

Overzicht: Richtlijnen, Wetgeving en Best Practices voor Digitale Gemeenschapsgoederen

Beleidskaders en richtlijnen van de overheid

- **Open source beleid ("Open, tenzij")** – De Nederlandse overheid hanteert het principe "Open, tenzij": overheidssoftware moet in principe als open source beschikbaar zijn, tenzij er zwaarwegende redenen zijn om dat niet te doen [1](#) [2](#). Dit kabinetsbeleid voor transparantie blijkt o.a. uit het openstellen van broncode, zoals de DigiD-app waarvan Logius de code publiek maakte in lijn met dit beleid [3](#). Het Ministerie van BZK heeft in 2023 ook een Open Source Program Office opgericht om open source werken binnen de overheid te stimuleren en interne drempels weg te nemen [4](#).
- **Handreikingen voor AI en algoritmen (VNG/IBD)** – De Informatiebeveiligingsdienst (IBD) van de VNG publiceerde een *Handreiking AI en Algoritmen* voor gemeenten (jan 2024) [5](#). Deze gids (13 pag.) geeft Functionarissen Gegevensbescherming en Privacy Officers een overzicht van wat AI en algoritmen zijn, de kansen en risico's, en passende maatregelen [6](#). Er worden rollen en verantwoordelijkheden beschreven en praktijkvoorbeelden gegeven (bijv. een druktemeter en een chatbot), inclusief aandacht voor privacyregels [7](#). Doel is gemeenten handvatten te bieden om veilig en verantwoord met AI om te gaan.
- **Overheidsbrede handreiking Generatieve AI** – In april 2025 is een overheidsbrede handreiking verschenen met spelregels voor het gebruik van generatieve AI binnen alle bestuurslagen [8](#) [9](#). Hierin staan technologische, organisatorische, ethische en juridische randvoorwaarden voor verantwoorde inzet van AI [10](#). Ambtenaren krijgen hiermee ruimte om bijvoorbeeld ChatGPT-achtige tools te testen, mits ze voldoen aan voorwaarden rondom privacy, veiligheid en betrouwbare modellen [8](#) [11](#). De handreiking moedigt het gebruik van Europese toepassingen en open-source oplossingen aan [12](#). Deze richtlijn is tot stand gekomen onder coördinatie van BZK in samenwerking met gemeenten, provincies en waterschappen [13](#).
- **Nederlandse Digitale Strategie (NDS)** – De Nederlandse Digitaliseringstrategie is het overheidsbrede strategisch kader voor digitalisering (onder coördinatie van de Staatssecretaris Digitalisering). Hierin wordt aandacht besteed aan digitale soevereiniteit, het gebruik van open technologie en samenwerking tussen overheden. Een nieuwe NDS wordt in 2025 verwacht [13](#). Onder deelstrategieën vallen o.a. de datastrategie, AI-strategie en cybersecuritystrategie.
- **Logius en standaardisatie** – Logius beheert de digitale overheidsinfrastructuur (zoals DigiD, eHerkenning) en bevordert het gebruik van open standaarden. Voorbeeld is de Nederlandse API Strategie (gecoördineerd via Logius/Geonovum), die afspraken en NL GOV-standaarden biedt voor het ontwerpen van interoperabele, veilige en toegankelijke API's. Ook maakt Logius broncode openbaar (zoals DigiD) ter bevordering van transparantie [3](#). Verder werkt Logius samen met het **Forum Standaardisatie** aan de "*pas-toe-of-leg-uit*"-lijst van open standaarden (zie onder *Open standaarden*).

- **ICTU en open source samenwerking** – ICTU (ICT Uitvoeringsorganisatie) ondersteunt digitale projecten voor overheden en beheert platforms zoals het *Developer Overheid* open-source register. In dit register kunnen overheden bestaande open source componenten vinden en hergebruiken ¹⁴. Ook initieert ICTU pilots en communities (bijv. Pleio) waar ontwikkelaars en beleidmakers kennis delen over open source oplossingen en standaarden.
- **RDDI en informatiehuishouding (Woo)** – Het Rijksprogramma Duurzaam Digitale Informatiehuishouding (RDDI) helpt overheden hun informatiebeheer op orde te brengen in het kader van de Wet open overheid. RDDI ontwikkelt samen met Platform Open Overheid praktische hulpmiddelen voor actieve openbaarmaking per Woo-informatiecategorie ¹⁵. Voor elke categorie overheidsinformatie is een werkdefinitie, manier van publiceren en hulpmiddel (checklist, sjabloon) beschikbaar op Open-overheid.nl ¹⁵. Ook biedt RDDI handreikingen (“Woo, dat zit zo”) en e-learnings via het Leerhuis Informatiehuishouding, zodat vooral riksorganisaties maar ook decentrale overheden voldoen aan Woo-verplichtingen (zoals het tijdig publiceren van besluitenlijsten, Kamerstukken, etc.).

Relevante wet- en regelgeving

- **Wet open overheid (Woo)** – Vervangt de Wob en heeft als doel transparantie te vergroten. Overheden moeten actief 17 categorieën informatie openbaar maken (zoals beleid, vergaderstukken, beschikkingen) via portalen als **PLOOI** ¹⁶. Ook vereist de Woo een goede *informatiehuishouding*: bestuursorganen moeten hun documenten duurzaam opslaan en toegankelijk houden zodat verzoeken om informatie tijdig kunnen worden beantwoord ¹⁷. RDDI ondersteunt bij de uitvoering, bijvoorbeeld met definities en toolkits per categorie ¹⁵. Verder stelt de Woo een **contactpersoon openbaarheid** verplicht en bevat deze wet een antimisbruikbepaling voor oneigenlijke verzoeken ¹⁸. Kleine overheden doen er goed aan een Woo-plan op te stellen (wat moet actief online, hoe om te gaan met Woo-verzoeken intern).
- **Wet digitale overheid (Wdo)** – Sinds 1 juli 2023 gefaseerd in werking ¹⁹. Richt zich op veilige en toegankelijke digitale dienstverlening. Belangrijk onderdeel is **veilig inloggen**: publieke dienstverleners moeten per dienst vaststellen welk betrouwbaarheidsniveau (laag, substantieel, hoog) nodig is voor digitale toegang ²⁰. Middelen als DigiD en eHerkenning krijgen wettelijke basis en niveaus, waardoor burgers en bedrijven veilig kunnen inloggen en identiteit gecontroleerd is ²⁰. Gemeenten classificeren nu hun diensten; VNG biedt hiervoor een **classificatiemodel** ²¹. Daarnaast implementeert de Wdo de EU-richtlijn digitale toegankelijkheid: alle overheidswebsites en -apps moeten voldoen aan toegankelijkheidsnorm WCAG 2.1 (EN 301 549) ²². Overheidsinstellingen moeten een **toegankelijkheidsverklaring** publiceren en hun sites/apps regelmatig laten toetsen op toegankelijkheid. Voor kleine organisaties is dit een aandachtspunt bij het implementeren van nieuwe digitale tools (zoals chatbotwebinterfaces).
- **Algemene Verordening Gegevensbescherming (AVG)** – De Europese privacywet (GDPR) geldt onverkort voor gemeenten en overheden. Bij gebruik van chatbots of AI die persoonsgegevens verwerken, moeten organisaties voldoen aan beginselen als doelbinding, minimale data-opslag, transparantie en juiste grondslag ²³ ²⁴. Vaak is voor zulke nieuwe verwerkingen een **Data Protection Impact Assessment (DPIA)** verplicht ²⁵ – dit is een risico-analyse om privacyrisico's in kaart te brengen en mitigerende maatregelen te treffen. Ook moeten overheden zorgen voor een rechtmatige basis (bijv. toestemming of publiek taak) voordat burgers via een chatbot gegevens verstrekken. De Autoriteit Persoonsgegevens heeft leidraden (zoals *Aan de slag met AI*-

(geletterdheid) die benadrukken dat organisaties intern kennis opbouwen over AI & privacy, en dat ze extra alert zijn op data-uitwisseling met externe AI-diensten ²⁶ ²⁴.

- **Baseline Informatiebeveiliging Overheid (BIO)** – Het informatiebeveiligingsraamwerk (gebaseerd op ISO27001/2) is sinds 2019 van kracht voor alle overheidslagen. Kleine overheden moeten bij digitale projecten de BIO toepassen om voldoende beveiligingsmaatregelen te borgen (denk aan toegangsbeheer, logging, versleuteling). Voorheen hadden gemeenten de BIG, maar nu is er één overheidsbrede baseline (BIO). Dit is geen wet, maar wel beleid verankerd via bijvoorbeeld de ENSIA-verantwoording. Zeker bij het inzetten van open source software en cloudservices is naleving van de BIO essentieel om aan de Wbp/AVG en Wdo veiligheidseisen te voldoen.
- **Andere relevante kaders** – *Archiefwet*: zorgt dat digitale informatie op termijn toegankelijk blijft (denk aan chatlogs als mogelijk archiefstuk). *Auteurswet*: speelt bij open source licenties – zorg dat software-inkoopcontracten regelen dat de overheid rechten heeft om broncode te openbaren (zie ook de Handreiking OSS-aanbesteding hieronder). Ook de *Wet hergebruik overheidsinformatie* (implementatie van de Open Data Richtlijn) stimuleert dat data en softwarecomponenten door anderen hergebruikt kunnen worden, wat aansluit bij digitale gemeenschapsgoederen.

Praktische hulpmiddelen en checklists

- **GIBIT Toolbox (VNG)** – *Gemeentelijke Inkoopvoorwaarden bij IT* (GIBIT) is een set modelvoorwaarden, normen en checklists voor ICT-inkoop door gemeenten ²⁷. De GIBIT (versie 2023) is door VNG als *pas-toe-of-leg-uit*-standaard aangemerkt ²⁸: gemeenten worden geacht deze voorwaarden te hanteren bij IT-aanbestedingen, tenzij gemotiveerd afgeweken wordt. De toolbox bevat onder meer standaardcontractclausules (bijv. over eigendom van broncode, opensourcelicenties, beveiligingseisen, SLA's), een lijst kwaliteitsnormen (denk aan ISO/IEC-normen, OWASP voor webbeveiliging, etc.) en checklists voor het formuleren van eisen en wensen. Door GIBIT te gebruiken zorgen kleine overheden dat ze niets belangrijks over het hoofd zien in hun opdrachten en bevorderen ze leveranciers-onafhankelijkheid en herbruikbaarheid van oplossingen.
- **Handreiking Aanbesteden van Open Source Software II** – Een uitgebreide gids (47 pag., mei 2022) van het Ministerie van BZK voor het inkopen en ontwikkelen van ICT met publieke waarden centraal ²⁹. Deze handreiking beschrijft stap voor stap hoe je bij aanbestedingen bepaalde rechten kunt bedingen om open en toekomstbestendige oplossingen te garanderen ²⁹. Denk aan: eisen dat maatwerksoftware onder een open-source licentie wordt opgeleverd, dat er geen vendor lock-in is, dat data-portabiliteit en open standaarden worden geborgd, enz. Het document (*"Publieke waarden en rechten bij aanbesteden van ICT"*) adviseert strategisch na te denken over intellectueel eigendom en langdurige community-ontwikkeling bij de start van een aanbesteding ³⁰. Praktische tips zijn o.a. het gebruik van marktconsultaties om leveranciers vroeg te betrekken bij open eisen, en voorbeeldbepalingen voor contracten. Voor kleine overheidsorganen is deze handreiking waardevol om bij beperkte middelen toch maximaal effect uit aanbestedingen te halen richting gemeenschapsgoederen.
- **Kwaliteitsraamwerken en toetsing** – Er zijn diverse (gratis) hulpmiddelen om de kwaliteit van digitale producten te controleren:

- “**Software Quality Model**” zoals ISO 25010 voor bijv. onderhoudbaarheid en beveiliging – kan dienen als checklist bij oplevering van software.
- **Open Source Scan Tools:** tools als de *OSS License Compliance Checker* om te verifiëren of geleverde software geen licentieconflicten heeft.
- **DigiToegankelijk Toets:** de overheid biedt via DigiToegankelijk.nl een invulassistent en checklist om websites/apps op toegankelijkheid te testen en een verplichte toegankelijkheidsverklaring op te stellen.
- **ENSIA-vragenlijsten:** jaarlijkse vragenlijsten die gemeenten invullen over informatieveiligheid en privacy (onder toezicht van BZK/LOGIOUS). Deze vragenlijsten kunnen indirect dienen als checklist of minimaal eisenkader waar nieuwe digitale systemen aan moeten voldoen (denk aan logging, backups, autorisaties).
- **Open source projectenkatalogus** – Via het **Open Source Software Register** op Developer.overheid.nl is een overzicht beschikbaar van open source projecten van Nederlandse overheden ¹⁴. Hier kunnen kleine gemeenten of uitvoeringsorganisaties kijken of een gewenst product al door een collega-organisatie is gebouwd en gedeeld. Denk aan open source chatbots, zaaksystemen, dataplatformen, etc. Hergebruik bespaart kosten en versterkt samenwerking. Ook GitHub organisaties van gemeenten (zoals Amsterdam, Rotterdam) en van ministeries bevatten herbruikbare bouwstenen. De site bevat zoek- en filtermogelijkheden (per thema of organisatie) om snel relevante repositories te vinden.
- **Algoritmeregister handreiking** – Voor transparantie over algoritmen is er een *Handreiking Algoritmeregister* beschikbaar ³¹. Hierin staat welke organisaties en welke typen algoritmes geregistreerd (kunnen) worden in het (nu nog vrijwillige) **Algoritmeregister** ³². Ook wordt uitgelegd hoe je als overheid je algoritmes (zoals AI-modellen of beslissingsregels) kunt documenteren en publiceren, inclusief voorbeeldformaten. Hoewel deze tool vooral voor grotere overheden bedoeld is, kunnen ook kleinere overheden er inspiratie uit halen om intern bij te houden welke geautomatiseerde beslismodellen ze inzetten – wat voorbereidt op toekomstige wettelijke verplichtingen (zie AI Act hieronder).

Voorbeelden en best practices

- **Chatbot “Guus” – Gemeente Goes:** een publiek toegankelijke chatbot die burgers 24/7 te woord staat met vragen aan de gemeente. Chatbot Guus is zo ingericht dat hij uitsluitend betrouwbare, vooraf geverifieerde bronnen gebruikt (zoals inhoud van de eigen website goes.nl) om vragen te beantwoorden ³³. Dit beperkt risico’s en zorgt voor controleerbare antwoorden. Goes deelt ervaringen dat zo’n chatbot veelvoorkomende vragen afvangt, terwijl complexere gevallen worden doorgestuurd naar medewerkers. Guus is een voorbeeld van een kleinschalige gemeente die met een relatief simpele AI-toepassing de dienstverlening verbetert.
- **PZH Assistant – Provincie Zuid-Holland:** een interne generatieve AI-assistent voor provincieambtenaren, bedoeld als veilig alternatief voor ChatGPT ³³. Deze assistent draait in een afgeschermd omgeving, is alleen toegankelijk voor medewerkers en gebruikt geen externe data, zodat vertrouwelijkheid gewaarborgd blijft. Dit experiment toont hoe een overheid met eigen AI-modellen of open source LLMs een oplossing kan bouwen die voldoet aan publieke waarden. Hoewel het (nog) geen directe burgerdienst is, helpt het ambtenaren efficiënter werken (bijv. samenvattingen maken, concept-teksten genereren) binnen duidelijke kaders.
- **OpenZaak community (gemeenten):** OpenZaak is een open source zaaksysteem ontwikkeld door en voor gemeenten (initieel door Utrecht, Tilburg e.a.) om zaakgericht werken volgens

Common Ground principes te ondersteunen ³⁴. Het vervangt dure gesloten zaaksuites door een gezamenlijk ontwikkeld platform (implementatie van de VNG-standaard ZGW API's). Inmiddels gebruiken tientallen gemeenten OpenZaak, waardoor zij gezamenlijk de kosten en kennis delen. Dit is een best practice hoe samenwerking en open source tot een volwaardig alternatief kunnen leiden voor proprietaire software. De *OpenZaak community* organiseert zich via GitHub en pleio-groepen, waar gemeenten en leveranciers samen de software verbeteren.

- **Algoritmeregisters (Amsterdam & landelijk):** Amsterdam pionierde met een eigen **AI-register** (als onderdeel van hun open AI-ecosysteem), waarin ze per ingezet algoritme uitleggen wat het doet, welke data het gebruikt en welke maatregelen zijn genomen tegen bias. Landelijk werkt BZK aan het Algoritmeregister (nu in bèta) waar al vrijwillig algoritmes worden gemeld ³⁵. Dit bevordert transparantie en vertrouwen. Kleine overheden kunnen hiervan leren door bijvoorbeeld op hun website te publiceren welke algoritmes of beslissingsregels zij gebruiken – ook al is het nog niet wettelijk verplicht. Zo deed gemeente Tilburg dat voor hun woonfraude-detectiesysteem, om raad en inwoners inzicht te geven in de werking.
- **Open broncode en transparantie:** Steeds vaker publiceren overheden de broncode van hun applicaties als gemeenschapsgoed. Naast de genoemde DigiD-app (Rijk) ³, heeft b.v. de Sociale Verzekeringsbank code van regelingen gedeeld en het ministerie van OCW de code achter het algoritme voor studiefinanciering openbaar gemaakt. Dit laat zien dat ook grotere organisaties het “*open, tenzij*”-principe toepassen in de praktijk. Publicatie gebeurt via platforms als GitHub (zie bijv. de GitHub van BZK voor het algoritmeregister ³⁶). Een ander voorbeeld is de **GEMMA Online** community van VNG Realisatie, waar gemeenten API-specificaties en referentie-implementaties (zoals voor adressen, personen, etc.) samen ontwikkelen en openzetten. Deze best practices tonen dat broncode delen leidt tot peer-review door derden, betere beveiliging en hergebruik door andere overheden.
- **Gebruik van Common Ground principes:** Gemeente Haarlem paste bij de bouw van hun nieuwe gegevensplatform Common Ground toe door data uit verschillende bronnen via gestandaardiseerde API's beschikbaar te maken voor eigen applicaties en externe ontwikkelaars. Dit maakte de gemeente flexibeler en minder afhankelijk van één leverancier. Door intensief gebruik van open standaarden en het scheiden van data en applicatielogica kunnen ze nu makkelijker nieuwe digitale diensten (zoals een chatbot die op meerdere databronnen zoekt) realiseren. Zulke cases illustreren hoe Common Ground in de praktijk werkt (zie onder).

Open standaarden en Common Ground

- **Forum Standaardisatie - pas-toe-of-leg-uit:** Om interoperabiliteit en onafhankelijkheid te bevorderen is het gebruik van bepaalde open standaarden verplicht gesteld voor overheden. Via het *Forum Standaardisatie* is een lijst van “Pas toe of leg uit”-standaarden vastgesteld ³⁷. Dit houdt in dat bij de aanschaf of ontwikkeling van ICT-systeem de betreffende open standaarden toegepast moeten worden, of dat in het jaarverslag moet worden uitgelegd waarom dat niet is gebeurd ³⁸ ³⁹. Deze verplichting geldt voor alle overheidslagen ⁴⁰. Denk aan standaarden als: **StUF/HL7** (gegevensuitwisseling), **Digikoppeling** (overheidsdata-uitwisseling), **OWMS** (metadatastandaard), **PDF/A** en **ODF** (documentformaten), **DNSSEC**, **DKIM** (veiligheid internet), **WCAG** (toegankelijkheid) etc. Voor gemeenten is op GEMMA Online een overzicht beschikbaar welke standaarden zij specifiek moeten toepassen ⁴¹. Het naleven van open standaarden zorgt ervoor dat digitale diensten van kleine overheden aansluiten op landelijke voorzieningen en dat leveranciers kunnen worden uitgewisseld.

- **Common Ground** – Dit is de visie en beweging binnen de gemeentelijke overheid om de informatievoorziening fundamenteel te hervormen ⁴². Kernidee: weg van verkokerde, monolithische systemen naar een gedeelde **lagsamenstelling** waarin gegevens losgekoppeld zijn van processen en front-ends. Gemeenten werken collectief aan modulair opgebouwde oplossingen met API-koppelingen en gedeelde gegevensmodellen. Common Ground principes zijn onder meer:
 - **Gebruik open standaarden en open data waar mogelijk** – zodat gegevensuitwisseling tussen gemeenten en met partners soepel loopt.
 - **Herbruik bestaande bouwstenen** – als één gemeente een module (bijv. voor chatbot-NLP of een zaakregistratie) bouwt, kan een andere die hergebruiken of samen verbeteren (open source ontwikkeling).
 - **Scheid data van applicaties** – data blijft bij de bron (b.v. een basisregistratie) en applicaties vragen data op via uniforme APIs. Hierdoor voorkom je redundantie en lock-in; een chatbot kan zo via API's gegevens opvragen uit diverse registraties zonder afzonderlijke integraties per leverancier.
 - **Gezamenlijke ontwikkeling** – via VNG Realisatie en communities (zoals CommonGround.nl, GitHub-organisaties) werken gemeenten, leveranciers en developers samen aan nieuwe oplossingen. Voorbeelden zijn eerder genoemd: OpenZaak, maar ook **NLX** (veilig berichtenverkeer tussen overheden), **VNG Realisatie API's** (standaarden en referentie-implementaties voor adres, vergunningen, etc.) en **OpenGem** initiatieven.

Common Ground wordt ondersteund in het GGU (Gezamenlijke Gemeentelijke Uitvoering) programma en is een continu proces. Kleine gemeenten profiteren door aan te haken bij Common Ground-projecten: ze krijgen toegang tot kennis en tools die anders alleen grote steden zouden kunnen ontwikkelen. Common Ground maakt zo digitale gemeenschapsgoederen een kernonderdeel van toekomstige gemeentelijke ICT, met focus op **flexibiliteit, samenwerking en kostenbesparing** ⁴².

Europese ontwikkelingen (AI Act, DSA, e.a.)

- **EU AI Act (AI-verordening)** – De komende Europese verordening voor AI zal directe gevolgen hebben voor overheidsgebruik van AI-systemen. De AI Act hanteert een risicogebaseerde benadering:
 - **Verboden AI:** systemen die onacceptabel risico vormen (bijv. sociale scoring) worden verboden.
 - **Hoog-risico AI:** hier komen strenge eisen aan, zoals transparantie, menselijke monitoring, risicomagement en registratie. Overheden gebruiken bijvoorbeeld AI voor kredietverstrekking, werving, rechtshandhaving – die vallen vaak onder hoog risico. Deze systemen zullen straks moeten voldoen aan de AI Act (denk aan certificering en toezicht). Ook wordt waarschijnlijk verplicht dat general-purpose AI (zoals grote taalmodellen) extra verplichtingen krijgen ⁴³.
 - **Beperkt risico:** zoals chatbots die met burgers communiceren, moeten tenminste transparant maken dat een AI-systeem het is (disclosure) en wellicht basisregels rond accuraatheid volgen.

Naar verwachting treedt de AI Act in 2025-2026 in werking. Nederland anticipeert hierop: de hierboven genoemde handreikingen verwijzen al naar de AI Act om organisaties voor te bereiden ⁴⁴ ⁴⁵. Ook de verplichting tot **AI-geletterdheid** (trainen van personeel in AI) uit de AI Act wordt benadrukt door toezichthouders ⁴⁶. Kleine overheidsorganen doen er dus goed aan nu al bij AI-projecten te handelen

naar de geest van de AI Act: risicoanalyse uitvoeren, documentatie van gebruikte algoritmen (mogelijk inschrijven in algoritmeregister), betrokkenheid van juridische en ethische experts, enzovoort ⁴⁷ ⁴⁸.

- **Digital Services Act (DSA)** – Deze EU-verordening (van kracht 2024) richt zich primair op online platforms en heeft als doel een veiliger digitaal ecosysteem te creëren. Voor kleine overheden is de DSA relevant als zij optreden als:
 - *Afnemer van platformdiensten*: bij gebruik van bv. Facebook, YouTube of cloudplatforms voor burgercommunicatie gelden strengere regels voor die platforms (transparantie over algoritmes, moderatie van illegale content). Overheden kunnen hier rekening mee houden door contractueel af te dwingen dat leveranciers voldoen aan de DSA-verplichtingen.
 - *Aanbieder van een online dienst*: Mocht een gemeente zelf een forum of publiek interactief platform beheren, dan gelden onder de DSA baseline-verplichtingen rond het melden en verwijderen van illegale inhoud, en transparantie voor gebruikers. Overheidswebsites vallen veelal niet onder “tussenpersoon” in de zin van de DSA, maar als bijvoorbeeld een provincie een marktplaats-app faciliteert of een waterschap een communityplatform host, kan het wel van toepassing zijn.
 - *Very Large Online Platform (VLOP) gebruiker*: Hoewel onwaarschijnlijk dat een kleine overheid *zelf* als VLOP kwalificeert, is het goed te weten dat de DSA extra plichten oplegt aan Big Tech (risicobeoordelingen, externe audits). Dit zorgt indirect voor betere borging van gebruikersrechten – iets wat overheden ten goede komt als zij van deze platforms gebruikmaken.

Samengevat biedt de DSA een kader voor **verantwoorde digitale diensten**. Voor onze context betekent dit: wees bewust welke online diensten je inzet, check of ze DSA-compliant zijn, en stel waar nodig eigen gebruiksvoorwaarden op die aansluiten bij deze nieuwe regelgeving.

- **Overige EU-regelgeving** – Noemenswaardig is ook de **Digital Markets Act (DMA)** (gericht op het voorkomen van lock-in door Big Tech gatekeepers) en de **Data Governance Act/Dataverordening**, die data-altruïsme en hergebruik van overheidsdata bevorderen. Daarnaast komt er een **Cyber Resilience Act (CRA)** die minimale cybersecurity-eisen stelt aan software/hardware – open source communities volgen dit op de voet omdat het implicaties kan hebben voor ontwikkelmodellen ⁴⁹. Tot slot blijft de **Privacyregelgeving** evolueren (e-Privacy verordening in aantocht) wat relevant is voor chatbots die bijvoorbeeld cookies of communicatiegegevens verwerken. Het loont voor kleine overheden om via kanalen als Europa Decentraal of het Nationaal Cyber Security Centrum op de hoogte te blijven van EU-wetgeving, zodat implementaties van digitale gemeenschapsgoederen toekomstbestendig en compliant zijn.

Bronnen: Dit overzicht is samengesteld uit officiële documenten en richtlijnen van onder andere Digitale Overheid, Rijksoverheid, VNG en Forum Standaardisatie, alsmede praktijkvoorbeelden uit recente nieuwsberichten en communities. Alle genoemde bronnen en documenten zijn via de klikbare referenties te raadplegen voor meer detail en volledige tekst.

¹ ² Beleid Opensourcewerken - Digitale Overheid

<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/open-source/beleid/>

³ ⁴ ⁴⁹ Berichten in de categorie ‘nieuws’ en dossier ‘opensourcewerken’ - Digitale Overheid

<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/open-source/dossier-berichten/dossier-categorie/nieuws/>

- 5 6 7 IBD helpt gemeenten bij risico's van AI
<https://www.binnenlandsbestuur.nl/digitaal/natuur-en-milieu/ibd-helpt-gemeenten-bij-risico-s-van-ai>
- 8 9 11 12 13 33 Overheid verruimt standpunt inzet generatieve AI - Digitale Overheid
<https://www.digitaleoverheid.nl/nieuws/overheid-verruimt-standpunt-inzet-generatieve-ai/>
- 10 Overheidsbrede handreiking voor de verantwoorde inzet van generatieve AI | Rapport | Rijksoverheid.nl
<https://www.rijksoverheid.nl/documenten/rapporten/2025/04/16/overheidsbrede-handreiking-generatieve-ai>
- 14 Zoek repositories - Developer Overheid
<https://oss.developer.overheid.nl/repositories?thema=logboek>
- 15 18 Openbaarmaking en informatiehuishouding | Projecten | Riksprogramma voor Duurzaam Digitale Informatiehuishouding
<https://www.informatiehuishouding.nl/projecten/actieve-openbaarmaking-overheidsinformatie>
- 16 17 Betrokken organisaties Informatiehuishouding - Digitale Overheid
<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatiehuishouding/ihh-betrokken-organisaties/>
- 19 20 21 Wet digitale overheid van kracht | VNG
<https://vng.nl/nieuws/wet-digitale-overheid-van-kracht>
- 22 Wet- en regelgeving - WCAG.nl
<https://wcag.nl/kennis/wet-en-regelgeving/>
- 23 24 25 26 Privacy en AI: hier moeten scholen op letten - Kennisnet
<https://www.kennisnet.nl/artificial-intelligence/privacy-en-ai-hier-moeten-scholen-op-letten/>
- 27 28 GIBIT | VNG
<https://vng.nl/projecten/gibit>
- 29 Handreiking aanbesteden van open source software II - Digitale Overheid
<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/open-source/dossier-documenten/handreiking-aanbesteden-van-open-source-software-ii/>
- 30 Publieke waarden en rechten bij aanbesteden van ICT - Handreiking aanbesteden van open source software II | Rapport | Rijksoverheid.nl
<https://www.rijksoverheid.nl/documenten/rapporten/2022/05/18/publieke-waarden-en-rechten-bij-aanbesteden-van-ict---handreiking-aanbesteden-van-open-source-software-ii>
- 31 32 35 36 45 48 Algoritmereserve voor de overheid Algoritmes - Digitale Overheid
<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/algoritmes/algoritmereserve/>
- 34 OpenZaak: van samen organiseren naar samen realiseren
<https://commonground.nl/news/view/752192c5-7222-4769-a738-de47dfcfb6f5/openzaak-van-samen-organiseren-naar-samen-realiseren>
- 37 38 39 40 'Pas toe of leg uit'-beleid | Forum Standaardisatie
<https://www.forumstandaardisatie.nl/pas-toe-leg-uit-beleid>
- 41 Overzicht Gemeentelijke Standaarden | VNG
<https://vng.nl/artikelen/overzicht-gemeentelijke-standaarden>
- 42 Common Ground | VNG
<https://vng.nl/rubrieken/onderwerpen/common-ground>
- 43 44 47 open.overheid.nl
<https://open.overheid.nl/documenten/9c273b71-cebb-4e11-b06f-fa20f7b4b90e/file>

⁴⁶ Autoriteit Persoonsgegevens: maak van AI-geletterdheid prioriteit

<https://theinnovativelawyer.ai/insights/autoriteit-persoonsgegevens-maak-van-ai-geletterdheid-prioriteit>