Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

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. 17 **BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 10 oktober 2022

In het plenaire debat over de novelle bij het wetsvoorstel digitale overheid (hierna: de Wdo) d.d. 1 juni jl. heb ik u toegezegd om uw Kamer het concept toe te zenden van de ministeriële regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo (hierna: de MR) (Handelingen II 2021/22, nr. 86, item 8). Met deze brief bied ik u de MR aan. Gelijktijdig met de toezending zal ik de internetconsultatie starten, waardoor ook belanghebbenden hun reactie op de regeling kunnen geven.

De MR bevat, in combinatie met twee algemene maatregelen van bestuur die in het kader van de voorhang aan Uw Kamer zijn voorgelegd, de eisen waaraan publieke en private inlogmiddelen moeten voldoen voordat zij worden toegelaten onder de Wdo. Die eisen borgen dat burgers en bedrijven deze inlogmiddelen kunnen gebruiken om veilig en betrouwbaar in te loggen bij de (semi-)overheid. Na toelating dienen de eisen als basis voor het doorlopend toezicht dat is ingeregeld, om te zorgen dat de inlogmiddelen veilig en betrouwbaar blijven. Het Agentschap Telecom zal de toelating en het toezicht gaan verzorgen.

Omdat de MR primair een juridisch document is – en ook moet zijn – hecht ik eraan in deze brief vanuit de politieke context de achtergrond van deze regeling uiteen te zetten. Daarbij stip ik de achtergrond van de regeling aan en leg ik uit wat er geregeld wordt.

Daarnaast bied ik u, om het totaal aan regelingen onder de wet digitale overheid inzichtelijk te maken, bij deze brief een overzichtsplaat aan van de uitvoeringsregelgeving die onder de Wdo tot stand wordt gebracht. Daarbij geef ik aan welke onderwerpen worden geregeld, waar die onderwerpen worden geregeld (wet, algemene maatregel van bestuur of minsteriele regeling) en schets ik de (onderlinge) context.

kst-35868-17
ISSN 0921 - 7371
's-Gravenhage 2022

Uitgangspunt: Europese eIDAS-verordening en de Algemene Verordening gegevensbescherming (AVG)

Het uitgangspunt voor de betrouwbaarheidseisen in de MR vormen de Europese eIDAS-verordening, en de bijbehorende uitvoeringsverordening 1502, die minimale eisen stelt aan de betrouwbaarheid van inlogmiddelen die Europees worden genotificeerd. Daarbij gaat het om verplichte controles die moeten worden uitgevoerd om te zorgen dat inlogmiddelen met zekerheid aan de juiste (rechts)persoon worden uitgegeven en dat veilig kan worden ingelogd. Daarnaast vormt de Algemene verordening gegevensbescherming (AVG) een belangrijk uitgangspunt voor de bescherming van persoonsgegevens.

De MR, als uitwerking van de Wdo (waarvan de novelle deel gaat uitmaken), vertaalt waar nodig deze eisen naar de Nederlandse context en stelt eisen die ik in deze context beleidsmatig en politiek belangrijk vindt om burgers te beschermen. Een voorbeeld daarvan zijn de eisen die zijn opgenomen in de novelle bij het wetsvoorstel digitale overheid.

Voor de volledigheid schets ik kort de gelaagdheid van de regelgeving aan de hand van voorbeelden. Zo worden op het niveau van de wet de waarborgen geregeld, zoals privacybescherming, die in de AMvB nader worden uitgewerkt. Voorbeelden daarvan zijn de verplichting om gegevens van burgers gescheiden op te slaan en digitale inzagerechten voor burgers. In de onderliggende ministeriële regeling worden meer praktisch/technische zaken geregeld die snel (moeten) kunnen wijzigen, of concrete detailvoorwaarden zoals openingstijden van de helpdesk, onderhoudstijden (wanneer en hoe laat updates uitgevoerd mogen worden), de vormvereisten voor een aanvraag (d.w.z. wat een bedrijf allemaal aan informatie/stukken moet indienen om het middel te laten erkennen) en aanwijzen van componenten waarvoor open source software moet worden ingezet. De zaken die in de ministeriële regeling worden geregeld lenen zich vanwege hun praktische en vaak gedetailleerde aard minder goed voor regeling op het niveau van algemene maatregel van bestuur.

Hieronder licht ik de meest relevante eisen in de minsteriele regeling nader toe.

Privacybescherming en transparantie voor burgers

Beperking verwerking burgerservicenummer

In Nederland werkt de overheid in haar contact met burgers op basis van het burgerservicenummer. Aan de verwerking daarvan worden specifieke regels gesteld. Om in te loggen bij de overheid is het noodzakelijk dat overheden waar een burger inlogt, het burgerservicenummer van de desbetreffende burger kunnen ontvangen. De MR bevat voorschriften die ervoor zorgen dat het burgerservicenummer door aanbieders van inlogmiddelen te allen tijde versleuteld wordt verwerkt, en dat gewerkt wordt op basis van pseudoniemen. Overheidsorganisaties kunnen met een eigen sleutel uit het pseudoniem het burgerservicenummer herleiden. Hierdoor wordt de verwerking van het BSN bij het inloggen beperkt tot slechts de overheidsorganisaties die dit nummer daadwerkelijk nodig hebben. Dit heeft een belangrijke privacybeschermende werking.

Transparantie: verplicht digitale inzage en correctie bij aanbieders van inlogmiddelen

Daarnaast verplicht de MR dat aanbieders van inlogmiddelen burgers en bedrijven digitaal inzage moeten bieden in de (persoons)gegevens die worden verwerkt. Daarbij gaat het zowel om gegevens die worden verwerkt om het inlogmiddel te kunnen aanbieden als om gegevens over het gebruik van het middel. Ook wordt geregeld dat de burger een overzicht wordt geboden van de inlogmiddelen waarover hij beschikt. De burger heeft hierdoor een laagdrempelige toegang tot zijn gegevens. Dit past in de bredere ontwikkeling om de burger meer regie te bieden op zijn gegevens. Bovendien stelt de laagdrempelige beschikbaarheid van deze gegevens de burger in staat om aan te bel te trekken op het moment dat er onverhoopt iets niet klopt en dat te laten corrigeren.

Bescherming bij inloggen

Ook regelt de MR dat burgers op het moment dat zij willen inloggen, voordat zij inloggen te zien krijgen bij welke publieke dienstverlener zij inloggen, de specifieke dienst waarvoor de authenticatie plaatsvindt en de gegevens die bij het inloggen worden verstrekt. Aanbieders van inlogmiddelen moeten borgen dat de wijze waarop de informatie aan de burger wordt getoond niet door een derde partij kan worden gemanipuleerd, zodat de burger op de informatie kan vertrouwen. De burger kan zo goed geïnformeerd en bewust de keus maken om in te loggen. Tijdens het authenticatieproces wordt een gebruiker ten slotte in de gelegenheid gesteld het authenticatieproces af te breken tot het moment waarop dit is voltooid.

Hulp aan burgers die in de knel komen: herstelvermogen

De eisen die in de MR worden gesteld beogen de kans op misbruik van inlogmiddelen tot een minimum te beperken. Echter, het is nooit geheel uit te sluiten dat burgers het slachtoffer worden van misbruik doordat anderen hun middel buiten hun medeweten gebruiken of door onjuiste werking van processen. Daarom wordt in de MR aan aanbieders van inlogmiddelen de verplichting opgelegd om mogelijk misbruik te kunnen herkennen en te herstellen. Herstellen wil in dit kader zeggen dat ervoor dient te worden gezorgd dat een middel wordt ingetrokken of wordt teruggebracht onder de controle van de gebruiker.

Voor de volledigheid merk ik op de MR niet gaat over de gegevens die voor de genoemde specifieke dienst mogen worden gebruikt. Dat is gedetailleerd en per doel vastgelegd in het Besluit digitale overheid, zoals dat aan de beide Kamers in het kader van de voorhangprocedure is voorgelegd.

Beschikbaarheidseisen aan ondersteuning en bereikbaarheid: menselijk contact

Een burger of bedrijf moet voor vragen, instructies of meldingen over zijn inlogmiddel terecht kunnen bij een helpdesk van de aanbieder waar goede en tijdige informatie wordt verstrekt. Niettemin moet worden voorkomen dat de serviceverlening op enig moment zodanig beperkt is dat de toegang tot publieke dienstverlening daardoor in gevaar komt. Daarom bevat deze regeling minimumregels over de bereikbaarheid van zo'n helpdesk.
De regeling schrijft bijvoorbeeld voor dat een helpdesk ten minste 60 uur per week telefonisch bereikbaar moet zijn voor burgers. Daarmee wordt geborgd dat burgers voldoende mogelijkheden hebben om direct in

contact te treden met de partij waarvan zij het identificatiemiddel afnemen.

Privacy by design (novelle)

Het principe van privacy by design is primair verankerd in artikel105396625 AVG. Dat is het reguliere kader voor toepassing van het privacy by design-principe. De AVG kan echter niet dienen als afwijzingsgrond voor een erkenningsaanvraag of als grond voor de intrekking van een verleende erkenning. Hiervoor is een nadere wettelijke basis nodig. Daarom is met de novelle voorzien in een specifieke afwijzingsgrond voor aanvragen die niet voorzien in «privacy by design». Ook wordt geregeld dat een reeds verleende erkenning kan worden ingetrokken wanneer niet langer is voldaan aan het principe van privacy by design. Bepalend is dat er een afweging wordt gemaakt tussen de verschillende AVG-beginselen (doelbinding, transparantie, bewaartermijnen, dataminimalisatie en veiligheid). Daarbij wordt aangehaakt bij de richtsnoeren die daarvoor door de gezamenlijke Europese privacy toezichthouders zijn opgesteld. In de MR is geregeld dat een aanvrager bij een aanvraag voor toelating van een inlogmiddel ter onderbouwing van conformiteit met artikel105396625 AVG een gegevensbeschermingseffectbeoordeling (DPIA) aanlevert als bedoeld in artikel105396635 AVG. De DPIA moet zien op de activiteiten waarop de aanvraag ziet en een beschrijving bevatten van de wijze waarop de maatregelen die zijn beschreven in de DPIA zijn opgenomen in de processen van de aanvrager die voor de erkenning van belang zijn.

Verhandelverbod (novelle)

De Wdo regelt dat private partijen die een inlogmiddel willen aanbieden waarmee bij de overheid ingelogd kan worden, slechts de beschikking hebben over persoonsgegevens indien en voor zover nodig om het middel in gebruik te hebben. Enig ander gebruik van deze gegevens is niet toegestaan. Hiermee is binnen de reikwijdte van de Wdo sluitend geregeld dat deze partijen de gegevens waarover ze uit hoofde van die verhouding met de burger en de overheid beschikken niet op een andere manier mogen worden gebruikt.

Het is mogelijk dat deze partijen nog op een andere manier over persoonsgegevens van burgers kunnen beschikken. Bijvoorbeeld als zij die gegevens aan de personen om wie het gaat hebben gevraagd, als onderdeel van (andere) commerciële dienstverlening. Over het gebruik van op die manier verkregen gegevens gaat dit voorstel niet. Het reguleren van dergelijke verstrekkingen gaat het bestek van deze wet te buiten. Wel zorgt de regeling in de Wdo ervoor dat de gegevens die de aanbieder in het kader van de inlogdienstverlening heeft verkregen, niet mogen worden gekoppeld aan deze gegevens en krijgen gebruikers een mogelijkheid, als vangnet, om verstrekkingen aan derden te beëindigen zonder dat daar financiële of functionele gevolgen aan verbonden zijn.

Open source (novelle)

Open source heeft een grote rol gespeeld in het debat over de novelle. Ik neem de gelegenheid te baat om daarover een aantal zaken te verduidelijken[1].

[1] Deze verduidelijking bied ik onder meer in de Memorie van Antwoord op vragen van de Eerste Kamer over de novelle Wdo. Deze wordt gelijktijdig verzonden met deze brief en voeg ik tevens bij deze brief.

In de MR is de wijze waarop ik wil zorgen dat de inlogmiddelen open source worden nader uitgewerkt. Het voornaamste doel dat mij in dit verband voor ogen staat is om transparantie te realiseren over de werking van inlogmiddelen. Zo is voor eenieder kenbaar hoe inlogmiddelen werken, en is daarmee controleerbaar hoe de verwerking van persoonsgegevens plaatsvindt. Dit doel wordt bereikt door de broncode te publiceren. Van belang is daarbij dat dit op een zodanige manier gebeurt dat deze ook daadwerkelijk raadpleegbaar en controleerbaar is. Dat regelt de MR.

De MR regelt ook een groeimodel voor open source. Dit wordt vormgegeven door een proces waarin stapsgewijs componenten van inlogmiddelen, die gebruikt worden voor de verwerking van persoonsgegevens ten behoeve van inlogdienstverlening, worden aangewezen waarvan de broncode gepubliceerd moet zijn. Deze lijst van componenten is in de bijlage bij de MR opgenomen. De broncode van deze componenten dient door de aanbieder – dan wel een derde, zoals de auteursrechthebbende – gepubliceerd te zijn. Het is goed denkbaar dat een aanzienlijk deel van de componenten al bij de toetreding tot het stelsel open source is. Daarom dient de aanbieder ten behoeve van die toetreding tevens een overzicht van zijn functionele componenten en een overzicht van de software die daarvoor wordt gebruikt aan het Agentschap Telecom te verstrekken.

De aanwijzingen en ingangsdatums voor open source zullen worden vastgelegd in de bijlage bij de ministeriële regeling[2]. In deze consultatieversie zijn de componenten nog niet voorzien van een ingangsdatum. Om te zorgen dat met deze aanwijzing zal worden voldaan aan de vereisten van veiligheid, continuïteit en een breed beschikbaar aanbod van inlogmiddelen is het nodig om hierover tevoren kennis in te winnen bij experts. Ook wil ik hiervoor de internetconsultatie van de MR benutten, die ik gelijktijdig met de toezending van de regeling aan uw Kamer zal starten.

Open source en een community

In het debat over de wet digitale overheid hebben wij uitgebreid van gedachten gewisseld over de rol en aanwezigheid van een gemeenschap die zich bezighoudt met het controleren en verbeteren van de open source software. Zoals ik eerder heb aangegeven hecht ik grote waarde aan het bestaan van gemeenschappen die meekijken. Dit stelt iedereen die dat wil in staat om de broncode te onderzoeken, kwetsbaarheden te melden en eventueel verbetervoorstellen te doen. Dit veel-ogen-principe is een aanvullende waarborg voor de veiligheid en betrouwbaarheid van inlogmiddelen. Een belangrijk voordeel van open source.

Om deze voordelen te behalen is het regelen van transparantie als verplichting voor de aanbieders alleen niet voldoende. Het is, zoals ik tijdens de plenaire behandeling van novelle op de wet digitale overheid heb aangegeven, belangrijk dat er een community is of komt die daadwerkelijk meekijkt op de software.
Ik ga zelf stimuleren dat er een community komt. Hoe en in welke mate of vorm stimulering nodig is zal ik bezien in het licht van de ontwikkeling.

Ik hecht eraan te benadrukken dat dit los staat van de MR, in die zin dat in de MR geen regels over communities worden opgenomen. Waar het in de kern om gaat, en waaraan de MR wel regels stelt, is dat de software veilig

[2] Deze systematiek is tot stand gekomen als gevolg van de discussie over dit onderwerp met Uw Kamer en met Eerste Kamer. De artikelen in de beide algemene maatregelen van bestuur over open source zijn als gevolg daarvan ook aangepast om deze systematiek mogelijk te maken. De aangepaste versies van de desbetreffende artikelen zijn als bijlage bij deze brief gevoegd.

is, onderhouden wordt, en beschikbaar is en blijft. Vertaald naar de veiligheid van de inlogmiddelen, het doel van de Wdo, gelden de eisen zoals die in de ministeriële regeling zijn opgenomen. De aanbieders van inlogmiddelen moeten daaraan voldoen bij de toelating en ook daarna. Daarop wordt toezicht gehouden gedurende de periode dat inlogmiddelen zijn toegelaten. De veiligheid van de gebruikte softwarecomponenten maakt daarvan onderdeel uit. De primaire veiligheid van de middelen borg ik door de aanbieders aan de toelatingseisen te houden en hen daarop aan te spreken als dat nodig is.

In het geval van toegelaten inlogmiddelen zal het de leverancier van het inlogmiddel in kwestie zijn die als onderdeel van zijn dienstverlening ervoor moet zorgen dat de onderdelen van diens software op de bovenstaande manier worden beheerd en dat adequaat wordt gereageerd op inbreng van de gemeenschap. Het vormt (bij zowel gesloten als open software) onderdeel van de verantwoordelijkheid van leveranciers om te zorgen voor een deugdelijk product. Het gebruiken van veilige en betrouwbare softwarecomponenten maakt inherent onderdeel uit van de verantwoordelijkheid van de aanbieder om veilige en betrouwbare dienstverlening aan te bieden binnen de eisen zoals gesteld in de MR.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen