

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2514 CV DEN HAAG

**Directie Bestuurlijke en
Politieke Zaken**

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6011 (algemeen)
www.rijksoverheid.nl/ezk

Datum 24 april 2026
Betreft Toezeggingen Digitalisering april 2026

Ons kenmerk
BPZ / 105954431

Bijlage(n)
2

Geachte Voorzitter,

Met deze brief wordt uw Kamer geïnformeerd over een drietal toezeggingen en ontvangt uw Kamer de evaluatie van de Wet digitale overheid (Wdo). Deze brief bevat onderwerpen die vallen onder de Staatssecretaris Economische Zaken en Klimaat (EZK) - Digitale Economie en Soevereiniteit en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (BZK) - Koninkrijksrelaties en Slagvaardige Overheid. Op deze manier wordt uw commissie voor Digitalisering in één keer geïnformeerd.

De volgende drie toezeggingen worden in deze brief behandeld:

1. De Kamer is toegezegd, naar aanleiding van een vraag van het lid Van Hattem (PVV), om de auditvereisten voor de aansluiting op DigiD en de resultaten van de risico-inventarisatie over het plaatsen van het BSN-nummer op de ID-kaart BES, wanneer gereed, naar de Kamer te sturen.
2. De Kamer is, in de Kamerbrief "Beantwoording vragen over de voortgang Rijksbrede strategie voor de effectieve aanpak van desinformatie en aankondiging nieuwe acties, toegezegd te worden geïnformeerd over de resultaten van het onderzoek naar een meldvoorziening, onafhankelijk geschillenbeslechtsorgaan en kenniscentrum in het kader van de Digitaal dienstenverordening (DSA).
3. De Kamer is toegezegd, naar aanleiding van een vraag van het lid Ganzevoort (GroenLinks), dat zij een afschrift krijgt van het toezichtkader betreffende private aanbieders van inlogmiddelen onder de Wet digitale overheid wanneer deze er is.

1. Auditvereisten en risico-inventarisatie BSN BES

Tijdens het debat in de Eerste Kamer over de Wet invoering BSN en voorzieningen digitale overheid BES¹ is toegezegd de auditvereisten en de risico-inventarisatie aan uw Kamer te sturen.² Hierbij is aangegeven dat de auditvereisten gebruikt worden die nu al gelden voor een aansluiting op DigiD. Deze auditvereisten zijn dezelfde als in Europees Nederland.³ De werking van de Wet digitale overheid,

¹ Handelingen I 2025/2026, nr. 2, item 3, p. 8.

² Toezeggingsnummer: T04077

³ Kamerstukken II, 2011/12, 26 643, nr. 193, p. 2

waarin deze verplichting een basis krijgt, is per 11 november 2025 uitgebreid naar de openbare lichamen Bonaire, Sint-Eustatius en Saba. Daarmee zullen de eisen in het Europese en het Caribische deel van Nederland hetzelfde zijn. Om de openbare lichamen te ondersteunen om aan deze voorwaarden te voldoen zijn door een externe partij initiële beveiligingsbeoordelingen uitgevoerd. De organisatie-overstijgende resultaten van deze beoordelingen zijn tijdens de behandeling in de Tweede Kamer van bovengenoemd wetsvoorstel aan het dossier toegevoegd.⁴ Via de Regeling bijzondere uitkering digitalisering BES zijn middelen beschikbaar gesteld om bevindingen te adresseren en verdere verbeteringen te realiseren.⁵ Met deze informatie geven we uitvoering aan de gedane toezegging.

2. *Onderzoek naar een meldvoorziening, onafhankelijk geschillenbeslechtsorgaan en kenniscentrum in het kader van de digitale dienstenverordening (DSA)*

In de Kamerbrief "Beantwoording vragen over de voortgang Rijksbrede strategie voor de effectieve aanpak van desinformatie en aankondiging nieuwe acties d.d. 20 december 2024"⁶ is toegezegd uw Kamer te informeren over de resultaten van het onderzoek naar een meldvoorziening, onafhankelijk geschillenbeslechtsorgaan en een kenniscentrum. Een geschillenbeslechtsorgaan biedt gebruikers een aanvullende mogelijkheid om beslissingen van onlineplatforms over inhoudsmoderatie aan te vechten. Op dit moment is er geen onafhankelijk geschillenbeslechtsorgaan aanwezig in Nederland zoals beschreven in artikel 21 van de Digitaal dienstenverordening (DSA). Wel zijn er binnen de EU vier van dit soort instanties die klachten over Nederlandstalige inhoud behandelen. Er is een scenarioanalyse gedaan om te kijken of en op welke manier een dergelijk orgaan in Nederland kan worden gevormd. Hierbij bied ik u de resultaten van de scenarioanalyse aan (zie bijlage 1), waarmee ik de gedane toezegging nakom.

Een van de belangrijkste bevindingen uit de scenarioanalyse is dat er behoefte is aan een actievere maar niet-dominante rol van de overheid. Dit kan bijvoorbeeld in de vorm van een overheids campagne waarbij gebruikers worden geïnformeerd over hun rechten om beslissingen van onlineplatforms aan te vechten, en worden geholpen bij het benaderen van bestaande geschillenbeslechtsorganen binnen de EU. Daarnaast willen respondenten uit het onderzoek met name dat de overheid actiever wordt om bestaande meldvoorzieningen, waar onder andere *trusted flaggers* zoals Offlimits, en Meld.Online Discriminatie, zichtbaar te maken, te structureren en op elkaar af te stemmen. Hierbij kan gedacht worden aan een website met een overzicht van alle meldvoorzieningen in Nederland, waar gebruikers terecht kunnen met hulpvragen over online content. Respondenten pleiten niet voor een volledig gecentraliseerd – of door de overheid beheerd – meldsysteem. De voorkeur gaat uit naar een gematigde tot beperkte rol, gericht op verbetering van de vindbaarheid van relevante meldpunten en coördinatie om overlappen te vermijden. En dit bij voorkeur zonder verlies van thematische specialisatie of autonomie van bestaande meldvoorzieningen en

⁴ Kamerstukken II 2024/2025, 36 639, nr. 9

⁵ Staatscourant 2025, 31026

⁶ Referentie BZK: 2024-0000872208

geschillenbeslechtingorganen. De scenarioanalyse maakt duidelijk dat het opzetten van een onafhankelijk geschillenbeslechtingorgaan in Nederland een strategische uitdaging vormt.

Gezien de complexiteit van en de zorgvuldigheid die bij dit vraagstuk vereist is, heeft het ministerie van BZK sinds de oplevering van de analyse verkennende gesprekken gehouden met bestaande geschillenbeslechtingen in de EU, en maatschappelijke organisaties om de mogelijkheden rond een geschillenbeslechting in Nederland te bespreken. Het kabinet houdt bij het uitwerken van de volgende stappen rekening met de adviezen uit het onderzoek.

3. Update Toezichtkader Wet digitale overheid (Wdo)

Uw Kamer is toegezegd, naar aanleiding van een vraag van het lid Ganzevoort (GroenLinks-PvdA), een afschrift te krijgen van het toezichtkader betreffende private aanbieders van inlogmiddelen onder de Wet digitale overheid wanneer deze er is.⁷ De Wdo zal onder andere de toelating en het gebruik van nieuwe en bestaande publieke en private inlogmiddelen reguleren. De Wdo wijst de Rijksinspectie voor Digitale Infrastructuur (RDI) aan als toezichthouder. Het toezichtkader van de RDI wordt ontwikkeld aan de hand van de eisen van de Wdo en het toelatingsproces voor inlogmiddelen. Dit toelatingsproces is in ontwikkeling en zal naar verwachting in juni 2027 van start kunnen gaan. Op dat moment zal ook het toezichtkader gereed zijn. Uw Kamer krijgt een afschrift zodra het toezichtkader gereed is.

Evaluatie Wet digitale overheid (Wdo)

De Wet digitale overheid (Wdo) is op 1 juli 2023 gefaseerd in werking getreden. Artikel 23 van de Wdo bepaalt dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) binnen 3 jaar na de inwerkingtreding van de Wdo een verslag over de doeltreffendheid en de effecten van de wet in de praktijk aan beide Kamers toestuurde. Hierbij moet in het bijzonder aandacht worden geschonken aan de getroffen maatregelen op het gebied van beveiliging, privacybescherming en de toegankelijkheid van elektronische dienstverlening.

Op grond van artikel 1 van het Besluit houdende departementale herindelingen met betrekking tot digitale zaken is de Minister van Economische Zaken en Klimaat⁸ belast met aangelegenheden op het terrein van digitale zaken die voorheen waren opgedragen aan de Minister van BZK. Ingevolge de portefeuilleverdeling kabinet-Jetten is Staatssecretaris Digitale economie en soevereiniteit verantwoordelijk voor de kaderstelling digitale overheid en daarmee voor de Wdo.⁹ De Staatssecretaris van BZK is verantwoordelijk voor de realisatie van de digitale overheid, waaronder de realisatie en het beheer van de Generieke Digitale Infrastructuur (GDI). Daarom sturen wij u gezamenlijk de evaluatie van de Wdo toe (zie bijlage 2). Deze heeft betrekking op de eerste fase die nu in werking is. De onderzoekers hebben bij deze evaluatie de volgende vraag beantwoord: *in hoeverre is de Wdo doeltreffend en wat zijn de effecten van de*

⁷ Toezeggingsnummer: T03658

⁸ Staatscourant 2026 nr. 8180, 24 februari 2026.

⁹ <https://www.rijksoverheid.nl/documenten/besluiten/2026/02/23/portefeuilleverdeling-kabinet-jetten>.

Wdo, in het bijzonder op het gebied van privacybescherming en toegankelijkheid van elektronische dienstverlening in de praktijk?

Zodra de overige bepalingen in werking zijn getreden, zullen ook die geëvalueerd worden en zal die evaluatie aan beide Kamers toegezonden worden.

Wet digitale overheid

De Wdo is een kaderwet die waarborgen biedt aan burgers en ondernemers bij de dienstverlening van de digitale overheid. De wet regelt algemene principes, taken en verantwoordelijkheden en procedures, geen gedetailleerde regels. De wet zorgt zo voor flexibiliteit bij nieuwe ontwikkelingen. De Wdo is ook toekomstbestendig: belangrijke waarden en zekerheden voor burgers, zoals gebruikersvriendelijkheid, betrouwbaarheid, veiligheid, privacy en digitale inclusie zijn geborgd.

De Wdo vormt de eerste tranche van regelgeving ten behoeve van verdere digitalisering van de overheid en beoogt de beweging naar de inzet van veiligere inlogmiddelen overheidsbreed te bewerkstelligen. De eerste tranche van de Wdo regelt dat alleen erkende inlogmiddelen voor toegang tot publieke dienstverlening zijn toegestaan, en biedt ook handvatten waarmee publieke dienstverleners het juiste beveiligingsniveau van hun dienstverlening kunnen bepalen. Ook biedt de Wdo de Minister van EZK de bevoegdheid om standaarden te verplichten in het elektronische verkeer met de overheid en regelt de wet de verantwoordelijkheid van de Minister van BZK voor het beheer van de voorzieningen en diensten binnen de GDI.

Op dit moment wordt gewerkt aan een uitvoeringswet, inclusief aanpassing van de Wdo, waarmee de herziene eIDAS-verordening wordt geïmplementeerd. Hierdoor wordt het voor burgers mogelijk om veilig en betrouwbaar met een publieke EDI-wallet in te loggen en gegevens te delen met de overheid, maar ook met andere organisaties. Belangrijk daarbij is dat burgers daarvoor zelf kunnen kiezen, want gebruik van deze de wallet wordt vrijwillig. De beleidsvorming wordt naar verwachting dit jaar afgerond. Op basis hiervan zou eind 2026 een uitvoeringswet in consultatie gebracht kunnen worden. Verwachting is dat de uitvoeringswet - afhankelijk van de parlementaire behandeling - in 2028 in werking zou kunnen treden.

Bevindingen onderzoekers

De onderzoekers constateren dat de Wdo (als kader), voor zover in werking getreden, een toereikend instrumentarium biedt om het beoogde doel te kunnen bewerkstelligen. De Wdo heeft bijgedragen aan bewustwording rond veilig digitaal handelen en aan het bepalen van het juiste betrouwbaarheidsniveau bij digitale transacties.

De onderzoekers stellen ook vast dat de Wdo nadrukkelijk de verantwoordelijkheid van de Minister van BZK voor het beheer van GDI voorzieningen en diensten vastlegt en ruimte biedt voor de ontwikkeling van aanvullende GDI voorzieningen. Tenslotte wordt als positief punt aangemerkt dat er al enkele verplichte standaarden zijn aangewezen.

Aanvullend hierop geven de onderzoekers aan dat er in de uitvoering nog wel belangrijke stappen zijn te zetten om de doelen van de Wdo daadwerkelijk te kunnen bereiken.

Zo is de realisatie van de randvoorwaardelijke ICT-voorzieningen (Stelsel Toegang) nog niet gereed. Het effect - de toelating van betrouwbare nieuwe inlogmiddelen - blijft daardoor uit, aldus de onderzoekers. De onderzoekers stellen tevens dat aan de inrichting van het toezicht op de Wdo nog geen invulling is gegeven. Zij bevelen aan om het toezicht onder de Wdo te heroverwegen en bij een onafhankelijke toezichthouder te beleggen.

De onderzoekers wijzen ook op het ontbreken van een voorziening ten behoeve van wettelijke vertegenwoordiging en op het feit dat DigiD op het betrouwbaarheidsniveau hoog nog niet breed beschikbaar is.

De onderzoekers bevelen tot slot aan om de dialoog met het veld te intensiveren, en in te zetten op verwachtingenmanagement bij publieke dienstverleners over de effectuering van de Wdo, ook in relatie tot toekomstige ontwikkelingen op het terrein van het EDI-stelsel en de wallet.

Reactie op de bevindingen

Wij zijn blij met de constatering van de onderzoekers dat de Wdo een toereikend instrumentarium biedt om het beoogde doel te kunnen bewerkstelligen en bijdraagt aan het toekomstvast regelen van de digitale overheid en aan bewustwording rond veilig digitaal handelen en aan het bepalen van het juiste betrouwbaarheidsniveau van digitale transacties.

De bevindingen worden voor een belangrijk deel herkend en de aanbevelingen worden ter harte genomen. Daarbij is het belangrijk om aan te geven dat de onderzoekers de evaluatie niet beperkt hebben tot de artikelen die in werking zijn getreden. Zij doen ook uitspraken over artikelen die niet in werking zijn getreden. Ook ziet een deel van de bevindingen op de realisatie van de Wdo, hetgeen ressorteert onder de staatssecretaris van BZK.

Met de realisatie van de randvoorwaardelijke ICT-voorziening, het Stelsel Toegang, geeft de Minister van BZK uitvoering aan een stelsel waarmee (semi-)publieke dienstverleners geholpen worden om te voldoen aan de acceptatieplicht van toegelaten inlogmiddelen onder de Wdo. Het toelaten van private inlogmiddelen zal naar verwachting leiden tot meer innovatie binnen de markt van inlogmiddelen en burgers en bedrijven krijgen zelf de keuzevrijheid met welk inlogmiddel ze kunnen inloggen. Daarnaast wordt met het Stelsel Toegang uitvoering gegeven aan de politieke en maatschappelijke wens om wettelijk vertegenwoordigen mogelijk te maken, zodat burgers en bedrijven namens een ander digitaal zaken kunnen doen met de overheid¹⁰. Thans lopen de consultaties van het besluit waarin dit geregeld wordt (Verzamelbesluit digitale overheid i.v.m vertegenwoordigen). Over een verkenning naar gebruiksvriendelijke alternatieven

¹⁰ Tweede kamer, vergaderjaar 2025-2026, 26643, nr. 1497.

voor DigiD Hoog is gecommuniceerd in de Verzamelbrief van 11 juli 2025.¹¹ De acceptatieplicht voor de onder de Wdo toegelaten middelen zal naar verwachting eind 2027 in werking kunnen treden. Hiervoor is nodig dat een toelatings- en erkenningsproces is ingericht waarmee belangstellende partijen zich kunnen aanmelden.

De dialoog met het veld over de realisatie van het Stelsel Toegang is vanuit het ministerie van BZK al geïntensiveerd. Er is een implementatieteam ingericht dat publieke dienstverleners informeert over de voortgang van de realisatie van het Stelsel Toegang en de wijze van aansluiten. Ook worden er op reguliere basis overleggen georganiseerd met publieke dienstverleners. Daarbij wordt samen met publieke dienstverleners ook uitdrukkelijk aandacht besteed aan de samenhang tussen het Stelsel Toegang en de wallet/Europese Digitale Identiteit-stelsel (EDI-stelsel).

Voor wat betreft de naleving van de overige verplichtingen onder de Wdo, zal bij het aansluiten van de publieke dienstverleners op het Stelsel Toegang worden getoetst of zij hun diensten hebben geclassificeerd. Mocht er op basis van de praktijk aanleiding toe zijn, kan het toezicht worden aangescherpt. Het toezicht op publieke dienstverleners voor wat betreft de beveiliging van de toegang tot elektronische diensten zal met een auditplicht, volgens de huidige praktijk van de ICT-beveiligingsassessments DigiD, ingericht worden. Daarnaast is, om het feitelijk gebruik te meten, onder het Stelsel Toegang een monitoringsysteem voorzien, zoals nu bijvoorbeeld ook gehanteerd wordt voor de GDI-voorzieningen. De aanbeveling om het toezicht onder de Wdo weg te halen bij verantwoordelijke ministers en bij een onafhankelijke toezichthouder te beleggen, neem ik in overweging.

¹¹ Tweede Kamer, vergaderjaar 2024-2025, 26 643, nr. 1371.

De naleving van een aantal verplichtingen, die gelden onder de Wdo, is nog niet voldoende ingeregeld. Dit geldt met name voor het toezicht op de naleving van de verplichte standaarden. De Kamer is bij brief van 16 februari 2026 geïnformeerd dat vanuit de Nederlandse Digitaliseringsstrategie (NDS) wordt ingezet op een versterkte aanpak op het afspreken, invoeren en handhaven van (digitale) standaarden, inclusief ondersteuning bij het invoeren daarvan.¹² Het ministerie van BZK zet hierbij in eerste instantie in op het, via implementatieteams, helpen van overheidsorganisaties bij de implementatie van de verplichte standaarden. Eventuele handhavingsinstrumenten kunnen ingezet worden wanneer deze helpende hand niet tot het gewenste resultaat leidt.

W.J.M. Aerdts
De staatssecretaris Digitale Economie en Soevereiniteit

Eric van der Burg
De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

¹² Tweede Kamer, vergaderjaar 2025–2026, 26 643, nr. 1491.

Scenario analyse: opzetten van een nieuw DSA Buitengerechtelijk Geschillenbeslechtingorgaan in Nederland

Dr. Mathias Vermeulen
7 juli 2025

1. Introductie

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verkent momenteel verschillende mogelijkheden om de moderatie van online inhoud op digitale platformen te verbeteren. Deze verkenning vindt plaats met het oog op een goede uitvoering van de Digital Services Act (DSA). Het Ministerie heeft in het bijzonder interesse in twee activiteiten:

(a) het ondersteunen van bestaande meldmechanismen voor Nederlandse burgers en organisaties om verschillende vormen van schadelijke of illegale inhoud op online platformen te melden, en

(b) het ondersteunen van de mogelijkheid voor Nederlandse burgers om gebruik te maken van buitengerechtelijke geschillenbeslechting, zoals voorzien in artikel 21 van de Digital Services Act (DSA).

Momenteel zijn er 7 gecertificeerde Europese buitengerechtelijke geschillenbeslechtingsorganen (of “*out-of-court dispute settlement bodies*” – hierna “ODSBs”), waarvan er 3 klachten in het Nederlands aanvaarden.

Naam	Vestigingsland	Platformen	Toepassingsgebied	Taal
ADROIT	Malta	Alle	Alle vormen van geschillen.	Nederlands , Engels, Frans, Duits, Italiaans, Maltees, Portugees,
Appeals Centre Europe	Ierland	Instagram Facebook TikTok YouTube	Alleen geschillen die betrekking hebben de volgende bepalingen in de gebruikersovereenkomst: <ul style="list-style-type: none">• Misleidende informatie• Zelfdoding & zelfbeschadiging• Pesten & intimidatie	Aanvaard klachten in het Nederlands , Engels. Frans, Duits, Italiaans en Spaans – maar het geschil zelf kan gaan over inhoud in elke taal die gesproken wordt in de EU.

			<ul style="list-style-type: none"> • Haatzaaien • Gevaarlijke activiteiten & uitdagingen • Gewelddadige & schokkende inhoud • Geweld & opruiing • Gevaarlijke organisaties & individuen • Naaktheid voor volwassenen • Seksuele inhoud • Taal & diensten • Gereguleerde goederen & diensten • Veiligheid van minderjarigen 	
ADR Point	Griekenland	Geen publieke informatie momenteel beschikbaar	Geen publieke informatie momenteel beschikbaar.	Nederlands , Grieks, Engels, Frans, Duits, Italiaans, Spaans, Pools, Roemeens, Bulgaars, Kroatisch, Litouws, Tsjechisch
RTR-GmbH, Fachbereich Medien	Oostenrijk	Alle	Alle vormen van geschillen	Duits
ADR Center	Italië	Alle	Alle vormen van geschillen	Italiaans, Engels
User Rights GmbH	Duitsland	Instagram Facebook TikTok Linkedin Pinterest	Geschillen die te maken hebben met het verwijderen van een bericht, het opschorten van een account of een besluit om gerapporteerde inhoud niet te verwijderen op basis van de gebruiksovereenkomst	Duits, Engels, Frans (alleen voor geschillen inzake gebruikersovereenkomsten), Italiaans

			van de betreffende platforms als ook ook specifieke gebieden van de Duitse wetgeving (StGB) met betrekking tot belediging, seksuele intimidatie, haatzaaiende uitlatingen, aanzetten tot haat, stalking, smaad, doxing, discriminatie of misdrijven tegen de openbare orde.	
Online Platform Vitarend ező Tanács	Hongarije	Alle	Alle vormen van geschillen	Hongaars

Op basis van een (academische) literatuurstudie, interviews met vertegenwoordigers van gecertificeerde Europese buitengerechtelijke geschillenbeslechtsorgaanen (of “*out-of-court dispute settlement bodies*” – hierna “ODSBs”), en een vragenlijst die beantwoord werd door 10 Nederlandse stakeholders in de Rijksoverheid, zelfstandige bestuursorganen, het middenveld en bestaande meldpunten, werd de volgende beleidsvraag onderzocht:

Moet Nederland een (uitgebreidere vorm van) een ODSB opzetten waar burgers niet alleen terechtkunnen voor het beslechten van geschillen over besluiten van online platformen maar ook voor meldingen van schadelijke of illegale inhoud als – en zo ja, hoe kan een dergelijke ODSB georganiseerd worden?

In dit document worden verschillende institutionele scenario’s geanalyseerd die deze vraag kunnen helpen beantwoorden. Daarbij is bijzondere aandacht voor:

- De mogelijke rol van de overheid
- De organisatievorm van een ODSB, inclusief de mate van integratie met bestaande meldpunten of andere ODSBs.

De scenario’s zullen worden beoordeeld op basis van hun haalbaarheid en wenselijkheid.

2. Haalbaarheid en wenselijkheid parameters van de scenario's

De **haalbaarheid** van een scenario is de mate waarin het voorstel binnen een redelijke termijn kan worden geïmplementeerd, gegeven de juridische, institutionele en financiële randvoorwaarden, en de bestaande beschikbare capaciteit van betrokken actoren. De onderliggende beoordelingscriteria voor dit beoordelingscriterium zijn

- **Juridische haalbaarheid:** Is het scenario wettelijk mogelijk binnen bestaande nationale en EU-regelgeving? Zijn er wetswijzigingen nodig?
- **Financiële haalbaarheid:** Hoe hoog zijn de geschatte kosten van dit scenario?
- **Institutionele capaciteit:** Zijn er bestaande actoren of infrastructuren waarop kan worden voortgebouwd?
- **Tijdspad:** Hoelang duurt de implementatie?
- **Operationele uitvoerbaarheid:** Zijn er praktische belemmeringen (bijv. IT-complexiteit, personeelstekort?)

De haalbaarheid van de scenario's wordt beoordeeld op een schaal van 1 tot 5

- **5: Zeer haalbaar** – kan direct worden uitgerold zonder grote obstakels
- **4: Goed haalbaar** – kan worden uitgerold binnen 1 à 2 jaar
- **3: Matig haalbaar** – vergt coördinatie en investeringen, maar juridisch mogelijk
- **2: Moeilijk haalbaar** - stuit op substantiële juridische, financiële of organisatorische belemmeringen; implementatie vergt langdurig traject
- **1: Onhaalbaar** - vereist structurele wetswijzigingen, ontbreekt aan draagvlak of is praktisch onuitvoerbaar in huidige context

De **wenselijkheid** van de scenario's is de mate waarin zij bijdragen aan de beleidsdoelstellingen, met name de verbetering van contentmoderatie met betrekking tot Nederlandstalige inhoud voor (a) platformgebruikers die in Nederland wonen, ongeacht hun nationaliteit en (b) Nederlandse staatsburgers, waar zij zich ook bevinden binnen de EER. In onze bevraging van 10 stakeholders is expliciet gepeild naar de steun voor de oprichting van een nieuw ODSB dat geschillen zou behandelen voor alle Europese platformgebruikers, ongeacht de taal. Voor dit voorstel bleek echter geen draagvlak te bestaan.

Hoewel 'het verbeteren van de content moderatie door platformen' een normatief en contextafhankelijk begrip is, worden op basis van de literatuur en ons onderzoek enkele gemeenschappelijke elementen naar voren geschoven:

- **Laagdrempeligheid voor de gebruiker:** klachten en meldingen moeten ingediend kunnen worden in het Nederlands op een eenvoudige en gebruiksvriendelijke manier
- **Consistentie:** vergelijkbare moderatiebeslissingen van platformen worden vergelijkbaar behandeld

- **Transparantie:** gebruikers krijgen beter inzicht in de afwegingen achter moderatiebeslissingen

Dit korte onderzoek wijst op een potentiële behoefte aan een buitengerechtelijke geschilinstantie die deze doelstellingen kan ondersteunen, met name wanneer deze beschikt over gespecialiseerde kennis van zowel de Nederlandse taal en culturele context (zoals symboliek, satire of contextuele vormen van haatspraak) als van het juridisch kader, waaronder de Nederlandse discriminatiewetgeving.

Die behoefte wordt mede verklaard door het breed gedeelde beeld onder respondenten dat het voor burgers in de praktijk vrijwel onmogelijk is om via de rechter op te komen tegen platformbeslissingen door de aanzienlijke juridische en praktische drempels. Eén respondent noemde de drempels “van wolkenkrabberhoogte”. Civiele procedures worden als kostbaar, complex en tijdrovend ervaren, en vereisen vaak juridische bijstand die voor veel burgers onhaalbaar is — zeker wanneer het financiële belang gering is. Daarnaast is er sprake van een grote machtsongelijkheid tussen individuen en juridisch goed uitgeruste platformen, wat de kans op succes verder verkleint. Ten slotte wordt de traagheid van gerechtelijke procedures genoemd: waar snel rechtsherstel nodig is, bijvoorbeeld bij een geblokkeerd account, duurt een procedure vaak anderhalf jaar, wat voor velen neerkomt op feitelijke ontoegankelijkheid van het recht.

Een cruciale factor daarbij is hoe burgers en maatschappelijke organisaties de onafhankelijkheid van een mogelijk ODSB ervaren: slechts indien het instituut als eerlijk en neutraal wordt gezien, zullen gebruikers geneigd zijn om daadwerkelijk klachten of meldingen in te dienen.

De wenselijkheid van de scenario's worden beoordeeld op een schaal van 1 tot 5

- **5: Zeer wenselijk** - Scenario voorziet in geïdentificeerde noden
- **4: Wenselijk** - Scenario voldoet grotendeels aan geïdentificeerde noden
- **3: Beperkt wenselijk** - Scenario mist op een of meerdere punten een oplossing voor geïdentificeerde noden, of roept twijfels op over neutraliteit of belangenverstrengeling.
- **2: Onwenselijk** - Scenario voldoet niet aan de meeste geïdentificeerde noden
- **1: Zeer onwenselijk** - Scenario kan geen geïdentificeerde noden realiseren of wordt gepercipieerd als politiek gestuurd of commercieel gedreven

De beoordeling van de scenario's op het vlak van haalbaarheid en wenselijkheid is gebaseerd op een combinatie van literatuuronderzoek, gesprekken met vertegenwoordigers van bestaande ODSB's en de antwoorden van tien Nederlandse stakeholders. Hoewel deze aanpak een degelijk eerst beeld oplevert van de belangrijkste knelpunten, voorkeuren, opportuniteiten en randvoorwaarden, moet worden benadrukt dat de uiteindelijke scores op beide assen subjectief blijven. De beoordelingen zijn gemaakt op basis van de huidige stand van zaken, beleidscontext en inschattingen van de stakeholders, en kunnen evolueren naarmate de juridische en institutionele context verandert. Ook is de steekproefgrootte van respondenten beperkt, waardoor sommige perspectieven mogelijk onderbelicht zijn gebleven. De scenarioanalyse dient dan ook als richtinggevend instrument en niet als definitieve

aanbeveling. Verdere consultatie, validatie en maatschappelijke dialoog blijven noodzakelijk voor beleidsvorming.

3. Afbakening van de scenario's

Bij de ontwikkeling en analyse van de scenario's is gekozen voor een tweedimensionaal afwegingskader. Deze aanpak maakt het mogelijk om uiteenlopende modellen systematisch te vergelijken op hun wenselijkheid en haalbaarheid. In totaal werden negen scenario's overwogen, gebaseerd op twee dimensies:

3.1 Keuzedimensie 1: Rol van de overheid

De eerste dimensie betreft de rol van de overheid in de ontwikkeling, financiering en aansturing van een (uitgebreide versie van) de ODSB. De mate van overheidsbetrokkenheid wordt onderverdeeld in vier niveaus:

Niveau Omschrijving

- 1 **Volledig privaat:** de overheid speelt geen enkele rol
- 2 **Faciliterend:** de overheid biedt beperkte signalerende of informerende steun, met minimale inhoudelijke of financiële inmenging
- 3 **Gematigd sturend:** de overheid levert eenmalige financiering en stelt kaders op
- 4 **Volledig publiek:** de overheid is verantwoordelijk voor oprichting, eigenaarschap en aansturing

Twee cruciale aspecten voor de beoordeling van wenselijkheid en haalbaarheid zijn de financiering en de onafhankelijkheid van de ODSB. De DSA bepaalt dat de kosten van een ODSB gedragen moeten worden door de zeer grote online platformen. In de praktijk zijn er echter opstartkosten verbonden aan onder meer de inrichting van een IT-infrastructuur voor klachtverwerking, juridische oprichting, werving van personeel en promotie van de ODSB zodat burgers de weg ernaartoe vinden. Deze kosten moeten vaak gemaakt worden voordat er inkomsten gegenereerd worden.

Tegelijkertijd leeft onder respondenten de overtuiging dat een ODSB moet worden ondergebracht in een onafhankelijke, maatschappelijk verankerde structuur, bijvoorbeeld een stichting zonder winstoogmerk. Er is ook appreciatie voor samenwerkingsmodellen waarin verschillende actoren (maatschappelijk middenveld, academici, juridische experts) hun krachten bundelen om legitimiteit en expertise te combineren.

De meeste respondenten vinden dat de overheid een ondersteunende, maar geen bepalende financiële rol moet spelen. Eenmalige of beperkte structurele bijdragen worden acceptabel geacht, mits dit bijdraagt aan de onafhankelijkheid ten opzichte van zowel platformen als de staat. Wel bestaat het besef dat een effectieve ODSB waarschijnlijk niet levensvatbaar is zonder enige vorm van publieke startinvestering.

De uitdaging is dan ook het vinden van een duurzaam financieringsmodel dat onafhankelijkheid, toegankelijkheid en effectiviteit combineert.

Verder hangt de schaalbaarheid en snelheid van besluitvorming van een ODSB mede af van de mate van technologische ondersteuning. Een goed ontworpen backoffice die gebruik maakt van gestandaardiseerde en/of geautomatiseerde besluitvormingsprocessen kan helpen bij een consistente en efficiënte afhandeling van geschillen.

Drie financieringsopties werden door de respondenten genoemd:

- Eenmalige subsidie voor de volledige opstartkosten van een ODSB (meest genoemd);
- Sommige respondenten vinden ook dat er naast de opstartsubsidie potentieel ook periodiek hernieuwbare bijdrage kunnen zijn voor de werkingskosten. Deze respondenten zien de noodzaak van een blijvende publieke bijdrage, om de onafhankelijkheid, kwaliteit en toegankelijkheid te kunnen garanderen, bijvoorbeeld als gebruikersvergoedingen niet direct kostendekkend zijn.
- Alleen projectfinanciering na oprichting van de organisatie.

3.2: Keuzedimensie 2: Organisatorisch model

De tweede dimensie betreft de institutionele organisatie van de meld- en geschilfuncties. Er werden drie organisatiemodellen onderscheiden.

1. **Geïntegreerd instituut** – Meldpunt en geschilbeslechting worden samengebracht in één juridische entiteit.
2. **Gecoördineerd netwerk** – De functies blijven gescheiden, maar zijn operationeel verbonden via een centraal coördinatiemechanisme.
3. **Gescheiden entiteiten** – Meldpunten en ODSB opereren volledig los van elkaar.

De meningen van de respondenten over de wenselijkheid en haalbaarheid van deze structuurvarianten liepen sterk uiteen.

Sommige respondenten vrezen belangenverstrengeling als meldpunten en ODSB onder één dak huizen. Zij wijzen op het verschil in functie: meldpunten signaleren en escaleren, terwijl een ODSB een oordelende of quasi-rechterlijke taak heeft. Het combineren van meldfunctie en geschilbeslechting binnen één organisatie zou volgens hen de onafhankelijkheid van de ODSB kunnen ondermijnen.

Voorstanders van integratie benadrukken juist de voordelen van overzichtelijkheid en toegankelijkheid voor gebruikers. Een centraal instituut zou volgens hen gebruikers beter kunnen ondersteunen en herkenbaarheid bevorderen. Een geïntegreerd instituut zou ook een escalatiemechanisme kunnen ontwikkelen, waarbij meldingen die naar mening van de klager onvoldoende zijn behandeld, simpel kunnen worden verwezen naar de geschilleninstantie.

Meerdere respondenten stellen dat samenwerking tussen meldpunten en ODSB's wenselijk is, maar eerder via coördinatie dan via integratie. Duidelijke mandaten en

scheiding van bevoegdheden zijn daarbij cruciaal. Er moet vooral een duidelijk mandaat zijn voor de aparte entiteiten, zodat burgers precies weten wat de instantie mag doen, in welke gevallen zij bevoegd is, en hoe zij zich verhoudt tot andere instanties (zoals toezichthouders of de rechter).

Respondenten zijn verdeeld over welk organisatiemodel het meest geschikt is. Sommige respondenten stellen voor om een nieuwe onafhankelijke entiteit op te richten; anderen suggereren uitbreiding van bestaande meldpunten. Weer anderen achten geen van de huidige meldpunten geschikt als basis voor een geschilleninstantie.

Er bestaat dus een spanningsveld tussen de wens tot onafhankelijkheid en een zuivere rolverdeling enerzijds, en de wens tot efficiëntie en integratie van bestaande structuren anderzijds. Elke beleidskeuze zal expliciet rekening moeten houden met deze twee perspectieven.

3.3 Niet weerhouden scenario's op basis van keuzedimensies

	Geïntegreerd instituut	Gecoördineerd netwerk	Gescheiden entiteiten
1. Volledig privaat			ADROIT-scenario
2. Faciliterend			Campaigne-scenario Meldpuntintegratie-scenario
3. Gematigd sturend	Scenario 1: Geïntegreerd Instituut	Scenario 2: Gecoördineerd Netwerk met/tussen ODSB en meldpunten	Scenario 3: Parallele ondersteuning
4. Volledig publiek			Scenario 4: Versnelde opstart RTR-scenario Pan-Europees ODSB- scenario

Uit ons onderzoek blijkt dat de meeste stakeholders alleen scenario's in rij 3 wenselijk vonden. Er is behoefte aan een actiever informierend en structurerend optreden van de overheid, maar zonder dat dit leidt tot volledige staatssturing. Respondenten willen met name dat de overheid actiever wordt in het zichtbaar maken, structureren en afstemmen van het bestaande meldlandschap. Maar dat betekent niet dat er gepleit wordt voor een volledig gecentraliseerd – of door de overheid beheerd – meldsysteem. De voorkeur gaat uit naar een gematigde tot beperkte rol, gericht op verbetering van de vindbaarheid van relevante meldpunten en coördinatie om overlappen te vermijden, bij voorkeur zonder verlies van thematische specialisatie of autonomie van bestaande meldpunten. Er is brede kritiek dat de overheid momenteel te weinig doet om burgers te informeren. Niets doen is daarmee geen aanvaardbaar scenario voor de meeste respondenten.

Artikel 21.6 DSA staat lidstaten toe om zelf een ODSB op te richten. Deze optie werd niet wenselijk geacht door de meerderheid van de respondenten. Uit het onderzoek komen twee grote redenen naar voor. Ten eerste, de institutionele betrokkenheid van overheden kan de perceptie van onafhankelijkheid ondermijnen en afbreuk doen aan de legitimiteit van de instantie. Dit werkt in twee richtingen. Beslissingen van gecertificeerde ODSB's onder de DSA zijn niet-bindend, wat betekent dat platformen zelf kunnen beslissen of ze de aanbevelingen opvolgen. Een door de overheid beheerde instantie zou niets veranderen aan deze juridische realiteit, wat uiteindelijk ook negatief kan afstralen op de overheid. Ten tweede, de kosten die gemaakt worden aan de oprichting van een dergelijk instituut zouden ook gespendeerd kunnen worden aan het verhogen van het budget van de toezichthouder, die wel dwingende beslissingen kan nemen.

Als gevolg van deze overweging wordt het “**RTR scenario**” niet uitgewerkt. RTR is een “publieke” ODSB die opgericht is per Oostenrijkse wet en die de taken vervult van een arbitrage-instantie (op grond van de Audiovisual Media Services Act), een buitengerechtelijke geschillenbeslechtsinstantie (als coördinator voor de Digital Services Act), en een klachtenloket (op grond van de Auteurswet). RTR aanvaardt enkel klachten in het Duits. In dit scenario wordt een ODS volledig opgericht, gefinancierd en aangestuurd door de overheid, bijvoorbeeld als een nieuwe entiteit binnen een ministerie of eventueel ondergebracht bij een bestaande toezichthouder. Hoewel dit model op papier overzichtelijk en bestuurbaar oogt, wordt het momenteel als weinig haalbaar en wenselijk beschouwd. Dit zou ook wettelijke aanpassingen vereisen.

Op basis van deze overweging is ook het ‘**ADROIT**’ scenario niet wenselijk. In dit scenario wordt de organisatie van een ODSB volledig aan de markt overgelaten, zoals het geval is bijvoorbeeld bij ADROIT in Malta of ADR Point in Griekenland. ADROIT is een commerciële aanbieder van verschillende ‘alternative dispute settlement solutions’ uit Malta die klachten in het Nederlands aanvaard over elk platform. Zo’n aanbieder kan een ODSB zijn dat speciaal wordt opgericht in de context van de DSA, of kan een bestaand arbitrage instituut zijn dat al andere vormen van geschillenbeslechting aanbiedt (bv. inzake crowdfunding of fintech). Hoewel dit model voldoet aan de onafhankelijkheidsvereisten van de DSA en aantrekkelijk lijkt vanuit kosten- en schaalperspectief, werden in de bevraging zorgen geuit over een exclusief commerciële logica achter een ODSB, waarbij efficiëntie (i.e. een snelle afhandeling van een klacht) boven kwaliteit van de motivering en transparantie van de eindbeslissing zou kunnen gaan.

Het “**campagne scenario**”, waarbij de rol van de Nederlandse overheid zich zou beperken tot het vergroten van de zichtbaarheid van bestaande (voornamelijk buitenlandse) ODSB's, wordt op basis van dit criterium ook niet verder doorgelicht. De burger bewust maken van bestaande ODSB's zou de burger enigszins ondersteunen om meer gebruik te maken van ODSBs. Maar opnieuw zou de overheid geen enkele manier hebben om de kwaliteit of het mandaat van deze ODSBs te waarborgen. Fundamentele rijzen hier ook vragen over de voorlichtersrol van de overheid en wie te ondersteunen. Momenteel zijn er 3 ODSBs (Adroit, Appeals Centre Europe en ADR Point) die klachten over Nederlandstalige inhoud behandelen, maar bij minstens twee actoren zijn er commerciële belangen gemoeid, wat vragen stelt over een eventuele voorkeursbehandeling als de een of de ander

ondersteund zou worden. In de praktijk worden regelmatig ook nieuwe ODSB's opgericht, wat het moeilijk maakt om burgers consistent en neutraal te informeren.

Het “**integratie meldpunten scenario**” werd ook niet weerhouden als apart scenario. Hierbij zou gekozen worden voor een loutere integratie en doorgezette ondersteuning van de bepaalde meldpunten. Maar gezien de wenselijkheid van een ODSB, werd dit als een te beperkende keuze gezien.

Ook het scenario van een “**pan-Europese ODSB**” wordt in deze nota niet verder uitgewerkt. In dit scenario zou de Nederlandse overheid samenwerken met andere lidstaten om gezamenlijk een overkoepelend, pan-Europees orgaan voor geschilbeslechting (ODSB) op te richten. Deze instantie zou zich kunnen specialiseren in een specifiek thema dat grensoverschrijdende relevantie heeft, zoals klachten over satire, manipulatie van verkiezingen of gendergerelateerd geweld. Een dergelijke instelling zou ook uitsluitend klachten behandelen die geen betrekking hebben op illegale inhoud, maar bijvoorbeeld op vermeende schendingen van gebruiksvoorwaarden. De ODSB zou klachten in ontvangst nemen van gebruikers uit de hele Europese Unie, in alle officiële talen, ongeacht hun land van herkomst.

Een dergelijk scenario brengt verschillende voordelen met zich mee. Een pan-Europese ODSB zou in staat zijn om diepgaande en gespecialiseerde expertise te ontwikkelen die niet gebonden is aan een specifieke taal of lidstaat. Hierdoor kunnen beslissingen consistentener worden genomen over platformen heen en kan er sprake zijn van meer coherente handhaving van Europese normen.

Deze aanpak wordt momenteel al in de praktijk gebracht door Appeals Centre Europe, een onafhankelijke ODSB die met een eenmalige donatie van Meta's Oversight Board werd opgericht. Deze instantie aanvaardt klachten van Europese gebruikers, ook in het Nederlands, over beslissingen van platforms zoals Facebook, Instagram, YouTube en TikTok met betrekking tot het verwijderen of behouden van content op basis van hun gebruiksvoorwaarden.

De haalbaarheid van dit scenario hangt echter deels af van de bereidheid van andere lidstaten om een dergelijke ODSB te ondersteunen, en ligt dus deels buiten het bereik van nationale besluitvorming. Een dergelijk scenario zou ook het behandelen van Nederlandstalige content niet als prioriteit stellen.

Er werd uiteindelijk gekozen om scenario's uit te werken die uitgaan van een gematigde overheidssturing, waarbij de overheid de richting van de ODSB initieel beïnvloedt via kaderstelling, tijdelijke financiering en/of partnerschappen, zonder directe operationele verantwoordelijkheid. In deze scenario's

- ondersteunt de overheid de oprichting van een nieuwe onafhankelijke ODSB (bijv. via startfinanciering of projectfinanciering);
- blijft de inhoudelijke werking onafhankelijk en wordt er voldaan aan de eisen uit artikel 21(3) DSA (o.a. onpartijdigheid, transparantie, taaltoegankelijkheid);
- ligt de focus op Nederlandstalige inhoud.

4. Scenario's

Op basis van de overwegingen hierboven zijn dit de vier potentiële scenario's die we verder verdiepen en scoren op basis van de wenselijkheid en haalbaarheid.

Scenario 1: Oprichting onafhankelijk geïntegreerd instituut

Scenario 2: Gecoördineerd netwerk met nieuwe ODSB

Scenario 3: Parallele ondersteuning ODSB en gecentraliseerd meldpunt

Scenario 4: "Versneld opstartscenario"

	Haalbaarheid	Wenselijkheid
Scenario 1: Oprichting onafhankelijk geïntegreerd instituut	2	3
Scenario 2: Gecoördineerd netwerk met nieuwe ODSB	3	5
Scenario 3: Parallele ondersteuning ODSB en gecentraliseerd meldpunt	4	4
Scenario 4: "Versneld opstartscenario"	4	4

4.1 Scenario 1: Oprichting onafhankelijk geïntegreerd instituut

Beschrijving: In dit scenario wordt een volledig nieuwe entiteit opgericht (bijvoorbeeld een stichting) die zowel de coördinerende meldfunctie als de functie van buitengerechtelijke geschillenbeslechting integreert. De entiteit kan bestuurlijk worden verankerd in een NGO of universiteit, met een diverse raad van toezicht waarin vertegenwoordigers van het maatschappelijk middenveld, juridische experts en technologie-experts zitting hebben. Gebruikers kunnen meldingen doen over schadelijke of illegale inhoud, en – indien zij menen dat het platform ontoereikend heeft gereageerd – een procedure starten bij de geschilleninstantie.

Haalbaarheid:

- Financieel is dit een van de duurste opties, aangezien zowel de oprichting van een nieuwe ODSB als een gecentraliseerd meldpunt vereist zijn.
- De combinatie van meldfunctie en geschilbeslechting in één organisatie is institutioneel ongebruikelijk en vergt aanzienlijke tijd en juridische uitwerking
- De operationele uitvoerbaarheid is complex, zeker indien er een eigen IT-backend en workflowbeheer wordt opgezet. Dit vergt investeringen in technische infrastructuur, personele capaciteit en juridische expertise.
- Een geïntegreerd instituut laat toe dat informatie kan terugvloeien naar beleidsmakers of toezichthouders, en kan potentieel leiden tot snellere correctie van structurele problemen.

Wenselijkheid

- Het scenario biedt een duidelijke en laagdrempelige ‘one-stop-shop’ voor Nederlandse gebruikers met problemen rond contentmoderatie op grote platformen.
- Een geïntegreerde structuur creëert mogelijkheden voor snelle escalatie: meldingen die onvoldoende behandeld worden, kunnen intern worden opgevolgd door de geschilleninstantie.
- Dat levert ook mogelijkheden op naar institutionele branding toe wat kan uitgespeeld worden in communicatiecampagnes. Die zijn nodig om meer zichtbaarheid te creëren zodat de burger ook makkelijk de weg vindt naar het instituut, en er gebruik van maakt.
- Een geïntegreerd instituut kan ook trendrapportages opstellen over specifieke problematische inhoud of gedrag waarop inadequaat wordt gereageerd. Dat kan dan gesignaleerd worden aan de Europese Commissie in haar rol als toezichthouder.
- Tegelijkertijd is er een risico op belangenverstremming of schijn van partijdigheid. Als dezelfde entiteit meldingen verzamelt én oordeelt over platformbesluiten, kan dit afbreuk doen aan de waargenomen onafhankelijkheid van de geschilleninstantie.

4.2 Scenario 2: Gecoördineerd netwerk met nieuwe ODSB

Beschrijving: In dit scenario worden meldingen en geschillenbeslechting georganiseerd door aparte entiteiten die echter worden samengebracht in een coördinatieorgaan of gezamenlijk digitaal portaal. De meldfunctie kan worden ondergebracht bij een bestaande organisatie met expertise in meldpunten, terwijl de ODSB wordt opgericht als onafhankelijke stichting.

Haalbaarheid:

- Financieel potentieel goedkoper dan scenario 1 aangezien een bestaande organisatie de taak van centraal meldpunt op zich zou nemen. De financiering van een ODSB zou nog steeds gedragen moeten worden.
- De oprichting van een ODSB blijft vereist, maar is juridisch en institutioneel duidelijker als aparte entiteit.
- De coördinatie vereist wel duidelijke governance-afspraken om een nodeloos complexe governance structuur te vermijden, maar biedt tegelijk flexibiliteit.
- Een dergelijke coördinatie laat toe dat informatie ook kan terugvloeien naar beleidsmakers of toezichhouders, en kan potentieel leiden tot snellere correctie van structurele problemen.
- De operationele uitvoerbaarheid is haalbaar maar kan ook langer op zich laten wachten als een nieuwe backoffice/”legal tech” oplossing gecreëerd zou worden.

Wenselijkheid

- Dit scenario laat nog altijd toe een duidelijke one-stop-shop aan te bieden voor Nederlandse platformgebruikers voor elk ‘probleem’ met online content moderatie. Dit kan zelfs in de vorm van een gezamenlijk digitaal portaal als toegankelijke toegangspoort voor burgers, met een routewijzer die hen naar het juiste kanaal leidt.

- De functionele scheiding tussen melding en beoordeling versterkt de onafhankelijkheid.
- Een platformstructuur maakt het mogelijk om iteratief op te schalen, feedback te verzamelen en partners toe te voegen.
- Biedt een goede balans tussen transparantie, gebruikersvriendelijkheid en legitimiteit.

4.3 Scenario 3. Parallele ondersteuning van nieuwe ODSB en gecentraliseerd meldpunt

Beschrijving: In dit scenario kiest de overheid ervoor om twee gescheiden trajecten parallel te ondersteunen. Enerzijds wordt de oprichting van een nieuwe buitengerechtelijke geschilleninstantie (ODSB) ondersteund. Anderzijds ondersteunt de overheid de centralisatie van de bestaande meldpunten, bijvoorbeeld via de ondersteuning van een al bestaande organisatie die de rol van coördinerend meldpunt op zich neemt. Er is geen formele coördinatie, maar samenwerking kan gestimuleerd worden via vrijwillige afspraken of gedeelde technische standaarden.

Haalbaarheid

- Operationeel goed uitvoerbaar en relatief kostenefficiënt doordat gebruik gemaakt wordt van bestaande infrastructuur;
- Minder complex qua governance, mits heldere afbakening van verantwoordelijkheden;
- Wel risico op inconsistent gebruik door burgers bij gebrek aan centrale navigatie.

Wenselijkheid

- Sterke waarborg van onafhankelijkheid doordat meldfunctie en geschilinstantie strikt gescheiden blijven;
- Minder zichtbaar en minder toegankelijk voor gebruikers, zeker als zij zelf moeten achterhalen waar ze met hun probleem terecht kunnen;
- Beperkte mogelijkheid tot institutionele synergie of gezamenlijke beleidsfeedback.

4.4 Scenario 4: Versneld opstartscenario

Beschrijving: Dit scenario is een variant van de eerste drie scenario's, waarbij doelbewust wordt gekozen voor een intensieve samenwerking met een bestaande buitenlandse organisatie (met name User Rights of Appeals Centre Europe) die al over een technische backoffice voor geschilbehandeling beschikt.

Beide organisaties partners beschikken reeds over een volledig geautomatiseerde intake- en besluitvormingsketen, die makkelijk vertaald zou kunnen worden. Verder hebben zij verschillende manieren om om te gaan deadlinebeheer en beveiligde dataopslag. Interessant is vooral dat er gewerkt wordt met visueel ondersteunde beslisbomen die juridische normen gebaseerd op het EVRM vertalen naar de context van platformbesluiten. Daarbij krijgt het personeel direct meerdere relevante

handvaten die het kan gebruiken bij het nemen van een beslissing. Deze handvaten kunnen ook aangepast worden aan een Nederlandse context.

Het scenario kan geïntegreerd of gecoördineerd worden uitgevoerd, net zoals scenario 1 t/m 3 – het onderscheid zit niet in de governance-structuur, maar in de technische en operationele versnelling via hergebruik van bestaande infrastructuur, bijvoorbeeld door het nemen van een licentie op de ontwikkelde “legal-tech” infrastructuur.

Haalbaarheid:

- Kostenbesparend: de noodzaak om een nieuwe digitale infrastructuur te bouwen wordt grotendeels vermeden.
- Snelle implementatie: partnerorganisaties beschikken over gestandaardiseerde intakeprocedures, beslismodules, en praktijkervaring.
- Begeleide kennisoverdracht: partners zoals User Rights kunnen lokale teams trainen in het gebruik van de technologie, zonder dat directe afhankelijkheid ontstaat.

Wenselijkheid:

- Risico op afhankelijkheid van een externe leverancier of technologiepartij, zeker als het om een commerciële speler gaat.
- Mogelijkheid tot iteratieve opschaling: men kan starten met een beperkte functie (bijvoorbeeld voor één klachtencategorie zoals het verwijderen van content, en deze geleidelijk uitbreiden.
- Betere waarborgen voor uitlegbaarheid en transparantie: doordat beslissingen onderbouwd worden met toegankelijke motiveringen, is de kans groter dat platforms de aanbevelingen overnemen en dat gebruikers het proces als eerlijk ervaren.

5. Conclusie

De scenarioanalyse maakt duidelijk dat het opzetten van een DSA ODSB in Nederland een strategische uitdaging vormt. Er is een breed gedeeld gevoel onder stakeholders dat de huidige toegang tot effectieve moderatie van online inhoud voor Nederlandstalige gebruikers tekortschiet, en dat een ondersteunende structuur voor zowel meldingen als geschillenbeslechting wenselijk is. Tegelijkertijd bestaat er een duidelijke spanning tussen ambitie, snelheid, kosten, onafhankelijkheid en institutionele haalbaarheid. Deze conclusie beoogt de vier onderzochte scenario's in breder perspectief te plaatsen.

Het eerste scenario, de oprichting van een volledig geïntegreerd DSA-instituut, lijkt vanuit gebruikersperspectief het meest coherente model te bieden. Door meldingen en geschillenbeslechting te combineren binnen één entiteit ontstaat er een overzichtelijke en gebruiksvriendelijke infrastructuur. Dit zou niet alleen de toegankelijkheid voor burgers vergroten, maar ook synergiën mogelijk maken tussen signalering, escalatie en beleidsfeedback. Echter, dit scenario kent aanzienlijke financiële en institutionele drempels. Het vraagt een hoge initiële investering in personeel, IT-infrastructuur en communicatiecampagnes. De operationele

complexiteit en het risico op perceptie van belangenverstremming maken dat dit model op korte termijn waarschijnlijk weinig haalbaar is.

Het tweede scenario, een gecoördineerd netwerk met een aparte ODSB en meldpunten die onderling verbonden zijn via een centrale toegangspoort of kennisplatform, combineert veel van de voordelen van scenario 1 met mindere nadelen. Door functies te scheiden, maar samenwerking en doorverwijzing potentieel te faciliteren, kan een hoge mate van toegankelijkheid en transparantie worden bereikt zonder dat de onafhankelijkheid van de geschilinstantie in het geding komt. Dit scenario wordt door stakeholders als het meest wenselijk beschouwd. Dit scenario is bijzonder geschikt voor een modulair opgebouwde aanpak waarin verschillende onderdelen (meldportaal, intake, geschilbehandeling) stapsgewijs kunnen worden geactiveerd.

Scenario 3, waarbij de overheid tegelijkertijd een nieuwe ODSB ondersteunt en het bestaande meldlandschap centraliseert zonder institutionele koppeling, scoort hoog op uitvoerbaarheid, maar laat kansen liggen op het vlak van gebruikerservaring en structurele coördinatie. Het model biedt een duidelijke rolverdeling en minimaliseert het risico op belangenconflicten, maar het gebrek aan centrale toegang of gemeenschappelijk front-end zou kunnen leiden tot verwarring bij gebruikers. Ook de mogelijkheid om trends te signaleren of beleidsimpact te realiseren is beperkter wanneer meldpunten en geschilinstanties geen structureel overleg of informatiedeling organiseren. Dit scenario is vooral aantrekkelijk als tussenoplossing, bijvoorbeeld wanneer politieke of institutionele randvoorwaarden een nauwere samenwerking tijdelijk onmogelijk maken.

Het vierde scenario, het versneld opstarten van een ODSB via samenwerking met een bestaande buitenlandse organisatie, biedt de snelste route naar operationele capaciteit. Door gebruik te maken van een bestaande backoffice en juridische infrastructuur, kan Nederland binnen enkele maanden een functionerende geschilinstantie opzetten die voldoet aan de eisen van artikel 21 DSA. Tegelijk roept dit scenario vragen op over autonomie, technologische afhankelijkheid en publieke legitimiteit. Stakeholders hechten waarde aan transparantie, onafhankelijkheid en publieke verantwoording, en het is essentieel dat samenwerking met buitenlandse partners niet leidt tot verlies van zeggenschap over procedures, taaltoegankelijkheid of databeheer.



Evaluatie Wet digitale overheid

Colofon

Hooghiemstra & Partners
Bezuidenhoutseweg 161
2594 AG Den Haag

www.hooghiemstra-en-partners.nl
info@hooghiemstra-en-partners.nl

Dit onderzoek is uitgevoerd door Hooghiemstra & Partners, strategisch en juridisch adviesbureau op het raakvlak van data en recht.

Auteurs: Thijs Drouen, Riëlle Osepa, Helen Hukshorn, Theo Hooghiemstra.
Opdrachtgever: Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
Datum: 14 januari 2026
Status: definitief rapport

Begeleidingscommissie:

Prof. dr. ir. Nitesh Bharosa (Technische Universiteit Delft)
mr. Ludwig Oberendorff (Bureau Forum Standaardisatie)
drs. Mariska Zwinkels MPA (ministerie van Onderwijs, Cultuur en Wetenschap)
mr. drs. Odette Bies (ministerie van Binnenlandse Zaken en Koninkrijkrelaties)

Voor de inhoud van het rapport zijn de onderzoekers verantwoordelijk. Het leveren van een bijdrage (als medewerker van een organisatie of als lid van de begeleidingscommissie) betekent niet automatisch dat de betrokkene instemt met de gehele inhoud van het rapport. Dat geldt eveneens voor het ministerie van Binnenlandse Zaken en Koninkrijkrelaties en zijn minister.

©2026 Hooghiemstra & Partners. Auteursrechten voorbehouden.

Inhoudsopgave

Samenvatting	5
1. Aanpak van de evaluatie	9
1.1 Inleiding	9
1.2 Reikwijdte van de evaluatie	10
1.3 Centrale vraag	10
1.4 Opdrachtbeschrijving en methodiek	10
1.5 Leeswijzer	11
2. Voorgeschiedenis	12
2.1 Inleiding	12
2.2 Voorgeschiedenis eNIK in relatie tot de Wdo	12
2.3 Voorgeschiedenis DigiD in relatie tot de Wdo	12
2.4 Voorgeschiedenis eHerkenning in relatie tot de Wdo	13
2.5 Voorgeschiedenis eIDAS	14
2.6 Van Wetsvoorstel GDI naar Wet digitale overheid	15
2.7 Geschiedenis van de Wdo	16
3. Wettelijk kader	18
3.1 Inleiding	18
3.2 Doelen en gefaseerde inwerkingtreding van de Wdo	18
3.3 Reikwijdte	18
3.4 Standaarden	19
3.5 Werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten	20
3.6 Beheer van de generieke digitale infrastructuur	20
3.7 Toegang tot elektronische dienstverlening: betrouwbaarheidsniveaus	22
3.8 Toegang tot elektronische dienstverlening: gebruik in publiek domein	22
3.9 Toegang tot elektronische dienstverlening: regels ten aanzien van gebruik	23
3.10 Bescherming persoonsgegevens	23
3.11 Naleving	23
3.12 Experimenteerruimte	24
4. Het functioneren van de eerste fase van de Wdo	26
4.1 Inleiding	26
4.2 De keuze voor het gefaseerd in werking treden van de Wdo	26
4.3 Beperkt materieel effect en afhankelijkheid van andere ontwikkelingen	27
4.4 Implementatie Wdo	27
4.5 Standaarden	28
4.6 Stelsel toegang	29
4.7 Toegang tot elektronische dienstverlening	31
4.8 Naleving	33
5. Conclusie	34
5.1 Inleiding	34
5.2 Bevindingen	34
5.3 Aanbevelingen	36

Bijlage 1: Bronvermelding	38
Bijlage 2: Lijst van geïnterviewde organisaties	41

Samenvatting

Inleiding

De Wet digitale overheid (hierna: Wdo) is op 1 juli 2023 gedeeltelijk en daarmee gefaseerd in werking getreden. Op grond van artikel 23 Wdo dient de minister van Binnenlandse Zaken en Koninkrijksrelaties binnen drie jaar na de inwerkingtreding van de Wdo aan de Staten-Generaal een verslag te sturen over de doeltreffendheid en de effecten van de Wdo in de praktijk. Hierbij moet in het bijzonder aandacht worden geschonken aan de getroffen maatregelen op het gebied van beveiliging, privacybescherming en de toegankelijkheid van elektronische dienstverlening. De reikwijdte van de evaluatie zal zich daarmee beperken tot de eerste fase.

De centrale vraag van de evaluatie is:

In hoeverre is de Wdo doeltreffend en wat zijn de effecten van de Wdo, in het bijzonder op het gebied van beveiliging, privacybescherming en toegankelijkheid van elektronische dienstverlening in de praktijk?

Het vertrekpunt van de wetsevaluatie, zoals beschreven in dit rapport, is de doelen van de Wet digitale overheid. De wet beoogt de beweging naar de inzet van veiligere inlogmiddelen overheidsbreed te regelen en af te dwingen. In de kern bepaalt deze wet hoe de overheid op basis van dezelfde uitgangspunten en normen voldoet aan de eisen van de Algemene verordening gegevensbescherming (hierna: AVG) en de Europese verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (hierna: eIDAS-verordening). Verder dwingt de wet af dat alleen erkende en toegelaten inlogmiddelen voor toegang tot overheidsdienstverlening zijn toegestaan, maar biedt ook handvatten, waarmee overheidsdienstverleners het juiste beveiligingsniveau van hun digitale diensten kunnen bepalen.

Met het oog daarop is onderzoek gedaan naar de doeltreffendheid en de effecten van deze wet in de praktijk. In het bijzonder wordt hierbij volgens de evaluatiebepaling in de wet aandacht geschonken aan de getroffen maatregelen op het gebied van beveiliging, privacybescherming. Daarnaast wordt bijzondere aandacht geschonken aan de toegankelijkheid van elektronische dienstverlening. Hierbij dient in aanmerking te worden genomen dat een beperkt aantal artikelen op 1 juli 2023 in werking is getreden, waardoor de getroffen maatregelen op het gebied van beveiliging niet bij de evaluatie kunnen worden betrokken. De bepaling uit de wet die daarop ziet is nog niet van toepassing.

Methodiek

In dit rapport is gebruik gemaakt van drie onderzoeksmethoden om de wetsevaluatie uit te voeren, namelijk een literatuurstudie, diepte-interviews en het voorleggen van een vragenlijst aan het Ministerie van BZK ter validatie van de verkregen inzichten uit de diepte-interviews.

Het kwalitatieve (literatuur)onderzoek maakt gebruik van de wettekst, de parlementaire stukken die daaraan ten grondslag liggen en andere relevante publicaties. Deze laatstgenoemde publicaties betreft publiek beschikbare informatie. Vervolgens zijn diepte-interviews gehouden met personen die betrokken zijn geweest bij de totstandkoming van de wet en betrokken organisaties die uitvoering aan de wet geven. De inzichten van beide groepen zijn relevant om de effectiviteit en de doelmatigheid van de wet binnen drie jaar na de inwerkingtreding te kunnen vaststellen. Om de verkregen inzichten te valideren zijn een vijftiental controle vragen gesteld aan het Ministerie van BZK.

Tot slot is een diepte-interview gehouden met de Rijksinspectie Digitale Infrastructuur om zicht te krijgen op het toezicht op de Wdo. In dat licht is ook om een interview verzocht met de Autoriteit Persoonsgegevens (AP). Helaas heeft de AP geen medewerking kunnen verlenen aan een interview,

omdat de AP gedurende de periode waarop de evaluatie ziet geen noemenswaardige ervaringen heeft gehad met de Wdo.

Bevindingen

De onderzoekers zien in de Wdo, voor zover in werking getreden, een toereikend instrumentarium om het daarmee beoogde doel in de basis te kunnen bewerkstelligen. Daar staat tegenover dat de concrete uitvoering van de Wdo achter blijft bij wat de wet beoogt mogelijk te maken. Dit alles maakt dat de beantwoording van de centrale vraag beperkt blijft tot de meer algemene vraag of de Wdo doeltreffend en effectief is.

In de praktijk wordt in zeer beperkte mate uitvoering gegeven aan de Wdo. Hierdoor blijft het effect van de Wdo in de uitvoering uit. De reden waardoor dit effect uitblijft, is onder meer dat het daarvoor voorwaardelijke Stelsel Toegang, waarmee dienstverleners kunnen voldoen aan de geldende verplichtingen onder de Wdo, gedurende de evaluatieperiode in de praktijk niet gereed en operationeel was en ook thans nog niet is. Zo blijkt bijvoorbeeld dat de functionaliteit voor burgers om te komen tot betrouwbaarheidsniveau hoog ontoereikend is en deze functionaliteit slechts in geringe mate wordt gebruikt. Ook blijkt dat de voorzieningen voor ouderlijk gezag en bewindvoering, die onder de reikwijdte van artikel 5 zijn mogelijk gemaakt, zich nog in een pilotfase bevinden en dat het benodigde betrouwbaarheidsniveau met DigiD Machtigen (nog) niet kan worden verkregen. Bovendien is ondanks het technologie-neutrale karakter van de Wdo, DigiD het enige publieke middel. Daarmee wordt DigiD als single point of failure niet weggenomen.

Door het uitblijven van de uitvoering van de Wdo wordt afbreuk gedaan aan de relevantie van de Wdo voor die uitvoering. Het effect wordt nog eens versterkt doordat de planning van de tweede fase en de inwerkingtreding van de resterende artikelen van de eerste fase voor organisaties nog ongewis is, waardoor het voor organisaties lastig is om te anticiperen op de doorontwikkeling van de Wdo.

Een belangrijk positief punt van de eerste fase van de Wdo is dat het nadrukkelijk de verantwoordelijkheid van de minister van BZK voor het beheer van de voorzieningen en diensten binnen het Stelsel Toegang vastlegt. Bovendien lijkt de Wdo te hebben bijgedragen aan bewustwording rond veilig digitaal handelen en aan het bepalen van het juiste betrouwbaarheidsniveau bij digitale transacties. Ook heeft de minister van BZK – zij het terughoudend – gebruik gemaakt van zijn bevoegdheid om standaarden aan te wijzen.

Doordat aan het toezicht op de Wdo in de praktijk geen invulling is gegeven, is de naleving van de Wdo ook op deze onderdelen niet geborgd. Te meer nu ook de AP in het kader van het toezicht op de AVG gedurende de evaluatieperiode geen aandacht lijkt te hebben gehad voor de werking van de eerste fase van de Wdo. Daarnaast ontbreekt het BZK aan instrumenten om in de breedte het feitelijke effect – de zogenoemde outcome – van de uitvoering van de Wdo te monitoren. Waar het gaat om de verplichte open standaarden monitort het Forum Standaardisatie deze standaarden binnen de landelijke voorzieningen van de Generieke Diensten Infrastructuur (GDI) als onderdeel van de jaarlijkse monitor en metingen van het Forum Standaardisatie.

Positief is dat de Wdo voldoende mogelijkheden biedt voor de ontwikkeling van aanvullende GDI voorzieningen onder artikel 5, zoals door naast de bestaande voorziening voor vrijwillig machtigen tevens voorzieningen te ontwikkelen voor wettelijke vertegenwoordiging.

Ondanks dat dit buiten de reikwijdte van het onderzoek valt, kan als positief worden beoordeeld dat het stelsel van eHerkenning voor rechtspersonen op toereikende wijze functioneert, ondanks dat de bepaling over inlogmiddelen voor bedrijven in de Wdo nog niet in werking zijn getreden. In dat kader kan tevens worden gewezen op het feit dat er sprake is van actief toezicht. In het verlengde daarvan

wordt eveneens gewezen op DigiD dat op dit moment breed wordt gebruikt, maar niet breed beschikbaar is op betrouwbaarheidsniveau hoog.

Mede in het licht van de centrale onderzoeksvraag, vragen de onderzoekers in het bijzonder nog aandacht voor enkele gegevensbeschermingsrechtelijke aspecten.

Door het ontbreken van een in gebruik zijnde bevoegdheidsverklaringsdienst ten behoeve van de wettelijke vertegenwoordiging doet de situatie zich voor dat inloggegevens van DigiD door een betrokkene aan een ander beschikbaar worden gesteld om van elektronische dienstverlening gebruik te kunnen maken. Het risico op identiteitsfraude ligt daarmee op de loer.

Daarnaast ontbreekt het inzicht bij BZK of elektronische diensten het juiste betrouwbaarheidsniveau hanteren, waardoor het risico zich kan voordoen dat de vertrouwelijkheid van gegevens niet kan worden gewaarborgd.

Tenslotte kunnen elektronische diensten aan burgers die het betrouwbaarheidsniveau hoog vereisen momenteel niet op dit niveau worden geïmplementeerd aangezien er geen publiek middel breed beschikbaar is op dit niveau. Daarmee kunnen de overheidsdienstverleners en aangewezen organisaties in de huidige situatie bij elektronische diensten, die betrouwbaarheidsniveau hoog vereisen, niet voldoen aan de vereisten vanuit de AVG en eIDAS.

Aanbevelingen

De bovenstaande bevindingen brengen de onderzoekers tot de hiernavolgende aanbevelingen

Gelet op het benodigde draagvlak bij uitvoerende organisaties wordt aanbevolen om vanuit BZK de dialoog met het veld te intensiveren, zodat aan verwachtingenmanagement richting het speelveld kan worden gedaan.

Verwachtingenmanagement bij uitvoeringsorganisaties over de effectuering van het Stelsel Toegang en de inwerkingtreding van de rest van de artikelen van de eerste fase van de Wdo, is noodzakelijk om organisaties in de gelegenheid te stellen om in hun bedrijfsvoering op de (door)ontwikkeling van de Wdo te anticiperen. Dit vergt wel dat BZK transparant is naar betrokken organisaties wat het tijdschema is, waarbinnen deze ontwikkelingen zullen plaatsvinden en op welke wijze gewaarborgd wordt dat de gemaakte planning ook daadwerkelijk wordt gehaald. Dit biedt BZK bij uitstek de gelegenheid om het vertrouwen in de Wdo en de uitvoering daarvan te vergroten.

Aanbevolen wordt verder om duidelijk de samenhang in kaart te brengen tussen het huidige Stelsel Toegang en de huidige inlogmiddelen (DigiD voor burgers en eHerkenning voor rechtspersonen) en het stelsel dat noodzakelijk is voor de implementatie van de EDI-Wallet (inlogmiddel op hoog).

Ook wordt aanbevolen om het toezicht op de Wdo te heroverwegen. Haal het toezicht weg bij de minister van BZK en andere verantwoordelijke ministers en plaats het bij een toezichthouder die meer op afstand staat en onafhankelijk toezicht kan uitoefenen. Zet, gelet op de aard van het stelsel, in op stelseltoezicht, waardoor één toezichthouder in staat is het gehele stelsel te overzien en op het niveau van het stelsel kan ingrijpen in tegenstelling tot het meer fragmentarische toezicht waar de Wdo op dit moment in voorziet.

De onderzoekers vragen in het kader van het toezicht op de Wdo nog in het bijzonder aandacht voor het toezicht op de verplichte standaarden als bedoeld in artikel 3. De vrees bestaat bijvoorbeeld bij het Forum Standaardisatie dat geen toezichthouder zal worden aangewezen op toezicht op de desbetreffende standaarden te houden. Los van de aanbeveling om tot stelseltoezicht te komen,

bevelen de onderzoekers aan om vooruitlopend daarop in overweging te nemen om een toezichthouder aan te wijzen voor het toezicht op de verplichte standaarden als bedoeld in artikel 3.

Het is wenselijk om te onderzoeken of in een expliciete verplichting voor organisaties dient te worden voorzien om periodiek te toetsen of het vereiste betrouwbaarheidsniveau, gelet op technologische en organisatorische ontwikkelingen, is gewijzigd. Op deze wijze wordt geborgd dat het betrouwbaarheidsniveau actueel is en de vereiste bescherming biedt.

1. Aanpak van de evaluatie

1.1 Inleiding

De Wet digitale overheid (hierna: Wdo) is op 1 juli 2023 gedeeltelijk in werking getreden. Het wetsvoorstel werd op 19 juni 2018 ingediend bij de Tweede Kamer en op 18 februari 2020 aangenomen door de Tweede Kamer. Op 22 juni 2021 werd een novelle Wdo ingediend bij de Tweede Kamer. Aanleiding daarvoor waren met name zorgen vanuit de Eerste Kamer met betrekking tot privacybescherming, vanwege deelname aan het stelsel door private partijen.¹ Op 21 maart 2023 werd de Wdo ten slotte aangenomen door de Eerste Kamer.

In de Memorie van Toelichting bij het wetsvoorstel wordt verwezen naar het Regeerakkoord Vertrouwen in de toekomst (2017 – 2021) dat benadrukt dat aanpassing van de overheid aan de digitale samenleving niet alleen noodzakelijk is, maar dat het ook mogelijkheden biedt voor betere dienstverlening. Het kabinet ontwikkelt daartoe een brede en ambitieuze agenda voor de verdere digitalisering van het openbaar bestuur op verschillende niveaus. De Wdo, zo wordt aangegeven, past in die ambitie en legt de basis voor die verdere digitalisering waaronder de regulering van de digitale overheid en meer in het bijzonder de generieke digitale voorzieningen in een gemeenschappelijke infrastructuur van de overheid.

De Wdo vormt een eerste tranche van regelgeving ten behoeve van deze verdere digitalisering van de overheid en bevat de meest urgente onderwerpen van regelgeving, te weten:

- de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid;
- het stellen van regels over informatieveiligheid;
- de verantwoordelijkheid van de Minister van BZK 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).²

De Wdo beoogt kaderstellend te zijn voor verdere ontwikkeling op basis van de hiervoor genoemde maatregelen en biedt nadrukkelijk de basis voor verdere uitbreidingen en modernisering. De Wdo is technologie-neutraal geformuleerd, waardoor er geen afhankelijkheid mag zijn van gebruikte technologieën. De bepalingen zijn functioneel geformuleerd, in zeer nauwe samenspraak met de uitvoeringsorganisatie en de ontwerpers van de technische systemen. De wet bevat kaders die kunnen worden uitgewerkt in nadere regelgeving. Deze nadere regelgeving kan snel worden aangepast om ruimte te bieden voor verdere ontwikkeling van de digitale overheid. Bij de inwerkingtreding van de Wdo is uitgegaan van een gefaseerde aanpak, om systemen en uitvoeringsorganisaties binnen het eigen tempo te faciliteren.

Evaluatiebepaling

Op grond van artikel 23 Wdo dient de minister van Binnenlandse Zaken en Koninkrijksrelaties binnen drie jaar na de inwerkingtreding van de Wdo aan de Staten-Generaal een verslag te sturen over de doeltreffendheid en de effecten van de Wdo in de praktijk. Hierbij moet in het bijzonder aandacht worden geschonken aan de getroffen maatregelen op het gebied van beveiliging, privacybescherming en de toegankelijkheid van elektronische dienstverlening.

¹ EK 34 972 /35 868, W1.

² Kamerstukken II 2017/18, 34972, nr. 3, p. 1.

1.2 Reikwijdte van de evaluatie

De Wdo biedt de mogelijkheid om het tijdstip voor inwerkingtreding voor de verschillende artikelen of onderdelen daarvan verschillend te kunnen vaststellen om rekening te houden met de uitvoeringspraktijk. Zoals eerder aangegeven, is de Wdo gedeeltelijk en daarmee gefaseerd in werking getreden. De reikwijdte van de evaluatie zal zich daarmee beperken tot de eerste fase. De volgende artikelen in de Wdo zijn (gedeeltelijk) in werking getreden:

- Artikel 1 Definities;
- Artikel 2 Reikwijdte;
- Artikel 3 Standaarden;
- Artikel 5 Verantwoordelijkheid voor het beheer (gedeeltelijk);
- Artikel 6 Betrouwbaarheidsniveaus
- Artikel 8 Gebruik in publieke domein
- Artikel 10 Regels ten aanzien van gebruik;
- Artikel 16 Bescherming persoonsgegevens (gedeeltelijk);
- Artikel 17 Toezicht en handhaving (gedeeltelijk);
- Artikel 18 Bijzondere bevoegdheden;
- Artikel 19 Informatieverstrekking;
- Artikel 20 Leges voor verstrekking publiek identificatiemiddel;
- Artikel 23 Evaluatie;
- Artikel 25 Parlementaire betrokkenheid bij gedelegeerde regelgeving;
- Artikel 26 Experimenteeruimte;
- Artikel 28 Omhangen;
- Artikel 29 Inwerkingtreding; en
- Artikel 30 Citeertitel.

1.3 Centrale vraag

De centrale vraag van de evaluatie is:

In hoeverre is de Wdo doeltreffend en wat zijn de effecten van de Wdo, in het bijzonder op het gebied van beveiliging, privacybescherming en toegankelijkheid van elektronische dienstverlening in de praktijk?

1.4 Opdrachtbeschrijving en methodiek

Dit rapport bevat het verslag van het onderzoek 'Evaluatie Wet digitale overheid' dat in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (hierna: BZK) is uitgevoerd door Hooghiemstra & Partners. Aanleiding voor dit onderzoek is de toezegging aan de Tweede Kamer om de Wdo binnen drie jaar na de inwerkingtreding te evalueren. De Wdo is op 1 juli 2023 gedeeltelijk in werking getreden.

Het vertrekpunt van de wetsevaluatie, zoals beschreven in dit rapport, is de doelen van de Wet digitale overheid. De wet beoogt de beweging naar de inzet van veiligere inlogmiddelen overheidsbreed te regelen en af te dwingen. In de kern bepaalt deze wet hoe de overheid op basis van dezelfde uitgangspunten en normen voldoet aan de eisen van de Algemene verordening gegevensbescherming (hierna: AVG) en de Europese verordening betreffende elektronische identificatie en

vertrouwensdiensten voor elektronische transacties in de interne markt (hierna: eIDAS-verordening).³ Verder dwingt de wet af dat alleen erkende en toegelaten inlogmiddelen voor toegang tot overheidsdienstverlening zijn toegestaan, maar biedt ook handvatten, waarmee overheidsdienstverleners het juiste beveiligingsniveau van hun digitale diensten kunnen bepalen.

Met het oog daarop is onderzoek gedaan naar de doeltreffendheid en de effecten van deze wet in de praktijk. In het bijzonder wordt hierbij volgens de evaluatiebepaling in de wet aandacht geschonken aan de getroffen maatregelen op het gebied van beveiliging, privacybescherming. Daarnaast wordt bijzondere aandacht geschonken aan de toegankelijkheid van elektronische dienstverlening. Hierbij dient in aanmerking te worden genomen dat een beperkt aantal artikelen op 1 juli 2023 in werking is getreden, waardoor de getroffen maatregelen op het gebied van beveiliging niet bij de evaluatie kunnen worden betrokken. De bepaling uit de wet die daarop ziet is nog niet van toepassing.

In dit rapport is gebruik gemaakt van drie onderzoeksmethoden om de wetsevaluatie uit te voeren, namelijk een literatuurstudie, diepte-interviews en het voorleggen van een vragenlijst aan het Ministerie van BZK ter validatie van de verkregen inzichten uit de diepte-interviews. Het kwalitatieve (literatuur)onderzoek maakt gebruik van de wettekst, de parlementaire stukken die daaraan ten grondslag liggen en andere relevante publicaties. Deze laatstgenoemde publicaties betreft publiek beschikbare informatie. Vervolgens zijn diepte-interviews gehouden met personen die betrokken zijn geweest bij de totstandkoming van de wet en betrokken organisaties die uitvoering aan de wet geven. De inzichten van beide groepen zijn relevant om de effectiviteit en de doelmatigheid van de wet binnen drie jaar na de inwerkingtreding te kunnen vaststellen. Om de verkregen inzichten te valideren zijn een vijftiental controle vragen gesteld aan het Ministerie van BZK. Tot slot is een diepte-interview gehouden met de Rijksinspectie Digitale Infrastructuur om zicht te krijgen op het toezicht op de Wdo. In dat licht is ook om een interview verzocht met de Autoriteit Persoonsgegevens (AP). Helaas heeft de AP geen medewerking kunnen verlenen aan een interview, omdat de AP gedurende de periode waarop de evaluatie ziet geen noemenswaardige ervaringen heeft gehad met de Wdo.

1.5 Leeswijzer

Hierna gaan we in hoofdstuk 2 in op de geschiedenis die voorafging aan de totstandkoming van de Wdo. Hoofdstuk 3 betreft een analyse van de eerste fase van het wettelijk kader, waarbij de bevindingen uit de interviews zijn betrokken. In hoofdstuk 4 gaan we in op het functioneren van de eerste fase van de Wdo. Vervolgens volgen in hoofdstuk 5 de bevindingen van het onderzoek. Tot slot volgt in hoofdstuk 6 de beantwoording van de onderzoeksvraag en volgen enkele aanbevelingen.

³ Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

2. Voorgeschiedenis

2.1 Inleiding

De Wdo is de uitkomst van ruim vijftientig jaar geleidelijk evoluerend beleid en regelgeving rond digitalisering van de overheid, voortbouwend op Europese en internationale verplichtingen.

Sinds het eind van de jaren '80 in de vorige eeuw is de basis gelegd voor wat nu de Wdo is. In de Beleidsnota Informatievoorziening Openbare Sector (BIOS 1) (1988) en later in de Nota elektronische overheid (2004)⁴ werd al gesproken over het belang van elektronische identificatiemiddelen voor burgers. Dit vormt één van de eerste beleidsmatige kaders waaruit het concept van de elektronische Nederlandse Identiteits Kaart (eNIK) en de latere Wdo konden ontstaan. Om de Wdo goed te kunnen begrijpen is de voorgeschiedenis en relatie met de Wdo van belang. Daarbij gaat het met name om de eNIK; DigiD, eHerkenning en de eIDAS (Electronic Identification, Authentication and trust Services) - verordening. Achtereenvolgens komen deze relevante kaders en ontwikkelingen uit de voorgeschiedenis van de Wdo aan de orde.

2.2 Voorgeschiedenis eNIK in relatie tot de Wdo

Er is een duidelijke relatie tussen de voorgeschiedenis van de eNIK en de Wdo.⁵ De eNIK was bedoeld als een veilig elektronisch identificatiemiddel waarmee burgers zich bij de overheid online konden identificeren.⁶ De rechter heeft op dinsdag 18 september 2007 bepaald dat het ministerie van BZK de productie van de eNIK moest aanbesteden.⁷ Het centrale idee van de eNIK – veilige, gestandaardiseerde digitale toegang tot overheidsdiensten – is één van de kernpunten van de huidige Wdo. De eNIK heeft inzichten opgeleverd die de Wdo beoogt te benutten, zoals de noodzaak voor duidelijke betrouwbaarheidsniveaus en interoperabiliteit met Europese eID-stelsels. De ervaringen met de eNIK zijn onderdeel van de bredere voorgeschiedenis en beleidsontwikkeling rond digitale identificatie, standaardisatie en veiligheid, waarop de Wdo expliciet voortbouwt. De geleerde lessen van de eNIK hebben rechtstreeks bijgedragen aan de opzet en de inhoud van de Wdo, evenals de opgedane lessen met DigiD, eHerkenning en de eIDAS-verordening.

2.3 Voorgeschiedenis DigiD in relatie tot de Wdo

DigiD is het Nederlandse systeem waarmee burgers zich digitaal kunnen authenticeren bij overheidsdiensten. Het werd in 2003 gelanceerd als de "Nieuwe Authenticatie Voorziening" (ook wel Burgerpin genoemd) en heeft zich sindsdien ontwikkeld tot de kern van het digitale identificatie- en authenticatiestelsel van de Nederlandse overheid. De naam DigiD bestaat sinds 2004.⁸

Eind jaren '90 ontstond de behoefte aan een overheidsbrede authenticatievoorziening als onderdeel van het actieprogramma Elektronische Snelwegen en verdere digitaliseringsinitiatieven van de overheid. DigiD werd ontwikkeld door stichting ICTU in opdracht van het ministerie van Binnenlandse

⁴ Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 'De elektronische overheid', *kennisvandeoverheid.nl*. Zie ook *Kamerstukken II*, 2003/04, 26 643, nr. 47.

⁵ Zie ook Internetconsultatie Wijziging Paspoortwet i.v.m. introductie elektronische identificatie I, *internetconsultatie.nl*.

⁶ Zie ook Vertegenwoordiging van Nederland in Aruba, Curaçao en St. Maarten, 'eNIK aanvragen', *nasc.nl*.

⁷ Rb. 's-Gravenhage 18 september 2007, ECLI:NL:RBSGR:2007:BB5302. Zie ook Hof: Gerechtshof 's-Gravenhage 13 december 2007, ECLI:NL:GHSGR:2007:BC0036.

⁸ Logius, 'DigiD door de jaren heen', onder 2004, *logius.nl*.

Zaken en de Vereniging van Nederlandse Gemeenten, met ondersteuning van het Bureau Keteninformatisering Werk en Inkomen (BKWI). Het beheer ging achtereenvolgens van de Belastingdienst naar Logius, het huidige beheerorgaan.

DigiD begon als gebruikersnaam-wachtwoord oplossing en werd later versterkt met extra beveiligingsmogelijkheden, zoals sms-authenticatie en het scannen van een fysieke ID of paspoort.

In 2006 werd DigiD verplicht voor elektronische belastingaangifte door burgers. Sindsdien neemt het gebruik jaarlijks toe.⁹ DigiD voor bedrijven werd vervangen door het afsprakenstelsel eHerkenning, waarover hierna meer.

DigiD vormt de praktische en technische basis onder de uitvoering van de Wdo.

De historie en de technische positionering van DigiD zijn grotendeels leidend voor het ontwerp en de standaarden van de Wdo, in samenwerking met de praktijk.

2.4 Voorgeschiedenis eHerkenning in relatie tot de Wdo

Het afsprakenstelsel eHerkenning is halverwege 2010 in werking getreden als zakelijk inlogstelsel waarmee bedrijven, organisaties en intermediairs zich digitaal kunnen identificeren en veilig zaken kunnen doen met (overheids)dienstverleners.¹⁰ eHerkenning is het publiek-private afsprakenstelsel dat regelt dat bedrijven zich digitaal kunnen authenticeren en autoriseren wanneer ze online zaken regelen met de overheid en met private partijen.¹¹ De aanleiding voor eHerkenning was de behoefte aan een veilige, gestandaardiseerde manier voor bedrijven om online toegang te krijgen tot allerlei diensten, vergelijkbaar met DigiD voor burgers, maar dan via marktwerking gericht op het bedrijfsleven.

De middelen van eHerkenning worden uitgegeven door gecertificeerde private partijen, terwijl de overheid civielrechtelijk toezicht houdt door gebruik te maken van het zogeheten Elektronische Toegangsdiensten-afsprakenstelsel. Als toezichthouder op het stelsel voor elektronische toegangsdiensten (ETD) werd 14 april 2016 door de Minister van Economische Zaken de Commissie van Deskundigen (CvD van het ETD-stelsel) ingesteld.¹²

Gedurende de eerste jaren lag de focus op het aansluiten van overheidsdiensten, met als mijlpaal de opname van partijen als UWV en Belastingdienst.¹³

Er vonden ook pilots bij diverse zorgpartijen, gemeenten en de Belastingdienst plaats met Idensys: het afsprakenstelsel eHerkenning voor burgers. Idensys was gericht op een geïntegreerd eID-stelsel voor burgers en bedrijven.¹⁴ Deze pilots zijn beëindigd op 31 december 2018. Ook de pilots met iDIN, het inlogmiddel via banken, werden toen beëindigd door het ministerie van BZK. Later is het gebruik van eHerkenning als bedrijvenmiddel gegroeid, met steeds meer aangesloten (semi-)overheden,

⁹ Zie ook Digital Government, DigiD Usage Reaches 550 Million Logins in 2024, 6 februari 2025, *ndigitalgovernment.nl*.

¹⁰ Logius, 'DigiD door de jaren heen', onder 2010, *logiul.nl*.

¹¹ Logius, 'Begrippenlijst', onder eHerkenning, *logius.nl*.

¹² Besluit van de Minister van Economische Zaken tot instelling van de Commissie van Deskundigen voor toezicht op het ETD-stelsel, van 14 april 2016 (Stcrt, 2016, 20595).

¹³ eHerkenning, 'Aansluiten op eHerkenning', onder Wat zijn de voordelen van aansluiten op eHerkenning?'. Eherkenning.nl.

¹⁴ Hooghiemstra & Partners, 'Rapport Strategische visie Plan van Aanpak geïntegreerd eID-stelsel', 22 april 2020, *hooghiemstra-en-partners.nl*.

gemeenten en private partijen. Inmiddels zijn er meer dan een miljoen zakelijke gebruikers en wordt er dagelijks veelvuldig ingelogd met eHerkenning.¹⁵

De Rijksdienst voor Ondernemend Nederland (RVO) verplicht sinds 2015 eHerkenning. Daarnaast verplicht de Belastingdienst sinds 2022 eHerkenning voor toegang tot het ondernemersportaal. De Wdo vormt de basis voor het nieuwe toegangsstelsel, dat de bestaande systemen samenbrengt waarin ruimte is voor private samenwerking onder publieke governance.¹⁶

2.5 Voorgeschiedenis eIDAS

De voorgeschiedenis van de eIDAS-verordening begint met de groeiende behoefte om elektronische identificatie, authenticatie en vertrouwensdiensten in Europa te standaardiseren. In de jaren 2000 ontstond vanuit de EU de wens om digitale economische groei te stimuleren door veilige, grensoverschrijdende digitale interactie mogelijk te maken. De eerste stap was Richtlijn 1999/93/EG over elektronische handtekeningen, maar deze was beperkt omdat die alleen elektronische handtekeningen regelde en niet voorzorg in een breed interoperabel systeem.

Projecten als STORK en STORK 2.0¹⁷ toonden aan dat erkenning van nationale eID's tussen landen technisch mogelijk was, maar er was geen bindend juridisch kader. Dit leidde tot het opstellen van de eIDAS-verordening, die een juridisch kader biedt voor wederzijdse erkenning van elektronische identificatiemiddelen en vertrouwensdiensten binnen de EU. Op 20 mei 2024 is eIDAS 2.0 in werking getreden¹⁸, waarmee nieuwe vertrouwensdiensten zijn geregeld, zoals de Europese digitale portefeuille.¹⁹

eIDAS verplicht overheidsinstanties in Nederland om digitale inlogmiddelen uit andere lidstaten te accepteren die voldoen aan eIDAS; dit betekent dat burgers en bedrijven uit andere lidstaten met erkende Europese inlogmiddelen toegang moeten krijgen tot Nederlandse (overheids)diensten en Nederlandse burgers toegang moeten krijgen tot (overheids)diensten in andere lidstaten met de Nederlandse erkende Europese inlogmiddelen.²⁰ Het toepassingsbereik van eIDAS is grensoverschrijdend.

De eIDAS-verordening en de uitvoeringsverordeningen van de Europese Commissie vormen de basis voor de uitvoering van de Wdo, voor zover het de inlogmiddelen betreft.²¹ Het doel is dat de Nederlandse digitale infrastructuur direct aansluit op de uitgangspunten en technische vereisten van eIDAS, zodat burgers en bedrijven eenvoudiger en veiliger grensoverschrijdend online zaken kunnen doen. De Wdo regelt de acceptatieplicht van digitale inlogmiddelen voor overheidsinstanties als het gaat om nationale dienstverlening, dit artikel van de Wdo is nog niet in werking getreden.

Naast de regels over inlogmiddelen is er ook gewerkt aan het opstellen van normen om dienstverleners te helpen hun dienstverlening in te schalen naar betrouwbaarheidsniveau aan de hand van risico inschatting. Het Forum Standaardisatie heeft op basis van eIDAS in 2016 de Handreiking Betrouwbaarheidsniveaus versie 4 uitgebracht. De eerste versie van deze handreiking, toen nog

¹⁵ Logius, 'Ruim één miljoen gebruikers eHerkenning', 15 januari 2024, *logius.nl*

¹⁶ Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 'Stelsel toegang: wat dienstverleners kunnen verwachten', 21 juni 2024, *digitaleoverheid.nl*.

¹⁷ STORK en STORK 2.0 zijn voorlopers van eIDAS wat betreft grensoverschrijdende identificatie, authenticatie, betrouwbaarheidsniveaus, definities en infrastructuur.

¹⁸ Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit

¹⁹ European Commission, 'The EU Digital Identity Framework Regulation Enters into Force', 21 mei 2024

²⁰ In Nederland zijn DigiD en eHerkenning Europees erkende inlogmiddelen.

²¹ *Kamerstukken II*, 2017/18, 34 972, nr. 3, p. 44-45.

gebaseerd op STORK en het beveiligingsadvies van de Autoriteit Persoonsgegevens²², dateert van 2011. De meest recente versie van de Handreiking betrouwbaarheidsniveaus van het Forum Standaardisatie is overigens verschenen in november 2024.²³

2.6 Van Wetsvoorstel GDI naar Wet digitale overheid

De oorspronkelijke naam van de Wdo was Wet Generieke digitale infrastructuur (Wet GDI). Dit wetsvoorstel was bedoeld om te voorzien in de basis-infrastructuur voor digitale diensten van zowel overheden als bedrijven en betrof een samenvoeging van twee wetgevingstrajecten:

- 1) Een wet voor elektronisch zakendoen voor bedrijven (vanuit het ministerie van EZ);
- 2) Een wet elektronisch zakendoen voor burgers (vanuit het ministerie BZK).

In 2016 werden beide wetgevingstrajecten samengevoegd tot het wetsvoorstel GDI.²⁴

Het belangrijkste doel van het wetsvoorstel GDI was het verplichten van open standaarden voor elektronisch verkeer, het verbeteren van informatieveiligheid, en het bevorderen van veilige en betrouwbare digitale toegang voor burgers en bedrijven tot (semi)overheidsdiensten.²⁵

De GDI is de verzameling van generieke voorzieningen, standaarden en afspraken die door de hele publieke sector worden gebruikt, zoals DigiD, het stelsel van basisregistraties, en de MijnOverheid-berichtenbox.²⁶ Gezamenlijk vormen deze bouwstenen het fundament voor digitale publieke dienstverlening.

De vraag was of de GDI een wet van een voorziening of van functionaliteiten zou worden. Bij de totstandkoming van het wetsvoorstel GDI is rekening gehouden met de inbreng van onder andere de ministeries van OCW en VWS om rekening te houden met de aansluiting op de domeinspecifieke basisinfrastructuur op basis van functionaliteiten en een multimiddelenstrategie.²⁷

De Wet GDI markeerde het begin van de wettelijke verankering van digitale basisvoorzieningen voor de overheid en transformeerde in de Wdo.²⁸

²² Autoriteit Persoonsgegevens, brief aan de Minister van Volksgezondheid, Welzijn en Sport inzake patiëntauthenticatie van 4 oktober 2018.

²³ Forum Standaardisatie, 'Handreiking betrouwbaarheidsniveaus voor digitale dienstverleners', versie 5 (2024), forumstandaardisatie.nl.

²⁴ Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 'Wdo biedt toekomstbestendige basis voor digitale overheid', 4 mei 2023, digitaleoverheid.nl.

²⁵ VNG, 'Wet Digitale Overheid', 26 november 2024, vng.nl.

²⁶ VNG, 'Generieke Digitale Infrastructuur (GDI)', vng.nl.

²⁷ Ministerie van Onderwijs, Cultuur en Wetenschap, 'Nota Aanvulling op OCW-consultatie wet GDI', 7 september 2017.

²⁸ Forum Standaardisatie, 'Wet GDI wordt Wet digitale overheid', 20 november 2017, forumstandaardisatie.nl. Zie ook Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 'Wdo biedt toekomstbestendige basis voor digitale overheid', 4 mei 2023, digitaleoverheid.nl.

2.7 Geschiedenis van de Wdo

2.7.1 Parlementaire behandeling Wdo

Het wetsvoorstel Wdo werd op 19 juni 2018 ingediend bij de Tweede Kamer en op 18 februari 2020 aangenomen.²⁹ Hieraan voorafgaand en gedurende het proces vonden diverse technische briefings en consultaties plaats, onder andere bij de vaste Kamercommissie voor Digitale Zaken.³⁰

Tijdens de totstandkoming uitte onder andere gemeenten (VNG) zorgen over de uitvoerbaarheid en financiering van de wet.

Op 7 juni 2022 werd een novelle ter wijziging van de wet aangenomen door de Tweede Kamer.³¹ De kern van de discussie met het parlement vormde de kritische houding van het parlement over de inzet van private aanbieders van inlogmiddelen, onder gesternte van de inmiddels opgelaaide discussie over de macht van grote ICT bedrijven en de afhankelijkheid daarvan. Zowel qua privacy als verdienmodel.

Bij de totstandkoming van de Wdo is in het parlement een golfbeweging te zien van meer marktwerking naar uiteindelijk de wens voor meer publiek. Dit verklaart in belangrijke mate de inrichting van de Wdo: een systematiek waarin zowel publieke als private inlogmiddelen hun plaats hebben, met specifieke waarborgen voor inzet van private partijen.

De opname van de onderstaande eisen is vanuit het parlement randvoorwaardelijk geweest om private inlogmiddelen toe te staan. Het gaat om de volgende voorwaarden:

- 1) Versterking privacy- en gegevensbescherming: De eisen rond privacy by design zijn door de novelle duidelijker en steviger in de Wdo zelf vastgelegd in plaats van vooral in lagere regelgeving. Dit houdt in dat bij alle digitale processen rond de Wdo privacy en gegevensbescherming vanaf het begin volgens wettelijke kaders moet worden meegenomen en geborgd;
- 2) Verhandelverbod gegevens: De novelle heeft het verbod op handel in persoonsgegevens wettelijk vastgelegd. De wet bepaalt nu expliciet dat gegevens die in het kader van de Wdo worden verwerkt, niet mogen worden verhandeld, wat vooral relevant is vanwege de betrokkenheid van private technologiebedrijven.
- 3) Verankering opensource-eis: Er is een verplichting tot gebruik van opensource-oplossingen zo veel mogelijk in de wet zelf vastgelegd. Dit is bedoeld om transparantie, controleerbaarheid en beveiliging te vergroten.³²
- 4) Parlementaire controle en wetgevingsniveau door voorhangprocedures: het parlement krijgt zo meer invloed op de uitwerking van de regels in algemene maatregelen van bestuur;
- 5) Specifieke vereisten voor publieke en private inlogmiddelen: De novelle voegt de onder 1 tot en met 3 genoemde eisen toe voor zowel publieke als private toegangsmiddelen, met aandacht voor de bescherming van persoonsgegevens van gebruikers.

Deze aanpassingen zijn gedaan op verzoek van de Eerste Kamer en vormen een reactie op knelpunten en zorgen die leefden rond het oorspronkelijke wetsvoorstel, vooral op het terrein van privacy, marktwerking, en parlementaire zeggenschap.

De Eerste Kamer behandelde het wetsvoorstel en de novelle op 21 maart 2023 en heeft deze beide aangenomen.³³ De stemming liet een meerderheid zien voor beide onderdelen, maar er was politieke

²⁹ Eerste Kamer, 'Wet digitale overheid'.

³⁰ Eerste Kamer, 'Wet digitale overheid'.

³¹ Eerste Kamer, 'Novelle Wet digitale overheid'.

³² Eerste Kamer, 'Novelle Wet digitale overheid'.

³³ Eerste Kamer, 'Wet digitale overheid' en Eerste Kamer, 'Novelle Wet digitale overheid'.

verdeeldheid, met zowel voor- als tegenstemmen uit verschillende partijen. De grootste zorgen hadden veel politieke partijen op dat moment over het toelaten van private partijen.

De Wdo wordt vanaf 1 juli 2023 in fases ingevoerd.³⁴

Samengevat laat de parlementaire geschiedenis van de Wdo een langdurig traject zien, met meerdere consultatierondes, technische en juridische discussies, aanpassingen via een novelle en uiteindelijke aanname door beide Kamers, waarna gefaseerde invoering in 2023 is gestart.

³⁴ Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Wet digitale overheid op 1 juli van kracht', 30 juni 2023, [digitaleoverheid.nl](https://www.digitaleoverheid.nl).

3. Wettelijk kader

3.1 Inleiding

Dit hoofdstuk geeft een omschrijving van het wettelijk kader van de Wdo, voor zover dat op 1 juli 2023 van toepassing is geworden.³⁵ In dat licht worden de meest relevante onderdelen van de wet behandeld. Voor dit hoofdstuk zijn de Kamerstukken over de Wdo (34 972) geanalyseerd. Om de achtergrond van deze wet nader te doorgronden zijn tevens relevante inzichten uit de gehouden interviews bij de analyse betrokken.

De Wdo heeft het karakter van een kaderwet, waarin hoofdzaken zijn geregeld en het om redenen van flexibiliteit door de wetgever opportuun werd geacht om door middel van delegatiebepalingen gedetailleerde (technische) uitwerking van de wet in de uitvoering vorm te geven.³⁶

3.2 Doelen en gefaseerde inwerkingtreding van de Wdo

De Wdo beoogt de beweging naar de inzet van veiligere inlogmiddelen overheidsbreed te regelen en af te dwingen. In de kern bepaalt deze wet hoe de overheid op basis van dezelfde uitgangspunten en normen voldoet aan de eisen van de AVG en de eIDAS-verordening. Verder dwingt de wet standaarden af, zoals het alleen nog toestaan van erkende en toegelaten inlogmiddelen, maar biedt ook handvatten, waarmee overheidsdienstverleners het juiste beveiligingsniveau van hun digitale diensten kunnen bepalen.³⁷ De Wdo is daarmee primair gericht op de publieke digitale dienstverlening en niet zoals veel andere wetgeving direct op de burger.

3.3 Reikwijdte

De *hoofdstukken 4 tot en met 7* van deze wet die zien op generieke digitale infrastructuur, toegang tot elektronische dienstverlening, bescherming van persoonsgegevens, naleving en financiële bepalingen, zijn van toepassing wanneer het gaat om het verlenen van elektronische diensten aan natuurlijke personen, ondernemingen of rechtspersonen ter uitoefening van een publieke taak, in het algemeen belang of waarbij het burgerservicenummer wordt verwerkt, door een bestuursorgaan in de zin van artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht³⁸, waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog is vereist.³⁹

Naast a-bestuursorganen, vallen eveneens onder de reikwijdte van de hoofdstukken 4 tot en met 7 van deze wet de organisaties behorende tot een in de bijlage bij de wet aangewezen categorie alsmede de organisaties die bij besluit van de Minister van Binnenlandse Zaken en Koninkrijkrelaties (hierna: de minister) in overeenstemming met de betrokken vakminister zijn aangewezen.⁴⁰ Het gaat hierbij om semipublieke of private organisaties die elektronische diensten verlenen ter uitoefening van een publieke taak, in het algemeen belang of waarbij het burgerservicenummer wordt verwerkt, waarvoor eveneens authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is. Gedacht kan

³⁵ Stb. 2023, 160.

³⁶ *Kamerstukken II*, 2017/18, 34 972, nr. 3, p. 24.

³⁷ *Kamerstukken II*, 2019/20, 34 972, nr. 37, p. 1.

³⁸ Het gaat het om de organen van rechtspersonen die krachtens publiekrecht zijn ingesteld. Het gaat dan om alle organen van bijvoorbeeld het Rijk, provincies, gemeenten en waterschappen en uitvoeringsinstanties, zoals bijvoorbeeld de Dienst Uitvoering Onderwijs, de Belastingdienst en zelfstandige bestuursorganen als de Sociale Verzekeringsbank, de Kamer van Koophandel, de Rijksdienst voor het Wegverkeer en de Huurcommissie.

³⁹ Artikel 2, eerste lid, in samenhang gezien met artikel 6, tweede lid. Zie ook *Kamerstukken II*, 2017/18, 34 972, nr. 3, p. 56.

⁴⁰ Artikel 2, tweede lid.

daarbij worden aan de zorgsector, onderwijsinstellingen en pensioenfondsen. De a-bestuursorganen en aangewezen organisaties worden in dit kader aangeduid als dienstverleners.⁴¹ De rechtspraak, inclusief de Afdeling Bestuursrechtspraak van de Raad van State, is in deze wet gelijkgesteld aan de a-bestuursorganen en de aangewezen organisaties.⁴²

De verplichting tot de toepassing van aangewezen *standaarden* heeft een ruime reikwijdte en strekt zich uit tot bestuursorganen in de zin van artikel 1:1, eerste lid, van de Algemene wet bestuursrecht, organen, personen en colleges als bedoeld in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht en rechtspersonen met een wettelijke taak (hierna: RWT), zoals bijvoorbeeld onderwijsinstellingen en academische ziekenhuizen.⁴³ Deze verplichting is niet van toepassing op aangewezen organisaties.

Overigens moet in dit kader worden opgemerkt dat bij de aanwijzing van een open standaard het toepassingsbereik nader wordt omschreven, zo wordt bepaald voor welke (bestuurs)organen, colleges en RWT's de standaard toepasselijk zijn, in welke gevallen en vanaf welk moment. Hierbij kan het toepassingsbereik van de aangewezen standaard beperkter zijn. Zo kan een open standaard bijvoorbeeld niet geschikt zijn om door b-bestuursorganen of door RWT's te worden toegepast. Het toepassingsbereik wordt dus per geval, dat wil zeggen per aan te wijzen standaard, worden geregeld.⁴⁴

3.4 Standaarden⁴⁵

De wet voorziet in een bevoegdheid voor de minister om, wanneer dit noodzakelijk en proportioneel is voor de werking, de veiligheid, de betrouwbaarheid of de doelmatigheid van het elektronische verkeer of indien dit voortvloeit uit internationale verplichtingen (waaronder mede begrepen EU-regelgeving), bij algemene maatregel van bestuur een toe te passen open standaard dwingend voor te schrijven. De verwachting van de wetgever was dat inherent aan de criteria, noodzakelijkheid en proportionaliteit in relatie tot werking, veiligheid, betrouwbaarheid en doelmatigheid van het elektronisch verkeer met de bevoegdheid tot aanwijzing terughoudend wordt omgegaan en dat het de beschikbare lijst van open standaarden in zijn geheel en/of voor de gehele (semi)publieke sector niet verplichtend zou worden. Daarnaast brengen genoemde criteria mee, dat aanwijzing ziet op niet-domeinspecifieke, dus op bovensectorale en daarmee generieke standaarden.⁴⁶

Bij het gebruik van de bevoegdheid door de minister om bepaalde standaarden aan te wijzen, wordt een zorgvuldig en transparant proces doorlopen. De ingerichte en beproefde procedure voor plaatsing op de *pas-toe-of-leg-uit lijst* waarborgt brede en representatieve betrokkenheid vanuit diverse geledingen van de overheid, wetenschap en uitvoering. Aanwijzing zal doorgaans betrekking hebben op een standaard die reeds op de bestaande lijst van open standaarden is opgenomen dan wel daarvoor is aangemeld. Voor nieuwe standaarden kan de procedure voor plaatsing op de lijst en de aanwijzing parallel lopen.⁴⁷

De bevoegdheid om bij algemene maatregel van bestuur standaarden aan te wijzen, laat de mogelijkheid om in sectorregelgeving voor specifieke doelen standaarden aan te wijzen ongewijzigd.

⁴¹ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 57.*

⁴² Artikel 2, derde lid.

⁴³ Artikel 3, eerste lid.

⁴⁴ Artikel 3, derde lid, zie ook *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 60.*

⁴⁵ Standaarden zijn afspraken over bijvoorbeeld elektronische gegevensuitwisseling, toegankelijkheid of beveiliging, vastgelegd in zogeheten specificatiedocumenten, die beschrijven hoe gegevens eruitzien, wat ze betekenen en hoe ze kunnen worden uitgewisseld (*Kamerstukken II, 2017/18, 34 972, nr. 3, p. 59*).

⁴⁶ Artikel 3, tweede lid, zie ook *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 60.*

⁴⁷ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 59-60*

Echter sectorale standaarden mogen niet belemmerend of concurrerend werken in het bovensectorale verkeer. De aan te wijzen standaarden zelf komen tot stand volgens een eenieder toegankelijke procedure. Het open proces van totstandkoming bestaat uit een brede consultatie van betrokkenen en experts binnen en buiten de overheid alsmede breed samengestelde overleggremia. Bij de aanwijzing van een standaard wordt, zoals hiervoor beschreven, het toepassingsbereik omschreven.

De minister is bevoegd een bindende aanwijzing⁴⁸ te geven aan een orgaan waarvoor de verplichting tot toepassing van een standaard geldt, indien dit orgaan deze verplichting niet naleeft.⁴⁹ Deze aanwijzingsbevoegdheid wordt door de wetgever aangeduid als reguleringsinstrument en niet zozeer als een bestuurlijke sanctie.⁵⁰

3.5 Werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten

Dienstverleners⁵¹ worden gezien als een belangrijke schakel in de authenticatieketen waarin de processen op elkaar zijn aangesloten om erkende of toegelaten identificatiemiddelen te kunnen accepteren. De wetgever wijst erop dat het de elektronische diensten van dienstverleners zijn die door burgers en bedrijven worden afgenomen. De burger moet zich daarvoor bij de dienstverleners authenticeren met al dan niet toegelaten of erkende middelen.

Uitgangspunt is dat de betrokken dienstverleners een eigenstandige verantwoordelijkheid hebben voor informatiebeveiliging. Om te toetsen of de dienstverleners daadwerkelijk voldoen aan de te stellen regels voorziet de wet in een verplichting voor hen om regulier een verklaring van een auditor te overleggen aan de minister.⁵² De te overleggen auditverklaring biedt naar verwachting van de wetgever, naast een handvat voor gesprek, verdere afspraken of eventueel bestuurlijk ingrijpen, ook inzicht in de wijze waarop dienstverleners voldoen aan de gestelde regels. Dit zou volgens de wetgever inzicht kunnen bieden in de naleving daarvan en de stand van zaken omtrent informatieveiligheid bij de toegang tot elektronische dienstverlening.⁵³

3.6 Beheer van de generieke digitale infrastructuur

Op de minister rust de zorgplicht voor de inrichting en het beheer van de GDI. Met het neerleggen in de Wdo van het beheer bij de minister is de minister ten aanzien daarvan aanspreekbaar. De GDI betreft aan elektronische identificatie gerelateerde voorzieningen.⁵⁴ In de praktijk wordt in dit verband vaak gesproken van het Stelsel Toegang.⁵⁵

De wet bevat een indicatieve opsomming⁵⁶ van functionaliteiten van een aantal belangrijke voorzieningen (centrale onderdelen), waarbij concretisering, waaronder de begrippen, en uitwerking in algemene maatregelen van bestuur en ministeriële regelingen plaatsvindt. De grondslagen hiervoor zijn in de wet gegeven.⁵⁷ Door gebruik te maken van een indicatieve opsomming strekt de zorgplicht

⁴⁸ Tegen deze bindende aanwijzing kunnen door het orgaan rechtsmiddelen worden aangewend.

⁴⁹ Artikel 3, vijfde lid.

⁵⁰ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 61.*

⁵¹ Zie artikel 2, eerste en tweede lid.

⁵² Artikel 4, tweede lid.

⁵³ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 63.*

⁵⁴ Artikel 5, eerste lid, aanhef.

⁵⁵ Ondanks dat het Stelsel Toegang niet letterlijk wordt genoemd in de Wdo, wordt het Stelsel Toegang in de toelichtende en uitwerkingsdocumenten van de Wdo genoemd. In beleidsdocumenten, Kamerstukken, advies van de Raad van State, Rekenkamer etc wordt Stelsel Toegang als eigenstandig begrip gebruikt.

⁵⁶ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 64.*

⁵⁷ Artikel 5, eerste lid.

van de minister zich ook uit tot andere infrastructuur van generieke aard die de digitalisering van het openbaar bestuur beoogt.⁵⁸ Door het hanteren van deze systematiek heeft de wetgever beoogd een zekere mate van toekomstbestendigheid en flexibiliteit te bewerkstelligen.⁵⁹

Om zorg te kunnen dragen voor veilige en betrouwbare toegang tot elektronische diensten van dienstverleners bevat *artikel 5, onderdeel a* de verantwoordelijkheid voor identificatiemiddelen waarmee natuurlijke personen (burgers) zich kunnen identificeren (Wie ben je?) en authenticeren (Ben je wie je zegt te zijn?) bij het afnemen van dan wel toegang verkrijgen tot online diensten.

De wet voorziet in de mogelijkheid voor burgers om anderen te machtigen om voor hen overheidsdiensten te verrichten of af te nemen. De Minister draagt op grond van *artikel 5, eerste lid, onderdeel b* zorg voor een voorziening, de zogenoemde publieke machtigingsdienst, die het mogelijk maakt dat een elektronische verklaring wordt afgegeven waaruit blijkt dat een natuurlijke persoon of rechtspersoon gemachtigd is namens een (andere) natuurlijke persoon op te treden bij de toegang tot elektronische dienstverlening. In deze voorziening wordt vastgelegd dat de elektronische dienstverlening is terug te voeren op de wil van de vertegenwoordigde om zich op die wijze te laten vertegenwoordigen en verschaft in ieder geval de mogelijkheid om de bevoegdheid tot het handelen namens natuurlijke personen te verifiëren.

De verantwoordelijkheid van de minister omvat op grond van *artikel 5, eerste lid, onderdeel c*, eveneens de inrichting en werking van een routeringsvoorziening om de toegang tot elektronische dienstverlening te faciliteren. In deze (technische) voorziening worden verschillende koppelvlakken ontsloten, waardoor dienstverleners eenvoudig kunnen aansluiten op de identificatiemiddelen voor burgers die zij moeten accepteren. De verwachting van de wetgever is dat dienstverleners daarmee door de minister in zekere mate worden ontzorgd.

Daarnaast voorziet *artikel 5, eerste lid, onderdeel d* om redenen van veiligheid en betrouwbaarheid in een zorgplicht van de minister om een voorziening mogelijk te maken, waarmee de identiteit van een natuurlijke persoon of rechtspersoon die een elektronische dienst afneemt bij een dienstverlener op unieke wijze geïdentificeerd kan worden.

Artikel 5, eerste lid, onderdeel e regelt de verantwoordelijkheid van de minister voor het beheer van het Stelsel Toegang voor identificatie van ondernemingen en rechtspersonen.⁶⁰ Dit artikel beoogt het bedrijvendomein onderdeel te laten zijn van de verantwoordelijkheid van de minister van BZK.

Tot slot is de minister verantwoordelijk voor het elektronisch berichtenverkeer met en informatieverschaffing aan natuurlijke personen, ondernemingen en rechtspersonen, waarvan MijnOverheid een voorbeeld is.

Op het gebied van de grensoverschrijdende toegang tot elektronische dienstverlening draagt de minister in dit verband zorg voor een knooppunt als bedoeld in artikel 12 van de eIDAS-verordening. Deze voorziening maakt het mogelijk dat Nederlandse dienstverleners de in andere EU-lidstaten ingevolge de eIDAS-verordening genotificeerde middelen kunnen accepteren door wederzijdse erkenning.⁶¹ Dit knooppunt voegt aan de uit een andere lidstaat ontvangen set gegevens een burgerservicenummer of andere aan de natuurlijke persoon of rechtspersoon gekoppelde gegevens toe. Het gaat hier om gegevens die noodzakelijk zijn voor dienstverleners om de betrokken natuurlijke

⁵⁸ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 64.*

⁵⁹ *Kamerstukken II, 2017/18, 34 972, nr. 4, p. 15.*

⁶⁰ De uitwerking daarvan in de artikelen 11 tot en met 15 zijn nog niet van toepassing.

⁶¹ Artikel 5, tweede lid.

persoon of rechtspersoon ten behoeve van het verrichten van de elektronische dienstverlening in hun systemen te herkennen.⁶²

De wet voorziet in een delegatiebepaling om nadere regels te stellen aangaande elektronische identificatie en elektronisch berichtenverkeer.⁶³

3.7 Toegang tot elektronische dienstverlening: betrouwbaarheidsniveaus

Bij dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog is vereist, wordt gebruik gemaakt van middelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben. Een gebruiker kan daarmee voor alle diensten met een middel op betrouwbaarheidsniveau hoog terecht, ook als de dienstverlener slechts een middel met een lager betrouwbaarheidsniveau vereist en een publiek middel op niveau laag wordt geaccepteerd door de dienstverlener.⁶⁴ Het DigiD-middel op betrouwbaarheidsniveau hoog is vanaf begin 2021 beschikbaar, maar nog niet breed beschikbaar. Om op DigiD hoog over te kunnen gaan is er een speciale chip, een 'applet', nodig op onder meer het rijbewijs. De RDW draagt daar in opdracht van de minister zorg voor.⁶⁵ De verantwoordelijkheid daarvoor blijft daarmee liggen bij de minister.

Een dienstverlener bepaalt in beginsel zelf welk betrouwbaarheidsniveau hij passend acht voor welke soort dienstverlening. Bij het bepalen van het betrouwbaarheidsniveau moeten dienstverleners zich evenwel houden aan de bij ministeriële regeling gestelde criteria inzake betrouwbaarheidsniveaus voor authenticatie bij elektronische diensten. Het ministerie van BZK heeft samen met RVO een Regelhulp gemaakt om hierbij behulpzaam te zijn.⁶⁶ Daarnaast is ook een geactualiseerde Handreiking betrouwbaarheidsniveaus⁶⁷ opgesteld, om dienstverleners te helpen een eenduidige, efficiënte en bewuste keuze te maken in de betrouwbaarheidsniveaus van hun digitale diensten. Ook is voorgeschreven dat ten behoeve van de rechtszekerheid van de gebruiker dienstverleners het betrouwbaarheidsniveau voor hun diensten (onderbouwd) bekend maken. De wetgever verwacht dat als gevolg hiervan het aantal diensten met authenticatie op betrouwbaarheidsniveau laag de komende jaren zal afnemen. Het voorgaande geldt ook voor de toegang voor gemachtigden.⁶⁸

3.8 Toegang tot elektronische dienstverlening: gebruik in publiek domein

Een publiek middel en de machtigingsvoorziening worden uitsluitend gebruikt voor de toegang tot elektronische dienstverlening door publieke dienstverleners. Authenticatie in het elektronische verkeer met commerciële dienstaanbieders, bijvoorbeeld webwinkels, valt niet onder de werkingssfeer van deze wet.⁶⁹ Het gebruiken van een publiek middel voor commerciële dienstverlening is niet toegestaan om marktverstoring tegen te gaan. Als voorbeeld wordt door de wetgever genoemd dat een gemeente voor de elektronische verkoop van kaartjes voor een concert in het gemeentehuis of bij de elektronische aankoop van een bloemstuk niet om het gebruik van een publiek middel mag verzoeken.⁷⁰ Hierop bestaan uitzonderingen. Zo kan een publiek middel tevens voor de toegang tot

⁶² Artikel 5, derde lid.

⁶³ Artikel 5, vijfde lid.

⁶⁴ Artikel 6, eerste lid.

⁶⁵ Artikel 5, vierde lid.

⁶⁶ Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Regelhulp betrouwbaarheidsniveaus, *regelhulpvoorbedrijven.nl*.

⁶⁷ Forum Standaardisatie, 'Handreiking betrouwbaarheidsniveaus voor digitale dienstverleners', versie 5 (2024), *forumstandaardisatie.nl*.

⁶⁸ Artikel 6, tweede en derde lid.

⁶⁹ Artikel 8, eerste lid.

⁷⁰ *Kamerstukken II*, 2017/18, 34 972, nr. 3, p. 74.

welbepaalde private elektronische diensten van deze dienstverleners worden gebruikt. Gedacht kan bijvoorbeeld worden aan zorgverzekeraars en zorgverleners.⁷¹ Daarnaast kan worden bepaald dat een publiek identificatiemiddel ten behoeve van aangewezen organisaties kan worden gebruikt voor het verlenen van toegang tot een systeem voor de elektronische uitwisseling van gegevens waarbij het burgerservicenummer wordt verwerkt, anders dan een systeem voor elektronische dienstverlening. Het kan daarbij gaan om het gebruik binnen interne/ gesloten systemen, zoals bijvoorbeeld het binnen en tussen zorginstellingen – binnen de grenzen van de wet – onderling digitaal uitwisselen van patiëntgegevens.⁷²

3.9 Toegang tot elektronische dienstverlening: regels ten aanzien van gebruik

De burger die in het bezit is van een elektronisch identificatiemiddel heeft een aantal verplichtingen ter bescherming van zijn elektronische identificatiemiddel. Hij moet zorgen dat hij het middel onder zijn exclusieve controle houdt, wat onder meer inhoudt dat wachtwoorden en pincodes strikt geheim moeten worden gehouden. Hij moet alle nodige maatregelen nemen om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om ingeval van diefstal, verlies of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.⁷³ ⁷⁴ De wet voorziet in een delegatiebepaling om daartoe nadere regels te stellen.⁷⁵

3.10 Bescherming persoonsgegevens

De wet biedt grondslagen voor verwerking van persoonsgegevens door genoemde normadressaten, waaronder het burgerservicenummer,⁷⁶ voor zover 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.⁷⁷ Daarmee verankert de wet volgens de wetgever de principes van de AVG. Artikel 16 bevat de hoofdelementen van privacybescherming bij de toegang tot elektronische dienstverlening; uitwerking is geschied bij AMvB namelijk het Besluit digitale overheid.⁷⁸ De omstandigheden waarin van de gedelegeerde bevoegdheid gebruik mag worden gemaakt zijn geconcretiseerd, alsmede de te regelen onderwerpen en doelen.⁷⁹

3.11 Naleving

Voor centrale overheden geldt, voor zover thans van toepassing, dat de betrokken vakministers zorgdragen voor de naleving door hun eigen uitvoeringsorganisaties ten aanzien van de standaarden, de betrouwbaarheidsniveaus en het restrictief gebruik van het publieke identificatiemiddel en de voorziening. De vakminister moet in dat verband toezichthoudende ambtenaren aanwijzen.⁸⁰ In lijn

⁷¹ Dit is mogelijk in geval van gecombineerde dienstverlening wanneer een klant van bijvoorbeeld een verzekeraar naast een BSN-dienst als een pensioenverzekering ook nog andere verzekeringen heeft waarvoor geen BSN nodig is. Het kan hierbij bijvoorbeeld gaan bij een verzekeraar naast zogenaamde BSN-diensten ook een koppeling kan worden gemaakt met een autoverzekering

⁷² *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 75.*

⁷³ Artikel 10, eerste lid.

⁷⁴ *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 77.*

⁷⁵ Artikel 10, tweede lid.

⁷⁶ Hiermee wordt voldaan aan artikel 46 van de Uitvoeringswet AVG.

⁷⁷ Artikel 16, eerste lid.

⁷⁸ Artikel 28 in samenhang bezien met artikel 16, vierde lid.

⁷⁹ *Kamerstukken I, 2020/21, 34 972, L, p. 8.*

⁸⁰ Artikel 17, eerste lid, zie ook *Kamerstukken I, 2022/23, 34 972, V, p. 1.*

met het reguliere interbestuurlijke toezicht houdt de minister toezicht op provincies en bestuursorganen op het niveau van provincies (gemeenschappelijke regelingen, waaraan provincies deelnemen). De minister geeft invulling aan dat toezicht op de hiervoor genoemde onderwerpen door daartoe ambtenaren aan te wijzen.⁸¹ De minister houdt eveneens toezicht op de naleving door bestuursorganen en aangewezen organisaties van de eisen inzake informatieveiligheid en de in dit verband opgelegde auditverklaring alsmede van de regels inzake gebruik buiten het publieke domein. Ook hiertoe wijst de minister ambtenaren aan.⁸² Van het besluit, waarmee de minister ambtenaren ten behoeve van het toezicht aanwijst wordt mededeling gedaan in de Staatscourant.⁸³⁸⁴

Naast het houden van toezicht beschikt de minister over de mogelijkheid om operationele maatregelen te nemen om (dreigende) compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties te voorkomen of beëindigen. Mits proportioneel kan de minister bij het vermoeden van of manifeste integriteits- of beveiligingsinbreuken maatregelen treffen die zich richten op de dienstverlening van dienstverleners met als doel de borging of het herstel van de betrouwbare toegang tot hun elektronische diensten.

Om als minister zicht te krijgen op de vraag of sprake is van de hiervoor genoemde omstandigheden is het van belang dat de minister op de hoogte is van wat er speelt. Een dienstverlener is dan ook verplicht om de minister onverwijld in kennis stellen van een inbreuk op de beveiliging of de integriteit van een eigen elektronische dienst of van misbruik of oneigenlijk gebruik van de toegang tot de eigen elektronische dienstverlening. De dienstverlener verstrekt daarbij alle benodigde informatie. Hetzelfde geldt voor de toezichthouder die ernstige niet naleving door een bestuursorgaan of aangewezen organisatie constateert.⁸⁵ Daarnaast geldt een bredere informatieverplichting door dienstverleners aan de minister om desgevraagd en uit eigen beweging de gegevens en inlichtingen die de minister nodig heeft om maatregelen te kunnen nemen om inbreuk op de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of beëindigen.⁸⁶ Omgekeerd rust op de minister de verplichting om gegevens en inlichtingen te verstrekken aan betrokken partijen over de compromittering van de veilige en betrouwbare toegang elektronische dienstverlening voor zover dit noodzakelijk is voor een goede uitoefening van hun taken respectievelijk te verlenen diensten.⁸⁷

3.12 Experimenteerruimte

De wet biedt de mogelijkheid om bij AMvB in ieder geval⁸⁸ af te wijken van de acceptatieplicht met het oog op het onderzoeken van nieuwe methoden waarmee authenticatie doeltreffender kan plaatsvinden. Het betreft de realisering van een innovatieve toepassing of het in het kader van de doorontwikkeling testen van een nieuw publiek middel bij specifieke bestuursorganen of aangewezen organisaties. Hierdoor kan proefondervindelijk worden vastgesteld of een (door)ontwikkeld publiek of privaat middel een bijdrage kan leveren aan efficiënte, betrouwbare en gebruiksvriendelijke

⁸¹ Artikel 17, tweede lid, zie ook *Kamerstukken II, 2017/18, 34 972, nr. 3, p. 86.*

⁸² Artikel 17, vierde lid.

⁸³ Artikel 17, zesde lid.

⁸⁴ Artikel 17, achtste lid, is ook in deze fase van toepassing verklaard. Echter de daarin opgenomen boetebevoegdheid ziet op artikelen die nog niet van toepassing zijn verklaard.

⁸⁵ Artikel 18, tweede en derde lid.

⁸⁶ Artikel 19, eerste lid.

⁸⁷ Artikel 19, tweede lid.

⁸⁸ BZK sluit niet uit dat deze bepaling ook ruimte biedt om te experimenteren zolang de open toelating (en daarmee de acceptatieplicht) nog niet is gestart.

authenticatie in het publieke domein.⁸⁹ Een experiment wordt dan ingesteld met een duur van ten hoogste vier jaar.⁹⁰

Gedurende de periode, waarop de evaluatie ziet, heeft BZK geen aanleiding gezien om van deze zogenoemde experimenteerruimte gebruik te maken.

⁸⁹ *Kamerstukken II*, 2017/18, 34 972, nr. 3, p. 93

⁹⁰ Artikel 26

4. Het functioneren van de eerste fase van de Wdo

4.1 Inleiding

In dit hoofdstuk staat het functioneren van de eerste fase van de Wdo centraal. Daarbij maken we gebruik van de informatie uit de gevoerde gesprekken met medewerkers van BZK, waarin de achtergrond en de totstandkoming van de Wdo nader zijn toegelicht, diepte-interviews met betrokken organisaties die uitvoering geven aan de Wdo en een toezichthouder. Naar aanleiding van deze gesprekken zijn ter verificatie aan BZK nader vragen voorgelegd. Deze vragen zijn door BZK beantwoord. De uitkomst daarvan is eveneens betrokken bij dit hoofdstuk. Tot slot heeft BZK de onderzoekers voorzien van een nadere aanvullende schriftelijke reactie die eveneens bij dit hoofdstuk is betrokken.

In dit hoofdstuk wordt aan de hand van verschillende thema's een beeld gegeven van het functioneren van de eerste fase. Het doel hiervan is om een beeld te krijgen van de doelmatigheid en effectiviteit van de Wdo tot dusver.

In de paragrafen 4.2 tot en met 4.4 wordt allereerst stilgestaan bij hoe de geïnterviewden meer in het algemeen het functioneren van de Wdo ervaren. In de overige paragrafen wordt stilgestaan bij specifieke onderwerpen uit de eerste fase van de Wdo.

4.2 De keuze voor het gefaseerd in werking treden van de Wdo

Hoewel de Wdo formeel gedeeltelijk in werking is getreden, zijn veel van de bijbehorende voorzieningen nog niet (volledig) gerealiseerd. Dit leidt ertoe dat de Wdo in de huidige fase door verschillende geïnterviewden wordt getypeerd als een symboolwet: een juridisch kader dat richtinggevend is, maar waarvan de feitelijke werking in de praktijk beperkt blijft. Een groot deel van de geïnterviewden geeft aan dat het BZK niet gelukt is om tijdig te voorzien in het vereiste stelsel voor toegang waardoor het ook niet mogelijk is om de artikelen die nog niet in werking zijn, in werking te laten treden. Deze artikelen zijn met name van belang voor de effectiviteit en doelmatigheid van de Wdo in de praktijk.⁹¹ Door gefaseerde inwerkingtreding wordt het risico genomen dat interventies en systemen in tijd worden ingehaald. BZK benadrukt dat de wet formeel geen stelsel voor toegang vereist, maar wel randvoorwaardelijke ICT-voorzieningen⁹² die de publieke dienstverleners helpen om te kunnen voldoen aan de acceptatieplicht. BZK heeft met bestuurlijke afstemming de keuze gemaakt om dit in te vullen door het stelsel toegang. Verder brengt BZK naar voren dat de gefaseerde inwerkingtreding tot doel heeft om juist rekening te houden met ontwikkelingen bij uitvoeringsorganisaties en geen onmogelijkheden te vereisen.

De uitvoering van de Wdo heeft volgens verschillende geïnterviewden verder beperkt prioriteit gekregen bij de betrokken organisaties. Organisaties vinden het namelijk lastig om plannen te maken op basis van een wet die gefaseerd in werking treedt en afhankelijkheden bevat van de stand van de uitvoering. In dat licht is van belang om op te merken dat BZK in afstemming met de publieke dienstverleners gekozen heeft voor een releasematige aanpak, waarmee de ontwikkeling van het Stelsel Toegang in kleinere beheersbare stappen zal plaatsvinden. Enkele geïnterviewden brengen naar voren dat een planning van het Stelsel Toegang voor betrokken organisaties niet kenbaar is. BZK erkent

⁹¹ Zie ook de brief van de Rijksinspectie Digitale Infrastructuur inzake het resultaat UHT Regeling nadere eisen Wdo van 24 mei 2024

⁹² Zie ook voetnoot 56.

dat er geen externe beleidsplannen zijn gepubliceerd. Wel wordt intern gewerkt aan de hand van een plan van aanpak.

4.3 Beperkt materieel effect en afhankelijkheid van andere ontwikkelingen

Het merendeel van de geïnterviewden meent dat de onderdelen die met de eerste fase in werking zijn getreden weinig tastbare verandering hebben gebracht in de dagelijkse uitvoering. Digitale toegang tot overheidsdiensten is grotendeels operationeel geregeld via bestaande systemen als DigiD en eHerkenning. Zo worden voor DigiD afspraken over aansluiting en beveiliging gemaakt met tussenkomst van Logius en door Logius in opdracht van BZK gehandhaafd. De Wdo was strikt genomen niet nodig om dit te regelen. Wel draagt de Wdo er zorg voor dat de eerdergenoemde afspraken gelden voor een aansluiting op het stelsel en niet alleen, zoals nu, voor een aansluiting op DigiD.

Bovendien lijkt de Wdo niet bepalend voor de naleving van de daaruit voortvloeiende verplichting, zoals gegevensbescherming en informatiebeveiliging, nu deze verplichtingen reeds worden voorgeschreven in onder meer de AVG, de BIO en de NIS2. In dat licht wordt benadrukt dat de Wdo niet los kan worden gezien van bestaande Europese kaders, zoals NIS2 en eIDAS.

Uit de interviews komt het beeld naar voren dat BZK te lang heeft gearzeld met het vervolg van de gefaseerde inwerkingtreding om continu rekening te willen houden met wensen en zorgen van stakeholders en wordt vanuit praktische bezwaren teruggekomen op gestelde doelen. Dit leidt volgens geïnterviewden ertoe dat een onvoldoende internationale visie lijkt te bestaan over onderwerpen, zoals de EDI-wallet en de Data Act.

Tegelijkertijd delen de geïnterviewden het beeld dat de eerste fase van de Wdo heeft bijgedragen aan bewustwording rond veilig digitaal handelen en aan het bepalen van het juiste betrouwbaarheidsniveau bij digitale transacties.

4.4 Implementatie Wdo

Diverse geïnterviewden wijzen op praktische knelpunten in de implementatie.

BZK heeft in het kader van het doen van de uitvoeringstoets met gebruikmaking van het toetspanel, waaraan vrijwel alle uitvoeringsorganisaties hebben deelgenomen, aandacht gegeven aan de toetsing of de wet zelf uitvoerbaar is. BZK heeft daarbij met name stil gestaan bij de kwalitatieve kant van de uitvoering. Een van de respondenten brengt naar voren dat tijdens het toetspanel nauwelijks aandacht is geschonken aan de kwantitatieve kant. Daarbij kan worden gedacht aan wat de publieke waarde is die moet worden bereikt en wat daarvoor nodig is aan onder meer geld, organisatie, voorzieningen, mandaat, doorlooptijd, tempo en het bereik van inlogmiddelen op hogere betrouwbaarheidsniveaus.

De uitvoering stuit verder op gebrekkige coördinatie en wisselende prioritering binnen BZK. Verschillende initiatieven worden volgens geïnterviewden regelmatig stopgezet, wat het vertrouwen bij uitvoeringsorganisaties ondermijnt. Hierdoor ontstaat volgens geïnterviewden het beeld dat de wetgever de Wdo als kader voor de verdere ontwikkeling van het Stelsel Toegang niet meer als urgent beschouwt. De beleving van BZK is daarentegen dat BZK in de Programmeringsraad GDI de urgentie tot op heden steeds onderstreept.

Meerdere geïnterviewden benadrukken dat de Wdo wel degelijk van waarde is als kapstok voor toekomstige ontwikkelingen, mits beter wordt nagedacht over de uitvoerbaarheid en samenhang tussen de verschillende stelsels. Daarbij is het cruciaal dat de verhouding tussen beleid, uitvoering en governance duidelijker wordt vormgegeven, en dat de lessen uit de huidige implementatiefase worden meegenomen bij de verdere uitbouw van het Stelsel Toegang.

4.5 Standaarden

De bevoegdheid van de minister van BZK om standaarden aan te wijzen en het gebruik daarvan te verplichten wordt door de geïnterviewden in het algemeen als positief ervaren; zij heeft bestuurlijke aandacht gegeneerd. Op dit moment zijn twee standaarden verplicht:

- HTTPS en HSTS, inclusief configuratie conform de TLS-richtlijnen en Webapplicatie-richtlijnen van het NCSC; en
- Digitale toegankelijkheid op basis van EN 301 549 inclusief WCAG 2.1.

Volgens sommigen moet, voordat meer standaarden verplicht worden gesteld, het huidige regime eerst goed op orde worden gebracht. Zo ontbreekt er effectief toezicht, waardoor verplichtingen die voortvloeien uit de standaarden niet voldoende worden nageleefd. Door geïnterviewden wordt gewezen op het feit dat alle standaarden van de 'Pas toe of leg uit'-zouden moeten worden verplicht. Het Forum Standaardisatie adviseert dat te doen voor de standaarden waarvoor in het Overheidsbreed Beleidsoverleg Digitale Overheid streefbeeldafspraken zijn gemaakt. Tot op heden heeft zich volgens BZK geen noodzaak voorgedaan om andere standaarden wettelijk te verplichten. Tegen dit standpunt van BZK heeft het Forum Standaardisatie zich uitgesproken.⁹³

Uit de Monitor Open Standaarden 2025 van het Forum Standaardisatie blijkt dat de wettelijke verplichte informatieveiligheidsstandaarden in aanbestedingen flink meer worden uitgevraagd, dan de informatieveiligheidsstandaarden waarvoor alleen een 'pas toe of leg uit' verplichting geldt. In de halfjaarlijkse meting van de daadwerkelijke toepassing van deze wettelijk verplichte standaarden, blijkt evenwel dat er een groep is van circa 37% van de circa 10.000 gemeten web domeinen van de overheid, waar de wettelijke standaarden nog niet worden toegepast, of nog niet correct zijn geconfigureerd. Dat aantal blijkt na het ingaan van de wettelijke verplichting in juli 2023 te weinig afgenomen. Daarmee is het voor BZK kenbaar of deze standaarden worden toegepast door alle bestuursorganen die daartoe verplicht zijn. In de interviews wordt hierbij de kanttekening geplaatst en wordt gewezen op een praktisch knelpunt dat er geen centraal uitgiftepunt is voor en geen algemeen register van overheidswebsites bestaat, waardoor het volledige overzicht ontbreekt.

Voor digitale toegankelijkheid wordt dit inzicht verkregen door de informatie die beschikbaar is op het Dashboard digitale toegankelijkheid. De informatie is afkomstig uit de Toegankelijkheidsverklaringen die organisaties moeten laten maken. Op de website kan gezocht worden op onder andere organisatie. Daarmee bestaat er inzicht welke organisatie en zelfs welke websites/apps voldoen aan de verplichtingen voortvloeiend uit de standaarden. BZK voldoet overigens zelf niet volledig aan de Toegankelijkheidsstandaarden.

De minister van BZK heeft de bevoegdheid om een bindende aanwijzing op te leggen wanneer de verplichtingen voortvloeiend uit de standaarden niet worden nageleefd. Op dit moment echter heeft de minister van BZK vanwege het ontbreken van toezicht dit reguleringsinstrument nog niet toegepast en is daartoe evenmin een proces ingericht. Wel is een bestuursorgaan aangeschreven en gevraagd om de naleving van de standaarden te verbeteren.

⁹³ Forum Standaardisatie, 'Duiding en Maatregelen Monitor Open Standaarden 2025', 26 juni 2025, forumstandaardisatie.nl.

4.6 Stelsel toegang

Het Stelsel Toegang wordt een publiekrechtelijk stelsel onder de Wdo, waarin private aanbieders van inlogmiddelen worden toegelaten. Het Stelsel Toegang is voor de start van de uitwerking van het wetsvoorstel rond 2014 aangevangen. Het heeft verschillende namen gekend, waaronder EID stelsel, maar het doel is volgens BZK altijd geweest om een stelsel te maken waarmee dienstverleners kunnen voldoen aan de verplichtingen die gelden onder de Wdo. Op dit moment is het Stelsel Toegang nog in ontwikkeling. De stelsel- en beleidsverantwoordelijkheid ligt bij BZK.

Het veld waarin het Stelsel Toegang moet worden ingericht en ontwikkeld is omvangrijk, en politiek, bestuurlijk en beleidsmatig complex. Het is daarom vanuit de rol en verantwoordelijkheden van BZK van belang om bij het ontwikkelen en doorontwikkelen van het stelsel regie te voeren op dit speelveld en de uitvoerbaarheid van het te vormen beleid in het vizier te houden. Daartoe heeft BZK een stelselregisseur aangesteld. Zijn taak behelst het in kaart brengen van de belangen en ontwikkelingen die spelen in de omgeving, binnen de vastgestelde beleidskaders. De stelselregisseur heeft daarmee meer de rol van bemiddelaar en heeft geen formele bevoegdheden voor de stelselinrichting.

4.6.1 Routeringsvoorziening

Dienstverleners geven aan dat oorspronkelijk door BZK is toegezegd dat dienstverleners niet langer afzonderlijk zouden hoeven aan te sluiten op diverse inlogmiddelen, maar via één gestroomlijnd stelsel toegang zouden krijgen. Eén gestroomlijnd stelsel is tot nu toe uitgebleven.

Uit de interviews volgt dat door het ontbreken van één gestroomlijnd stelsel sommige organisaties ervoor kiezen om een eigen routeringsvoorziening te ontwikkelen, omdat stilstand onverantwoord wordt geacht. Zij vrezen wel dat investeringen verloren gaan zodra een centrale voorziening wordt opgeleverd. Wat de organisaties hierin parten speelt, is dat er onduidelijkheid bestaat wanneer één gestroomlijnd stelsel daadwerkelijk beschikbaar is.

Aansluiten kan volgens BZK met een publieke voorziening (ToegangVerleningService; TVS), een private IT-leverancier of een zelf gebouwde voorziening.⁹⁴ Eind 2026 worden de technische specificaties voor het aansluiten van publieke dienstverleners met behulp van private IT-leveranciers op het Stelsel Toegang gepubliceerd en zal naar verwachting van BZK de eerste private aanbieder van authenticatiediensten worden toegelaten.

4.6.2 Publiek identificatiemiddel

Op dit moment is DigiD het enige functionerende publieke identificatiemiddel voor burgers. Enkele geïnterviewden geven aan dat naast DigiD ook andere publieke (en private) middelen beschikbaar zouden moeten komen om de continuïteit van dienstverlening binnen de overheid beter te borgen. Er is geen breed toegankelijke publiek identificatiemiddel beschikbaar op betrouwbaarheidsniveau hoog.

Vanuit de uitvoeringspraktijk wordt door enkelen bepleit om het Stelsel Toegang en het bestaande eHerkenning-stelsel te integreren om zo tot vereenvoudiging te komen.

⁹⁴ Zie ook Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Ontsluiten Stelsel Toegang', *digitaleoverheid.nl*.

4.6.3 Vertegenwoordigen

Het is niet toegestaan dat een DigiD door een ander wordt gebruikt. Uit de interviews blijkt dat in de praktijk mensen dit wel doen. Deze burgers delen soms hun inloggegevens (gebruikersnaam en wachtwoord), zodat anderen namens hen kunnen handelen. Dit wordt door de geïnterviewden als ongewenst en onveilig aangemerkt.

Vrijwillig machtigen

De Wdo regelt op grond van artikel 5, eerste lid, onderdeel b dat de minister zorg moet dragen voor een zogenoemde publieke machtigingsdienst. Handelingsbekwame burgers kunnen vrijwillig iemand machtigen om zich te laten vertegenwoordigen in de interactie met publieke dienstverleners. De voorziening voor vrijwillige machtiging is operationeel. Met de voorziening DigiD Machtigen kan een betrokkene iemand anders machtigen om digitaal zaken te doen bij (semi-) overheidsdienstverleners. Op de voorziening DigiD Machtigen zijn ruim 675 dienstverleners aangesloten, waaronder de Belastingdienst, DUO, UWV en Sociale Verzekeringsbank als ook dienstverleners in de zorgsector. Enkele geïnterviewden stellen dat de wijze van machtigen ook anders kan worden ingericht dan het gebruik van DigiD Machtigen.

Wettelijk vertegenwoordigen

Burgers die (deels) handelingsonbekwaam zijn en niet zelfstandig rechtshandelingen mogen verrichten, zoals personen die onder bewind of curatele staan of minderjarigen, hebben een door de wet of door de rechter aangestelde wettelijke vertegenwoordiger (bewindvoerder, curator, mentor of een persoon met gezag over een minderjarige). De noodzaak voor het digitaal mogelijk maken van wettelijk vertegenwoordigen (niet-vrijwillige machtiging) is na de inwerkingtreding van de Wdo naar voren gekomen en kent drie elementen:

1. het beschikbaar hebben van digitale bronnen waarin wettelijk vertegenwoordigingsrelaties zijn vastgelegd;
2. ICT voorziening om die bronnen te ontsluiten, de bevoegdheidsverklaringsdienst; en
3. dienstverleners die hun diensten aanbieden aan wettelijk vertegenwoordigers.

Voor wettelijk vertegenwoordigen zijn een tweetal digitale bronnen gerealiseerd:

1. Wettelijk vertegenwoordigingsrelaties (WVR) bij IVO Rechtspraak waarin bewindvoerders, curatoren en mentoren die digitaal met de Rechtspraak communiceren zijn opgenomen.
2. Gezagsmodule (BRP API gezag): Om het gezag over een minderjarige te kunnen vaststellen is deze module ontwikkeld tussen 2018 en 2023. Dit is een set van afleidingsregels waarmee op basis van de informatie in de BRP het ouderlijk gezag kan worden vastgesteld.

Om de twee digitale bronnen met vertegenwoordigingsrelaties (WVR en BRP) digitaal te ontsluiten heeft BZK binnen de ruimte die artikel 5 biedt een bevoegdheidsverklaringsdienst (BVD) laten ontwikkelen als onderdeel van het Stelsel Toegang. Met deze voorziening kunnen dienstverleners inzicht krijgen of een persoon of organisatie de bevoegdheid heeft om iemand anders wettelijk te vertegenwoordigen. Hiermee ontzorgt BZK de dienstverleners zodat zij zelf geen functionaliteit hoeven te bouwen, zoals bij de directe bevraging van de BRP voor ouderlijk gezag en voor het raadplegen van het WVR bij IVO Rechtspraak. Bovendien kunnen wijzigingen in de BVD op één centrale plek worden doorgevoerd, hierdoor hoeven individuele dienstverleners deze wijzigingen dan niet zelf door te voeren.

Burgers kunnen met deze voorziening met hun eigen DigiD inloggen om diensten af te nemen voor hun kind of voor de persoon die zij vertegenwoordigen. Deze voorziening is ten tijde van dit onderzoek

niet gereed⁹⁵, maar de BVD is wel in pilot vorm beproefd. Uit deze pilots komt naar voren dat het implementeren van de functionaliteit door de dienstverleners in hun systemen complex is. Bovendien moeten dienstverleners hun diensten op de juiste manier indelen, zodat wettelijk vertegenwoordigers toegang krijgen tot de juiste dienstverlening waar zij een bevoegdheid voor hebben. Deze dienstverleners hebben bovendien een eigen aparte aansluiting op de BVD. Om de BVD geschikt te maken voor fundamenteel meer bevragingen en het Stelsel Toegang heeft BZK deze BVD verbeterd en is gestart met ondersteuning bieden aan de dienstverleners voor de implementatie in hun eigen systemen.⁹⁶

Met de uitrol van het Stelsel Toegang met één aansluiting voor de dienstverleners voor alle toegelaten inlogmiddelen en voorzieningen voor vertegenwoordigen, maakt BZK stapsgewijs de BVD en daarmee de ontsluiting van ouderlijk gezag en het WVR beschikbaar.

4.7 Toegang tot elektronische dienstverlening

4.7.1 Betrouwbaarheidsniveaus

Figuren 1 en 2 geven een weergave van de actuele cijfers die zien op het aantal accounts onderscheidenlijk authenticaties per betrouwbaarheidsniveau voor DigiD. Deze cijfers zijn door BZK verzameld en aangeleverd. Wat betreft figuur 1 moet worden opgemerkt dat geen exacte cijfers van DigiD Hoog beschikbaar zijn. Op dit moment zijn er 250.000 accounts bij de Rijksdienst voor Identiteitsgegevens of de RDW geactiveerd.

	1 juli 2023	1 jan 2024	1 juli 2024	1 jan 2025	1 juli 2025	1 okt 2025
Basis	244.767	211.356	158.825	90.100	65.117	58.573
Midden (sms)	4.590.767	4.431.725	4.170.586	3.659.660	3.143.810	3.074.936
Midden (app)	4.086.928	3.997.229	3.962.683	3.838.958	3.725.301	3.694.026
Substantieel	8.141.680	8.539.464	8.936.592	9.239.674	9.586.043	9.753.664

Figuur1: accounts

	Q3/Q4 2023	Q1/Q2 2024	Q3/Q4 2024	Q1/Q2 2025	Q3/Q4 2025 (schatting totaal aantal authenticaties)
Basis	9.526.047	7.403.203	4.276.809	4.985.438	
Midden (sms)	64.542.395	86.030.440	69.320.298	90.039.918	
Midden (app)	45.885.251	63.440.556	62.251.421	80.501.360	
Substantieel	96.179.176	130.001.793	127.384.679	169.635.441	
Hoog	15.109	22.480	21.642	27.722	
Totaal	216.147.978	286.898.422	263.254.849	345.189.879	316.742.451

Figuur 2: authenticaties

⁹⁵ BZK verwacht dat deze voorziening per 1 juli 2026 gereed is voor ouderlijk gezag tot 12 jaar en dat de voorziening daarna wordt uitgebouwd.

⁹⁶ Staatssecretaris Digitalisering en Koninkrijksrelaties, brief van 16 mei 2025 inzake Spoedbrief Digitaal Vertegenwoordigen.

Uit de analyse van BZK volgt dat een sterke groei heeft plaatsgevonden in het aantal authenticaties. Dit doordat steeds meer dienstverleners (bijvoorbeeld in de zorgsector) online dienstverlening aanbieden. Eveneens ziet BZK een gestage afname in het gebruik van lagere betrouwbaarheidsniveaus en een groei in het aantal gebruikers dat DigiD op een hoger betrouwbaarheidsniveau hebben geactiveerd. Het gaat hier met name om betrouwbaarheidsniveau *substantieel*. Het betrouwbaarheidsniveau *basis* neemt in rap tempo af. Dit is volgens BZK te wijten aan het feit dat onder meer het inloggen met alleen gebruikersnaam en wachtwoord niet meer is toegestaan bij veel (grote) dienstverleners zoals de Belastingdienst, SVB en DUO en dienstverleners in de zorgsector.

Betrouwbaarheidsniveau *hoog* wordt in geringe mate gebruikt. Dit komt volgens BZK met name doordat de functionaliteit nog niet wordt gepromoot vanwege het ontbreken van de PIN-reset functionaliteit. De eID-functionaliteit op de ID-kaart/rijbewijs moet namelijk ontgrendeld worden met een PIN-code. Als een gebruiker deze kwijt of vergeten is, is er op dit moment geen mogelijkheid deze PIN-code te resetten. BZK verwacht dat in 2027 deze functionaliteit beschikbaar is.

In de interviews wordt het beeld bevestigd dat de implementatie van betrouwbaarheidsniveau *hoog* in de praktijk achterblijft. De reden die daarvoor wordt gegeven, is dat koplopers aanvankelijk meer lasten dan baten ervaren. Zo stellen gebruikers meer vragen en niet alle gebruikers kunnen een betrouwbaarheidsniveau *hoog* bereiken, bijvoorbeeld bij ontbreken van een Nederlands identiteitsmiddel. Enkele geïnterviewden merken op dat het huidige niveau hoog in de toekomst het niveau substantieel zou kunnen worden. Door de geïnterviewden wordt het als een gemis ervaren dat in de wettelijke systematiek een expliciete verplichting ontbreekt voor organisaties om periodiek te toetsen of het vereiste betrouwbaarheidsniveau, gelet op technologische en organisatorische ontwikkelingen, is gewijzigd en vervolgens aanpassing behoeft.

Voor de *machtigingsvoorziening* geldt dat de registratie van een machtiging overeen moet komen met het betrouwbaarheidsniveau van de af te nemen dienst. In de interviews is naar voren gekomen dat op dit moment het niet mogelijk is om vrijwillig te machtigen op betrouwbaarheidsniveau *substantieel* en hoger. Dit wordt door BZK desgevraagd bevestigd. Dit leidt ertoe dat de dienst bijvoorbeeld betrouwbaarheidsniveau *substantieel* heeft, maar dat de machtiging niet verder dan betrouwbaarheidsniveau *laag* kan gaan. Dit ondergraaft het te behalen betrouwbaarheidsniveau. Onder meer om deze reden is BZK in 2025 het project Vernieuwing DigiD Machtigen gestart. In 2025 wordt het programma van eisen opgesteld en met doorloop in 2026 bekeken of DigiD Machtigen kan worden aangepast of dat een nieuwe applicatie noodzakelijk is. In 2027 zal onder voorbehoud van financiering de realisatiefase plaatsvinden.

4.7.2 Classificeren betrouwbaarheidsniveaus

Wat betreft het classificeren van de betrouwbaarheidsniveaus volgt uit de interviews dat die handeling, ondanks de hulp die door het implementatieteam van het Stelsel Toegang wordt geboden, door de betrokken organisaties als best lastig wordt ervaren. Een ander obstakel dat wordt ervaren is dat het verkrijgen van het gewenste betrouwbaarheidsniveau in de praktijk kan schuren met het vraagstuk rond inclusie en toegankelijkheid van dienstverlening. Het beeld is dat in de praktijk in een dergelijke situatie de inclusie van burgers boven veiligheid wordt verkozen. Leveranciers leveren volgens geïnterviewden bovendien soms slechts één betrouwbaarheidsniveau voor alle diensten aan, waardoor differentiatie ontbreekt. Dit terwijl organisaties meerdere webdiensten op verschillende betrouwbaarheidsniveaus kunnen aanbieden. Al geldt daarbij de beperking dat dit op dit moment enkel beschikbaar is voor DigiD.

Bij BZK ontbreekt het inzicht in de vraag of organisaties de elektronische dienstverlening hebben geclassificeerd op het vereiste betrouwbaarheidsniveau. BZK onderzoekt een mogelijkheid om hierop

te monitoren. Of de classificatie van het betrouwbaarheidsniveau juist is, is aan de organisatie zelf. De organisatie draagt daarvoor de verantwoordelijkheid.

4.7.3 Overgangstermijn

De dekkingsgraad als het gaat om een inlogmiddel op betrouwbaarheidsniveau hoog is niet op een adequaat niveau, waarmee het niet mogelijk is te eisen dat de dienstverlening voldoet aan in de wet gestelde eisen. Het tijdelijk toestaan van een lager betrouwbaarheidsniveau dan eigenlijk gewenst, is volgens de wetgever naar aanleiding van het wetgevingsadvies van de Autoriteit Persoonsgegevens noodzakelijk. De door de regelgever gewenste overgangstermijn, waarbinnen dienstverleners op een lager betrouwbaarheidsniveau mogen aanbieden, is verlengd tot 1 juli 2028. Daarmee wordt extra tijd gegeven om middelen op hogere inlogniveaus (substantieel en hoog) breder beschikbaar te maken.

Deze verlenging onderschrijft het beeld dat in de te evalueren periode de gewenste betrouwbaarheidsniveaus niet zijn gehaald, dit komt zoals eerder beschreven doordat een inlogmiddel op betrouwbaarheidsniveau hoog niet breed beschikbaar is voor burgers. Hierdoor blijft het aanbod van diensten op betrouwbaarheidsniveau *hoog* ook uit. Hierdoor kunnen burgers en bedrijven niet altijd voldoen aan de gestelde eisen voor hoogwaardig digitaal inloggen, terwijl tegelijkertijd geen bruikbare alternatieven voor DigiD beschikbaar zijn. De Wdo biedt wel de ruimte voor het gebruik van private middelen in het publieke domein echter het artikel van de Wdo dat de toelating daarvan mogelijk maakt is nog niet in werking. De verplichting uit artikel 6 is eerder al uitgesteld en bij verschillende geïnterviewden leeft de verwachting dat dit opnieuw zal gebeuren.

Daarnaast vrezen sommige geïnterviewden dat een verlenging het signaal afgeeft dat de Wdo minder relevant is. Ook zou het afdoen aan het gecreëerde momentum en de geloofwaardigheid. Bovendien leidt dit volgens geïnterviewden ertoe dat de veilige toegang tot gegevens niet is geborgd. Daarmee lijkt te worden miskend dat op grond van de Wdo dienstverleners ook zelf aanvullende maatregelen kunnen nemen. Tegelijk bestaat de vrees dat de verlenging van de overgangstermijn op gespannen voet zou kunnen staan met artikel 5a/5bis van de (gewijzigde) eIDAS-verordening, waaruit de verplichting voortvloeit dat elke lidstaat verplicht is om vanaf eind 2026 ten minste één Europese portemonnee voor digitale identiteit (EDI-wallet) te verstrekken op grond van een stelsel voor elektronische identificatie op betrouwbaarheidsniveau *hoog*.

4.8 Naleving

Van de inzet van de bevoegdheden tot het uitoefenen van toezicht op de eerste fase van de Wdo is op basis van de interviews en deskresearch niet gebleken. Dit brengt volgens de geïnterviewden het risico met zich mee dat organisaties zich niet gehouden voelen om aan de wettelijke verplichting te voldoen. Meerdere geïnterviewden zien toezicht en handhaving als cruciaal voor welslagen van de (eerste fase van de) Wdo. Alleen verplichtingen opnemen is onvoldoende. Een van de geïnterviewden stelt het treffend: "Bij het ontbreken van toezicht oogt de wet dwingend, maar voelt de praktijk vrijblijvend".

Daarnaast spreekt uit de interviews een zorg dat BZK te veel petten op heeft binnen het stelsel van de Wdo, waaronder de toezichtspet. Het wordt van belang geacht om – in tegenstelling tot de huidige inrichting van het toezicht – het toezicht meer op afstand van BZK te organiseren. In lijn daarmee wordt geopperd om, gezien de aard van het stelsel van de Wdo, het toezicht in te richten als stelseltoezicht, waardoor het accent ligt op de werking van het stelsel van de Wdo als geheel en wordt afgestapt van het huidige toezicht dat meer gefragmenteerd is ingericht.

5. Conclusie

5.1 Inleiding

In dit hoofdstuk ronden we het onderzoek af. Dat betekent dat we hier de centrale vraag bespreken.

De centrale vraag van de evaluatie is:

In hoeverre is de Wdo doeltreffend en wat zijn de effecten van de Wdo, in het bijzonder op het gebied van beveiliging, privacybescherming en toegankelijkheid van elektronische dienstverlening in de praktijk?

Belangrijk hierbij is op te merken dat de artikelen over beveiliging niet in werking zijn getreden, waardoor dit onderwerp buiten de reikwijdte van het rapport valt.

Bij de verwachte doeltreffendheid van het instrumentarium gaat het om de wijze waarop en mate waarin wordt verwacht dat het instrumentarium bijdraagt aan het realiseren van de doelstellingen, waarmee een koppeling wordt gemaakt tussen de verwachte prestaties van het ingezette instrumentarium en de beoogde effecten. Ook wordt beoordeeld wat de effecten van de wet in de praktijk zijn.

De onderzoekers zien in de Wdo, voor zover in werking getreden, een toereikend instrumentarium om het daarmee beoogde doel in de basis te kunnen bewerkstelligen. Daar staat tegenover dat de concrete uitvoering van de Wdo achter blijft bij wat de wet beoogt mogelijk te maken. Dit alles maakt dat de beantwoording van de centrale vraag beperkt blijft tot de meer algemene vraag of de Wdo doeltreffend en effectief is.

In paragraaf 5.2 wordt ingegaan op de beantwoording van de centrale vraag, waarbij de onderzoekers zich baseren op de informatie uit hoofdstukken 3 en 4.

In paragraaf 5.3 doen de onderzoekers enkele aanbevelingen die mogelijkerwijs behulpzaam kunnen zijn bij het verder vormgeven van de Wdo en de uitvoering daarvan.

5.2 Bevindingen

Zoals reeds in hoofdstuk 3 uiteengezet, beoogt de Wdo de beweging naar de inzet van veiligere inlogmiddelen overheidsbreed te regelen en af te dwingen. In de kern bepaalt deze wet hoe de overheid op basis van dezelfde uitgangspunten en normen voldoet aan de eisen van de AVG en de eIDAS-verordening. Verder dwingt de wet open standaarden af, zoals het alleen nog toestaan van erkende en toegelaten inlogmiddelen, maar biedt ook handvatten, waarmee overheidsdienstverleners het juiste beveiligingsniveau van hun digitale diensten kunnen bepalen.

Zoals reeds hiervoor naar voren is gebracht voorziet de eerste fase van de Wdo op zichzelf in een toereikend instrumentarium om het beoogde doel van de Wdo in de basis te kunnen bewerkstelligen. Dat geldt ook voor de bijzondere aandachtspunten die de evaluatiebepaling – behoudens de beveiliging – benoemt, namelijk gegevensbescherming en toegankelijkheid van de elektronische dienstverlening.

Het functioneren van de Wdo in de praktijk laat echter een ander beeld zien, namelijk dat in zeer beperkte mate uitvoering wordt gegeven aan de Wdo. Hierdoor blijft het effect van de Wdo in de uitvoering uit. De reden waardoor dit effect uitblijft, is onder meer dat het daarvoor voorwaardelijke Stelsel Toegang, waarmee dienstverleners kunnen voldoen aan de geldende verplichtingen onder de Wdo, in de praktijk niet gereed en operationeel was en nog niet is;

- de functionaliteit voor burgers om te komen tot betrouwbaarheidsniveau *hoog* ontoereikend is en deze functionaliteit slechts in geringe mate wordt gebruikt;
- zijn de voorzieningen voor ouderlijk gezag en bewindvoering curatele en mentorschap die onder de reikwijdte van artikel 5 zijn mogelijk gemaakt nog in een pilotfase en kan het benodigde betrouwbaarheidsniveau met DigiD Machtigen, zoals nader uitgelegd in paragraaf 4.7.1, niet worden verkregen; en
- is, ondanks het technologie neutrale karakter van de Wdo, DigiD het enige publieke middel, waarmee DigiD als single point of failure niet wordt weggenomen.

Door het uitblijven van de uitvoering van de Wdo wordt afbreuk gedaan aan de relevantie van de Wdo voor die uitvoering. Het effect wordt nog versterkt doordat de planning van de tweede fase en de inwerkingtreding van de resterende artikelen van de eerste fase voor organisaties nog ongewis is, waardoor het voor organisaties lastig is om te anticiperen op de doorontwikkeling van de Wdo. Ondanks dat het geen onderdeel is van de Wdo, zoals inwerking getreden, leeft in het veld de zorg bij dienstverleners in hoeverre de samenhang tussen het Stelsel Toegang en het stelsel dat momenteel ontwikkeld wordt ten behoeve van de implementatie van de EDI-Wallet - zoals verplicht in de herziene eIDAS-verordening - is geborgd.

Een belangrijk positief punt van de eerste fase van de Wdo is dat het nadrukkelijk de verantwoordelijkheid van de minister van BZK voor het beheer van de voorzieningen en diensten binnen het Stelsel Toegang vastlegt. Bovendien lijkt de Wdo te hebben bijgedragen aan bewustwording rond veilig digitaal handelen en aan het bepalen van het juiste betrouwbaarheidsniveau bij digitale transacties. Ook heeft de minister van BZK – zij het terughoudend – gebruik gemaakt van zijn bevoegdheid om standaarden aan te wijzen. Echter nu aan het toezicht op de Wdo in de praktijk geen invulling is gegeven, is de naleving van de Wdo ook op deze onderdelen niet geborgd. Te meer nu ook de AP in het kader van het toezicht op de AVG gedurende de evaluatieperiode geen aandacht lijkt te hebben gehad voor de werking van de eerste fase van de Wdo. Daarnaast ontbreekt het BZK aan instrumenten om in de breedte het feitelijke effect – de zogenoemde outcome – van de uitvoering van de Wdo te monitoren. Waar het gaat om de verplichte open standaarden monitort het Forum Standaardisatie deze standaarden binnen de landelijke GDI voorzieningen als onderdeel van de jaarlijkse monitor en metingen van het Forum Standaardisatie.

Reeds voor de komst van de Wdo werd door BZK en publieke dienstverleners de noodzaak gezien om naast een voorziening voor vrijwillig machtigen tevens voorzieningen te ontwikkelen voor wettelijke vertegenwoordiging. Positief is dat de wet voldoende mogelijkheden biedt voor de ontwikkeling van aanvullende GDI voorzieningen onder artikel 5.

Ondanks dat dit buiten de reikwijdte van het onderzoek valt, kan als positief worden beoordeeld dat het stelsel van eHerkenning voor rechtspersonen op toereikende wijze functioneert ondanks dat de bepaling over inlogmiddelen voor bedrijven in de Wdo nog niet in werking zijn getreden. In dat kader kan tevens worden gewezen op het feit dat er sprake is van actief toezicht. In het verlengde daarvan wordt eveneens gewezen op DigiD dat op dit moment breed wordt gebruikt, maar niet breed beschikbaar is op betrouwbaarheidsniveau *hoog*.

De onderzoekers vragen in het bijzonder nog aandacht voor enkele gegevensbeschermingsrechtelijke aspecten.

Door het ontbreken van een in gebruik zijnde bevoegdheidsverklaringsdienst ten behoeve van de wettelijke vertegenwoordiging doet de situatie zich voor dat inloggegevens van DigiD door een betrokkene aan een ander beschikbaar worden gesteld om van elektronische dienstverlening gebruik te kunnen maken. Het risico op identiteitsfraude ligt daarmee op de loer.

Daarnaast ontbreekt het inzicht bij BZK of elektronische diensten het juiste betrouwbaarheidsniveau hanteren, waardoor het risico zich kan voordoen dat de vertrouwelijkheid van gegevens niet kan worden gewaarborgd.

Tenslotte kunnen elektronische diensten aan burgers die het betrouwbaarheidsniveau *hoog* vereisen momenteel niet op dit niveau worden geïmplementeerd aangezien er geen publiek middel (breed) beschikbaar is op dit niveau. Daarmee kunnen de overheidsdienstverleners en aangewezen organisaties in de huidige situatie bij elektronische diensten, die betrouwbaarheidsniveau hoog vereisen, niet voldoen aan de vereisten vanuit de AVG en eIDAS.

5.3 Aanbevelingen

Het zou het draagvlak voor de Wdo bij uitvoerende organisaties ten goede komen, wanneer BZK de dialoog met het veld intensiveert. Verwachtingenmanagement bij uitvoeringsorganisaties over de effectivering van het Stelsel Toegang en de inwerkingtreding van de rest van de artikelen van de eerste fase van de Wdo, is noodzakelijk om organisaties in de gelegenheid te stellen om in hun bedrijfsvoering op de (door)ontwikkeling van de Wdo te anticiperen. Dit vergt wel dat BZK transparant is naar betrokken organisaties wat het tijdschema is, waarbinnen deze ontwikkelingen zullen plaatsvinden en op welke wijze gewaarborgd wordt dat de gemaakte planning ook daadwerkelijk wordt gehaald. Dit biedt BZK bij uitstek de gelegenheid om het vertrouwen in de Wdo en de uitvoering daarvan te vergroten.

Aanbevolen wordt om duidelijk de samenhang in kaart te brengen tussen het huidige Stelsel Toegang en de huidige inlogmiddelen (DigiD voor burgers en eHerkenning voor rechtspersonen) en het stelsel dat noodzakelijk is voor de implementatie van de EDI-Wallet (inlogmiddel op hoog).

Aanbevolen wordt om het toezicht op de Wdo te heroverwegen. Haal het toezicht weg bij de minister van BZK en andere verantwoordelijke ministers en plaats het bij een toezichthouder die meer op afstand staat en onafhankelijk toezicht kan uitoefenen. Zet, gelet op de aard van het stelsel, in op stelseltoezicht, waardoor één toezichthouder in staat is het gehele stelsel te overzien en op het niveau van het stelsel kan ingrijpen in tegenstelling tot het meer fragmentarische toezicht waar de Wdo op dit moment in voorziet.

De onderzoekers vragen in het kader van het toezicht op de Wdo nog in het bijzonder aandacht voor het toezicht op de verplichte standaarden als bedoeld in artikel 3. De vrees bestaat bijvoorbeeld bij het Forum Standaardisatie dat geen toezichthouder zal worden aangewezen op toezicht op de desbetreffende standaarden te houden. De noodzaak om dit te doen is er als naar metingen, waaruit telkens duidelijk blijkt dat de wettelijke status ervan niet de beoogde groei in de adoptie heeft gebracht. Diverse partijen dringen aan op een “versterkte aanpak op het afspreken, invoeren en handhaven van (digitale) standaarden”.^{97 98} Los van de aanbeveling om tot stelseltoezicht te komen, bevelen de onderzoekers aan om vooruitlopend daarop in overweging te nemen om een toezichthouder aan te wijzen voor het toezicht op de verplichte standaarden als bedoeld in artikel 3.

Het is wenselijk om te onderzoeken of in een expliciete verplichting voor organisaties dient te worden voorzien om periodiek te toetsen of het vereiste betrouwbaarheidsniveau, gelet op technologische en

⁹⁷ NLdigital, ‘Nederland digitaal vooruit; een agenda voor de verkiezingen van 2025’, 15 juli 2025, nldigital.nl.

⁹⁸ Leden van de Tweede Kamer Commissie Digitale Zaken, *Digitaal Fundament*, 2024, geactualiseerd in september 2025, debibliotheken.nl.

organisatorische ontwikkelingen, is gewijzigd. Op deze wijze wordt geborgd dat het betrouwbaarheidsniveau actueel is en de vereiste bescherming biedt.

Bijlage 1: Bronvermelding

Wetgeving en parlementaire stukken, inclusief internetconsultaties

Besluit van 26 april 2023 tot vaststelling van het tijdstip van gedeeltelijke inwerkingtreding van de Wet digitale overheid, Stb. 2023, 160.

Besluit van de Minister van Economische Zaken van 14 april 2016, tot instelling van de Commissie van Deskundigen voor toezicht op het ETD-stelsel van 14 april 2016 (Stcrt. 2016, 20595).

Internetconsultatie Wijziging Paspoortwet i.v.m. introductie elektronische identificatie, 18 december 2017, internetconsultatie.nl

Kamerstukken II, 2017/18, 34972, nr. 3.

Kamerstukken II, 2018/19, Aanhangsel.

Kamerstukken II, 2017/18, 34 972, nr. 4

Kamerstukken II, 2019/20, 34 972, nr. 37

Kamerstukken II, 2003/04, 26 643, nr. 47

Kamerstukken I, 2020/21, 24 972, L

Kamerstukken I, 2022/23, 34 972, V

Staatssecretaris Digitalisering en Koninkrijkrelaties van 16 mei 2025 inzake Spoedbrief Digitaal Vertegenwoordigen.

Wetsvoorstel Wijziging van de Wet digitale overheid in verband met onder meer het stellen van regels over het Meldpunt Fouten in Overheidsregistraties en het Centraal Meldpunt Identiteitsfraude.

Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit

Rechtspraak

Gerechtshof 's-Gravenhage, 13 december 2007, ECLI:NL:GHSGR:2007:BC0036.

Rb. 's-Gravenhage, 18 september 2007, ECLI:NL:RBSGR:2007:BB5302.

Overige bronnen o.a. boeken, tijdschriftartikelen en (online) publicaties

Autoriteit Persoonsgegevens, brief aan het Ministerie van Volksgezondheid, Welzijn en Sport inzake patiëntauthenticatie, 4 oktober 2018.

Rijksinspectie Digitale Infrastructuur, brief inzake het resultaat UHT regeling nadere eisen Wdo, 24 mei 2024.

Digital Government, 'DigiD Usage Reaches 550 Million Logings in 2024', 6 februari 2025, *nldigitalgovernment.nl*.

Eerste Kamer, 'Wet digitale overheid', *eerstekamer.nl*.

Eerste Kamer, 'Novelle Wet digitale overheid', *eerstekamer.nl*.

eHerkenning, 'Aansluiten op eHerkenning', *eherkenning.nl*.

eHerkenning, 'Wat is eHerkenning', *eherkenning.nl*.

European Commission, 'The EU Digital Identity Framework Regulation Enters into Force', 21 mei 2024.

Forum Standaardisatie, 'Wet GDI wordt Wet digitale overheid, 20 november 2017', *forumstandaardisatie.nl*.

Forum Standaardisatie, 'Betrouwbaarheidsniveaus digitale dienstverlening', *forumstandaardisatie.nl*.

Forum Standaardisatie, 'Een handreiking betrouwbaarheidsniveaus voor digitale dienstverlening', Versie 5 (2024), *forumstandaardisatie.nl*.

Forum Standaardisatie, 'Duiding en Maatregelen Monitor Open Standaarden 2025', 26 juni 2025, *forumstandaardisatie.nl*.

Hooghiemstra & Partners, 'Rapport Strategische visie Plan van Aanpak geïntegreerd eID-stelsel', 22 april 2020, *hooghiemstra-en-partners.nl*.

Leden Tweede kamer Commissie Digitale Zaken, 'Digitaal fundament', 2024, geactualiseerd september 2025, *debibliotheken.nl*.

Logius, 'Begrippenlijst', onder eHerkenning, *logius.nl*.

Logius, 'Ruim één miljoen gebruikers eHerkenning', 15 januari 2024, *logius.nl*.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'De elektronische overheid', kennisvandeoverheid.nl.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Regelhulp betrouwbaarheidsniveaus', regelhupvoorbedrijven.nl.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Wdo biedt toekomstbestendige basis voor digitale overheid', 4 mei 2023, digitaleoverheid.nl.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Wet digitale overheid op 1 juli van kracht', 30 juni 2023, digitaleoverheid.nl.

NLdigital, 'Nederland digitaal vooruit; een agenda voor de verkiezingen van 2025', 15 juli 2025, nldigital.nl.

Vertegenwoordiging van Nederland in Aruba, Curaçao en St. Maarten, 'eNIK aanvragen', vnacs.nl.

VNG, 'Generieke Digitale Infrastructuur (GDI)', vng.nl.

VNG, 'Wet Digitale Overheid', 26 november 2024, vng.nl.

Bijlage 2: Lijst van geïnterviewde organisaties

We hebben tijdens de wetsevaluatie de volgende organisaties geïnterviewd:

- Belastingdienst
- Digidentity
- Forum Standaardisatie
- Helpdesk Digitale Zorg
- Kamer van Koophandel (KvK)
- Logius
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
- Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
- Nictiz
- Rijksdienst voor Identiteitsgegevens (RvIG)
- Rijksdienst voor Ondernemend Nederland (RVO)
- Rijksinspectie Digitale Infrastructuur (RDI)
- Uitvoeringsinstituut Werknemersverzekeringen (UWV)
- Vereniging van Nederlandse Gemeenten (VNG).

HOOGHIEMSTRA & PARTNERS

strategisch en juridisch advies



Bezuidenhoutseweg 161, 2594 AG Den Haag • T +31 (0) 6 39 27 85 33
E info@hooghiemstra-en-partners.nl • www.hooghiemstra-en-partners.nl
ING Bank NL49INGB0008938076 • KvK 73390356 • BTW 8595.06.447.B01

Directie PDD/CRD (BZK)

Aan de Staatssecretaris Digitale Economie en Soevereiniteit

Auteur

[Redacted]

Datum aangemaakt

14 april 2026

Kenmerk

nota

TER BESLISSING

Beslisnota brief toezeggingen digitalisering Eerste
Kamer april 2026

Kopie aan

Bijlage(n)

2

Parafenroute

[Redacted signature lines]

Aanleiding

Bijgevoegd vindt u een Brief aan de Eerste Kamer (EK) welke enkele toezeggingen bevat die betrekking hebben op de digitaliseringsportefeuille. In deze nota wordt u gevraagd kennis te nemen van de inhoud, en akkoord te geven op verzending van de brief. U stuurt deze brief samen met StasBZK, waarbij u eerste ondertekenaar bent. Op deze manier wordt de Commissie voor Digitalisering in één keer geïnformeerd. Separaat ontvangt u een beslisnota en te verzenden brief met moties en toezeggingen voor de Tweede Kamer.

Advies

- De brief te accorderen en daarmee te (laten) verzenden aan de EK, inclusief bijlage(n).

Kernpunten

De passages behorende tot uw portefeuille betreffen:

- De toezegging de Eerste Kamer te informeren over de resultaten van het onderzoek naar een meldvoorziening, onafhankelijk geschillenbeslechtsorgaan en kenniscentrum in het kader van de Digital Services Act (DSA) – zie ook onder 'Toelichting'.
- De toezegging de Eerste Kamer, naar aanleiding van een vraag van het lid Ganzevoort (GL), een afschrift te sturen van het toezichtkader betreffende private aanbieders van inlogmiddelen onder de Wet digitale overheid wanneer deze er is.
- De verzending van de evaluatie van de Wet digitale overheid is ook in deze brief opgenomen. U heeft dit eerder geaccordeerd samen met de in de brief opgenomen tekst, evenals verzending aan de Tweede Kamer.

Toelichting

Toezegging over het onderzoek naar een meldvoorziening, onafhankelijk geschillenbeslechtsorgaan en kenniscentrum

In de Voortgangsbrief Rijksbrede Strategie voor Effectieve Aanpak van Desinformatie werd aangekondigd dat het ministerie van BZK vervolgstappen zou zetten in de verkenning van een meldvoorziening, geschillenbeslechtsorgaan en kenniscentrum in het kader van de DSA. Hiervoor is een scenarioanalyse gemaakt. De scenarioanalyse identificeert verschillende scenario's die elk een andere aanpak voorstellen. Over de keuze tussen deze scenario's wordt u op een later moment geïnformeerd en dient u een beslissing te nemen. Toch vragen wij alvast uw akkoord om de scenarioanalyse toe te zenden aan de Eerste Kamer, om de gedane toezegging na te komen.

De resultaten van de scenarioanalyse zijn eind augustus 2025 opgeleverd. De analyse richtte zich op twee doelen:

- (a) het ondersteunen van bestaande meldmechanismen voor burgers en organisaties om schadelijke of illegale online inhoud te melden, en
- (b) het vergemakkelijken van toegang tot buitengerechtelijke geschillenbeslechting voor Nederlandse burgers, zoals voorzien in artikel 21 van de Digitaledienstenverordening.

De scenarioanalyse concludeert dat het opzetten van een onafhankelijk geschillenbeslechtsorgaan in Nederland een strategische uitdaging vormt. Er werden vier scenario's geïdentificeerd:

- Scenario 1: Een volledig geïntegreerd DSA-instituut dat meldingen en geschillenbeslechting combineert binnen één entiteit.
- Scenario 2: Een gecoördineerd netwerk met een apart geschillenbeslechtsorgaan en meldpunten, verbonden via een centrale toegangspoort of kennisplatform.
- Scenario 3: Een door de overheid ondersteund geschillenbeslechtsorgaan, gecombineerd met een centralisatie van het bestaande meldpuntlandschap.
- Scenario 4: Een versnelde opstart via samenwerking met een bestaande buitenlandse organisatie, waarbij gebruik wordt gemaakt van een bestaande backoffice en juridische infrastructuur.

Bijlagen

Volgnummer	Naam	Informatie
1	Brief Toezeggingen digitalisering Eerste Kamer maart 2026	Ter verzending
2	Bijlage - Scenario analyse: opzetten van een nieuw DSA Buitengerechtelijk Geschillenbeslechtsorgaan in Nederland	Ter verzending
3	Bijlage – Definitief rapport evaluatie Wdo	Ter verzending