



Rijksoverheid

Beleidskompasformulier voor internetconsultatie



 **Beleidskompas**

Wie zijn belanghebbenden en waarom?

Hulpvragen

- Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?

Direct betrokken:

- Organisaties die overheidsdiensten verlenen

Indirect betrokken

- Iedereen die inlogt bij overheden of semi-overheden
- ICT-Auditors

- Wie beschikken er over relevante kennis over en ervaring met het vraagstuk?

- ICT-auditors
- (Semi)-overheden

- Op welke wijze ga je belanghebbenden tot nu toe in de verschillende fasen van het beleidstraject betrekken?

(Semi)-overheden zijn specifiek gevraagd inbreng op een concept te leveren. ICT-auditors hebben bijgedragen aan de totstandkoming van de normen in de regeling.

1. Wat is het probleem?

Hulpvragen

- a) Wat is het probleem?

Toegang tot elektronische overheidsdiensten moet veilig zijn. Wanneer die veiligheid niet voldoende is geborgd kunnen onbevoegden toegang krijgen tot gevoelige gegevens en kan identiteitsfraude plaatsvinden. De Minister van BZK is verantwoordelijk voor het elektronische stelsel voor toegang tot overheidsdiensten. De veiligheid van dat stelsel kan in gevaar worden gebracht wanneer de ICT-voorzieningen die dienstverleners gebruiken om toegang te verlenen onvoldoende beveiligd zijn.

- b) Wat zijn de oorzaken van het probleem?

Beveiligingsrisico's kunnen verschillende oorzaken hebben, die verschillen van zeer technisch tot organisatorisch. Zo kan het invoeren van afwijkende tekens in een invoerscherm een risico vormen, maar ook het ontbreken van voldoende lerend vermogen in de organisatie.

- c) Wat is de omvang van het probleem?

Deze problemen kunnen zich bij alle verleners van overheidsdiensten voordoen.

d) Wat is het huidige beleid en wat heeft de evaluatie opgeleverd?

De huidige praktijk bestaat al meer dan 10 jaar. In die jaren zijn aanpassingen doorgevoerd. De meest recente wijzigingen zijn vorig jaar doorgevoerd. Voor een evaluatie daarvan is het nog te vroeg.

e) Wat gebeurt er als de overheid niets doet (Nuloptie)? Wat rechtvaardigt overheidsinterventie?

Wanneer de Wet digitale overheid in werking treedt moeten de bestaande regels, die privaatrechtelijke van aard zijn, worden omgezet in publiekrechtelijke regels, anders kunnen deze niet meer worden toegepast. Het omzetten van de regels naar een publiekrechtelijk kader is dus de-facto de nuloptie.

2. Wat is het beoogde doel?

Hulpvragen

- a) Wat zijn de beleidsdoelen?

Borgen van voldoende beveiliging bij publieke dienstverleners die aangesloten zijn op het stelsel toegang.

- b) Aan welke [duurzame ontwikkelingsdoelen \(sustainable development goals, SDG's\)](#) en [brede welvaartsuitkomsten](#) dragen de doelen bij?

De beleidsdoelen dragen niet specifiek bij aan een van de duurzame ontwikkelingsdoelen of welvaartsuitkomsten. Veilige toegang tot overheidsdiensten kan uiteraard wel van invloed zijn op deze doelen en uitkomsten.

3. Wat zijn opties om het doel te realiseren?

Hulpvragen

- a) Wat zijn kansrijke aangrijpingspunten om het doel te realiseren?

Er bestaat al enige jaren een praktijk voor dit vraagstuk. Binnen de context van de wet kan worden gekozen voor meer of minder vergaande veiligheidsnormen of het continueren van de bestaande situatie.

- b) Wat zijn, gegeven de aangrijpingspunten, kansrijke beleidsopties?

De huidige praktijk bestaat al enkele jaren en daarmee bestaat voldoende grip op de beveiligingsrisico's.

- c) Wat is de beleidstheorie per kansrijke beleidsoptie?

Gelet op de ervaringen in voorgaande jaren is het continueren van de bestaande praktijk de meest kansrijke wijze om het beleidsdoel te (blijven) halen.

4. Wat zijn de gevolgen van de opties?

Hulpvragen

- a) Wat zijn de verwachte gevolgen per beleidsoptie?

Wanneer de beveiligingsnormen worden beperkt nemen de lasten voor overheidsdienstverleners af, maar nemen de beveiligingsrisico's toe. Bij het handhaven

van de bestaande praktijk blijven zowel de lasten als de risico's gelijk en bij uitbreiding van de normen nemen de lasten toe en de risico's verder af.
Verwacht wordt dat de bestaande risico's voldoende worden gedekt door de huidige normen die met deze regeling worden gecontinueerd.

b) Welke verplichte toetsen zijn van toepassing en wat zijn daarvan de uitkomsten?

Geen.

5. Wat is de voorkeursoptie?

Hulpvragen

a) Wat is het voorstel?

Voorgesteld wordt de huidige normen en wijze van controle daarop vast te leggen in een ministeriële regeling op grond van de Wet digitale overheid.

b) Hoe houdt het voorstel rekening met:

- [Doeltreffendheid](#) en [doelmatigheid](#);
- Uitvoerbaarheid voor alle relevante partijen (inclusief [doenvermogen](#), [regeldruk](#) en [handhaving](#));
- Brede maatschappelijke impact?

In de bestaande praktijk zijn de maatschappelijke belangen van goed beveiligde overheidsvoorzieningen en van lage overheidslasten in balans.

c) Wat zijn de risico's en onzekerheden van dit voorstel?

Onbekend is hoe de beveiligingsrisico's zich zullen ontwikkelen. Afhankelijk van eventuele ontwikkelingen zal aanpassing van de regeling in de toekomst nodig kunnen zijn.

d) Hoe ziet de voorgenomen [monitoring en evaluatie](#) eruit?

De rapportagecyclus is jaarlijks. Op basis van die cyclus wordt geëvalueerd of het aanpassen van bestaande normen en wijze van controle wenselijk is.