Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Informatie
Wet Digitale Overheid (WDO) in het kort

Nederland digitaliseert. Er zijn steeds meer digitale transacties en de overheid moet hierin mee bewegen. Het is belangrijk om te zorgen dat veilig en overzichtelijk samengewerkt kan worden. Daarom komen er regels aan over veiligheid, regelen we de controle daarop en zorgen dat zoveel mogelijk met standaarden wordt gewerkt. Het wetsvoorstel Wet digitale overheid (WDO) legt de basis voor deze digitalisering van de overheid.

Het wetsvoorstel is een zogeheten kaderwet, de wet regelt algemene principes, verantwoordelijkheden en procedures, maar geen gedetailleerde regels. De uitwerking zal plaatsvinden in de lagere regelgeving, zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen (MR's). De wet zorgt er zo voor dat met de ontwikkelingen kan worden mee bewogen, maar dat belangrijke waarden en zekerheden voor burgers, zoals gebruikersvriendelijkheid, betrouwbaarheid, veiligheid, privacy en digitale inclusie altijd geborgd zijn. We doen dit stapsgewijs. In tranches. Dit is de eerste tranche.

De eerste tranche

Deze tranche van de wet:
- legt de taken en verantwoordelijkheden vast voor veilige toegang tot de digitale overheid;
- legt verplichtingen op aan mede-overheden om veilig en betrouwbaar aan te sluiten, en hun dienstverlening in te delen op een betrouwbaarheidsniveau;
- stelt regels over de bekostiging daarvoor en het toezicht daarop;
- biedt zekerheden voor burgers en bedrijven;
- biedt uitgangspunten voor informatiebeveiliging en de verwerking van persoonsgegevens;
- regelt het gebruik van open standaarden.

Reikwijdte van de wet

Het wetsvoorstel heeft betrekking op veilig inloggen met publieke en private inlogmiddelen op dienstverlening bij (semi-) overheidsinstanties/publieke dienstverleners.

Verplichtingen publieke dienstverleners

In de WDO is bepaald welke publieke dienstverleners onder de reikwijdte van de WDO vallen en te maken krijgen met de nieuwe regels voor de toegang tot hun elektronische dienstverlening.

Dit zijn:
- bestuursorganen in de zin van de Awb, zoals gemeenten en uitvoeringsinstanties (UWB, SVB, Belastingdienst, DUO, RDW, etc.);
- aangewezen organisaties als de zorgsector, onderwijsinstellingen en pensioenfondsen;
- de rechterlijke macht.

Na inwerkingtreding van de wet gelden de volgende verplichtingen:
- de genoemde (semi)overheidsinstanties/publieke dienstverleners moeten hun digitale diensten indelen naar betrouwbaarheidsniveau;
- zij hebben een acceptatieplicht met betrekking tot toegelaten inlogmiddelen;
- zij moeten hun informatiebeveiliging op orde hebben.

Inschalen betrouwbaarheidsniveau

Alle dienstverleners met een publieke taak moeten voor de diensten die zij verlenen **zelf** bepalen op welk eiDAS-betrouwbaarheidsniveau burger en bedrijven in moeten loggen (of op welk niveau het registreren van een machtiging vereist is). De instanties zullen dat vervolgens ook **zelf** aan hun doelgroepen moeten communiceren. Om te helpen bij het vaststellen van het betrouwbaarheidsniveau zal een ministeriële regeling opgesteld worden met criteria.

Acceptatieplicht

Alle publieke dienstverleners zijn verplicht om toegelaten en erkende inlogmiddelen te accepteren en om aan te sluiten op een publieke machtigingsvoorziening. Dit laatste is belangrijk aangezien er meer diensten digitaal aangeboden worden en iedereen het recht heeft om zich door een ander te laten vertegenwoordigen. Vertegenwoordiging moet daarom ook langs digitale weg kunnen.

Inloggen door burgers en bedrijven gebeurt met aparte inlogmiddelen. Dit heeft te maken met de aard van het gebruik (privé of zakelijk) en de daarmee samenhangende noodzaak om voor de af te nemen dienst een Burgerservicenummer (BSN) aan te leveren.

Inloggen burgers

Burgers kunnen gebruikmaken van publieke en private middelen, mits deze zijn toegelaten. Alleen toegelaten inlogmiddelen, dat wil zeggen middelen die door de overheid op veiligheid en betrouwbaarheid zijn gecontroleerd, zijn in het publieke domein toegestaan. Deze toelatingseisen zullen worden opgenomen in lagere regelgeving. Hierbij wordt aangesloten bij Europese ontwikkelingen op het gebied van digitale overheidsdienstverlening en inloggen bij de overheid: De toe te laten publieke en private inlogmiddelen moeten voldoen aan de Europese eisen aan inlogmiddelen (eIDAS-verordening). Ook het publieke inlogmiddel DigiD zal aan deze eisen moeten voldoen. Hoewel inloggen buiten de overheid bij diensten van commerciële/private partijen zoals webwinkels niet in deze wet wordt geregeld, is het toegestaan dat burgers met deze gecontroleerde private middelen (niet met het publieke middel!) ook bij deze partijen in kunnen loggen. Zo heeft het wetsvoorstel een breder effect en voordeel voor veilig inloggen.

Inloggen bedrijven
Voor bedrijven zijn reeds private inlogmiddelen beschikbaar. Ook voor deze middelen geldt dat zij erkend moeten worden door de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Erkenning wordt verleend indien voldaan wordt aan de daarvoor opgestelde eisen.

Fasering
De WDO zal gefaseerd in werking treden. De acceptatieplicht gaat pas gelden als een instantie technisch en organisatorisch klaar is om aan te sluiten. De departementen en de publieke dienstverleners stellen in samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een aansluitschema op. Dit schema bevat data waarop de acceptatieplicht geldt en een gebruiker hier rechten aan kan ontlenen. Ook hiervoor geldt dat het aansluiten op onderdelen gefaseerd kan gaan. Het aansluitschema zal daarom periodiek aangevuld worden.

Ontsluitende dienst
Om de publieke dienstverleners te ontzorgen kunnen zij via een ontsluitende dienst (routeringsvoorziening) worden aangesloten op de toegelaten en erkende inlogmiddelen. Het inloggen verloopt in dat geval via één aansluiting, ongeacht welk inlogmiddel gebruikt wordt. Dienstverleners zijn niet verplicht om zo'n ontsluitende dienst te gebruiken, zij kunnen er ook voor kiezen om direct aan te sluiten op de toegelaten en erkende middelen.

Eisen aan informatieveiligheid
De WDO stelt eisen aan informatieveiligheid. Binnen de digitale overheid werken verschillende organisaties in een keten met elkaar samen. Het is daarom voor zowel afzonderlijke overheidsorganisaties als de Generieke Digitale Infrastructuur (GDI) zelf belangrijk dat iedereen de informatiebeveiliging op orde heeft. Immers beveiligingsproblemen bij een organisatie kunnen uitwaaieren naar andere organisaties. Daarom stelt de WDO beveiligingseisen aan de digitale toegang tot overheidsdienstverlening.

De wet regelt daarnaast ook:

Toezicht
De WDO regelt dat er toezicht is op de verplichtingen die worden opgelegd.
- onafhankelijk toezicht op de aanbieders van inlogmiddelen (door Agentschap Telecom)
- toezicht op de veiligheid van overheidsdienstverleners door een jaarlijkse auditverplichting
- interbestuurlijk toezicht op overheden ten aanzien van acceptatieplichten van middelen, toepassing juiste betrouwbaarheidsniveaus door de overheidsdienstverleners

Privacybescherming
Het wetsvoorstel van de WDO bevat grondslagen voor de verwerking van persoonsgegevens die voor overheden en private partijen noodzakelijk zijn voor de uitvoering en het verlenen van veilige toegang tot de elektronische dienstverlening.

Daarnaast zullen er nog regels opgesteld worden over de verstrekking van persoonsgegevens en de bewaartermijnen ervan. Ook zullen er eisen gesteld worden aan verwerking, beveiliging en betrouwbaarheid van persoonsgegevens. Uitgangspunt hierbij zullen AVG-beginselen zijn als dataminimalisatie, transparantie en het waarborgen van kwaliteit van de persoonsgegevens. Om burgers te kunnen helpen als er onverhoopt zaken verkeerd gaan, regelt de WDO dat er mogelijkheden zijn om dat snel te onderkennen en de gevolgen te herstellen.

Standaardisatie door verplichting van open standaarden
Burgers en bedrijven moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid goed en veilig verloopt. Het gebruik van open standaarden draagt daaraan bij. In het wetsvoorstel is daarom een grondslag opgenomen, waarmee open standaarden bij algemene maatregel van bestuur (AMvB) verplicht kunnen worden gesteld. Het is niet de intentie om *alle* standaarden verplicht te gaan stellen, maar dit per geval te bezien.

De HTTPS-standaard ('het slotje op een website') wordt zonder meer verplicht.

Dit is een publicatie van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011 | 2500 EA Den Haag

September 2020