlogmiddel te vervaardigen en aan te bieden, regelmatig zullen worden gecontroleerd. Soms wordt er ook gesproken over continue monitoring. Kan de regering aangeven of er nu sprake is van continue monitoring dan wel van regelmatige controle. Aan welke inzet wordt gedacht bij regelmatige controle? En zo ja, waarom? Ook wordt in de memorie van antwoord aangegeven dat bij misbruik besloten kan worden om de vergunning in te trekken.[4] In hoeverre is het niet meer toestaan van een inlogmiddel daadwerkelijk te realiseren? Welke effecten kan dit hebben voor de burgers en bedrijven die juist van dat inlogmiddel gebruikmaken? Wat is hiertoe de aanpak en welke afspraken worden daartoe gemaakt met de geselecteerde aanbieders?

[4] Kamerstukken I, 2020/21, 34 972, L, p. 15.

Hebben deze leden de memorie van antwoord goed begrepen dat als commerciële online-aanbieders ook van dit inlogmiddel gebruik willen maken, het verboden is om daarnaast een «eigen», meer commercieel inlogmiddel aan te bieden met aantrekkelijke voorwaarden voor de gebruikers, die hiervoor kiezen, waardoor er als het ware concurrentie tussen de inlogmiddelen ontstaat?

4. Vragen en opmerkingen van de leden van de fracties van GroenLinks, de PvdA en de CU gezamenlijk (onder aansluiting van de leden van de fractie van 50Plus)

Gegevensverwerking door private partijen

Naast de gezamenlijke commissievragen zouden de leden van de fracties van GroenLinks, de PvdA en de CU nogmaals met de regering van gedachten willen wisselen over de fundamentele keuze van de regering om private aanbieders toe te laten met toegang en beschikking over persoonsgegevens van burgers. De leden van de fractie van 50Plus sluiten zich bij deze vragen aan. Twijfelt de regering weleens aan de gemaakte keuze van drie jaar geleden om dit mogelijk te maken? «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», antwoordt de regering.[5] Kan de regering uitgebreider en puntsgewijs ingaan op de toegevoegde waarde van private aanbieders in het licht van de noodzakelijkheid, proportionaliteit en doelmatigheid? Heeft de regering overwogen om zelf een tweede systeem te (laten) ontwikkelen? Zo nee, waarom niet?

De regering geeft aan dat tijdens marktconsultaties met private partijen 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. Met welke partijen heeft de regering allemaal gesproken tijdens de marktconsultaties en wat is hiervan de invloed geweest op de inhoud van de wet?

De regering bevestigt dat de keuze voor private aanbieders betekent dat zij meer moet investeren in onderhoud en toezicht.[6] Kan de regering schetsen wat hiervoor voor nodig is van overheidswege? Hoeveel kosten deze inspanningen? De regering zegt dat de extra inspanningen gerechtvaardigd zijn omdat de private middelen zich niet alleen uitstrekken tot het overheidsdomein maar ook tot het commerciële domein. Op basis waarvan is vastgesteld dat hier behoefte aan en noodzaak voor was vanuit de burger? Is er naast marktpartijen ook voorafgaand met andere organisaties gesproken en zo ja, met wie allemaal? De regering geeft aan dat burgers juist beter worden beschermd dankzij de private aanbieders, omdat zij nu buiten het publieke domein deze sleutels kunnen gebruiken.[7] Kan de regering dit nader toelichten? Hoe beoordeelt de regering het risico voor burgers die bij één partij een inlogmiddel voor alle diensten gaan gebruiken met alle persoonsgegevens van de desbetreffende persoon? Hoe beoordeelt de regering het risico van hacks en aanvallen, ook in verhouding tot de veronderstelde winst van beschikbaarheid? Zorgen van de leden over de grootte van ons zogenoemde «aanvalsoppervlak» -dat beduidend groter wordt door het toelaten van private aanbieders- tracht de regering weg te nemen door te benadrukken dat alle

[5] Kamerstukken I, 2020/21, 34 972, L, p. 37.
[6] Kamerstukken I, 2020/21, 34 972, L, p. 37.
[7] Kamerstukken I, 2020/21, 34 972, L, p. 28.

partijen voorafgaand aan toelating worden onderworpen aan strenge controles en toezicht. Hoe zit dat met partijen die al door andere lidstaten zijn goedgekeurd?

Lagere regelgeving

De regering schrijft op pagina 2 van de memorie van antwoord dat alleen de hoofdelementen in beginsel opname in de wet behoeven. Mogen deze leden concluderen dat de regering elementen als informatieveiligheid, het beheer van de infrastructuur, de toelating en erkenning van de aanbieders, de rechten en plichten die zij hebben, het beschermen van persoonsgegevens en het doorberekenen van kosten géén hoofdelementen vindt?

De regering schrijft: «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.»[8] Tijdens de deskundigenbijeenkomst in de Eerste Kamer op 30 juni 2020 waren er ook diverse deskundigen (een meerderheid) die juist kritischer waren op deze keuzen van het kabinet. Zou de regering, net als bij de heer Van Lochem, in aansluiting op die andere deskundigen haar appreciatie willen geven van de mate van delegatie naar lagere regelgeving? En zou de regering in de memorie van antwoord van pagina 3 tot 7, waar zij op verzoek van diverse partijen per artikel aangeeft of het in de wet, per AMvB of ministeriële regeling wordt geregeld, hierbij ook de argumentatie per artikel kunnen toelichten op de elementen waar ook subdelegatie («bij of krachtens algemene maatregel van bestuur») is toegestaan? De Raad van State wees ook duidelijk op dit punt in relatie tot centrale onderdelen van de generieke digitale infrastructuur (GDI).[9] Kan de regering dit ook betrekken in haar antwoord?

Toezicht

De Autoriteit Persoonsgegevens (AP) zal toezicht houden op de uitvoering van de Wet Digitale Overheid en vormt daarmee een belangrijke pijler rondom de handhaafbaarheid. Is de regering het met deze leden eens dat dit een verzwaring zal betekenen voor werkdruk van de AP? Is zij bereid de AP financieel meer te ondersteunen? De toezichthouder Agentschap Telecom (AT) heeft aangegeven dat harmonisatie van de domeinen burgers en bedrijven vanuit oogpunt van uitvoerbaarheid en handhaafbaarheid wenselijk is. Hoewel het momenteel werkbaar wordt geacht, is het niet wenselijk, zo blijkt uit het verhaal van de toezichthouder. Kan de regering het proces van harmonisatie schetsen in tijd en inhoud?

Toekomstig beleid

De regering geeft aan dat in de toekomst (met tranches) «wordt gedacht over 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

[8] Kamerstukken I, 2020/21, 34 972, L, p. 10.
[9] Kamerstukken II, 2017/18, 34 972, nr. 4.

van het burger- en bedrijvendomein, bredere toepassing van standaarden voor digitale dienstverlening en machtigen. Over deze onderwerpen vindt de gedachtenvorming momenteel volop plaats.»[10] Betreft dit slechts voorbeelden waarover wordt nagedacht of zijn er meer onderwerpen in de gedachtenvorming? Hoe ziet deze gedachtenvorming eruit? Wie is hierbij betrokken? Deze leden zouden graag een schets krijgen van de gedachtenvorming die volop gaande is. In hoeverre houdt dit verband met de aanstaande novelle?

De regering schrijft dat België Wdo-achtige wetten kent. Deze leden vragen naar aanleiding van de antwoorden om een casusschets van de situatie in België. Waarom stelt de regering dat België dergelijke wetgeving kent? Welke overeenkomsten zijn er en welke verschillen? Zou de regering hierbij specifiek kunnen ingaan op de rol die private aanbieders spelen op de Belgische markt? Wat gaat daar goed en wat kan er beter? Is er structurele samenwerking en/of uitwisseling?

5. Vragen en opmerkingen van de leden van de D66-fractie

Gegevensverwerking door private partijen

Deze leden zijn verheugd dat wettelijk zal worden vastgelegd dat partijen gegevens niet mogen verwerken voor andere doeleinden dan vervaardiging en werking van het inlogmiddel. Er is natuurlijk, zoals de regering zelf ook aangeeft, een verschil tussen gebruikers- en gebruiksgegevens. De regering stelt in de memorie van antwoord dat «persoonsgegevens» niet commercieel uitgenut mogen worden, niet gebruikt mogen worden voor profilering en niet verhandeld mogen worden.[11] Deze leden zouden graag een bevestiging ontvangen dat deze «persoonsgegevens» zowel gebruikers- als (alle denkbare vormen van) gebruiksgegevens omvatten.

Toezicht

De leden van de D66-fractie blijven daarnaast zorgen houden over de facilitering van toezichthouders. De regering geeft aan dat alle partijen die inlogmiddelen willen aanbieden alle vereisten aantoonbaar moeten naleven. Hier wordt zowel voorafgaand aan toelating op gecontroleerd als ook gedurende hun dienstverlening. Het Agentschap Telecom (AT) en (voor aspecten aangaande de bescherming van persoonsgegevens) de Autoriteit Persoonsgegevens (AP) houden toezicht en handhaven. Deze leden zijn ervan overtuigd dat sterk toezicht essentieel is. Zij begrijpen dat de AP zelf haar prioriteiten bepaalt en dat de regering hier dus geen uitspraken over kan doen, maar als de toegekende middelen simpelweg niet toereikend zijn, zal toezicht tekortschieten. Op dit moment kan de AP al maar slechts bij een deel van alle gemelde datalekken in actie komen door een tekort aan budget[12]. In de Tweede Kamer is recentelijk een motie aangenomen over verhoging van het budget van de AP[13] waar Minister Dekker o.a. op antwoordde[14] dat het niet aan het demissionaire kabinet is om ongedekte moties uit te voeren. De leden van de D66-fractie hebben hier begrip voor, maar vragen zich sterk af of het geen recept voor ongelukken is om deze wet aan te nemen zonder dat de facilitering van de

---

[10] Kamerstukken I, 2020/21, 34 972, L, p. 13.
[11] Kamerstukken I, 2020/21, 34 972, L, o.a. p. 11.
[12] Zie bijvoorbeeld Trouw (1 maart 2021): *Datadiefstal is explosief gegroeid. Het gevaar? «Mensen kunnen al hun spaargeld kwijtraken»* https://www.trouw.nl/binnenland/datadiefstal-is-explosief-gegroeid-het-gevaar-mensen-kunnen-al-hun-spaargeld-kwijtraken~b1e95096/.
[13] Motie van het lid Hijink c.s. over verhoging van het budget van de Autoriteit Persoonsgegevens, Kamerstukken II, 2020/21, 27 529 nr. 240.
[14] Kamerstukken II, 2020/21, 25 268/32 761, nr. 197.

toezichthouders gewaarborgd is – sterker nog, terwijl we weten dat de facilitering van de AP op dit moment niet afdoende is.

Closed source

De leden van de D66-fractie vinden het goed dat aan open source zal worden getoetst bij het behandelen van een toelatingsaanvraag, omdat open source het uitgangspunt zou moeten zijn. Volgens de memorie van antwoord is het echter denkbaar dat closed source software ook aan de orde zal komen, vanwege de mogelijke veiligheidsargumenten die de regering aanhaalt in haar beantwoording. De regering stelt dat er in zo'n geval «nadrukkelijk door anderen dan de leverancier zelf» zal moeten worden vastgesteld dat de closed software werkt zoals beschreven en veilig is. Deze leden vragen zich af wie deze «anderen» zullen zijn. Zal dit ook worden getoetst door het Agentschap Telecom?

6. Vragen en opmerkingen van de leden van de PVV-fractie

Open source – closed source

De regering geeft in de memorie van antwoord enerzijds aan in te willen zetten op open source, maar geeft tegelijkertijd aan op pagina 19: «De eigenschap open source als zodanig biedt niet de garantie voor transparantie en veiligheid» en op pagina 22: «Open source software die niet actief ondersteund en onderhouden wordt kan dan zelfs een veiligheidsrisico worden in plaats van een veiligheidsmaatregel.» Kan de regering verduidelijken welke concrete eisen gesteld zullen worden aan open source en welke vormen van open source licenties er toegestaan zullen worden en/of op basis van welke criteria open source licenties beoordeeld zullen worden voor toelating?

Kan de regering aangeven welke criteria gehanteerd zullen worden ten aanzien van het actief ondersteunen en onderhouden van open source software?

Verder geeft de regering aan de beweging naar open source in te zetten in een transitieproces; kan de regering verduidelijken welke stappen in deze «beweging naar open source» concreet gezet zullen gaan worden, op basis van welke criteria en indicatoren en wat de termijn van dit transitieproces wordt?
Daarnaast geeft de regering aan in voorkomende gevallen voor closed source te kiezen, omdat veiligheid met open source niet gegarandeerd kan worden. Kan de regering concreet aangeven op basis van welke criteria deze gevallen bepaald zullen worden en bij wie deze bevoegdheid komt te liggen? Kan de regering tevens aangeven in hoeverre in dergelijke gevallen alsnog tot open source oplossingen kan worden overgegaan indien de veiligheid wel gewaarborgd kan worden en of hier (periodiek) op getoetst zal worden?

Veiligheid, privacy by design

Kan de regering aangeven op welke wijze risico's op (grootschalige) hacks ondervangen zullen worden als gekozen wordt voor centrale oplossingen? Kan de regering tevens nader ingaan wat de ervaringen hiermee zijn bij bestaande systemen, zoals de elektronische patiëntengegevens?
Zo concludeert een rapport van de Autoriteit Persoonsgegevens (AP) over toegang tot digitale persoonsgegevens in het HagaZiekenhuis: «De AP constateert dat het HagaZiekenhuis onvoldoende passende maatregelen heeft getroffen ten aanzien van de beveiligingsaspecten «authenticatie» en «controle van de logging». Het HagaZiekenhuis handelt hierdoor in

strijd met artikel 32, eerste lid, aanhef, van de AVG.»[15] Kan de regering concreet aangeven hoe de beveiligingsaspecten authenticatie en controle van logging binnen de kaders van dit wetsvoorstel worden geregeld? Kan de regering meer specifiek aangeven welke privacy by design-middelen zij wil verplichten en of het hierbij gaat om het loggen van middelen waarbij gebruikers inloggen, of loggen zij ook de specifieke persoonsgegevens waarmee wordt ingelogd?

Voorts heeft SIDN aangegeven dat onduidelijk is wat de technische veiligheidsrichtlijnen in dit kader zijn. Kan de regering aangeven of deze gegevens versleuteld zijn en apart opgeslagen ten behoeve van functiescheiding? Gaat het om het bijhouden van welke gebruiker waar op welk moment inlogt, of moet door de aanbieder van een inlogmiddel ook geregistreerd worden welke persoonsgegevens bij dat inloggen onthuld worden? Moeten deze loggegevens versleuteld worden, niet alleen als bescherming bij eventuele aanvallen, maar ook ter bekrachtiging van de vereiste functiescheiding (persoonsgegevens/gebruikersgedrag)?

eID op Europees niveau en in andere landen

De EU werkt momenteel aan de introductie van een eID op Europees niveau. Kan de regering aangeven hoe dit wetsvoorstel zich verhoudt tot de introductie van de eID en in hoeverre er al rekening wordt gehouden met interoperabiliteit? Acht de regering een dergelijke eID wenselijk? Kan de regering bovendien aangeven wat de introductie van een eID betekent voor de persoonsgegevens van Nederlandse burgers en in hoeverre de EU hier over zou kunnen beschikken?

De Noordse en Baltische staten hebben in het kader van het NOBID-project een Nordic-Baltic eID ontwikkeld. Kan de regering aangeven in hoeverre de plannen voor de Wdo vergelijkbaar zijn met dit project?

7. Vragen en opmerkingen van de leden van de SP-fractie

Open source

Als eerste willen de leden van de SP-fractie opmerken dat de beantwoording in de memorie van antwoord niet altijd even consistent is. En al zijn deze leden blij dat de regering nu ook open source omarmt, conform het kabinetsbeleid, het is natuurlijk niet zo dat open source minder veilig is. Integendeel. Zeker is het zo dat open source onderhouden dient te worden, evenals alle andere software, en dat daar aandacht voor dient te zijn. Deze leden nemen aan dat dit meegenomen wordt in de verdere uitrol van de Wdo.

Verheugd zijn de leden van de SP-fractie over de toezegging dat er een wetswijzing nodig is om open source, evenals privacy by design en een wettelijk verbod op verhandelen van gegevens te verankeren in de Wdo. Uit de memorie van antwoord was het deze leden niet duidelijk welke route bewandeld zou worden, inmiddels begrijpen zij dat hiertoe een novelle zal worden ingediend. Hoe de open source zal worden ingezet is nog vaag. Kan de regering ingaan op wat voor soort open source-licentie opgenomen gaat worden in de wetswijziging? En is de open source dan ook echt een vereiste voor toelating? Deze leden willen benadrukken dat dit laatste voor hen een belangrijk punt is.

---

[15] Autoriteit Persoonsgegevens, Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis, Onderzoeksrapport maart 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/haga_rapport_def.pdf.

De leden van de SP-fractie begrijpen uit de beantwoording dat de regering streeft naar open source voor de aanbieders, maar onduidelijk is hoe het streven zijn beslag zal krijgen. Zij begrijpen dat de druk groot is van gevestigde bedrijven die van nature misschien niet allemaal gewend zijn om dit traject van open source in te gaan. Toch willen deze leden ervoor waken dat deze bedrijven een voorlopige toetreding krijgen, waarin ze met closed source kunnen beginnen. Een dergelijk stap zal er voor zorgen dat deze bedrijven ook de omschakeling in een latere fase zullen vertragen. Bovendien, wanneer deze bedrijven niets te verbergen hebben, dan hoeft men toch niet met closed software te beginnen? Deze leden vragen om een helder standpunt van de regering in dezen.

Decentraal en centraal

De regering geeft in de beantwoording aan niet te willen afdwingen dat de gegevens decentraal worden opgeslagen. De argumenten die zij hiervoor aandraagt, liggen met name in de uitvoering: problemen oplossen met gebruikers is lastiger als alles decentraal is opgeslagen. Tegelijkertijd is decentraal wel de trend, zo constateren de leden van de fractie van de SP. Deze leden begrijpen echter de denkrichting van de regering, maar zouden ervoor willen pleiten om wettelijk af te dwingen dat de gebruikersgegevens wel decentraal moeten worden opgeslagen. Daarmee wordt de kans op het stelen van gevoelige gegevens aanmerkelijk verkleind.

Privacy by design

Dan de toezegging om de principes van privacy by design in de wet op te nemen. Ook hierover zijn deze leden verheugd. Wel vragen zij zich af wat er precies opgenomen gaat worden. Kan de regering nader omschrijven welke elementen van privacy by design in de wet meegenomen gaan worden?

Kenbaar maken van voornemens

De leden van de SP-fractie willen de regering vragen om over haar voornemens naar buiten toe helder te communiceren. Nog weinigen zijn op de hoogte van het voornemen om de wet op deze punten aan te scherpen, terwijl wel al een fors aantal partijen voorsorteren op de Wdo. Zo worden systemen van de apotheker aangesloten op een koppelvlak om aan de eisen van inloggen te voldoen. Ook zij moeten op de hoogte zijn van de nieuwe vereisten die in de wet gaan komen. Op welke wijze wil de regering dit kenbaar maken aan de betrokken partijen, zo vragen deze leden. Bovendien wordt door de vertraging ook de verplichting van HTTPS op overheidswebsites uitgesteld, evenals de toegankelijkheidseisen. Dit zou echter overheden er niet van moeten weerhouden hun websites veilig en toegankelijk te houden. Is de regering bereid om de overheden hier nogmaals op te wijzen?

8. Vragen en opmerkingen van de leden van de ChristenUniefractie (onder aansluiting van de leden van de fractie van 50Plus)

Toegankelijkheid burgers

Een mogelijk gevaar van het gebruik van veilige middelen om elektronisch met de overheid en publieke diensten te communiceren is dat deze middelen niet toegankelijk zijn voor sommige burgers vanwege de kosten of vanwege het vereiste kennisniveau. Is de regering het eens met de leden van de fractie van de ChristenUnie, met aansluiting van de leden van de fractie van 50Plus, dat in principe elke burger toegang moet

hebben tot de genoemde veilige middelen? Welke maatregelen neemt de regering om dit te realiseren?

De vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning ziet met belangstelling uit naar de nadere memorie van antwoord en ontvangt deze graag binnen vier weken na vaststelling van dit nader voorlopig verslag.

De voorzitter van de commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning,
Dittrich

De griffier van de commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning,
Bergman