35 868 Wijziging van het voorstel van wet houdende algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 3 Memorie van Toelichting

Deze wijziging behelst, naast herstel van redactionele omissies (onderdeel D), enkele aanpassingen van beleidsinhoudelijke aard (onderdelen A, B en C).

Aanleiding voor de aanpassingen zijn de door de Eerste Kamer bij haar behandeling van het wetsvoorstel geuite vragen en zorgen inzake privacybescherming. In het bijzonder is door de fracties, bij gelegenheid van prealabele vragen (dd 10 juli 2020) en in het voorlopig verslag (dd 29 september 2020) aandacht gevraagd voor het grote belang van bescherming van persoonsgegevens in relatie tot de positie van (grote) private technologie ondernemingen.

Om gestand te doen aan de geuite vragen en zorgen worden met het onderhavige wijzigingsvoorstel privacy by design, verhandelverbod inzake gegevens en open source als hoofdelementen van de te regelen materie wettelijk verankerd.

Privacy by design

In de eerste plaats wordt voorgesteld in artikel 9, zesde lid, te specificeren dat een erkenning (toelating) van een privaat inlogmiddel wordt geweigerd indien het ontwerp van het identificatiemiddel of de ontsluitende (= routerings)dienst onvoldoende voorziet in de bescherming van gegevens. Het principe dat bij het ontwerpen (*design*) van een informatiesysteem of nieuw product rekening moet worden gehouden met privacy, waarbij zo min mogelijk persoonsgegevens worden verwerkt en sprake is van doelbinding, vindt zijn basis in de privacywetgeving, met name de Algemene verordening gegevensbescherming (AVG). Ingevolge artikel 25 AVG moeten er door het hele proces van het verwerken van persoonsgegevens technische en organisatorische maatregelen genomen worden om aan de privacybeginselen te voldoen. De AVG is als Europese verordening rechtstreeks toepasselijk in de lidstaten; omzetting middels nationaal-wettelijke bepalingen is in beginsel niet toegestaan. 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; het is een ontwerpprincipe dat bij de inrichting van de techniek, processen en organisatie leidend is.

Partijen die gegevens verwerken zijn dus rechtstreeks op grond van de AVG gehouden om privacy by design toe te passen en de Autoriteit Persoonsgegevens houdt toezicht op de naleving daarvan. Het hanteren van dit principe als afwijzingsgrond voor een erkenningsaanvraag moet dan nog expliciet worden geregeld. Dat was eerder voorzien door nadere regels gebaseerd op artikel 9. De door leden van de Eerste Kamer geuite zorg is aanleiding om deze afwijzingsgrond op het niveau van de wet te verankeren.

Bij de beoordeling van de aanvraag om erkenning is de actuele stand van processen en technieken leidend: bezien wordt of het ontwerp naar de stand der techniek en andere redelijkerwijs beschikbare mogelijkheden op het moment van aanvraag voldoende voorziet in de bescherming van gegevens. Deze formulering brengt tot uitdrukking dat privacyvriendelijkheid niet enkel afhankelijk is van techniek, maar ook van (andere)

ontwerpkeuzes. “redelijkerwijs” geeft uitdrukking aan de hiermee gepaard gaande afweging van belangen, waaronder de kosten.

Voorts wordt geborgd dat ook na verlening van een erkenning nieuwe technieken en processen door erkenninghouders worden geïmplementeerd. De voorgestelde wijziging van het zevende lid van artikel 9 regelt namelijk dat een erkenning kan worden gewijzigd, geschorst of ingetrokken indien het ontwerp van het identificatiemiddel of de ontsluitende dienst niet (langer) voldoet aan de stand der techniek en andere redelijkerwijs beschikbare mogelijkheden voor de bescherming van gegevens. Een houder van een erkenning wordt geacht over te gaan tot het implementeren van eventuele nieuwe technieken en processen en daarvoor een wijziging van de erkenning aan te vragen. Gebeurt dat niet, dan kan de erkenning worden ingetrokken. Op grond van het negende lid van artikel 9 zal bij algemene maatregel van bestuur worden geregeld dat intrekking slechts plaatsvindt nadat de houder van een erkenning in de gelegenheid is gesteld alsnog de benodigde aanpassingen door te voeren en daarvoor eventueel een wijziging van de erkenning aan te vragen. De houder van de erkenning krijgt dus eerst een termijn om met een voorstel te komen waarmee nieuwe ontwikkelingen kunnen worden geïmplementeerd.

Deze wijzigingen van artikel 9 zorgen ervoor dat partijen nieuwe methoden en technieken toepassen zonder dat de rechtszekerheid in het geding komt. De eerder verleende erkenning is immers verleend voor de processen en technieken die in de aanvraag zijn vermeld. In beginsel mogen houders van een erkenning de in de aanvraag vermeldde technieken en processen niet aanpassen, tenzij daarvoor een wijziging van de erkenning wordt aangevraagd of wanneer het een beperkte wijziging betreft. Met het voorgestelde wordt gewaarborgd dat kenbaar is welke (grote) wijzigingen er door partijen worden toegepast en dat de minister van BZK hierover besluit.

Verhandelverbod
Het wetsvoorstel stelt regels aan private partijen die inlogmiddelen voor de toegang tot overheidsdienstverlening op de markt willen brengen en gaat daarbij uit van strikte doelbinding: persoonsgegevens mogen door private partijen alleen worden verwerkt voor zover dit noodzakelijk is voor de werking van het erkende identificatiemiddel en goede en veilige toegang met dat middel tot overheidsdiensten (artikel 16). Hieruit volgt dat met de verkregen gegevens niet mag worden geprofileerd (gekoppeld aan eigen gegevens om het klantprofiel te versterken) en dat de gegevens niet mogen worden verkocht of anderszins (bijvoorbeeld gratis) verstrekt voor commerciële doeleinden.

De gegevens die een middelenleverancier verkrijgt, zowel bij de aanvraag van het middel als bij het gebruik ervan door de klant, mogen uitsluitend worden ingezet voor het verlenen van authenticatiediensten aan de gebruiker. Bij amvb is dit uitgewerkt; het Besluit digitale overheid, het Besluit identificatiemiddelen voor burgers en het Besluit identificatiemiddelen voor bedrijven bevatten nadere regels om commerciële uitnutting te voorkomen, zoals een gespecificeerd verhandelverbod en de plicht tot gescheiden opslag van gegevens. Met het onderhavige voorstel wordt het verhandelverbod formeel-wettelijk geëxpliciteerd door als extra weigeringsgrond in de artikelen 9 en 11 de kans op overtreding van het verhandelverbod op te nemen; de aanvrager mag geen inkomsten verkrijgen uit het verhandelen of verstrekken van gegevens over gebruikers of authenticatie van gebruikers. Er moet dus een directie relatie bestaan tussen de gevraagde vergoeding voor het middel en de aan de burger of het bedrijf geleverde inlogdienst; de *businesscase* van de private partij mag alleen gebaseerd zijn op de productie en levering van de noodzakelijke functionaliteiten. De doelstelling daarvan is te

voorkomen dat de ‘burger het product wordt’, doordat zijn gegevens worden commercieel worden uitgenut. In het erkenningsproces zal hiertoe door de aanvrager moeten worden aangetoond dat zijn kosten worden gedekt met andere inkomsten dan met de verkoop van data. Ook gedurende de looptijd van de erkenning zal regulier worden getoetst of er door de erkenninghouder of diens rechtsopvolger geen gegevens worden verkocht of verstrekt voor commerciële doeleinden. Het verbod om persoonsgegevens verder te verwerken voor commerciële doeleinden geldt ook voor andere gegevens die ontstaan bij gebruik van het middel, gecombineerd met andere bij de houder van de erkenning bekende gegevens. Dit sluit aan bij doel en werkingssfeer van het wetsvoorstel: goede en veilige toegang tot elektronische overheidsdiensten door het gebruik van veilige, betrouwbare en goed werkende identificatiemiddelen.

Met het voorgaande wordt een barrière opgeworpen voor partijen die (indirect) verdienen aan gegevens van mensen en wordt tegelijkertijd ruimte gecreëerd voor partijen die dat juist niet doen. Dit zijn bedrijven die voor hun bestaansrecht afhankelijk zijn van het vertrouwen dat burgers en bedrijven in hun inlogmiddelen hebben. Het leveren van veilige inlogmiddelen, waartoe dit wetsvoorstel dient, vormt voor deze bedrijven een existentiële prikkel en daardoor een grote waarborg. Benadrukt zij dat het in algemene zin reguleren van alle vormen van commerciële uitnutting van persoonsgegevens niet het onderwerp van dit wetsvoorstel vormt; gereguleerd worden private partijen die inlogmiddelen voor de toegang tot overheidsdienstverlening op de markt willen brengen.

Open source
Voorgesteld wordt om in artikel 9, zesde lid, op te nemen dat een erkenning wordt geweigerd indien bij de voor de werking van het identificatiemiddel of de ontsluitende dienst noodzakelijke processen naar het oordeel van Onze Minister oordeel onvoldoende gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd. Dit betekent dat bij de aanvraag om erkenning zal worden bezien of open source redelijkerwijs mogelijk is, waarbij het geheel van door de aanvrager te nemen maatregelen wordt beoordeeld op veiligheid en proportionaliteit.

- Context

Bij open source is idealiter sprake van transparante en controleerbare verwerking van persoonsgegevens en openbaarmaking van de broncode. Dit kan, als gevolg van het ‘meer-ogen-principe’, bijdragen aan veiligheid en betrouwbaarheid; meer mensen (een zgh ‘*open source community’*) kijken of de software werkt zoals bedoeld en of deze veilig is. Open source software is door iedereen gratis te gebruiken, te kopiëren en te wijzigen, ook worden ontwikkelaars aangemoedigd om de software te verbeteren. Het is staand kabinetsbeleid dat de overheid haar eigen broncodes vrijgeeft, tenzij er gegronde redenen zijn om dat niet te doen, bijvoorbeeld omdat het strijdig is met de belangen van nationale of openbare veiligheid of indien de benodigde vertrouwelijke werkwijze van de overheid, zoals bij opsporing en toezicht, wordt geschaad. Het jegens private partijen, die inlogmiddelen willen aanbieden, hanteren van open source sluit aan bij dit kabinetsbeleid.

Open source als zodanig biedt geen garantie voor transparantie, veiligheid en privacybescherming. De wijze waarop de broncode wordt onderhouden en waarborgen rond beveiliging en continuïteit kunnen worden geboden, kan sterk verschillen per open source software(pakket). De kracht en meerwaarde van open source is dus vooral afhankelijk van de sterkte, activiteit en omvang van de gemeenschap en ontwikkelaars die dit ‘dragen’. Open

source software die niet actief ondersteund en onderhouden wordt kan dan een veiligheidsrisico worden in plaats van een veiligheidsmaatregel. Als een goede community ontbreekt kan dit leiden tot veiligheidslekken, doordat kwaadwillenden deze kunnen opmerken en benutten, in plaats van dichten. Zo lang andere ontwikkelaars het lek niet ontdekken, heeft een kwaadwillende vrij spel.

Voorts mag het gebruik van open source niet leiden tot ongewenste consequenties, zoals het niet of vertraagd beschikbaar komen van veilige inlogmiddelen voor burgers en bedrijven. Het is daarom essentieel dat de wijze waarop open source wettelijk wordt verankerd uitvoerbaar is. In dit verband moet worden onderkend dat het huidige landschap van – publieke en private – aanbieders van middelen in enige mate closed source software inzet, bijvoorbeeld voor het herkennen van misbruik en fraude. Dit geldt eveneens voor veel aspirant aanbieders. Dat de gehanteerde broncode niet openbaar beschikbaar is, is bij die middelen veelal een onderdeel van de veiligheid en zit bijvoorbeeld in het feit, dat de software zwakke of fraude gevoelige plekken in de hele werkwijze van inloggen adresseert. Op het moment dat per direct de broncode beschikbaar gesteld zou moeten worden, zou de veiligheid van deze middelen niet gewaarborgd kunnen worden en zou om die reden toelating (erkenning) niet aan de orde zijn. Een ‘harde’ verplichting voor die aanbieders om onverwijld over te gaan op open source bergt daarmee het reële risico in zich, dat de continuïteit van inloggen in gevaar komt omdat burgers dan geen veilige en betrouwbare middelen kunnen aanschaffen. Dat moet worden voorkomen.

Om open source veilig te kunnen inzetten is daarom meer nodig dan openbaarmaking van de broncode; het vergt ook dat de organisatie en het gehanteerde veiligheidsmodel meegroeien. Dat kost tijd en geld.

- Wegingsfactoren bij toetsing

Uitgangspunt is ‘open source, tenzij’. Dit betekent dat het concrete geval wordt bezien waar redelijkerwijs gebruik kan en moet worden gemaakt van open source software. In de eerste plaats wordt daarbij beoordeeld of de sterkte van de achterliggende open source gemeenschap voldoende is om ook op termijn veilige en betrouwbare inlog te kunnen garanderen. In de tweede plaats speelt mee of voor een bepaalde functionaliteit een open source software oplossing reeds voorhanden is en breed wordt ingezet, of dat de aanbieder van een inlogmiddel de functionaliteit zelf heeft moeten ontwikkelen omdat die er nog niet (open source beschikbaar) is. In dat geval zal – gelet op het feit dat het bij private aanbieders om oplossingen gaat die breder worden ingezet dan voor toegang tot de overheid – worden gewogen of het redelijk is de broncode van de ontwikkelde oplossing openbaar te maken. Dit hangt samen met de in het wetsvoorstel verankerde systematiek om bestaande marktproducten toe te laten, en niet alleen software die in opdracht of enkel en alleen ten behoeve van de overheid wordt ingezet.

Op het moment dat functionaliteiten meer gemeengoed worden, komen daar ook meer open source mogelijkheden voor beschikbaar. Daardoor zal het oordeel dat een functionaliteit op dit moment als closed source wordt geaccepteerd, over enige tijd niet meer voor de hand liggen omdat een adequaat open source alternatief voorhanden is. Een aspirant aanbieder die op een later moment een aanvraag doet, zal een onderdeel van de software dat eerder nog closed mocht worden aangeboden, dan open source moeten aanbieden. Doet hij dat niet, dan zal de erkenning (moeten) worden geweigerd. Ook erkende aanbieders moeten de beweging naar open source maken wanneer dit redelijkerwijs beschikbaar is en met inachtneming van

redelijke termijnen om aanpassingen door te voeren (artikel 9, leden 7 en 9 van het wetsvoorstel).

- Conclusie: een groeimodel

De wijze waarop open source in het wetsvoorstel wordt verankerd, brengt tot uitdrukking dat open source het uitgangspunt is, zonder dat in de praktijk veiligheids- en continuïteitsproblemen optreden. Dit leidt ertoe, dat enerzijds geen excessieve maatregelen worden geëist met disproportionele kosten of disproportionele aanpassingen in het productieproces. Anderzijds wordt van een aanvragende partij verwacht dat deze alle redelijke maatregelen treft teneinde open source zoveel mogelijk te hanteren, gelet op wat in de tijd open source beschikbaar is. Het enkele feit, dat het gebruik van open source meerkosten voor de aanbieder met zich brengt, is daarbij niet doorslaggevend. Ook de enkele omstandigheid dat in een concreet geval closed source veiliger is dan closed source, bijvoorbeeld wanneer closed source veiliger is dan op grond van de vereisten voor erkenning nodig is, zal bij het beoordelen van een aanvraag niet leiden tot het toestaan van closed source en kan leiden tot weigering van de erkenning.

Bedrijfs- en organisatiemiddel en publiek middel

Wettelijke verankering van privacy by design, verhandelverbod en open source heeft niet enkel gevolgen voor de toelating van identificatiemiddelen voor natuurlijke personen. Door deze principes wettelijk te verankeren met betrekking tot private inlogmiddelen voor natuurlijke personen (artikel 9, zesde lid, onder b, c en d), ligt het in de rede dit eveneens te doen ten aanzien van private bedrijfs- en organisatiemiddelen (artikel 11, vijfde lid en achtste lid, onder b, c en d en artikel 14, derde lid) en publieke middelen (art. 9, eerste lid). Er moet immers voor alle - private en publieke - identificatiemiddelen waarmee kan worden ingelogd in het publieke domein aan dezelfde toelatingseisen worden voldaan, teneinde tegemoet te komen aan overwegingen van veiligheid en betrouwbaarheid en daarmee gelijke waarborgen te bewerkstelligen.

Tot slot wordt een technische wijziging aangebracht in de eerste volzin van artikel 11, vijfde lid. Voor bedrijfs- en organisatiemiddelen moet bij een erkenningsaanvraag een verklaring van een aangewezen instantie worden aangeleverd, terwijl voor middelen voor natuurlijke personen niet geldt dat de instantie moet zijn aangewezen. Met deze wijziging wordt dit verschil weggenomen en wordt de erkenningsprocedure geüniformeerd en vereenvoudigd.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops