

202401039



Kabinet Minister-President
Ministerie van Algemene Zaken

> Retouradres Postbus 20001 2500 EA Den Haag

Tweede Kamer der Staten Generaal
t.a.v. de informateur dhr. R. van Zwol
Postbus 20018
2500 EA DEN HAAG

Kabinet Minister-President

Binnenhof 19
2513 AA Den Haag
Postbus 20001
2500 EA Den Haag
www.rijksoverheid.nl

Onze referentie

4396906

Datum 23 april 2024

Geachte heer Van Zwol,

Bijgaand doe ik u antwoorden toekomen op vragen gesteld aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (kenmerk 202400996).

DE MINISTER-PRESIDENT,
Minister van Algemene Zaken,
namens deze,
De Secretaris-Generaal

d



> Retouradres Turfmarkt 147

Aan de Minister-President
minister van Algemene Zaken
drs. M. Rutte
Binnenhof 19
2513 AA Den Haag

Turfmarkt 147
www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk
[www.linkedin.com/company/
ministerie-van-bzk](https://www.linkedin.com/company/ministerie-van-bzk)

Kenmerk
2024-0000243166

Uw kenmerk

Datum 22 april 2024
Betreft Verzoek informatie ten behoeve formatie
(202400996)

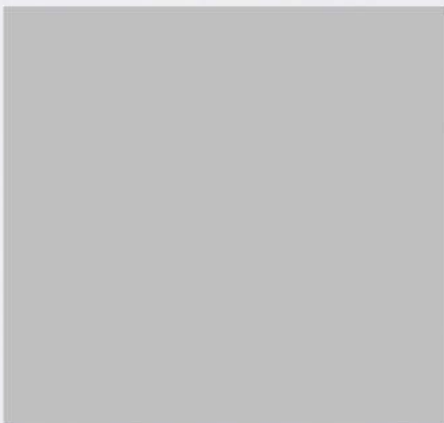
Geachte heer Rutte,

U heeft ons het verzoek doen toekomen van de informateurs te informeren over de voorwaarden waaraan het gebruik van AI door de overheid is/wordt gebonden. Onder meer ten aanzien van veiligheid, privacy en rechtsbescherming (kenmerk 202400996). Ik heb deze vraag geïnterpreteerd als de voorwaarden die gelden voor een verantwoorde inzet van AI door de overheid. Hierbij leg ik de term AI iets breder uit en betrek ik ook algoritmen in de beantwoording, omdat deze sterk verband houden met AI en er deels dezelfde regelgeving op van toepassing is.

Bijgaand treft u de verzochte informatie. Ik wil u vragen deze informatie door te geleiden naar de informateurs.

Hoogachtend,

Namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
de secretaris-generaal van het ministerie van Binnenlandse Zaken en
Koninkrijksrelaties,



Datum

Kenmerk
2024-0000243166

Bijlage 1: Beantwoording verzoek

Vooraf

Uw vraag ziet specifiek op het gebruik van AI door de overheid. Het thema AI is een belangrijk onderdeel van de digitale uitdagingen in Nederland en internationaal. In dat kader attendeer ik u graag op bijgaand document dat ingaat op de bredere context van digitalisering. In dit *hoofdfiche Digitalisering* hebben departementen, provincies, gemeenten en waterschappen gezamenlijk de meest urgente opgaven benoemd. Van digitale economie tot samenleving, van cybersecurity tot het doordacht delen van gegevens. Dit wordt verder uitgewerkt in het bijgevoegde interbestuurlijk afgestemde *hoofdfiche Digitalisering*.

Voorwaarden voor het gebruik van AI/algoritmen bij de overheid

De voorwaarden ten aanzien van het gebruik van AI/algoritmen bij de overheid vallen uiteen in een breed wettelijk kader. Te weten:

- **De AI-verordening (inwerkingtreding juni 2024, eisen worden daarna gefaseerd van toepassing)**
De AI-verordening stelt op EU-niveau eisen aan de ontwikkeling en het gebruik van AI-systemen. AI-systemen moeten veilig zijn en fundamentele rechten respecteren. De AI-verordening reguleert alle AI-systemen, maar stelt verschillende eisen aan verschillende categorieën.¹ Bijvoorbeeld bepaalde toepassingen binnen het domein van de rechtshandhaving (zoals recidivevoorspelling) en 'essentiële publieke en private diensten' vallen onder de hoog-risico categorie. Voor AI-systemen binnen die hoog-risico categorieën gaan eisen gelden zoals aan de kwaliteit van data(management) om representativiteit te borgen en 'bias' te vermijden, eisen aan risicomangement (gezondheid, veiligheid en mensenrechten), eisen aan het loggen en monitoren van het AI-systeem, mogelijk maken van menselijk toezicht en aan de cyberveiligheid van de AI. De aanbieders van deze systemen moeten dit aantonen via een conformiteitsbeoordeling.
- **De Algemene Verordening Gegevensbescherming (AVG)²**
Wanneer persoonsgegevens worden verwerkt bij het ontwikkelen en toepassen van algoritmen/AI, moet worden voldaan aan de AVG. Belangrijke aspecten zijn bijvoorbeeld rechtmatigheid, behoorlijkheid en transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, vertrouwelijkheid en integriteit. Verwerkingsverantwoordelijken hebben de plicht hierover verantwoording af te leggen.
- **Algemene wet bestuursrecht (Awb)**
Het gaat hierbij om het waarborgen van de algemene beginselen van goed bestuur, die ook van toepassing zijn op de inzet van AI/algoritmen. Hierin ligt een belangrijk stuk van de rechtsbescherming voor burgers bij de inzet van deze technologie door de overheid, zoals ook het recht op bezwaar en beroep.
- **Algemene Wet Gelijke Behandeling (AWGB)**

¹ De categorieën zijn: verboden AI, hoog-risico AI, General Purpose AI models, AI met specifieke manipulatieve risico's en laag-risico AI

² Voor de sector rechtshandhaving geldt de Wet Politiegegevens (Wpg) en de Wet Justitiële en Strafvorderlijke gegevens (Wjsg)

Datum

Kenmerk
2024-0000243166

Deze wet is erop gericht te waarborgen dat er geen verschil wordt gemaakt op basis van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, seksuele gerichtheid, burgerlijke staat.

Daarnaast dient de overheid bij de inzet van AI/algorithmen zich aan de kaders van internationale verdragen te houden, zoals het Europees Verdrag voor de Rechten van de Mens (EVRM).

Om voor de overheid (Rijk/ZBO's, provincies, gemeenten en waterschappen) op een eenduidige manier inzichtelijk te maken hoe aan de vereisten in deze regulering moet worden voldaan bij de inzet van AI/algorithmen, is het "Algoritmekader" tot stand gekomen en in ontwikkeling.³ Dit kader brengt bovengenoemde vereisten integraal in beeld, zodat overheden AI/algorithmen op een verantwoorde manier kunnen inzetten. Ook het algoritmeregister⁴ is hier onderdeel van. Dit register is een instrument om de transparantie van overheden over de inzet van impactvolle algoritmen te bevorderen.

De Baseline Informatiebeveiliging Overheid (BIO)⁵ werkt de verplichtingen op het gebied van veiligheid nader uit. Deze is ook van toepassing op AI/algorithmen. De naleving van deze bestaande en nieuwe kaders vergt een forse inspanning van uitvoeringsorganisaties en diverse medeoverheden.

Toezicht en rechtsbescherming

Voor wat betreft het toezicht op de inzet van algoritmen en AI-systemen door de overheid, zijn verschillende toezichthouders betrokken. Zo heeft de nieuwe Directie Coördinatie Algoritmen (DCA) binnen de Autoriteit Persoonsgegevens (AP) een signalerende en coördinerende rol. Maar is er ook een toezichthoudende rol vanuit de AP waar het gaat om het gebruik van persoonsgegevens, in samenwerking met diverse sectorale toezichthouders die beschikken over domein specifieke kennis en ook bestaande bevoegdheden hebben. De AP is vanuit die rol al meermalen onderzoeken gestart naar algoritmengebruik binnen de overheid⁶. Daarnaast zijn onder meer het College voor de Bescherming van de Rechten van de Mens en de Nationale Ombudsman actief op dit terrein.

Ook de Auditdienst Rijk en de Algemene Rekenkamer⁷ doen onderzoek naar de verantwoorde inzet van AI/algorithmen binnen de overheid. Als het gaat om toezicht op de AI-verordening specifiek, wordt momenteel gewerkt aan een voorstel voor het inrichten van dit toezicht. De Rijksinspectie Digitale Infrastructuur (RDI) en de eerder genoemde DCA werken hiervoor samen met andere sectorale en digitale toezichthouders een voorstel uit. Dit omvat ook de invulling van het klachtrecht dat onderdeel is van de AI-verordening.

Generatieve AI

De meest in het oog springende ontwikkeling op het gebied van AI is de opkomst van generatieve AI, zoals chatGPT, maar ook in de vorm van beelden, foto's en video die door AI worden gecreëerd. Vanwege de schaal, snelheid en de vele

³ Zie Verzamelbrief Algoritmes reguleren (juli 2023) en <https://minbzk.github.io/Algoritmekader/>

⁴ <https://algoritmeregister.nl/>

⁵ Stcrt. 2020, nr. 7857

⁶ [Staatscourant 2020, 7857 | Overheid.nl > Officiële bekendmakingen \(officielebekendmakingen.nl\)](https://www.staatscourant.nl/overheid/Officiële-bekendmakingen-officielebekendmakingen.nl)

⁷ Bijvoorbeeld bij gemeenten.

⁷ Bijvoorbeeld in het rapport 'Algoritmes getoetst', maar ook in verantwoordingsrapporten.

Datum

Kenmerk
2024-0000243166

mogelijke toepassingen, heeft deze vorm van AI mogelijk grote gevolgen voor onze samenleving. De Europese AI-verordening stelt daarom voorwaarden aan het gebruik van General Purpose AI modellen. General Purpose AI modellen zijn grote modellen die verwerkt kunnen worden in heel veel verschillende AI-systemen, zoals GPT-4, het model achter ChatGPT. Ook in de Overheidsbrede visie op generatieve AI⁸ is het voornemen uitgesproken om verder werk te maken van het monitoren van ontwikkelingen, en het versterken van het toezicht op deze vorm van AI. Eveneens is er een voorlopig standpunt ten aanzien van het gebruik van generatieve AI voor Rijksorganisaties.⁹

Door te werken aan naleving van bestaande en komende regels voor de toepassing van algoritmen en AI in de Nederlandse samenleving en specifiek voor de overheid, zorgen we ervoor dat mensen meer regie krijgen en houden op de digitale aspecten van het leven, met vertrouwen mee kunnen in digitalisering en Nederland optimaal de kansen van digitalisering kan benutten.

⁸ [Overheidsbrede visie Generatieve AI | Rapport | Rijksoverheid.nl](#)

⁹ [Kamerbrief over voorlopig standpunt voor Rijksorganisaties bij het gebruik van generatieve AI | Kamerstuk | Rijksoverheid.nl](#)

Hoofdliche Digitalisering

Digitalisering heeft de samenleving en economie ingrijpend veranderd en zal dat blijven doen. De opgave voor het komend kabinet is om de kansen van de digitale transitie te verzilveren. Zo borgen we niet alleen brede welvaart en vergroten we bestaanszekerheid, maar helpt digitalisering ons ook om maatschappelijke opgaven op te lossen. Gelijktijdig moeten we burgers en ondernemers beschermen tegen de ongewenste effecten en risico's van digitalisering. Meer nog dan in de afgelopen jaren vraagt dit om een integrale en een verbindende aanpak. In dit kopfiche benoemt de Ambtelijke Commissie Digitalisering daarom (i) de urgente uitdagingen op het gebied van digitalisering en (ii) stelt ze een versterking van de governance voor om die uitdagingen effectief aan te gaan.

Investerings in digitalisering en technologie - zowel in de publieke als private sectoren en domeinen - zijn onmisbaar om de kansen van de digitale transitie te verzilveren. Zorgen voor een voldoende ICT-vaardige arbeidsmarkt en het stimuleren van innovatie liggen aan de basis van het versterken van het Nederlandse verdienvermogen van onze samenleving en het behouden van onze positie in Europa en daarbuiten. Ook om onze brede welvaart te borgen en de grote uitdagingen van deze tijd aan te gaan moeten we investeren in digitalisering. Die grote uitdagingen vragen immers tenslotte (ook) om technologische oplossingen.

Deze kansen pakken betekent tegelijkertijd dat we ook aandacht moeten hebben voor de keerzijde: hoe zorgen we dat risico's worden beperkt, we digitaal veilig zijn én dat grondrechten in het digitale domein worden gerespecteerd? De inzet van technologie heeft maatschappelijk gezien immers alleen waarde als het ons ook lukt om digitalisering verantwoord en doordacht in te richten zodat burgers hier geen schade van ondervinden. Dat op dit vlak nog veel werk te doen is, blijkt helaas ook uit recente tekortkomingen bij de inzet van digitalisering bij de overheid zelf. Daarom moet de digitale basis bij de overheid verder op orde worden gebracht.

Hierbij gaat het om samenhang. Digitalisering doorsnijdt organisaties én afzonderlijke thema's. Door kansen en risico's integraal te beschouwen en hier de samenleving en het bedrijfsleven actief bij te betrekken, ontstaat er een gezamenlijkheid die vele malen krachtiger is dan de huidige manier van werken. De geopolitieke context noopt tot het mitigeren van de risico's van strategische afhankelijkheden in het digitale domein, via een mix van maatregelen gebaseerd op de drieslag *promote, protect, partnership*. Dit biedt onder meer het bedrijfsleven en de wetenschap de kans om hun positie te versterken, om digitale producten, diensten en processen weerbaarder te maken en grondrechten in digitale dienstverlening en methoden te verankeren.

Departementen, uitvoeringsorganisaties, en medeoverheden vragen via dit fische aandacht voor deze opgaven in de komende kabinetsperiode. Het fische bevat de gedeelde urgente opgaven die - om impact te hebben en effectief te zijn - breed moeten worden opgepakt. Waar nodig wordt in onderliggende fiches uiteengezet wat er naast continuering van al ingezet beleid kan worden geïntensiveerd. Het totaal aan fiches wordt zo voor u een palet aan mogelijkheden dat u in deze formatie kunt gebruiken om keuzes te maken.

Dit alles vraagt vandaag om investeringen die soms pas later zullen renderen, maar nú moeten worden gedaan. Die investeringen renderen financieel en strategisch, maar ook in een toenemend vertrouwen tussen samenleving, bedrijfsleven en overheid en een meer solide digitale rechtsstaat en democratie. Naast investeren vraagt dit ook om een volgende politieke stap: om de integraliteit te borgen, en om op basis van gezamenlijke prioriteiten (schaarse) middelen te kunnen vrijmaken en effectief in te zetten, is een versterking van de governance nodig.

Met de huidige bevoegdheden en structuur als uitgangspunt, pleiten wij daarom voor een coördinerend minister voor digitalisering en een ministeriële onderraad als gremium dat bewindspersonen structureel verbindt. Ambities, doelstellingen en activiteiten worden hiermee verbonden en realisatie wordt versneld. In dit fische presenteren we een aantal manieren waarop dit degewenst gerealiseerd zou kunnen worden.

Opgave A: De basis verder op orde brengen bij de digitale overheid

De overheid moet de digitale basis verder versterken. Alleen zo blijft het mogelijk om politieke ambities te realiseren op een uitvoerbare en doelmatige manier en te voorkomen dat recente schandalen zich herhalen. Het opruimen van legacy systemen is hierbij een belangrijke stap, maar ook is een andere kijk op publieke dienstverlening nodig. We moeten naar een minder complexe context waarin iedereen publieke dienstverlening ontvangt op een toegankelijke en begrijpelijke manier. Hierbij beginnen we niet op nul, veel trajecten zijn de afgelopen jaren ingezet, het gaat om doorpakken op het:

- Verder op orde brengen van de informatievoorziening en -huishouding waarmee burgers, organisaties en het parlement inzicht wordt gegeven in het handelen en de besluiten van de overheid.
- Uitfasen van belemmerende legacy-systemen, in bijzonder bij uitvoeringsorganisaties.
- Verbeteren en (opnieuw) inrichten van de publieke dienstverlening vanuit 'één-overheid-benadering' op een manier die aansluit bij de leefwereld en context van burgers en ondernemers.
- Versnellen van de aanpak van digitale toegankelijkheid van overheidswebsites en -apps;
- Versterken van de generieke digitale infrastructuur, voorzieningen en kennis en vaardigheden in Caribisch Nederland zodat ook zij volwaardig gebruik kunnen maken van digitalisering;
- Versterken van de beschikbare IT-expertise bij de overheid.

Achtergrond bij mogelijke intensivering treft u aan in: *Fiche 1 – Open en Transparante Overheid, Fiche 2 – Digitale overheid: de basis op orde, Fiche 3 – Tegengaan van niet gebruik sociale regelingen. Fiche 4 -Toekomstvaste Informatievoorziening (J&V), Fiche 5 – Informatiebeleid en archiefwet*

Opgave B: Verdienvermogen versterken in een groene digitale economie

Digitalisering draagt bij aan brede welvaart en is onmisbaar in de economie ten behoeve van een duurzame samenleving. Nederland loopt voorop in Europa, maar behoud van deze positie is geen rustig bezit. Om voorop te blijven is blijvende aandacht voor innovatie nodig. Toepassing van geavanceerde digitale technologieën door het bedrijfsleven helpt de productiviteit te vergroten en heeft daarmee een grote, positieve impact op het verdienvermogen en brede welvaart. Ook de ontwikkeling van digitale gemeenschapsgoederen kan hieraan bijdragen. Het fundament onder deze digitale economie is onze digitale infrastructuur. Het gaat om een breed netwerk van regionale en internationale verbindingen van onder meer zeekabels, datacenters en internetknooppunten. Dit moeten we versterken, terwijl we rekening houden met de impact van digitalisering op het klimaat. Tezamen met de EU is het belangrijk een groene digitale transitie te borgen. De opgave is om de sterke positie van Nederland op langere termijn te versterken en genoemde randvoorwaarden stevig te verankeren. Dit kan door het:

- Versterken van de hoogwaardige, betrouwbare en veilige infrastructuur met connectiviteit van wereldklasse met behoud van een vrij en open internet door het multi-stakeholder model;
- Versterken en verbinden van data-ecosystemen in samenwerking met de Europese Commissie;
- Versterken Nederlandse en Europese ecosysteem op het gebied van AI;
- Inzetten op digitalisering én duurzaamheid om een groene digitale economie te borgen: zowel verduurzaming van de IT-sector als de bijdrage van digitalisering aan verduurzaming van sectoren.
- Versteven van de samenwerking tussen het bedrijfsleven, de wetenschap en overheid om zo sneller tot nieuwe inzichten en innovatieve toepassingen te komen die bij succes opgeschaald kunnen worden.

Achtergrond bij mogelijke intensivering treft u aan in: *Fiche 6 – Digitale Infrastructuur, Fiche 7 – AI verdienvermogen, Fiche 8 - Waardengedreven AI benutten voor maatschappelijke opgaven, Fiche 9 – Digitalisering Goederenvervoer.*

Opgave C: Versterken van mensgerichte digitalisering

Iedereen moet erop kunnen vertrouwen dat grondrechten worden gerespecteerd; ook in de digitale wereld. Dat is nu niet altijd vanzelfsprekend. Zo ontwikkelen sommige bedrijven applicaties die kwetsbare groepen als jongeren verleiden, werken toepassingen soms discriminerend, en ondermijnt desinformatie het publieke debat. Actie is nodig om burgers in de samenleving te beschermen, hen meer regie te geven over het digitale leven en te zorgen dat mensen centraal staan bij de ontwikkeling en inzet van data en technologie. Dit kan onder meer door:

- Een duidelijke, scherpe aanpak voor de verantwoorde en mensgerichte inbedding van nieuwe technologie, met daarbij specifieke aandacht voor rechtshandhaving en rechtsbescherming;
- Versterkte inzet op mensgerichte artificiële intelligentie;
- Actieplan om kinderrechten in de digitale wereld verder te beschermen;
- Toezicht op wet- en regelgeving in het digitale domein te versterken;
- Stimuleren en inzetten van alternatieven voor online platformen en diensten bij publieke instellingen;
- Uitbouwen van instrumenten om discriminatie te voorkomen en kwetsbare groepen te beschermen.

Dit kan grotendeels worden verwezenlijkt door het continueren van bestaand beleid. Achtergrond bij een aantal mogelijke intensiveringen treft u aan in: *Fiche 10 – Digitaal toezicht*, *Fiche 11 – Digitale autonomie en eigen alternatieven (maatregelen inzake gemeenschapsgoederen)*, *Fiche 12 – Digitale rechtsstaat*,

Opgave D: Burgers versneld digitaal vaardiger maken

Veel Nederlanders hebben onvoldoende digitale vaardigheden en mediawijsheid om zich digitaal te kunnen redden en zich bijvoorbeeld te kunnen weren tegen phishing of desinformatie. Daarnaast is een aanzienlijk aantal bestuurders in het bedrijfsleven en de overheid onvoldoende geletterd en schat daardoor kansen én risico's verkeerd in. De opgave is om adequate ondersteuning te bieden aan burgers die digitaal vastlopen en digitale vaardigheden te verbeteren, met aandacht voor behoud van analoge alternatieven om digitale uitsluiting te voorkomen. Dit kan onder meer door:

- Sterker verankeren van digivaardigheden en mediawijsheid in het (groene) onderwijs.
- Opzetten van lokale ondersteuningsnetwerken voor hulp bij digitale vragen in gemeenten waarin bibliotheken, zorg- en welzijnsinstellingen en private organisaties samenwerken.
- Uitbreiding van lokaal leeraanbod, een impuls op online cursusaanbod waarmee mensen thuis kunnen oefenen en opschaling van de gratis Digihulplijn.

Achtergrond bij mogelijke intensiveringen treft u aan in: *Fiche 13 – Digitalisering funderend onderwijs*, *Fiche 14 – Versterken van digitale inclusie*, *Fiche 15 – Versterken vertrouwen journalistiek*

Opgave E: Arbeidsmarkt en ICT-tekorten

Er zijn grote uitdagingen op de arbeidsmarkt. Nederland en Europa kampen met een groot tekort aan ICT'ers en specialisten met digitale vaardigheden. Dit beperkt ons in de mogelijkheid om kansen te benutten en risico's te mitigeren. In het Actieplan groene en digitale banen zijn al stappen gezet, maar er is meer nodig. Dit kan door de instroom in bètatechnisch onderwijs te verhogen, instroom en behoud van technisch personeel op de arbeidsmarkt te versterken (door aantrekkelijk werkgeverschap), bijscholing en opschaling van succesvolle regionale publiek-private scholingsinitiatieven en het verhogen van productiviteitsgroei door inzet van (proces) innovaties via digitalisering.

Achtergrond bij mogelijke intensiveringen treft u aan in: *Fiche 16 – Digitaal Talent*.

Opgave F: Nederland digitaal veiliger en meer weerbaar maken

De digitale dreiging voor Nederland is groot. Statelijke actoren zetten cyberaanvallen in om geopolitieke doelen te bereiken, afpersing vormt een aantrekkelijk verdienmodel voor criminelen en de snelle ontwikkeling van nieuwe technologieën als Quantum en AI geeft kansen voor betere weerbaarheid maar gaat ook gepaard met nieuwe dreigingen. Tegelijkertijd blijft de groei in weerbaarheid en risicobesef achter. De opgave is om deze scheefgroei te verkleinen en te zorgen dat incidenten sneller worden opgemerkt en gemitigeerd zodat de gevolgen en schade voor economie en samenleving beperkt blijven.

Achtergrond bij mogelijke intensiveringen treft u aan in: *Fiche 17 – Cybersecurity en cybercrime* en in *Fiche 18 – Veilige havens (digitale veiligheid)*

Opgave G: Mitigeren van de risico's van strategische afhankelijkheden in het digitale domein

Als land autonoom keuzes kunnen maken is ook digitaal een belangrijk doel. De ontwikkeling van digitale technologie is onderdeel geworden van een geopolitieke krachtmeting. Landen bouwen daarom gericht strategische capaciteit op in cruciale posities binnen waardenketens. Het versterken van de digitale competenties, mitigeren van de risico's van strategische afhankelijkheden en uitbreiden van (Europese en mondiale) partnerschappen zijn daarom cruciale en urgente politieke thema's geworden. Om onze weerbaarheid en open strategische autonomie te vergroten is een gecoördineerde aanpak belangrijk, onder meer door gericht maatregelen te nemen om risico's te mitigeren en investeringen in essentiële technologieën als cloud, AI, cybersecurity en 5G/6G. Daarnaast is het belangrijk om te blijven inzetten op spelregels voor digitale markten en diensten. Mitigeren van de risico's van strategische afhankelijkheden kan onder andere via de volgende sporen:

- Promote: behoud en vergroten van kennis over – en stimuleren van – sleuteltechnologieën en – toepassingen in strategische sectoren, denk aan netwerktechnologieën (5G/6G), AI, Cloud, dataruimtes en Cybersecurity;
- Protect: beschermen van die onderdelen van het digitale domein waar ongewenste zeggenschap of afhankelijkheden kunnen leiden tot risico's voor ons verdienvermogen, de nationale veiligheid, grondrechten, publieke waarden of andere belangen;
- Partnership: samenwerking met strategische partners wereldwijd op de ontwikkeling van – en het kunnen beschikken over digitale sleuteltechnologieën. Tevens versterken van de Europese – en mondiale coalities voor waardengedreven digitaliseren, onder meer met het oog op het ontwikkelen van internationale kaders/normen op nieuwe technologieën;

- Opschalen van de ontwikkeling en het gebruik van digitale gemeenschapsgoederen als open leermaterialen, open source software en hardware en open data om publieke waarden te beschermen;
- Realiseren van specifieke, eigen toepassingen zoals een Nationale (Overheids)Cloud en Wallet;
- Scherpe regulering en bijbehorend toezicht van digitale markten en diensten in Europees verband.

Achtergrond bij mogelijke intensivering treft u aan in: *Fiche 19 – Economische Veiligheid en Weerbaarheid* en in *Fiche- 11 Digitale Autonomie en eigen alternatieven*

Opgave H: Data en digitalisering benutten voor maatschappelijke opgaven

Gelijktijdig met- en voortbouwend op het op orde brengen van de basis (opgave A) is er een gedeelde ambitie om gegevens beter en op rechtmatige wijze te benutten om aan maatschappelijke opgaven te werken. Van klimaat en mobiliteit, en van zorg-, agro- tot het justitiedomein: overal kan data worden gebruikt om ons land verder te helpen en te sturen op de beschikbaarheid en kwaliteit van voorzieningen. Dit geldt in bijzonder ook voor het sturen in de fysieke leefomgeving, op land én zee. In alle sectoren lopen overheden en bedrijven tegen vergelijkbare problemen aan omtrent infrastructuur, gegevensdeling en standaarden. Daarom missen we kansen. Dit doorbreken kan onder meer door:

- Het onderhouden¹ en organiseren van het verantwoord data delen tussen overheden en relevante partijen in data-ecosystemen, in het bijzonder door in te zetten op vergaande standaardisatie in een federatief datastelsel en dataspaces;
- In het verlengde daarvan inzetten op een centrale versnellingsaanpak voor verantwoorde gegevensdeling, bijvoorbeeld bij interpretatieverschillen van wet- en regelgeving of waardenspanning;
- Vergroten van vertrouwen in de data-economie door het versterken van grip op data door burgers en bedrijven via uitvoering van Europese wetgeving en het bevorderen van datadelings- en afsprakenstelsels;
- Het ontwikkelen van digitale representaties (digital twins) van fysieke leefomgevingen;
- Digitalisering van data-inwinning, -transport en -uitwisseling voor wettelijke overheidstaken op gebied van toezicht, handhaving, beheer en beleid in de fysieke leefomgeving. Zodat het samengaan van waterbeheer, bodemgebruik, energie opwekking, landbouw, infrastructuur, woningbouw én bescherming van onze natuur is geborgd. Hieronder valt ook de digitaliseringsopgave voor de beveiliging van strategische infrastructuur tegen statelijke dreigingen (zowel cyber - als fysieke dreiging)

Achtergrond bij mogelijke intensivering treft u aan in: *Fiche 20 – Doorbreek de problemen met gegevensdeling*, *Fiche 21 – Gegevensuitwisseling (VWS)*, *Fiche 22 – digitalisering in het landbouw-, natuur,- en voedseldomein* en *Fiche 23 – Data en digitalisering mobiliteit*. Daarnaast worden in de *Fiches 24 – Windenergie op de Noordzee*, *Fiche 25 – Beveiliging Noordzee infrastructuur* en *Fiche 26 – Bodemdaling (landelijke bodemdalingsmeetsysteem)* delen van bovengenoemde digitaliseringsopgave meegenomen.

Opgave I: Uitvoerbare wet- en regelgeving en adequaat toezicht

Duidelijke regels en stevig toezicht zijn essentieel voor een eerlijke digitale economie en betrouwbare toepassing van technologie in de samenleving. Om de digitale transitie te versterken, sturen en vertrouwen te vergroten, hebben de Europese en nationale wetgever nieuwe wetgeving geïntroduceerd die in samenhang dient te worden geïmplementeerd. Om dit op een haalbare en verantwoorde wijze te kunnen doen moeten departementen, uitvoeringsorganisaties, de toezichthouder, bedrijven en medeoverheden worden ondersteund met voldoende handvatten, beperkte regeldruk en standaarden. Als we nú niet investeren in de implementatie van die wetten en het toezicht daarop, zal de naleving van bestaande en nieuwe wetgeving tekort blijven schieten. Dit kan door het:

- Investeren in capaciteit om (nieuwe) regels uit te voeren.
- Stimuleren van kennisdeling en samenwerking om te borgen dat vraagstukken gezamenlijk worden opgelost, in plaats van ieder voor zich. Bijvoorbeeld kijkend naar de openbare registers bij verschillende ministeries.
- Versterken van effectief en meer integraal toezicht op digitale regelgeving en het digitale domein;

Achtergrond bij mogelijke intensivering treft u aan in: *Fiche 12 – Digitale Rechtsstaat*, *Fiche 10 – digitaal toezicht* en *Fiche 27 - efficiëntere implementatie digitale wet- en regelgeving*

¹ Bijvoorbeeld het digitaal stelsel mobiliteitsdata waarin private partijen, gemeenten, provincies en Rijksoverheden samenwerken om groene mobiliteit te stimuleren en waardoor Nederlanders efficiënter van A naar B kunnen reizen.

Governance

De huidige governance gaat uit van een coördinerend staatssecretaris voor digitalisering. Voor realisatie van kabinetsbrede ambities werkt die staatssecretaris samen met bewindspersonen en bestuurders van departementen en medeoverheden die vanuit eigen politieke- en bestuurlijke verantwoordelijkheden sturen op de verschillende digitaliseringsonderwerpen en de eigen digitale organisatie. Op beleidsmatig vlak wordt door de staatssecretaris intensief samengewerkt met de minister van Justitie en Veiligheid (digitale veiligheid) en de minister van Economische Zaken (digitale economie) gelet op hun brede coördinerende verantwoordelijkheden op digitale thema's. Om de samenwerking en (interdepartementale) afstemming op ambtelijk niveau te ondersteunen is de Ambtelijke Commissie Digitalisering ingesteld.

De huidige organisatie en werkwijze functioneren over het algemeen goed en dragen bij aan het goed bedienen van de Vaste Kamercommissie Digitale Zaken van de Tweede Kamer. Echter, in bepaalde gevallen wordt ervaren dat de huidige governance te weinig mogelijkheden biedt om politiek, beleid en uitvoering interbestuurlijk integraal te verbinden. Dit geldt in bijzonder in situaties waar snel gereageerd moet worden, of wanneer wordt gewerkt aan opgaven die niet helder of bij veel verschillende departementen belegd zijn.

Om dit voortbouwend op de kwaliteit van het huidig model te adresseren stellen wij voor om – met behoud van huidige bevoegdheden van departementen en medeoverheden als uitgangspunt – een coördinerend minister voor digitalisering te benoemen en een ministeriële onderraad voor digitalisering in te richten.² Dit biedt het kabinet en in het verlengde daarvan de beide Kamers de volgende voordelen:

- Werkbare en doelmatige uitvoering van digitalisering wordt beter dan nu meegenomen in besluitvorming;³
- Het wordt voor bewindspersonen makkelijker om over de grenzen van de eigen ministeriële verantwoordelijkheid samen te werken aan digitalisering vanuit een integrale blik;
- Er kan snel tot breed gedragen politieke keuzes worden gekomen volgens een inzichtelijk proces;

Een onderraad verbindt bewindspersonen structureel, brengt daarmee samenhang in ambities, doelstellingen en activiteiten en kan zowel lopende processen als de reactie op urgente kwesties versnellen. Daarnaast geeft het kabinet door het benoemen van een coördinerend minister het noodzakelijke gewicht aan het onderwerp. Binnen dit voorstel onderscheiden wij in ieder geval twee opties:

1. Minister voor digitalisering die werkt aan de domein overstijgende opgaven op het gebied van digitalisering, zoals onder meer beschreven in dit fiche⁴
2. Coördinerend minister voor digitalisering, geflankeerd door ministers die coördineren op de kernopgaven op het gebied van digitale veiligheid, economie, samenleving en overheid.

Om de governance verder te versterken wordt daarnaast voorgesteld om de bestaande overleg- en besluitvormende gremia te versterken, in bijzonder om de Nederlandse positie in de EU en internationaal goed voor het voetlicht te kunnen (blijven) brengen en de uitvoering de noodzakelijke ruimte te bieden.

² Voorstel hierbij is om cybersecurity zoals nu het geval is vanwege samenhang met economische en nationale veiligheid aangesloten te houden bij de bestaande Raad voor Defensie, Internationale, Nationale en Economische Veiligheid (RDINEV).

³ Hierbij zal verbinding moeten worden gezocht met de Ministeriële Commissie Uitvoering (MCU)

⁴ Hierbij wordt niet afgedaan aan bestaande verantwoordelijkheden van bewindspersonen op gebied van (digitale) veiligheid, economie en overheid.