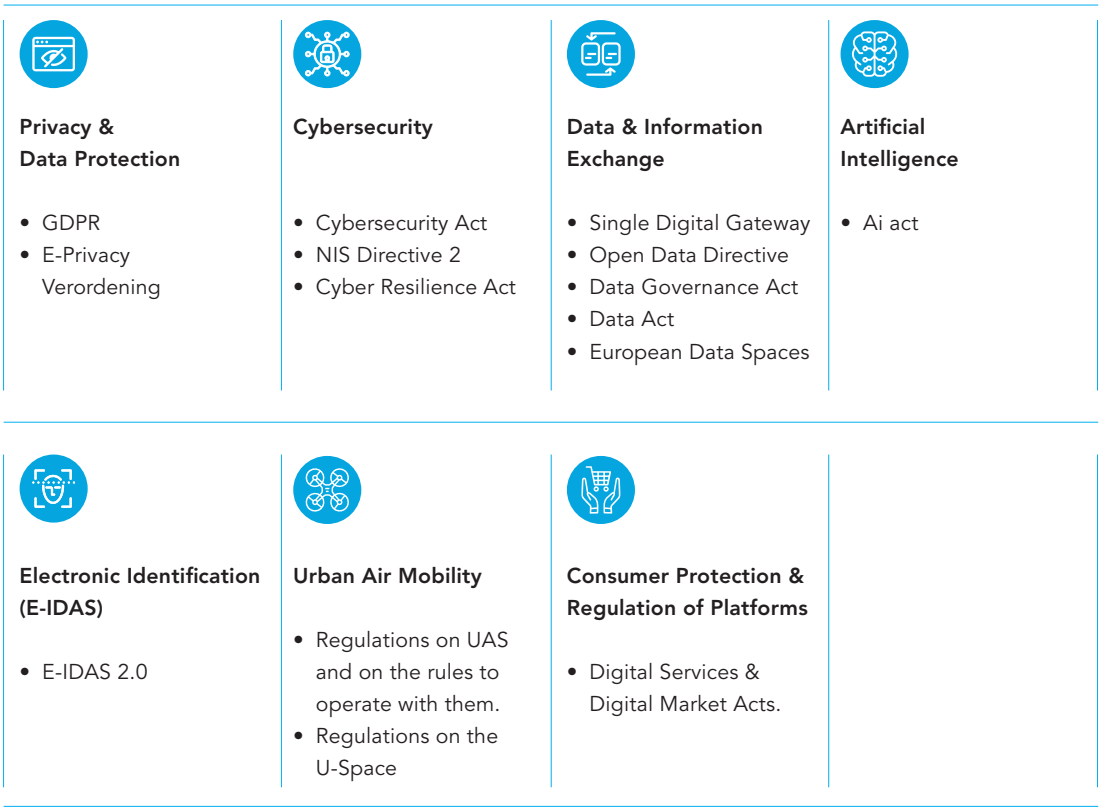
Analyse Samenhang Europese digitale wetgeving fase 1 Eindrapport

Samenvatting

De Europese Commissie heeft, als onderdeel van de Digital Decade, een aantal regelgevende voorstellen (die uitmonden in een verordening of richtlijn en die we hierna gemakshalve benoemen: als wetten[a]) gemaakt waarmee de digitale toekomst van Europa wordt vormgegeven. Deze wetten hebben rechtstreekse impact op de digitaliseringsopgave van gemeenten. VNG wil vroegtijdig in beeld hebben wat deze impact betekent en welke investeringen hiervoor nodig zijn. Hiervoor is een impactanalyse uitgevoerd die op hoofdlijnen de impact van de Europese digitale wetten op gemeenten inzichtelijk maakt.

Creëren van overzicht: De meeste relevante Europese wetten voor gemeenten

Om meer samenhang te brengen in Europese digitale wetten voor gemeenten is het belangrijk om overzicht te creëren van welke wetten en regels en onderliggende normen nu daadwerkelijk relevant zijn voor gemeenten. Het geven van overzicht kan zorgen voor meer (be)grip en urgentie en het tijdig kunnen inschatten van de impact van de wetten. In onderstaande figuur 1 is een overzicht gegeven van de wetten die in scope zijn van dit onderzoek.



Figuur 1. Wetgevingsoverzicht.

Een deel van de wetten zijn al van kracht. In de afgelopen jaren zijn er daarnaast een groot aantal nieuwe wetten (of updates van bestaande wetten) aangenomen (soon applicable) en voorstellen die op dit moment in onderhandeling zijn bij de commissie of in het Europees parlement. Om hier een beeld in te geven in het onderstaande figuur een beeld van de status van de wetten. Het betreft een momentopname, de VNG is voornemens dit overzicht regelmatig te actualiseren door statusveranderingen op te nemen en nieuwe wetgeving vanuit de EU toe te voegen.

a Een "verordening" is een bindende rechtshandeling die in de hele EU van toepassing is. Een "richtlijn" is een rechtshandeling die een bepaald doel vastlegt dat alle EU-landen moeten bereiken. Zij mogen echter zelf de wetgeving vaststellen om dat doel te bereiken

In Force and applicable	Soon applicable	Under Initiative or proposal
• GDPR • e-Privacy Directive • Cybersecurity Act • NIS Directive (+Digital Service Providers Regulation) • Open Data Directive • Single Digital Gateway (some provisions) • Whistleblowing Directive (some provisions) • e-IDAS • Payment Services Directive 2 (+ Regulation on Technical Standards) • 5th Anti-Money Laundering Directives • UAM: Regulation on UAS & on operation of UA* • E-Commerce Directive and Consumers Directives (some) • P2B Regulation	• Single Digital Gateway (some provisions) • Whistleblowing Directive (some provisions) • UAM: Regulations on the U-Space • Consumer protection: - Directive on contracts for the supply of digital content and digital services - Directive on sales of goods - Directive on Representative Actions - Directive in better enforcement and modernisation of consumer protection.	• ePrivacy Regulation • NIS 2 Directive • Delegated Regulation on the security of Internet-connected devices • Data Governance Act • Data Act • European Health Data Space • AI act • Civil liability – Digital Age & AI • eIDAS 2.0 • Anti-Money Laundering Directive 6th • Digital Services Act • Digital Markets Act • Transparency & targeting of political advertising

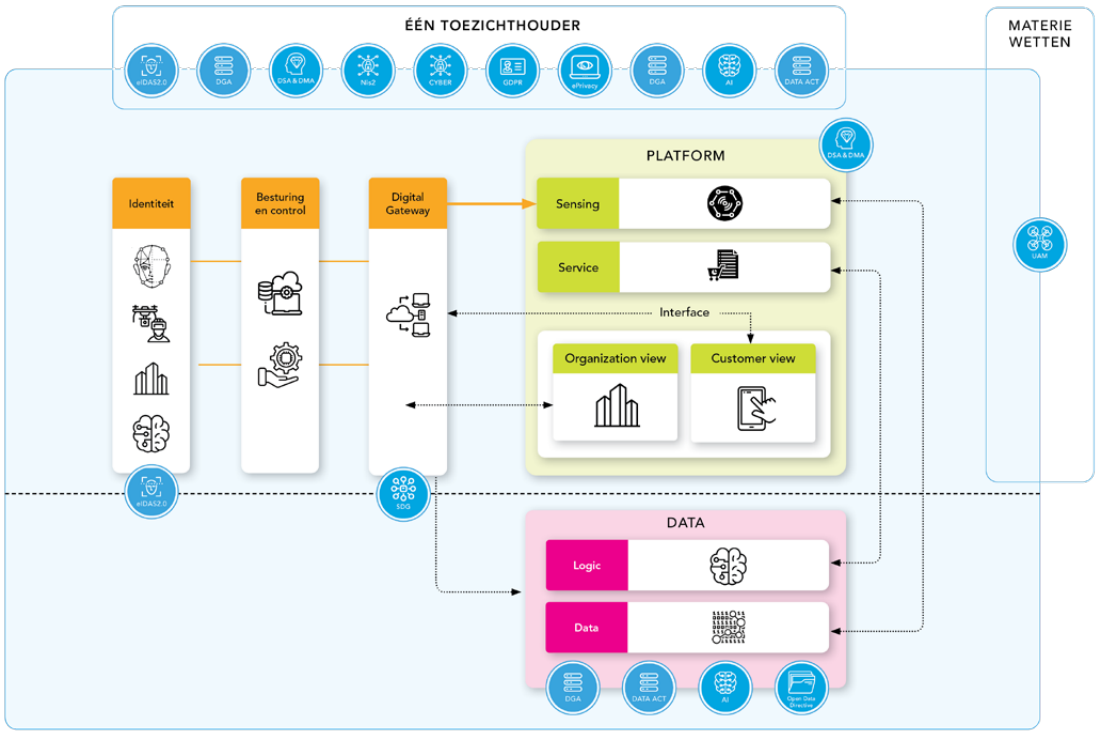
Figuur 2. Status wetgeving.

Vervolgens is binnen deze samenhang het doel en de status van de specifieke wetten beschreven en is een beschrijving gegeven over waar de wet over gaat in de gemeentelijke context (zie hoofdstuk 2). In onderstaande figuur is ook het beoogde tijdspad van de verschillende wetten beschreven.

Wet	Jaar publicatie voorstel	Jaar van kracht	Jaar van kracht, geschat	Jaar ingaan verplichting	Jaar ingaan verplichting geschat
DGA		2022		2023	
DA	2022	onbekend		onbekend	
ePrivacy verordening					
Open data richtlijn		2019		2021	
Europese digitale identiteit verordening	2021		2023		2025
SDG		2018		2023	
AI-act	2021		2023		2025
Data ruimten	2020	nvt		nvt	
NIS2		2023		2024	
Urban air mobility		2021		2023	
DSA		2022		2024	
DMA		2022		2023	
Cyberbeveiligings-verordening		2019		2022	

Figuur 3 Overzicht Europese digitale wetten in de tijd, opgemaakt in januari 2023

Het overzicht laat zien dat alle wetten in het overzicht uiterlijk eind 2026 geïmplementeerd moeten zijn. Om de wetten in samenhang te kunnen bekijken is de vertaling gemaakt naar de effecten op de digitale infrastructuur die een gemeente ingericht moet hebben om succesvol te kunnen zijn. Hierbij is sprake van organisatorische complexiteit omdat er onderlinge afhankelijkheden zijn tussen de verschillende overheidslagen en deels nog bepaald moet worden wie waarvoor verantwoordelijk is. V an belang is om tot een interbestuurlijke strategie te komen waarin rollen en verantwoordelijkheden helder zijn belegd. In het figuur hieronder is de samenhang in beeld gebracht.



Figuur 4 Samenhang Europese Digitale wetgeving

De wijzigingen hebben een effect op de gemeentelijk uitvoering en organisatie. In de analyse zijn per onderdeel de impact per wet in beeld gebracht.

Impact op hoofdlijnen

De impact van de bestaande en nieuwe digitale Europese wetten op de uitvoering van gemeenten is groot. Het aantal nieuwe wetten is dusdanig dat er een strategie nodig is op lokaal niveau waarin integraal gekeken wordt naar de digitale infrastructuur, beleidsdomeinen en organisatie. Volgens de geldende Europese planning moeten alle wetten eind 2026 geïmplementeerd zijn.

Bij de implementatie zijn er ook een aantal belangrijke randvoorwaarden waar een gemeente afhankelijk is van de beschikbaarheid van landelijke voorzieningen (vb digitale identiteit en/ of kenregistraties). Dit vraagt daarom om een interbestuurlijke strategie waarin helder is welke voorzieningen op EU, nationaal, regionaal en lokaal niveau beschikbaar komen.

Aanbevelingen

Dit onderzoek heeft een eerste verkennend beeld opgeleverd van de grote impact van relevante Europese digitale wetgeving op gemeenten. Het is van belang dat de VNG met voldoende daadkracht de benodigde inspanning en complexiteit om aan de wettelijke verplichtingen te voldoen voor het voetlicht brengt bij zowel de EU, als het rijk en gemeenten. Het is nodig dat bewustwording, kennis en urgentie wordt gecreëerd, financiële middelen worden vrijgemaakt en gemeenten concreet geholpen worden om de Europese digitale wetgeving te implementeren en uit te voeren. Dit leidt tot de volgende aanbevelingen:

- Blijf de Europese wetten vanuit samenhang benaderen en zorg voor integratie met nationale kaders zoals de Werkagenda waardegedreven digitalisering van BZK.
- Zorg voor een verdieping op dit onderzoek door per wet een uitvoeringstoets uit te voeren op basis van de samenhang.
- Zorg voor een bewustwordingscampagne onder de leden om te borgen dat gemeenten zich bewust worden van de nieuwe Europese kaders en de deadline (2026) wanneer die geïmplementeerd moeten zijn.
- Ga in gesprek met het kabinet om de financiering voor de implementatie van de nieuwe Europese kaders te borgen. Beschikbaarheid van de benodigde financiële middelen is randvoorwaardelijk om gemeenten in staat te stellen aan hun verplichtingen te voldoen.
- Ontwikkel een instrumentarium, bijvoorbeeld een toolbox met menukaart voor gemeenten dat gemeenten helpt om zelf de nieuwe Europese kaders te implementeren.

Bewustwording, kennis en urgentie

De gemeenten staan voor de uitdagende taak om de komende jaren digitale identiteiten, data-(platformen), artificiële intelligentie (AI), cybersecurity en nieuwe technische infrastructuren verantwoord in te zetten en dit te vertalen naar commitment, urgentie, financiering en organisatieverandering. Gemeenten hebben hierbij niet alleen te maken met een juridische werkelijkheid, gebaseerd op normatieve kaders (hoe het zou moeten zijn), of een technische werkelijkheid (zoals cloudinfrastructuren, wallets, vertrouwensdiensten, federatieve datastelsels, datastructuren, api's, biometrie, machine learning) maar ook met hoe ze verantwoord invulling kunnen geven aan de gemeentelijke taakopvatting en het perspectief van de inwoner(ethiek en ambitie). Het nadenken over ethiek roept allerlei vragen op over (democratische) verantwoordelijkheden en transparantie over de afweging. Nieuwe technologieën waarvoor uit Europa kaders komen als digitale identiteit, artificiële intelligentie, de werking van algoritmes, cybersecurity en de nog onbekendheid hierover vormen hierbij een extra uitdaging. Deze uitdaging moet bovendien plaatsvinden gelijktijdig met de enorme opgave die gemeenten hebben bij de uitvoering van de maatschappelijke opgaven zowel in het sociale als fysieke domein. Het gaat niet meer om het sec implementeren van techniek en de waarborgen daarbij, maar om het transformeren van de gemeentelijk organisatie in de 'Digital Decade', waarbij het sociale, fysieke, bedrijfsvoerende en digitale samenkomt en integraal moet worden aangestuurd en uitgevoerd.

Opvolging van dit verkennend onderzoek

De beschrijvingen in dit rapport geven op hoofdlijnen een eerste kwalitatieve indicatie van de grote impact die de Europese digitale wetgeving op gemeenten heeft. De precieze impact en uitvoerbare doorlooptijd voor gemeenten zal verder moeten worden onderzocht per wet (o.a middels een uitvoeringstoets) en zeker ook in samenhang met elkaar en met de staande (digitaliserings) opgaven voor gemeenten. Daarnaast zijn de onderhandelingen van een aantal wetsvoorstellen nog in de beginnende fase en vinden er op moment van schrijven nog discussies plaats over fundamentele vraagstukken in de wet, bijvoorbeeld over de definitie van AI. Dit kan bepalend zijn voor de uiteindelijke wet, implementatie in Nederland en de impact op gemeenten.

Het structureel in beeld brengen van de (samenhangende) impact van relevante Europese digitale wetgeving kan helpen om op tijd bewustwording, urgentie, geld, tijd en prioriteit te organiseren bij gemeenten evenals inzicht voor gemeenten waaraan ze qua wetgeving moeten voldoen en wat ze moeten doen om compliant te zijn. Deze taak lijkt binnen VNG nu versnipperd te zijn, het is nodig om deze taak beter in te richten zodat dit onderzoek geen eenmalig karakter heeft. Hier ligt ook een mogelijkheid om via een meer integrale aanpak met voldoende daadkracht de gemeentelijke belangen in te brengen (samen met het rijk) in de vormgeving van de Europese digitale wetten.

Versterking middelen uitvoering

Gemeenten staan zoals gezegd voor grote complexe verandering: enerzijds de verplichtingen uit de Europese digitale wetgeving implementeren en anderzijds een digitale transformatie waarbij gemeenten opereren in een wereld van platformen, data-economie en digitale identiteiten. Dit is een complex traject. Dit legt een druk op de gemeentelijke middelen. Het is randvoorwaardelijk dat deze middelen voor gemeenten beschikbaar zijn.

Implementatie strategie en instrumenten om gemeenten te helpen

Het is nodig de Europese digitale wetgeving verplichtingen in lijn te brengen met de landelijke visie en Werkagenda waardegedreven digitalisering en te zorgen dat het voor gemeenten inzichtelijk wordt waar landelijk gezamenlijk aan gewerkt wordt en niet iedere individuele gemeenten het wiel zelf hoeft uit te vinden. En aan de andere kant ook instrumenten ter beschikking stellen die gemeenten helpen om bepaalde onderdelen zelf te implementeren.

Inhoud

1. Inleiding

1.1. Achtergrond

De Europese Commissie heeft een aantal regelgevende initiatieven (hierna gemakshalve te noemen: wetten) ontplooid waarmee de digitale toekomst van Europa wordt vormgegeven. Deze wetten hebben rechtstreekse impact op de digitaliseringsopgave van gemeenten. VNG wil vroegtijdig in beeld hebben wat deze impact betekent en welke investeringen hiervoor nodig zijn.

Vanuit het programma Digitalisering en Europa wat binnen team informatiesamenleving van VNG wordt uitgevoerd is de vraag gesteld aan VNG Realisatie om een impactanalyse op hoofdlijnen uit te voeren van de Europese digitale wetten op gemeenten. VNG Realisatie heeft deze opdracht uitgevoerd.

1.2. Vraagstelling

De impactanalyse moet op hoofdlijnen de impact van de Europese digitale wetten op gemeenten inzichtelijk maken en dient als input voor VNG die op basis hiervan de benodigde investeringen in kaart brengt en hierover een advies uitbrengt aan de commissie i-Samenleving van de VNG. De impactanalyse is zodanig opgezet dat deze ge-update kan worden.

In deze analyse worden de volgende vragen beantwoord:
1. Wat is op hoofdlijnen de samenhang tussen de relevante bestaande en nieuwe Europese digitale wetten vanuit de bedoeling van de wet? Betrek hierbij ook relevante Nederlandse digitale wetgevingsinitiatieven.
2. Wat wijzigt er op hoofdlijnen in de werkwijze van de gemeente door deze Europese digitale wetten als deze in samenhang worden beschouwd?
3. Wat betekenen deze veranderingen[1] voor de gemeentelijke organisatie op hoofdlijnen?

1.3. Scope analyse

De impactanalyse beperkt zich tot de impact op hoofdlijnen van Europese digitale wetgeving op gemeenten. Dit is de eerste fase van de analyse. Dit betekent dat de analyse inzicht geeft in de samenhang van deze wetten op basis van de bedoeling van de wet, denk hierbij bijvoorbeeld aan elektronische identificatie en privacy en dataprotectie en binnen deze samenhang op hoofdlijnen de impact voor gemeenten. Op basis van deze hoofdlijnen maakt VNG een inschatting voor de benodigde investeringen. Ze helpen ook als input voor gesprekken rondom de werkagenda met BZK over de digitaliseringsopgave voor gemeenten. De opdrachtgever heeft een voorlopige lijst aangeleverd (zie bijlage B), welke als vertrekpunt heeft gediend voor deze analyse.

1.4. Aanpak & methodologie

Het onderzoek is uitgevoerd in de periode juni-oktober 2022. In deze paragraaf is de onderzoeksaanpak beschreven en is een korte toelichting gegeven op de gehanteerde methodologie om de onderzoeksvragen te kunnen beantwoorden.

Onderzoeksaanpak
Het onderzoek bestond uit drie fasen:
a) de inventarisatiefase;
b) de analysefase;
c) de rapportagefase.

1 Hierbij wordt zowel gekeken naar de primaire processen als naar de bedrijfsvoeringsaspecten (security, communicatie, organisatie, personeel, administratieve organisatie, financiën, informatievoorziening, juridisch, technologie, huisvesting)

Het proces werd begeleid door een begeleidingscommissie waarin vertegenwoordigers van VNG deelnamen. De eindrapportage is met de begeleidingscommissie afgestemd en akkoord bevonden.

Tijdens de **inventarisatiefase** is de onderzoeksaanpak verder uitgewerkt en is de selectie van de relevante Europese digitale wetten en documentatie daarover gemaakt. Op basis hiervan heeft een uitgebreide deskresearch plaatsgevonden. In deze rapportage is in eerste instantie gekeken naar de Europese digitale wetgeving zelf. Daarnaast zijn andere relevante documenten als Beoordeling Nieuwe Commissievoorstellen (BNC) fiches, beleidsnota's en position papers en uitgevoerde impact-analyses bestudeerd die meer inzage gaven in de Europese digitale wetgeving. Op basis hiervan is een lijst met gespreksonderwerpen gemaakt voor gesprekken met de opdrachtgever, betrokken VNG-beleidsmedewerkers en een aantal gemeenten waarvan bekend is dat zij zich bezighouden met Europese digitale wetgeving.

In de **analysefase** zijn interviews gehouden met betrokkenen. Er is in het totaal gesproken met 15 personen. In de bijlage A zijn de namen van de gesproken mensen opgenomen.

In de **rapportagefase** zijn de resultaten van de analyse voorgelegd aan de geïnterviewde personen in de vorm van een klankbordbijeenkomst, waarvoor alle geïnterviewden waren uitgenodigd. Ook de conceptrapportage is met deze groep gedeeld waarbij de mogelijkheid is geboden daarop te reageren. De resultaten van de impactanalyse zijn tot slot in de voorliggende rapportage opgenomen.

1.5. Leeswijzer

In hoofdstuk 2 beschrijven we de meest relevante Europese digitale wetten voor gemeenten. Voor het overzicht zijn de wetten samenhangend geclusterd naar overkoepelende onderwerpen, nl. Identiteit, Besturing en control, Digital gateway, Data, Platform en Privacy en Security. Vervolgens is binnen deze samenhang het doel en de status van de specifieke wetten beschreven en is een beschrijving gegeven over waar de wet over gaat in de gemeentelijke context. In hoofdstuk 3 verkennen we wat Europese digitale wetgeving op hoofdlijnen betekent voor gemeenten. Tot slot geven we in hoofdstuk 4 de conclusies en aanbevelingen van dit onderzoek.

2. Creëren van overzicht: De meest relevante Europese digitale wetten voor gemeenten

Om meer samenhang te brengen in Europese digitale wetten voor gemeenten is het belangrijk om overzicht te creëren van welke wetten en regels en onderliggende normen nu daadwerkelijk relevant zijn voor gemeenten. Het geven van overzicht kan zorgen voor meer (be)grip en urgentie en het tijdig kunnen inschatten van de impact van de wetten. In dit hoofdstuk beschrijven we daarom de meest relevante Europese digitale wetten voor gemeenten. In onderstaande figuur 1 is een overzicht gegeven van de wetten die in scope zijn van dit onderzoek.

Privacy & Data Protection

- GDPR
- E-Privacy Verordening

Cybersecurity

- Cybersecurity Act
- NIS Directive 2
- Cyber Resilience Act

Data & Information Exchange

- Single Digital Gateway
- Open Data Directive
- Data Governance Act
- Data Act
- European Data Spaces

Artificial Intelligence

- Ai act

Electronic Identification (E-IDAS)

- E-IDAS 2.0

Urban Air Mobility

- Regulations on UAS and on the rules to operate with them.
- Regulations on the U-Space

Consumer Protection & Regulation of Platforms

- Digital Services & Digital Market Acts.

Europese wetten in de tijd uitgezet

Om de opgave die het voldoen aan de Europese wetgeving voor gemeenten verder inzichtelijk te maken is ook in de tijd uitgezet in welk stadium de wetten zich bevinden en wanneer aan de verplichtingen die eruit voortvloeien voldaan moet worden. In de onderstaande figuur is zichtbaar dat een aantal wetten al van kracht zijn en dat andere nog in een voorbereidend stadium zijn. Overall is het beeld dat voor verreweg de meeste wetten in 2023 of 2024 al aan de verplichtingen voldaan moet worden, met twee uitschieters naar 2025.

Wet	Jaar publicatie voorstel	Jaar van kracht	Jaar van kracht, geschat	Jaar ingaan verplichting	Jaar ingaan verplichting geschat
DGA		2022		2023	
DA	2022	onbekend		onbekend	
ePrivacy verordening					
Open data richtlijn		2019		2021	
Europese digitale identiteit verordening	2021		2023		2025
SDG		2018		2023	
AI-act	2021		2023		2025
Data ruimten	2020	nvt		nvt	
NIS2		2023		2024	
Urban air mobility		2021		2023	
DSA		2022		2024	
DMA		2022		2023	
Cyberbeveiligings- verordening		2019		2022	

Figuur 3 Overzicht Europese digitale wetten in de tijd, opgemaakt in januari 2023

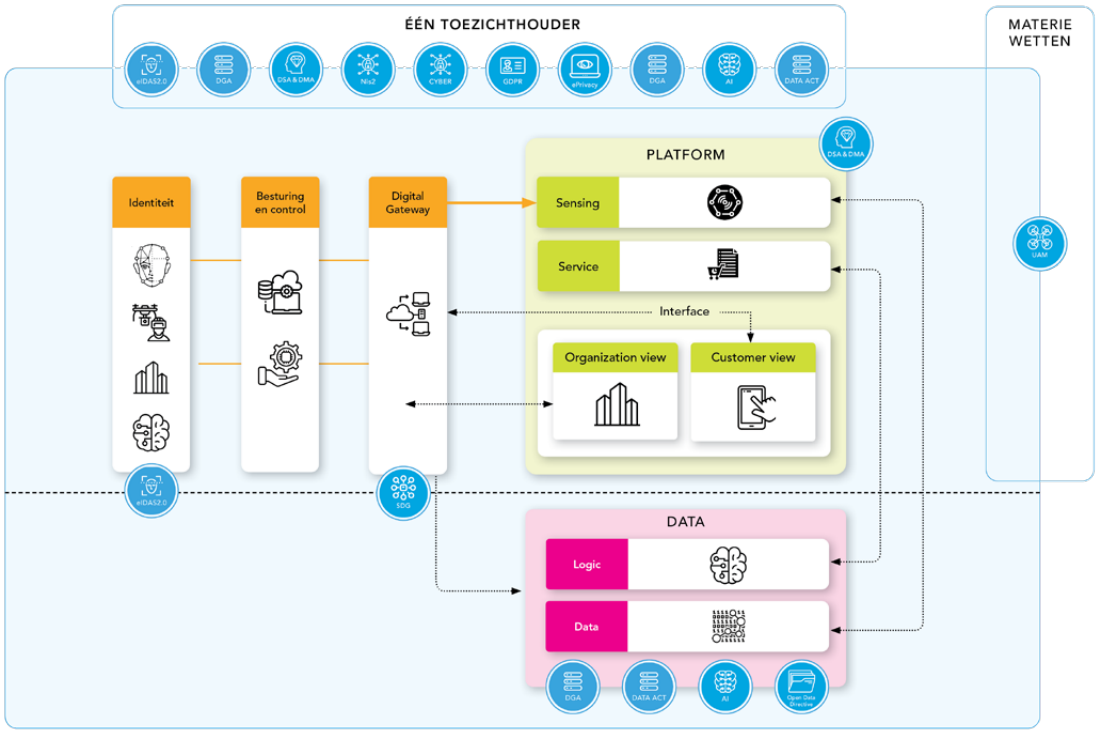
In de figuur is zichtbaar dat een aantal wetten al van kracht geworden is (ze zijn aangenomen door het Europees parlement en de Europese Raad en gepubliceerd in het publicatieblad van de Europese Unie). Voor deze wetten is aangegeven wanneer ze van kracht geworden zijn en wanneer aan de verplichtingen voldaan moet worden. Daar kan een periode van wisselende lengte tussen zitten: soms moet meteen aan de verplichtingen voldaan worden, soms zit daar een jaar tot maximaal vijf jaar (SDG) tussen. Wanneer er wel een voorstel is, maar dit voorstel nog niet is aangenomen, staat in de figuur het jaar waarin het voorstel is gepubliceerd, het jaar waarin het voorstel volgens de schatting van de VNG van kracht zal worden en het jaar waarin aan de verplichtingen voldaan moet worden. Bij dataruimten kunnen nu geen jaren worden ingevuld omdat hier sprake is van een strategie waarin wel is voorzien dat in de toekomst ook wetgeving aan de orde is maar er zijn nog geen wetsvoorstellen.

Om de figuur overzichtelijk te houden is per wet steeds 1 jaar aangegeven waarin de wet van kracht wordt en een jaar waarin aan de verplichtingen voldaan moet worden. De werkelijkheid is soms genuanceerder. Soms vallen onder één kopje meerdere verordeningen (dat is bijvoorbeeld bij urban air mobility het geval) die op verschillende momenten ingaan. Dan is de uiterste datum genoemd. Dat is ook het geval wanneer een wet geleidelijk wordt ingevoerd. Dat is bijvoorbeeld het geval bij de eIDAS 2.0 verordening, waarbij sommige verplichtingen volgens het voorstel na een jaar en andere na twee jaar zullen ingaan.

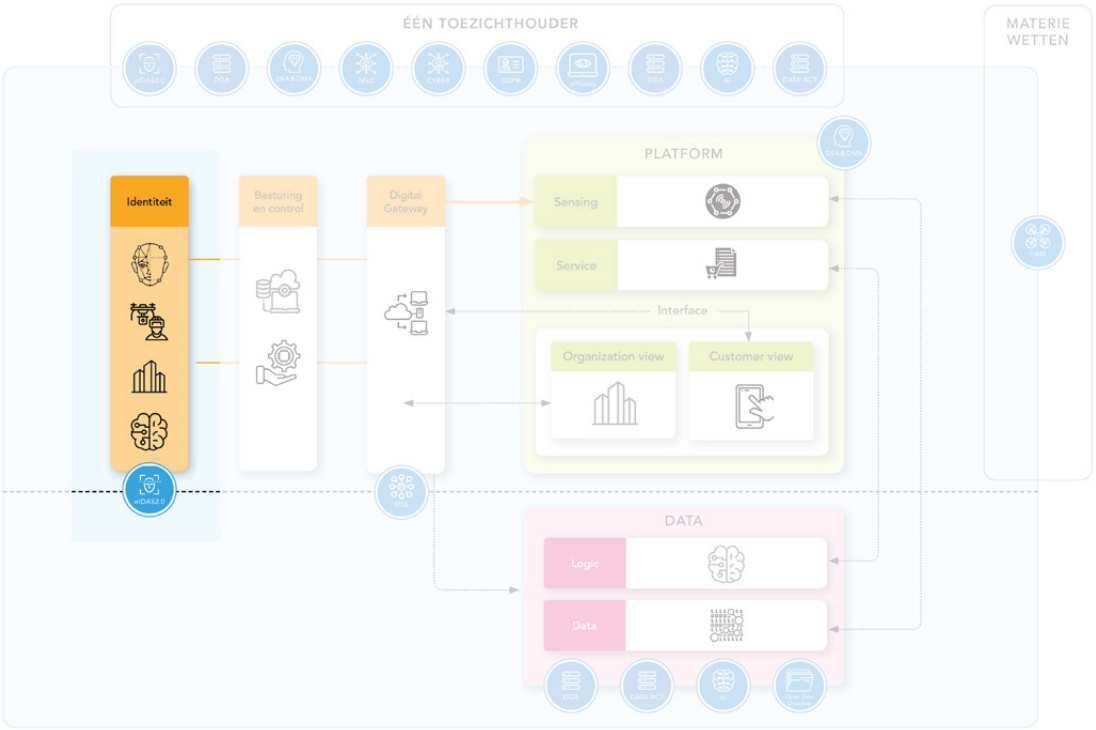
In de figuur zijn ook een aantal richtlijnen vermeld, die door de lidstaten in nationale wetgeving omgezet moeten worden voor ze kracht van wet krijgen. In de figuur is het moment opgenomen waarop deze omzetting volgens de richtlijn gereed moet zijn.

In dit hoofdstuk zijn de wetten samenhangend geclusterd naar overkoepelende onderwerpen, nl. Identiteit, Besturing en control, Digital gateway, Data, Platform en Privacy en Security. Zie hiervoor figuur 4.

Binnen deze samenhang beschrijven we het doel en de status van de specifieke wetten en geven we een beschrijving over waar de wet over gaat in de gemeentelijke context. Deze context is bij sommige wetten meer uitgewerkt dan anderen. De status van de wet maakt het nog niet mogelijk om specifieker te kunnen zijn.



Figuur 4: Samenhang Europese Digitale wetgeving



2.1. Identiteit

Er komt een Europese digitale identiteit voor elke EU-burger, elke inwoner en elke onderneming in de EU die dat wil. Ze kunnen zich daarmee identificeren en kiezen welke persoonlijke gegevens ze willen delen, zowel online als offline, met overheidsinstanties en bedrijven in de hele EU. Momenteel kunnen nog maar zo'n zes op de tien EU-burgers in 14 lidstaten hun nationale elektronische identiteits-bewijs in een ander land gebruiken. In alle EU-landen samen accepteert nog maar 14% van alle belangrijke openbare dienstverleners zo'n elektronisch bewijs uit een ander land, bijvoorbeeld om iemands identiteit te checken zonder extra wachtwoord. Erg vaak gebeurt dat nog niet, maar het aantal gevallen neemt wel toe[2].

2.1.1. Verordening Europees kader voor een digitale identiteit (eIDAS 2.0)

Doel

Met dit voorstel wil de EC de EU-verordening nr. 910/2014 (de eIDAS-verordening) wijzigen. De afkorting eIDAS staat voor 'electronic IDentities And Trust Services'. De Europese Unie wil met de verordening Europees kader voor een digitale identiteit regelen dat het makkelijker en veiliger wordt om binnen Europa online zaken te regelen, er wordt beoogd:

- om toegang tot sterk beveiligde en betrouwbare elektronische identiteitsoplossingen te bieden;
- dat openbare en particuliere diensten betrouwbare en veilige digitale- identiteitsoplossingen kunnen gebruiken;
- dat natuurlijke en rechtspersonen digitale-identiteitsoplossingen kunnen gebruiken;
- dat deze oplossingen verbonden zijn met een reeks attributen en dat daarmee identiteitsgegevens gericht kunnen worden gedeeld, binnen de grenzen van hetgeen voor de gevraagde specifieke dienst nodig is;
- dat gekwalificeerde vertrouwensdiensten in de EU worden aanvaard en dat gelijke voorwaarden gelden voor de verlening daarvan.

2 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl

Met het oog hierop worden in deze verordening de volgende onderwerpen gereguleerd:

Elektronische identificatiemiddelen (eID's)
De huidige eIDAS-verordening beoogt te zorgen voor een goede werking van de digitale interne markt door met wederzijdse erkenning van elektronische identificatiemiddelen (eID's) en met harmonisatie van vertrouwensdiensten[3] veilige en betrouwbare elektronische transacties tussen burgers, bedrijven en overheden te bevorderen.

De eIDAS-verordening stelt de voorwaarden vast waaronder lidstaten elkaars eID's voor burgers en bedrijven wederzijds moeten erkennen. Overheden en organisaties met publiekrechtelijke taken dienen erkende eID's op betrouwbaarheidsniveaus 'substantieel' en 'hoog' kosteloos toe te laten bij grensoverschrijdende transacties in het publieke domein.[4]

Voor eID's amendeert het voorstel de huidige eIDAS-verordening in de eerste plaats met de verplichting in plaats van de mogelijkheid van lidstaten om een eID voor burgers en bedrijven te hebben en Europees te laten erkennen. Het bestaande, als complex ervaren proces van wederzijdse erkenning door lidstaten op basis van 'peer review' (notificatie), wordt aangevuld met de mogelijkheid tot nationale certificering, waarbij wordt aangesloten bij de vereisten van de cyberbeveiligingsverordening. Daarnaast wordt verplicht om erkende eID-middelen toe te laten voor offline naast online authenticatie en niet alleen voor transacties in het publieke domein, maar ook voor transacties in het private domein. Dit is verplicht voor authenticatie op grote platformen en bij transacties met private partijen die hogere vormen van betrouwbaarheid vereisen, en is op basis van de te ontwikkelen 'codes of conduct' facultatief voor andere transacties in het private domein.

Elektronische vertrouwensdiensten
Het voorstel heeft ook gevolgen voor elektronische vertrouwensdiensten die tevens in de eIDAS-verordening worden gereguleerd. Een belangrijke wijziging is de toevoeging van vijf nieuwe soorten vertrouwensdiensten, namelijk het op afstand beheren van middelen (hardware en software) voor het aanmaken van elektronische handtekeningen, middelen (hardware en software) voor het aanmaken van elektronische zegels, elektronische attestatie van attributen, gekwalificeerde elektronische archiveringsdiensten en elektronische grootboeken (ledgers). Het op afstand beheren van middelen voor het aanmaken van elektronische handtekeningen of zegels zorgt ervoor dat gebruikers aparte dienstverleners kunnen gebruiken voor het verkrijgen van het middel en voor het beheer op afstand van het middel. Hierdoor is er minder afhankelijkheid van één partij voor het gebruik van deze middelen.

Elektronische attestatie van attributen
Een elektronische attestatie van attributen is de gewaarmerkte verklaring dat een natuurlijk of rechtspersoon een bepaalde eigenschap bezit, bijvoorbeeld dat iemand ouder is dan 18 jaar of dat iemand een bepaald diploma heeft behaald. Deze attestaties kunnen eIDAS-gecertificeerd (gekwalificeerd) zijn. De verordening verplicht de lidstaten dat een aantal attributen geverifieerd kunnen worden aan de hand van authentieke bronnen binnen de publieke sector. Daarnaast moeten deze attestaties ook via de wallet beschikbaar kunnen worden gemaakt. Gekwalificeerde elektronische archiveringsdiensten verwerken data en documenten op een wijze dat de integriteit en nauwkeurigheid van de oorsprong, alsook juridische eigenschappen, bewaard blijven voor de bewaarperiode. Een elektronisch grootboek is een fraudebestendige elektronische documentatie van data waarbij de authenticiteit, integriteit van de data, datum, tijd en de chronologische ordening worden vastgelegd. Hierbij moet worden gedacht aan technieken als blockchain. Bij al deze vertrouwensdiensten geldt dat de elektronische en niet-elektronische variant hetzelfde rechtsgevolg

3 Vertrouwensdiensten zijn elektronische diensten voor het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten of het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben. Elektronische transacties met eID-middelen kunnen een breed scala aan digitale handelingen omvatten, zoals belastingaangifte, bezwaar aantekenen, registreren of inzage in registers, het doen van meldingen en leveren of opvragen van informatie.

4 De betrouwbaarheidsniveaus laag, substantieel en hoog betreffen eID's die respectievelijk een beperkte, substantiële of een hoge mate van vertrouwen bieden in iemands opgegeven of beweerde identiteit. Worden erkende eID's met betrouwbaarheidsniveaus substantieel en hoog uit de ene lidstaat gebruikt in een andere lidstaat, dan moeten deze geaccepteerd worden in onlinediensten door openbare instanties. Erkende eID's met betrouwbaarheidsniveau laag, kunnen geaccepteerd worden in onlinediensten, maar in de praktijk zijn geen eID's met betrouwbaarheidsniveau laag erkend in de EU.

zullen hebben. Om elektronische attestatie van attributen te ondersteunen tussen Europese landen zorgt de EU voor het zogenoemde Once Only Technicals System. Dit moet eind 2023 beschikbaar zijn.[5] Het ondersteunt het eenmaligheidsbeginsel technisch, dat bepaalt dat burgers niet mogen worden gedwongen om informatie aan autoriteiten te verstrekken als een andere autoriteit die informatie al in elektronische vorm bezit.

Wallet
Elke lidstaat krijgt de plicht om tenminste één *'European Digital Identity Wallet'* te introduceren. De *wallet* kunnen lidstaten in eigen beheer of onder mandaat uitgeven of ze kunnen een onafhankelijk uitgegeven *wallet* erkennen. De lidstaten behouden daarbij dus de eigen regie en er zal geen sprake zijn van één Europese identiteit. Deze wallet dient burgers en bedrijven die dit willen, de mogelijkheid te bieden om onder een hoog beveiligingsniveau hun elektronische identiteit én daaraan gelinkte attributen, zoals kwalificaties, bevoegdheden en digitale documenten, zelf ter beschikking te stellen in online én offline transacties, in het publieke én het private domein. Het voorstel bepaalt dat het gebruik van de wallet gratis moet zijn voor natuurlijke personen.

Toolbox
Aanvullend heeft de Commissie een aanbeveling opgesteld om te komen tot een met de lidstaten te ontwikkelen '*Toolbox*' om de implementatie van het raamwerk voor een Europese Digitale Identiteit, in het bijzonder van de wallet en gekwalificeerde vertrouwensdiensten, te ondersteunen. Daarin worden de technische architectuur, het referentieraamwerk, gemeenschappelijke standaarden, technische specificaties, gemeenschappelijke richtlijnen en best practices opgenomen.

Daarnaast zitten er meerdere wijzigingen in dit voorstel die verband houden met de herziening van de Netwerk- en Informatiebeveiligings- richtlijn (hierna: NIS-richtlijn, zie ook paragraaf $$$) waar momenteel de onderhandelingen over lopen. In de herziening van de NIS-richtlijn wordt de zorg- en meldplicht voor vertrouwensdienstverleners verplaatst van de eIDAS-verordening naar de NIS-richtlijn. Daarom wordt de verordening op die punten aangepast.[6]

Ook zit er in de herziening van de eIDAS-verordening een verplichting voor browserleveranciers om gekwalificeerde certificaten van website-authenticatie te accepteren. Momenteel zijn browserleveranciers vrij om een eigen afweging te maken of gekwalificeerde websitecertificaten te vertrouwen zijn. In de praktijk betekent dat extra benodigde conformiteitsbeoordelingen en een grote afhankelijkheid van de browserleveranciers. Met deze wijziging mogen browserleveranciers deze eigen afweging niet meer maken en worden ze verplicht Europese standaarden voor betrouwbaarheid te accepteren.

Voorts is er nog een aantal kleinere wijzigingen zoals de verplichting voor de Commissie om binnen 12 maanden (6 maanden rondom de attestatie van attributen) na inwerkingtreding uitvoerings-besluiten te nemen ten aanzien van de relevante standaarden voor gekwalificeerde vertrouwens-diensten. Ten slotte zal de Commissie de bevoegdheid krijgen om wetgeving van derde (niet-EU) landen te beoordelen als gelijkwaardig aan de eIDAS-verordening.

Status

De Europese digitale identiteit verordening[7] is voorgesteld in juni 2021. De Wet digitale overheid (Wdo), waarvan de eerste tranche momenteel aanhangig is in de Eerste Kamer der Staten-Generaal, is het beoogde fundament voor regulering en doorontwikkeling van het eID-stelsel. De uitwerking zal waarschijnlijk plaatsvinden in de tweede tranche van de Wdo. De doelstelling van de EU-verordening is dat, in 2025, alle burgers en bedrijven gebruik kunnen maken van een hoogwaardige wallet.[8]

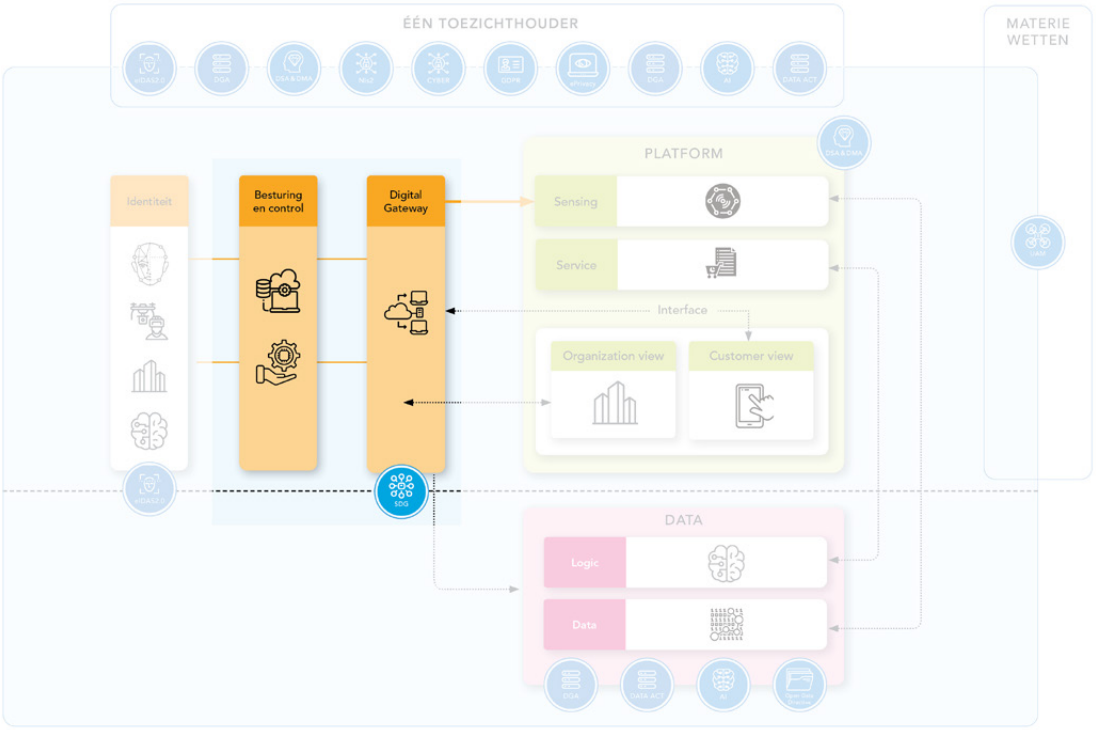
5 https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Once+Only+Technical+System
6 In relatie tot de NIB-richtlijn vraagt het kabinet zich af wat de toegevoegde waarde is van de verschuiving van de zorg- en meldplicht vanuit de eIDAS-verordening naar de NIB-richtlijn, en de daaraan gerelateerde wijzigingen in de eIDAS-verordening. Het kabinet ziet hierin het risico dat daarmee de bredere werking van waarborgen voor vertrouwensdiensten, anders dan gericht op netwerk- en informatiesystemen, die van cruciaal belang zijn, voor de betrouwbaarheid van de diensten onderbelicht of verloren raken. Het kabinet kan hier niet zonder meer mee akkoord gaan en zal hier nadere verduidelijking bij de Commissie over vragen. Te allen tijde zal het kabinet de coherentie tussen wetgeving, in het bijzonder tussen de NIB-richtlijn en de eIDAS-verordening, bewaken.
7 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

Europese burgers en vertegenwoordigers van bedrijven moeten sinds september 2018 bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met hun nationale inlogmiddel. Dit nationale elektronische inlogmiddel moet wel eerst erkend zijn door de Europese Commissie (het middel moet genotificeerd zijn). Gemeenten moeten daarom nu al zorgen dat de online dienstverlening achter DigiD (Substantieel of Hoog) of eHerkenning (3 en hoger) ook toegankelijk zijn voor EU-burgers en -ondernemers met hun genotificeerde nationale inlogmiddel. Als de Europese digitale identiteit verordening in werking is moeten gemeenten zorgen dat de genoemde middelen, als de wallet, inclusief attestatie van attributen en nieuwe vertrouwensdiensten worden ontsloten en worden ingebed in hun dienstverlening.

2.2. Digital gateway

De single digital gateway is een online centraal punt waarmee EU-burgers en bedrijven makkelijk toegang krijgen tot digitale overheidsdienstverlening in alle EU-lidstaten. Alle decentrale overheden moeten in het portaal een aantal diensten, producten en procedures digitaal beschikbaar en open-stellen voor grensoverschrijdende gebruikers.



2.2.1. Single Digital Gateway[9]

Doel

Met de verordening tot het oprichten van één digitale toegangspoort voor informatie, procedures en diensten voor ondersteuning en probleemoplossing (EU 2018/1724), wil het Europees Parlement en de Raad van de Europese Unie de volgende doelen bereiken:

9 Ontleend aan de impactanalyse Single Digital Gateway, april 2019 en https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX%3A32018R1724

1. Verbeteren functioneren van de interne markt
   "Door vrij verkeer van personen, goederen, diensten en kapitaal toe te staan, worden burgers en bedrijven nieuwe kansen geboden. Deze verordening is een belangrijk onderdeel van de strategie voor de eengemaakte markt (....). Die strategie is bedoeld om het volledige potentieel van de interne markt te benutten door het voor burgers en bedrijven eenvoudiger te maken zich binnen de Unie te bewegen en grensoverschrijdend handel te drijven, zich in een andere lidstaat te vestigen en hun zakelijke activiteiten naar een andere lidstaat uit te breiden." – overweging 1 uit de Verordening
2. Discriminatie wegnemen op het gebied van dienstverlening
   "Indien een gebruiker die zich in een situatie bevindt die uitsluitend onder één lidstaat ressorteert, in die lidstaat online toegang kan hebben tot een onder deze verordening vallende procedure en deze kan doorlopen, dan moet een grensoverschrijdende gebruiker ook online toegang kunnen hebben tot dezelfde procedure en deze kunnen doorlopen, via dezelfde technische oplossing dan wel via een andere, technisch onderscheiden oplossing die tot hetzelfde resultaat leidt, zonder discriminerende belemmeringen." – overweging 18
3. Verminderen van administratieve lasten
   "...administratieve belasting beperken voor burgers en bedrijven die geheel overeenkomstig de nationale voorschriften en procedures hun rechten met betrekking tot de interne markt, waaronder het vrije verkeer van burgers, uitoefenen of willen uitoefenen (...)" – overweging 6

Om dit mogelijk te maken, wordt er één digitale toegangspoort ontwikkeld, de Single Digital Gateway

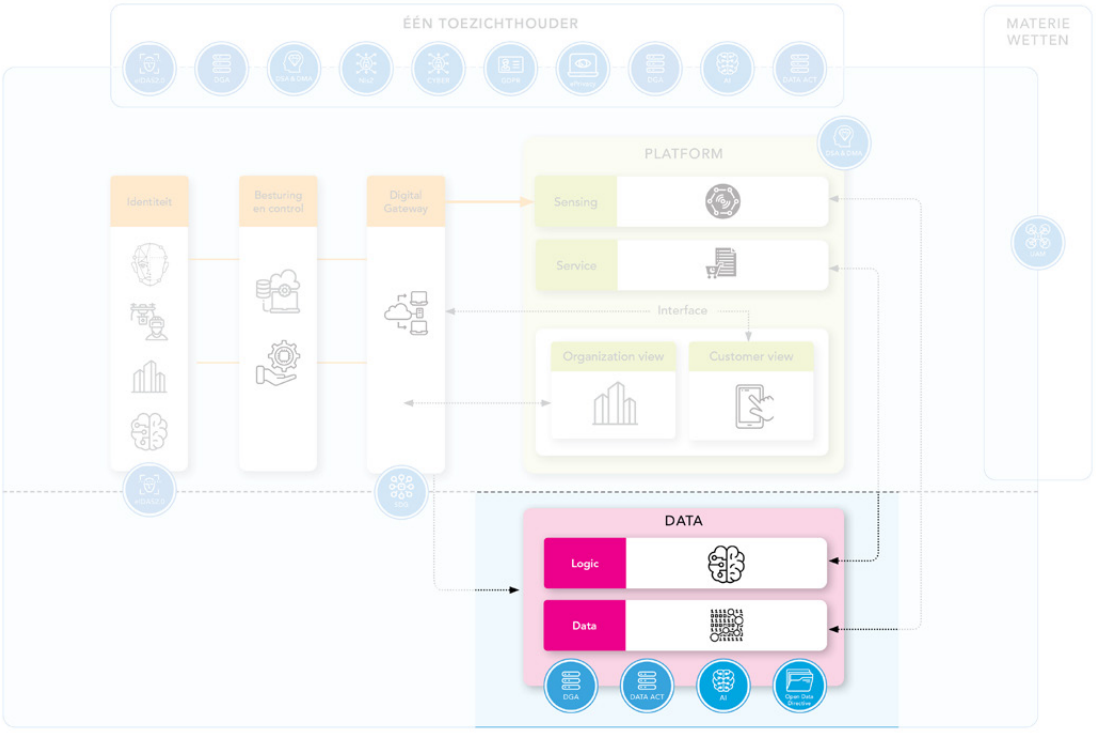
Status

Op 21 november 2018 is de verordening gepubliceerd en op 12 december 2018 trad de deze in werking. De verordening kent een aantal verplichtingen die tussen 2 en 5 jaar moet worden ingevoerd. In december 2022 zullen de eerste gemeentelijke informatieproducten ('Annex I') beschikbaar moeten zijn. Per 12 december 2023 zal vervolgens aan het transactionele deel van de verordening ('Annex II') voldaan moeten zijn.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

Gemeentelijke instanties (en afgeleide onderdelen zoals samenwerkingsverbanden en uitvoeringsdiensten, wanneer zij aanbieder zijn van producten die onder de SDG vallen) krijgen langer de tijd om te voldoen dan andere overheden:

- Vier jaar na inwerkingtreding om te voldoen aan de eis om informatie te verstrekken over de regels, procedures en diensten voor ondersteuning en probleemoplossing voor die producten die vallen onder de lijst die is opgenomen in de verordening onder de noemer 'Annex I'
- Vijf jaar na inwerkingtreding om die procedures die volledig online moeten worden aangeboden die in de Verordening zijn opgenomen in 'Annex II' geschikt te maken voor grensoverschrijdende toegang.



2.3. Data

Met de Europese datastrategie wil de EU het voortouw nemen in de datagestuurde economie. Met een interne markt voor data wil de EU zorgen dat gegevens binnen de hele EU en door alle sectoren heen vrij stromen zodat burgers, ondernemers, onderzoekers en overheden hiervan kunnen profiteren.[10]

De EU werkt hiertoe aan een interne markt voor data, waarin:
- Gegevens tussen de verschillende EU-landen en de sectoren kunnen circuleren ten voordele van iedereen
- De Europese regels volledig in acht worden genomen, vooral wat betreft privacy, gegevens-bescherming en mededinging
- Eerlijke, praktische en duidelijke regels voor de toegang tot en het gebruik van data gelden

De EU wil een aantrekkelijke, veilige en dynamische data-economie door:
- Duidelijke en eerlijke regels op te stellen voor toegang tot en hergebruik van data
- Te investeren in de volgende generatie van instrumenten en infrastructuren voor opslag en verwerking van data
- De krachten te bundelen voor de ontwikkeling van Europese cloudcapaciteit
- In belangrijke sectoren Europese data samen te brengen in de vorm van gemeenschappelijke en interoperabele dataruimten
- Gebruikers de rechten, tools en vaardigheden te geven om volledige controle over hun data uit te oefenen

2.3.1. Data governance act (DGA)[11]

Doel

De verordening is het eerste wetgevend voorstel uit de Europese datastrategie[12] en heeft als doel om databeschikbaarheid voor hergebruik in de EU te faciliteren door vertrouwen in data-tussen-personen te vergroten en datadeelmechanismes in de EU te versterken. De verordening heeft vier hoofdonderdelen: hergebruik van beschermde data in het beheer van openbare lichamen,

10 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl
11 Https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained
12 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl en COM(2020)66

voorwaarden voor datadeeldiensten, data-altruïsme en een Europese Data Innovatie Raad. Daarnaast gaat de verordening in op handhaving en toezicht en de internationale datastromen die verbonden zijn aan bovenstaande onderdelen.

Hergebruik van overheidsgegevens
De richtlijn open data (zie paragraaf hieronder) regelt het hergebruik van openbaar/beschikbare informatie waarover de publieke sector beschikt. De publieke sector beschikt echter ook over enorme hoeveelheden beschermde gegevens (bv. persoonsgegevens en commercieel vertrouwelijke gegevens) die niet als open gegevens kunnen worden hergebruikt, maar die op grond van specifieke EU- of nationale wetgeving kunnen worden hergebruikt. Een schat aan kennis kan uit dergelijke gegevens worden gehaald zonder afbreuk te doen aan het beschermde karakter ervan, en de DGA voorziet in regels en waarborgen om dergelijk hergebruik te vergemakkelijken wanneer dit mogelijk is op grond van andere wetgeving.

Voorwaarden voor datadeeldiensten
Veel bedrijven vrezen momenteel dat het delen van hun gegevens een verlies van concurrentie-voordeel zou betekenen en een risico op misbruik zou inhouden. De DGA definieert een reeks regels voor aanbieders van gegevensbemiddelingsdiensten (zogenaamde gegevensbemiddelaars, zoals gegevensmarktplaatsen) om ervoor te zorgen dat zij zullen functioneren als betrouwbare organisatoren van gegevensuitwisseling of -bundeling binnen de gemeenschappelijke Europese gegevensruimten (zie paragraaf hieronder). Om het vertrouwen in het delen van gegevens te vergroten, stelt deze nieuwe aanpak een model voor dat gebaseerd is op de neutraliteit en trans-parantie van gegevensbemiddelaars, terwijl individuen en bedrijven de controle over hun gegevens krijgen. Het raamwerk biedt een alternatief model voor de gegevensverwerkingspraktijken van de Big Tech-platforms, die een hoge mate van marktmacht hebben omdat ze grote hoeveelheden gegevens beheersen.

Data-altruïsme
Data-altruïsme gaat over individuen en bedrijven die hun toestemming geven om gegevens die zij genereren – vrijwillig en zonder beloning – beschikbaar te stellen voor gebruik in het algemeen belang. Dergelijke gegevens hebben een enorm potentieel om onderzoek te bevorderen en betere producten en diensten te ontwikkelen, onder meer op het gebied van gezondheid, milieu en mobiliteit. Onderzoek wijst uit dat er in principe weliswaar een bereidheid is om aan data-altruïsme te doen, maar dat dit in de praktijk wordt belemmerd door een gebrek aan tools voor het delen van gegevens. Het doel van de Data Governance Act is dan ook om betrouwbare tools te creëren waarmee data op een eenvoudige manier gedeeld kan worden ten behoeve van de samenleving. Het zal de juiste voorwaarden scheppen om personen en bedrijven ervan te verzekeren dat wanneer zij hun gegevens delen, deze zullen worden behandeld door vertrouwde organisaties op basis van de waarden en beginselen van de EU. Dit zal het mogelijk maken om pools van gegevens te creëren die groot genoeg zijn om gegevensanalyse en machine learning mogelijk te maken, ook over de grenzen heen.

European Data Innovation Board
Zoals bepaald in de DGA zal de Commissie het Europees Comité voor gegevensinnovatie (EDIB) oprichten om de uitwisseling van beste praktijken te vergemakkelijken, met name op het gebied van gegevensbemiddeling, gegevensaltruïsme en het gebruik van beschermde gegevens onder wetgeving als open gegevens beschikbaar kunnen worden gesteld, alsook op het gebied van de prioritering van sectoroverschrijdende interoperabiliteitsnormen.

Status

Over de Data Governance Act[13] is in november 2021 een akkoord bereikt tussen de EC, de Raad van EU en het EP. De Data Governance Act is op 23 juni 2022 in werking getreden en zal, na een verschoningsperiode van 15 maanden, van toepassing zijn vanaf september 2023.[14]

13 Https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
14 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

Hergebruik van overheidsgegevens
De verordening verplicht niet de openstelling van beschermde data, maar verbiedt exclusieve overeenkomsten over het hergebruik van deze data met derde partijen. Dit betekent dat als een gemeente een overeenkomst sluit om deze data beschikbaar te maken aan een derde partij, andere derde partijen ook het recht hebben om onder dezelfde voorwaarden toegang te krijgen tot deze data. Hiermee wil de Commissie kleinere spelers op de Europese markt ondersteunen. Bij wijze van uitzondering is een dergelijke exclusieve overeenkomst wel toegestaan indien dit nodig is voor de levering van een dienst of een product in het algemeen belang.

Voorwaarden voor datadeeldiensten
Mogelijk nemen gemeenten een rol als datadeeldienst voor het delen van gegevens en bevorderen een bepaald ecosysteem (bijv. mobiliteit, leefbaarheid), waarbij er een duidelijke scheiding bestaat tussen de bemiddelingsrol en andere activiteiten in verband met het gebruik van de gegevens. Gemeenten mogen dan niet de data ten gelde maken (bijvoorbeeld door ze aan een ander bedrijf te verkopen of te gebruiken om hun eigen product te ontwikkelen op basis van deze gegevens), maar functioneren als een neutrale derde partij die datahouders en datagebruikers met elkaar verbindt.

Verzamelen en verwerken van altruïstische gegevens
Het voorstel creëert de mogelijkheid voor organisaties en mogelijk dus ook voor gemeenten die data verzamelen voor een algemeen belang om zich te registreren als een 'data-altruïsme organisatie erkend door de EU'. Een voorbeeld is hier het Smart Citizen platform, dit platform stelt burgers in staat om gegevens over geluidsniveaus en vervuiling in hun huis te delen die via sensoren zijn verzameld. Dit levert essentiële informatie op om geluid en luchtkwaliteit in kaart te brengen en voor onderzoekers en overheden om gerichte oplossingen voor deze problemen te ontwikkelen.

2.3.2. Data act (DA)

Doel

Terwijl de DGA de processen en structuren creëert om data te faciliteren, maakt de DA duidelijk wie waarde kan creëren uit data en onder welke voorwaarden. Het voorstel voor een Dataverordening (DA) beoogt het gebruik van data te bevorderen en te verzekeren dat de waarde uit data gelijkwaardiger wordt verdeeld over de partijen die deelnemen aan de data-economie.

Wanneer iemand een 'traditioneel' product koopt, verkrijgt hij/zij alle onderdelen en accessoires van dat product. Wanneer echter een verbonden product (bijvoorbeeld een slim huishoudelijk apparaat of slimme industriële machines) wordt gekocht dat gegevens genereert, is het vaak niet duidelijk wie wat met de gegevens kan doen. Of in het contract kan worden bepaald dat alle gegenereerde gegevens uitsluitend door de fabrikant worden verzameld en gebruikt.
De Data Act geeft zowel particulieren als bedrijven meer controle over hun gegevens door middel van een versterkt recht op gegevensportabiliteit, waarbij gegevens eenvoudig worden gekopieerd of overgedragen vanuit verschillende services, waarbij de gegevens worden gegenereerd via slimme objecten, machines en apparaten. Een eigenaar van een auto of machine kan er bijvoorbeeld voor kiezen om gegevens die door het gebruik ervan zijn gegenereerd, te delen met zijn verzekeringsmaatschappij. Dergelijke gegevens, geaggregeerd van meerdere gebruikers, kunnen ook helpen bij de ontwikkeling of verbetering van andere digitale diensten, bijvoorbeeld met betrekking tot verkeer of gebieden met een hoog risico op ongevallen.
Het zal gemakkelijker worden om gegevens over te dragen aan en tussen dienstverleners en dit zal meer actoren, waaronder midden- en kleinbedrijven aanmoedigen om deel te nemen aan de data-economie, door:

- De toegang tot en het gebruik van data door consumenten en bedrijven te vergemakkelijken, met behoud van stimulansen om te investeren in manieren om door middel van data waarde te

16 https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114

genereren. Dit omvat het vergroten van de rechtszekerheid rond het delen van data die zijn verkregen uit of gegenereerd door het gebruik van producten of gerelateerde diensten, en het operationeel maken van regels die moeten leiden tot eerlijke data-uitwisselingsovereenkomsten. Het voorstel verduidelijkt de toepassing van de relevante rechten uit hoofde van Richtlijn 96/9/EG betreffende de rechtsbescherming van databanken (de databankrichtlijn) op de bepalingen ervan. Het gaat hier over het delen van data tussen bedrijven en consumenten (B2C) en tussen bedrijven en bedrijven (B2B).

- Voorzien in het gebruik door overheidsinstanties en EU-instellingen, - agentschappen of -organen van data die in handen zijn van ondernemingen in bepaalde situaties waarin er sprake is van een uitzonderlijke noodzaak om de data te gebruiken. Dit heeft voornamelijk betrekking op openbare noodsituaties, maar ook op andere uitzonderlijke situaties waarin het verplicht delen van data tussen bedrijven en overheden gerechtvaardigd is, ter ondersteuning van empirisch onderbouwd, doeltreffend, efficiënt en prestatiegericht overheidsbeleid en -diensten.

- Het overstappen tussen cloud- en edgediensten te vergemakkelijken. Toegang tot concurrerende en interoperabele dataverwerkingsdiensten is een voorwaarde voor een bloeiende data-economie, waarin data gemakkelijk kunnen worden gedeeld binnen en tussen sectorale ecosystemen. De mate van vertrouwen in dataverwerkingsdiensten is bepalend voor het gebruik van dergelijke diensten door gebruikers in alle sectoren van de economie.

- Voorzien in waarborgen tegen onrechtmatige data-overdracht zonder kennisgeving door aanbieders van clouddiensten. De reden hiervoor is dat er bezorgdheid is over de onrechtmatige toegang tot data door overheden van buiten de EU/de Europese Economische Ruimte (EER). Dergelijke waarborgen moeten leiden tot meer vertrouwen in de dataverwerkingsdiensten die de Europese data-economie in toenemende mate ondersteunen.

- Interoperabiliteitsnormen ontwikkelen voor data die tussen sectoren kunnen worden hergebruikt, om belemmeringen voor het delen van data tussen domeinspecifieke gemeenschappelijke Europese dataruimten overeenkomstig de sectorale interoperabiliteitsvereisten uit de weg te ruimen, evenals belemmeringen voor het delen van data die niet binnen het toepassingsgebied van een specifieke gemeenschappelijke Europese dataruimte vallen. Volgens het voorstel zal ook de vaststelling van normen voor "slimme contracten" worden ondersteund. Dit zijn computerprogramma's die werken met elektronische registers, die transacties uitvoeren en afwikkelen op basis van vooraf bepaalde voorwaarden. Zij kunnen houders en ontvangers van data garanderen dat de voorwaarden voor het delen van data worden nageleefd.

Status

De DA is voorgesteld in februari 2022[15] en wordt gezien als het tweede grote horizontale wetgevingsinitiatief na de Data Governance Act. Op moment van schrijven bevinden de besprekingen in de Raad van de EU en Euorpees Parlement zich in een beginnende fase. Er is nog geen indicatie van verwachte periode van akkoord of inwerkingtreding.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?[16]

Verzoek om data bij een uitzonderlijke behoefte/situatie
De DA heeft tot doel de waarde van gegevens van particuliere bedrijven te ontsluiten in uitzonderlijke situaties van groot openbaar belang, zoals overstromingen of bosbranden. De huidige mechanismen voor gegevenstoegang door de publieke sector zijn inefficiënt of bestaan niet in openbare noodsituaties. Met de nieuwe regels komt er een verplichting voor bedrijven om bepaalde gegevens te verstrekken, onder belangrijke voorwaarden (die bedrijven kunnen afdwingen in geval van misbruik).

15 Https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN
16 https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114

Als de gegevens nodig zijn om een openbare noodsituatie aan te pakken, moeten ze gratis worden verstrekt. In andere situaties: om een openbare noodsituatie te voorkomen of te herstellen, of om te voldoen aan een wettelijk opgelegd mandaat van algemeen belang - kan de gegevenshouder om compensatie vragen. Het moet de empirisch onderbouwde besluitvorming aanzienlijk verbeteren, met name een doeltreffende en snelle reactie op crises, zoals overstromingen en bosbranden of zoals tijdens de COVID-19-pandemie toen geaggregeerde en geanonimiseerde locatiegegevens van exploitanten van mobiele netwerken bijvoorbeeld essentieel waren voor het analyseren van de correlatie tussen mobiliteit en de verspreiding van het virus, met inbegrip van het informeren van systemen voor vroegtijdige waarschuwing voor nieuwe uitbraken en het nemen van de juiste maatregelen om de crisis te bestrijden.

De DA verandert niet andere bestaande verplichtingen of regelingen t.a.v. het opvragen van gegevens door de overheid bij bedrijven (zoals bijvoorbeeld het CBS).

Dataportabiliteit
Dataverwerkers moeten dataportabiliteit naar vergelijkbare diensten mogelijk maken, en dat moet contractueel met de klant zijn vastgelegd. En hiermee ook als de gemeente een klant is. Zulke dataportabiliteit moet gratis zijn voor de klant, al mogen in de eerste 3 jaren van de inwerkingtreding van de DA hooguit marginale kosten in rekening worden gebracht.

Interoperabiliteit
De DA geeft een reeks essentiële vereisten om interoperabiliteit mogelijk te maken tussen data spaces en data verwerkende diensten. Zo moeten data inhoud, structuur, licenties, verzamelmethode, kwaliteit en onzekerheden gedocumenteerd zijn, evenals datastructuren, formaten, classificaties, API beschrijvingen etc. De EC kan verdere regels stellen t.a.v. interoperabiliteit, ook voor bepaalde sectoren. De EC kan standaarden vereisen, en (internationale) standaarden adopteren en verplicht stellen, niet alleen t.a.v. data maar ook bijvoorbeeld t.a.v. architectuur, technische standaarden en federatie van clouddiensten t.b.v. de Europese dataspace(s). De regels streven interoperabiliteit en portabiliteit na op zowel transport, syntactisch, semantisch, beleid en gedragsniveau.

2.3.3. Open data richtlijn (Wetsvoorstel open data richtlijn)

Doel

De publieke sector in de EU-lidstaten produceert grote hoeveelheden data, zoals meteorologische gegevens, digitale kaarten, statistieken en juridische informatie. Die informatie is waardevol voor de digitale economie. Ze wordt niet alleen gebruikt als waardevolle grondstof voor de productie van op gegevens gebaseerde diensten en toepassingen, maar zorgt ook voor meer efficiëntie bij de levering van particuliere en openbare diensten en voor een beter onderbouwde besluitvorming. Daarom ijvert de EU reeds jaren voor het hergebruik van overheidsinformatie. De Open Data Directive (2019) is de opvolger van de Hergebruiksrichtlijn (uit 2003 en 2013). Nederland heeft deze regelingen omgezet in de Wet hergebruik overheidsinformatie (Who). In eerste instantie zijn regels inzake non-discriminatie, tariferingsbeginselen, exclusiviteitsregelingen, transparantie, licenties en praktische hulpmiddelen die ervoor moeten zorgen dat overheidsinformatie kan worden opgezocht en hergebruikt, opgesteld. In een nieuwe verplichting om het hergebruik van algemeen toegankelijke overheidsgegevens mogelijk te maken, is de uitbreiding van de werkingssfeer van de richtlijn tot documenten van openbare bibliotheken, musea en archieven, en standaardregels om de vergoedingen te beperken tot de marginale kosten voor de reproductie, de verstrekking en de verspreiding van informatie toegevoegd en openbare instanties werden verplicht transparantie te bieden over de regels en voorwaarden die zij hanteren.

In de open data directive is ingezet op het volledig kunnen benutten van het potentieel van overheidsinformatie ten behoeve van de Europese economie en samenleving door de richtlijn aan te passen aan de nieuwste ontwikkelingen op het gebied van databeheer en -gebruik. Het voorstel heeft in het bijzonder betrekking op de volgende aspecten:

1. Bevordering beschikbaarstelling van dynamische en realtime data met gebruik van Application Programming Interface (API), inclusief onderzoeksdata.
2. Vaststelling van een gemeenschappelijke Europese lijst van High Value Data Sets (Europese HVDL).
3. Bevordering van het beschikbaar stellen van data van overheidsbedrijven die een publiek belang dienen.
4. Verdere beperking van exclusieve overeenkomsten bij beschikbaarstelling van data.
5. Beperking van de mogelijkheden om een uitzondering te maken op het uitgangspunt waardoor organisaties meer dan de marginale kosten in rekening brengen voor het beschikbaar stellen van hun data.
6. Het verduidelijken van de verhouding van de richtlijn tot andere Europese regelgeving, zoals de databankenrichtlijn en de INSPIRE-richtlijn (betreffende geo-informatie).

Status

Met de Wet implementatie Open datarichtlijn[17] is het de bedoeling om de Who aan te passen door de regels uit de Open data richtlijn in de Who op te schrijven. Deze wet is in februari 2022 in consultatie geweest.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?[18]

- Met de inwerkingtreding van de nieuwe Europese Open Data Richtlijn moeten gemeenten niet alleen meer inspelen op Who-verzoeken, maar geldt ook dat bepaalde soorten data proactief aangeboden moeten worden voor hergebruik. Het gaat hier om dynamische en realtime verzamelde data; in de praktijk gaat het hier veelal om sensordata. Deze moeten aangeboden worden via API 's.
- Daarnaast wordt de reikwijdte van het begrip´ open data´ opgerekt. Gemeenten zullen ook op verzoek ook onderzoeksdata beschikbaar moeten kunnen stellen als open data. Dit is onder de huidige Who niet het geval.
- In de Europese Open Data Richtlijn wordt de vaststelling van een lijst met hoogwaardige datasets aangekondigd; de Europese High Value Data lijst (HVDL). Overheidsorganisaties moeten deze datasets machinaal leesbaar, kosteloos en via een API (of eventueel een bulkdownload) beschikbaar stellen. De lijst bestaat uit:
    - Geospatiale data (bijvoorbeeld postcodes, plaatsnamen, kadastrale kaarten);
    - Aardobservatie en milieu (bijvoorbeeld gegevens over biodiversiteit en geologie);
    - Meteorologische data (bijvoorbeeld in-situdata afkomstig van instrumenten en
    - weersvoorspellingen);
    - Statistiek (bijvoorbeeld demografische en economische indicatoren);
    - Bedrijven en eigendom van bedrijven (bijvoorbeeld bedrijfsactiviteiten en
    - registratienummers);
    - Mobiliteit (bijvoorbeeld transportnetwerken en gegevens over binnenwateren).

Voor deze categorieën van hoogwaardige gegevenssets gelden op zichzelf nog geen bijzondere regels. Maar de Europese Commissie heeft op grond van artikel 14 van de richtlijn de bevoegdheid om door middel van uitvoeringshandelingen een lijst vast te stellen met daarop specifieke hoog-waardige gegevenssets die binnen deze categorieën vallen en in bezit zijn van met een publieke taak belaste instellingen of overheidsondernemingen.

- Gemeenten hebben onder de huidige Who de mogelijkheid om kosten in rekening te brengen voor hergebruik van overheidsinformatie. De Europese Open Data Richtlijn heeft als uitgangspunt dat er geen kosten worden berekend voor hergebruik van overheidsinformatie, maar de kosten voor de vermenigvuldiging, verstrekking en verspreiding van de betreffende overheidsinformatie mogen nog steeds teruggevorderd worden. Evenals de kosten voor het anonimiseren van

17 https://www.internetconsultatie.nl/wetimplementatieopendatarichtlijn/b1
18 https://vng.nl/nieuws/impactanalyse-eu-open-datarichtlijn

persoonsgegevens en voor maatregelen ter bescherming van commercieel vertrouwelijke informatie, die in de herziene richtlijn expliciet genoemd worden.

- Gemeenten hebben onder de huidige Who de mogelijkheid om met bepaalde partijen exclusieve overeenkomsten af te sluiten over het leveren van datasets. Er kunnen afspraken gemaakt worden over bijvoorbeeld de (mate van) exclusiviteit, de nauwkeurigheid en/of de frequentie van de te leveren data. De gemeente mag hier kosten voor in rekening brengen. Op basis van de Europese Open Data Richtlijn is het maken van deze afspraken nog steeds mogelijk, maar moet de gemeente transparant zijn over het feit dat een dergelijke overeenkomst met een specifieke partij is afgesloten en de inhoud van die overeenkomst publiceren.

- Overheidsorganisaties en overheidsondernemingen moeten meer hun best doen om uit zichzelf zoveel mogelijk gegevens open en beschikbaar te maken voor hergebruik.

2.3.4. European Data Spaces (Data ruimten)[19]

Doel

Vanuit de Europese strategie voor data wil de Commissie de ontwikkeling van gemeenschappelijke Europese dataruimtes in strategische economische sectoren en gebieden van algemeen belang bevorderen. Deze sectoren of domeinen zijn die waar het gebruik van data een systemische impact zal hebben op het hele ecosysteem, maar ook op burgers. De EU-brede dataspace is waar alle aspecten uit de hiervoor genoemde DGA, DA en Open datarichtlijn tot praktische uitdrukking komen.

In de visie van de Europese strategie voor gegevens is de totstandbrenging van gemeenschappelijke, interoperabele gegevensruimten in de hele EU in strategische sectoren gericht op het wegnemen van juridische en technische belemmeringen voor het delen van gegevens door de nodige instrumenten en infrastructuren te combineren en vertrouwenskwesties aan te pakken door middel van gemeenschappelijke regels. Een gemeenschappelijke Europese gegevensruimte brengt relevante gegevensinfrastructuren en governancekaders samen om het poolen en delen van gegevens te vergemakkelijken.
Volgens de Europese strategie voor data zullen de dataruimtes het volgende omvatten:

1. de inzet van instrumenten en diensten voor het delen van gegevens voor het bundelen, verwerken en delen van gegevens door een open aantal organisaties, alsmede de federatie van energie-efficiënte en betrouwbare cloudcapaciteiten en aanverwante diensten;
2. structuren voor gegevensbeheer, die verenigbaar zijn met de relevante EU-wetgeving en die op transparante en eerlijke wijze het recht op toegang tot en verwerking van de gegevens bepalen;
3. verbetering van de beschikbaarheid, kwaliteit en interoperabiliteit van gegevens – zowel in domeinspecifieke omgevingen als in verschillende sectoren.

Afgezien van de verplichtingen inzake gegevensuitwisseling die zijn vastgelegd in de wetgeving van de Unie of de lidstaten, zullen gegevens in de gemeenschappelijke Europese gegevensruimten op vrijwillige basis beschikbaar worden gesteld en kunnen zij worden hergebruikt tegen vergoeding, met inbegrip van een vergoeding, of gratis, afhankelijk van het besluit van de gegevenshouder.

Voortbouwend op de lopende ervaring met de onderzoeksgemeenschap met de Europese open wetenschapscloud, zal de Commissie de oprichting van de volgende negen gemeenschappelijke Europese gegevensruimten ondersteunen:

- Een industriële (productie)gegevensruimte ter ondersteuning van het concurrentievermogen en de prestaties van de EU-industrie, waardoor de potentiële waarde van het gebruik van niet-persoonsgebonden gegevens in de industrie (geraamd op 1,5 biljoen euro tegen 2027) kan worden vastgelegd.

19 A European strategy for data: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

- Een Europese Green Deal-gegevensruimte, om het grote potentieel aan gegevens te benutten ter ondersteuning van de prioritaire acties van de Green Deal op het gebied van klimaatverandering, circulaire economie, nulvervuiling, biodiversiteit, ontbossing en nalevingsgarantie. De initiatieven 'GreenData4All' en 'Destination Earth' (digital twin of the Earth) zullen concrete acties omvatten.

- Een mobiliteitsdataruimte om Europa in de voorhoede te plaatsen bij de ontwikkeling van een intelligent vervoerssysteem, met inbegrip van geconnecteerde auto's en andere vervoerswijzen. Een dergelijke gegevensruimte zal de toegang tot, het bundelen en delen van gegevens uit bestaande en toekomstige vervoers- en mobiliteitsdatabanken vergemakkelijken.

- Een ruimte voor gezondheidsgegevens, die van essentieel belang is voor de vooruitgang bij het voorkomen, opsporen en genezen van ziekten en voor geïnformeerde, empirisch onderbouwde beslissingen om de toegankelijkheid, doeltreffendheid en duurzaamheid van de gezondheids-zorgstelsels te verbeteren.

- Een ruimte voor financiële gegevens om door middel van verbeterde gegevensuitwisseling innovatie, markttransparantie, duurzame financiering, toegang tot financiering voor Europese bedrijven en een meer geïntegreerde markt te stimuleren.

- Een ruimte voor energiegegevens, ter bevordering van een sterkere beschikbaarheid en sector-overschrijdende uitwisseling van gegevens, op een klantgerichte, veilige en betrouwbare manier, aangezien dit innovatieve oplossingen zou vergemakkelijken en het koolstofvrij maken van het energiesysteem zou ondersteunen.

- Een ruimte voor landbouwgegevens om de duurzaamheidsprestaties en het concurrentie-vermogen van de landbouwsector te verbeteren door de verwerking en analyse van productie- en andere gegevens, waardoor een nauwkeurige en op maat gesneden toepassing van productiebenaderingen op bedrijfsniveau mogelijk wordt.

- Gegevensruimte voor het openbaar bestuur, om de transparantie en verantwoordingsplicht van overheidsuitgaven en de kwaliteit van de uitgaven te verbeteren, corruptie te bestrijden, zowel op EU- als op nationaal niveau, en om tegemoet te komen aan de behoeften van rechtshand-havingsinstanties en om de effectieve toepassing van HET EU-recht te ondersteunen en innova-tieve "gov tech", "reg tech" en "legal tech"-toepassingen mogelijk te maken ter ondersteuning van beroepsbeoefenaars en andere diensten van algemeen belang

- Een ruimte voor gegevens over vaardigheden om de discrepanties tussen het onderwijs- en opleidingssysteem enerzijds en de behoeften van de arbeidsmarkt anderzijds te verminderen.

De Commissie kan overwegen om aanvullende gemeenschappelijke Europese gegevensruimten in andere sectoren op te zetten.

De dataspaces worden ondersteund met een federatieve data-infrastructuur, Gaia-X[20]

Status

Het werkdocument van de diensten van de Commissie geeft een overzicht van de gemeenschap-pelijke Europese gegevensruimten die in verschillende strategische sectoren of domeinen worden ontwikkeld als reactie op de Europese strategie voor gegevens.[21]
In februari 2020 werd in de Europese strategie voor gegevens het standpunt van de Commissie gepresenteerd voor het opzetten van in eerste instantie 10 sector-/domeinspecifieke gegevens-ruimten. Sindsdien zijn stappen gezet, zowel horizontaal als per sector/domein, om meer gegevens-uitwisseling mogelijk te maken en de basis te leggen, zowel in termen van wetgevende als financieringsmaatregelen, voor de dataruimtes. Er zijn financieringsprogramma's ter ondersteuning

20 https://gaia-x.eu/what-is-gaia-x/
21 https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

van de dataruimtes goedgekeurd en in 2021 zijn de eerste oproepen gelanceerd. Ook in andere sectoren, zoals media, cultuur, toerisme en bouw, is vooruitgang geboekt, waardoor de weg is vrijgemaakt voor meer gegevensuitwisseling. Daarnaast zal is in de eerste helft van dit jaar een wetgevingsvoorstel voorgesteld voor een governancekader tot oprichting van de European Health Data Space[22]. Andere belangrijke mijlpalen voor 2022 zijn de goedkeuring van een voorstel voor een open eu-financieringskader, een actieplan voor digitalisering van energie en de herziening van de bestaande EU-regels in de mobiliteitssector en inzake geospatiale milieugegevens en de toegang van het publiek tot milieu-informatie. Tegelijkertijd zullen de werkzaamheden die in het kader van de financieringsprogramma's zijn gepland, worden voortgezet voor alle betrokken gegevensruimten. De Commissie zal in 2023 verder verslag uitbrengen over de ontwikkeling van gemeenschappelijke Europese dataruimtes.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

De Commissie investeert in data ruimten door de ontwikkeling van infrastructuur voor gegevens-verwerking, instrumenten voor het delen van gegevens, architecturen en governancemechanismen voor een uitwisseling van gegevens en voor de federatie van energie-efficiënte en betrouwbare cloudinfrastructuren en aanverwante diensten. Nederland en gemeenten ontwikkelen en/of beheren ook dataruimten (zoals basisregistraties of voorziene gefedereerde basisregistratgies als mobiliteits-data, gegevensuitwisselingsmechanisme binnen GDI/Common Ground).

2.3.5. Artificial intelligence act (AI-act)

Doel

Het doel van het voorstel is om innovatie te stimuleren en burgers/consumenten te beschermen. Het voorstel wil ervoor zorgen dat AI-systemen die op de Europese markt worden gebracht en gebruikt, veilig en in overeenstemming zijn met de geldende fundamentele rechten en waarden binnen de EU zoals onder andere neergelegd in de Europese verdragen en internationale mensen-rechtenverdragen en in wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG). Het streven is om zo een interne markt voor veilige en betrouwbare AI-systemen te faciliteren terwijl marktfragmentatie wordt voorkomen. Tevens wil de verordening zorgen voor juridische zeker-heid om investeringen en innovatie in AI te faciliteren.
Het voorstel onderscheidt de volgende categorieën AI-systemen: Verboden praktijken waarbij bepaalde AI-systemen worden gebruikt met onacceptabele risico's; Hoog-risico AI-systemen die moeten voldoen aan verplichtingen en de nakoming hieraan moeten aantonen door middel van een ex ante conformiteitsbeoordeling; AI-systemen waarvoor bepaalde transparantievereisten gelden; en voor AI-systemen met geen of minimale risico's is een raamwerk voor vrijwillige gedragscodes voorzien.

Status

De AI-act is voorgesteld in april 2021. In de Raad zijn diverse compromisteksten opgesteld waarin wijzigingen worden voorgesteld. In november vindt er een plenaire stemming plaats in het Europees Parlement. Het voorstel zal mogelijk tijdens het Zweedse voorzitterschap van de Raad in de eerste helft van 2023 in werking treden.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

De Commissie hanteert een definitie van AI die naast zogenaamde machine learning technieken ook andere algoritmische systemen omvat. Het gaat hier dan bijvoorbeeld om besluitvormingssystemen op basis van klassieke statistiek, beslisbomen en zoekmethodes. Het voorstel is van toepassing

22 https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en

op AI-systemen die in de EU op de markt worden gebracht of in gebruik worden genomen, in sectoren uiteenlopend van speelgoed tot vervoersmiddelen, infrastructuur, machines en software die besluitvorming ondersteunt, ongeacht waar de ontwikkeling heeft plaatsgevonden en ongeacht of sprake is van privaat of publiek gebruik. Het voorstel introduceert verschillende vereisten voor de ontwikkeling, het op de markt brengen en het in gebruik nemen van hoog-risico AI-systemen die kunnen gelden voor providers[23], importeurs, distributeurs en gebruikers. AI-systemen exclusief ontwikkeld en gebruikt voor militaire doeleinden zijn uitgezonderd.

Onder het verbod valt een aantal 'praktijken' waarbij AI-systemen worden gebruikt: om menselijk gedrag, meningen of besluiten te manipuleren; om kwetsbaarheden van personen of groepen te exploiteren; en om personen sociaal te scoren (*social scoring*) of te beoordelen. Daarnaast is er ook een verbod op het gebruik van *real-time* biometrische identificatie[24] in de publieke ruimte ten behoeve van strafrechtelijke rechtshandhaving. Voor dit laatste verbod zijn er uitzonderingen mogelijk onder bepaalde omstandigheden. Om bij uitzondering real time biometrische identificatie in te mogen zetten door rechtshandhavingsautoriteiten is een ex ante autorisatieprocedure voorgesteld.

Risicobenadering
De verordening volgt een risico gebaseerde aanpak, waarbij een onderscheid wordt gemaakt tussen AI-toepassingen die i) een onaanvaardbaar risico, ii) een hoog risico, en iii) een laag of minimaal risico met zich meebrengen. In het voorstel worden daarvoor verplichtingen gesteld aan de providers van hoog-risico AI-systemen en, zij het in mindere mate, aan de gebruikers van hoog-risico AI- systemen. De verplichtingen hebben onder andere betrekking op data, menselijke controle, technische documentatie, nauwkeurigheid en cyberveiligheid. Ook onderdeel hiervan zijn documentatievereisten om inzicht te bieden in de werking en gemaakte keuzes bij AI-systemen.

Conformiteitsbeoordelingen
Providers dienen de naleving van de aanvullende verplichtingen voor hun hoog-risico AI-systemen aan te tonen door middel van een ex ante conformiteitsbeoordeling. Na het uitvoeren van de conformiteitsbeoordeling, dient een provider een verklaring van conformiteit op te stellen en het AI-systeem zichtbaar voorzien van een CE-keurmerk (EU-productcertificeringskeurmerk). Bij iedere substantiële verandering aan het AI-systeem na introductie op de markt of ingebruikname, moet een nieuwe conformiteitsbeoordeling te worden uitgevoerd.

Transparantie voor overige AI-systemen
De Commissie heeft specifieke transparantieverplichtingen (anders dan de transparantieverplichtingen die gelden voor hoog-risico AI-systemen) gesteld voor AI-systemen die bedoeld zijn om interactie met natuurlijke personen te hebben (zoals chatbots) of content te genereren of het zich voordoen als een (bestaand) persoon (zoals deepfakes). Daarnaast gelden deze verplichtingen voor AI-systemen die gebruikmaken van emotieherkenningstechnologie of biometrisch categoriseren[25]. De transparantieverplichtingen die gelden voor deze specifieke AI- systemen zien vooral op het duidelijk maken dat men te maken heeft met een AI-systeem, tenzij dit duidelijk is door omstandigheden of de gebruikscontext. Daarnaast geldt een verplichting om, als dat het geval is, duidelijk te maken dat een AI-systeem gebruik maakt van emotieherkenning en/of biometrische categorisatie. Wanneer deze systemen ook vallen onder een hoog-risico categorie, gelden deze verplichtingen aanvullend.

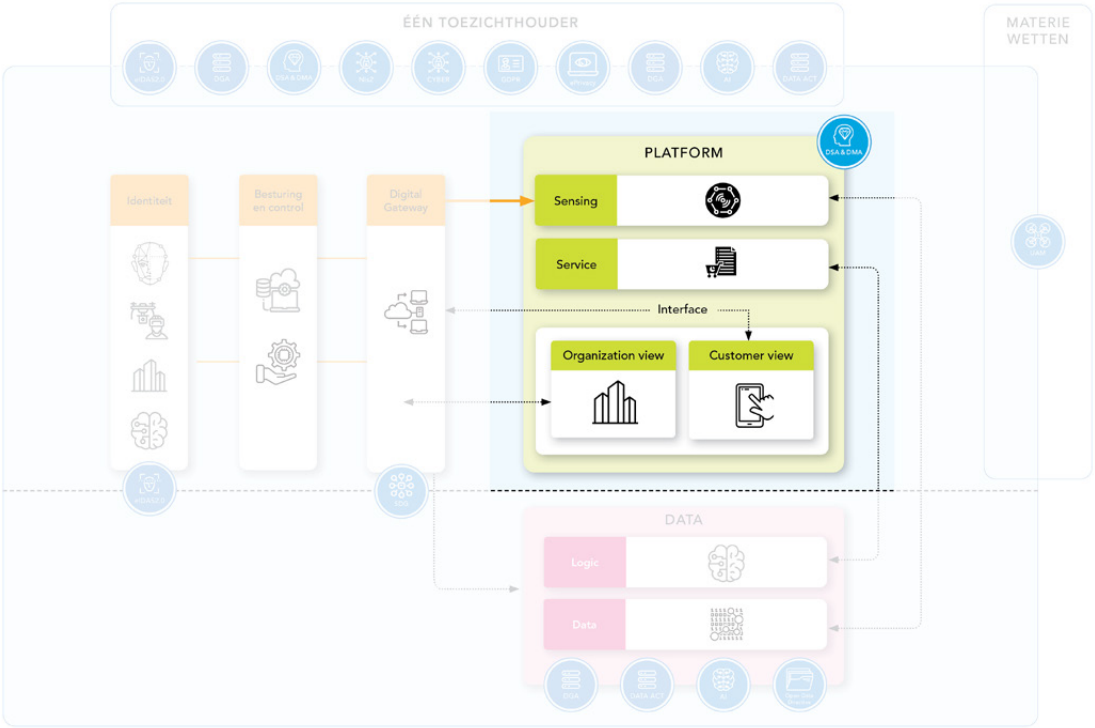
Experimenteerruimte
In experimenteerruimtes zoals *regulatory sandboxes*[26], digitale innovatiehubs (DIH) en test- en experimenteerfaciliteiten (TEF), kunnen bedrijven en andere (publieke) organisaties testen of hun AI-systemen – nog voordat ze in gebruik worden genomen – aan de geldende verplichtingen voldoen. Directe begeleiding door de toezichthoudende instelling zou daarbij het juridische risico tot een minimum beperken en de nalevingskosten voor deelnemende organisaties verlagen. De Commissie

23 Onder de term provider verstaat de Commissie in het voorstel iedere natuurlijke- of rechtspersoon, publieke autoriteit, agentschap of andere instelling die een AI-systeem ontwikkelt of laat ontwikkelingen met als doel om het op de markt te brengen of in gebruik te nemen
24 Systemen die biometrische data vastleggen en daarmee personen vergelijken met een dataset en identificeren zonder significante vertraging
25 De Commissie definieert biometrisch categoriseren als het toewijzen aan personen van een specifieke categorie, zoals geslacht, leeftijd, haar/oogkleur, tatoeages, etniciteit, seksuele of politieke oriëntatie, op basis van biometrische gegevens
26 Regulatory sandboxes zijn gecontroleerde omgevingen waar de ontwikkeling, het testen en het valideren van AI-systemen worden gefaciliteerd voordat deze op de markt worden gebracht of in gebruik worden genomen.

geeft aan dat dit bedrijven zal helpen hun producten en diensten sneller op de markt te brengen. Als gevolg hiervan zouden de regelgevingsvereisten geen belemmering moeten vormen voor het betreden van de markt.

2.4. Platform

De Europese Commissie wil een omgeving bevorderen waarin onlineplatforms gedijen, gebruikers eerlijk worden behandeld en actie wordt ondernomen om de verspreiding van illegale inhoud te beperken.



Onlineplatforms zijn volgens de EU sterke aanjagers van innovatie en spelen een belangrijke rol in de digitale samenleving en economie van Europa. Zij bestrijken een breed scala aan activiteiten, waaronder onlinemarktplaatsen, sociale media, creatieve inhoudsverkooppunten, app stores, prijsvergelijkingswebsites, platforms voor de deeleconomie en zoekmachines. Ze vergroten de keuze van de consument, verbeteren de efficiëntie en het concurrentievermogen van de industrie en kunnen de participatie van het maatschappelijk middenveld vergroten.

Onlineplatforms delen belangrijke kenmerken, zoals het gebruik van informatie- en communicatie-technologieën om interacties tussen gebruikers te vergemakkelijken, het verzamelen en gebruiken van gegevens over dergelijke interacties en netwerkeffecten. Deze netwerkeffecten maken het gebruik van de platforms met de meeste gebruikers het meest waardevol voor andere gebruikers.

Vandaag de dag verkopen al 1 miljoen EU-bedrijven goederen en diensten via onlineplatforms, en meer dan 50 % van de kleine en middelgrote ondernemingen die via onlinemarktplaatsen verkopen, verkoopt grensoverschrijdend.

De aanpak van de Europese Commissie ten aanzien van onlineplatforms is gericht op het bevorderen van een vertrouwensvolle, wettige en innovatiegedreven omgeving in de EU. Daartoe heeft de Europese Commissie leidende beleidsuitgangspunten opgesteld:

1. Het creëren en onderhouden van een gelijk speelveld voor vergelijkbare digitale diensten;
2. Zorgen voor verantwoordelijk gedrag van onlineplatforms om kernwaarden te beschermen;
3. Het bevorderen van vertrouwen en transparantie en het waarborgen van billijkheid op onlineplatforms;
4. Markten open en niet-discriminerend houden om een data-economie te bevorderen.

2.4.1. Verordening inzake digitale diensten (Digital Services Act)

Doel

Sinds de vaststelling van Richtlijn 2000/31/EG (de "richtlijn inzake elektronische handel") zijn er nieuwe en innovatieve (digitale) diensten van de informatiemaatschappij ontstaan, die het dagelijks leven van de Unieburgers veranderen en de manier waarop zij communiceren, verbinding maken, consumeren en zakendoen vormgeven en transformeren. Deze diensten leveren een grote bijdrage aan de maatschappelijke en economische veranderingen in de Unie en de rest van de wereld. Tegelijkertijd is het gebruik van die diensten ook de bron van nieuwe risico's en uitdagingen geworden, zowel voor de samenleving als geheel als voor de afzonderlijke personen die van deze diensten gebruik maken. Digitale diensten kunnen helpen om doelstellingen van duurzame ontwikkeling te bereiken door bij te dragen aan economische, sociale en milieuduurzaamheid. De COVID-19-crisis heeft aangetoond hoe belangrijk digitale technologieën zijn in alle aspecten van het moderne leven. De crisis heeft aangetoond dat onze economie en samenleving afhankelijk zijn van digitale diensten en heeft zowel de voordelen als de risico's van het huidige kader voor het functioneren van digitale diensten benadrukt.
In haar mededeling "De digitale toekomst van Europa vormgeven"[27] heeft de Commissie zich ertoe verbonden de horizontale regels die de verantwoordelijkheden en verplichtingen van de aanbieders van digitale diensten vastleggen, en met name die van onlineplatforms, te actualiseren.

In deze verordening worden geharmoniseerde regels vastgelegd over het aanbieden van tussenhandelsdiensten op de interne markt. In deze richtlijn is met name het volgende bepaald:
a) Een kader voor de voorwaardelijke vrijstelling van aansprakelijkheid van aanbieders van tussenhandelsdiensten optreden;
b) Regels over verplichtingen inzake gepaste zorgvuldigheid op maat van bepaalde specifieke categorieën van aanbieders van tussenhandelsdiensten;
c) Regels over de uitvoering en handhaving van deze verordening, ook met betrekking tot de samenwerking van en coördinatie tussen de bevoegde autoriteiten.

Deze verordening heeft de volgende doelstellingen:
a) Bijdragen tot de goede werking van de interne markt voor tussenhandelsdiensten;
b) Uniforme regels vaststellen voor een veilige, voorspelbare en betrouwbare onlineomgeving, waar de in het Handvest van de Grondrechten van de EU verankerde grondrechten doeltreffend worden beschermd.
Daartoe komt er een toezichtstructuur die effectief toezicht op de diensten van tussenpersonen moet waarborgen. Tegelijk met de DSA is de 'Digital Markets Act' (zie hieronder) gepubliceerd. Dat voorstel moet zorgen voor een goed functionerende Europese interne markt door concurrentie te stimuleren in digitale markten.

De wet onderscheidt vier categorieën partijen waarvoor verschillende regels gelden:[28]

1. Tussenhandelsdiensten die netwerkinfrastructuur aanbieden: internetproviders, domeinnaamregistrators, waaronder ook:
2. Hostingdiensten zoals cloud- en webhostingdiensten, waaronder ook:
3. Onlineplatforms waar verkopers en consumenten samenkomen, zoals onlinemarktplaatsen, appstores, deeleconomieplatforms en sociale media platforms

27 https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf
28 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_nl

4. Zeer grote onlineplatforms vormen een bijzonder risico wat betreft de verspreiding van illegale inhoud en het toebrengen van schade aan de maatschappij. Er zijn specifieke regels vastgesteld voor platforms die meer dan 10% van de Europeanen (dus 45 miljoen gebruikers) bereiken.

Status

De DSA is door de Raad van EU Ministers in november 2021 goedgekeurd, en door het Europees Parlement in januari 2022. In april 2022 zijn de onderhandelingen tussen deze partijen over de definitieve tekst afgerond. De eindtekst is nog niet gepubliceerd. Het EP keurde de finale tekst op 5 juli 2022 goed. Er volgt nog een laatste goedkeuring van de Raad. Naar verwachting wordt de wet in het derde kwartaal van 2022 van kracht, met een verschoningstijd tot 1 januari 2024 (of 15 maanden na de finale goedkeuring door de Raad, als dat later is).

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

Gemeenten vallen in de derde categorie van partijen die onderscheiden worden in de DSA (online platforms):

Dat kan op meerdere manieren[29]:

- de gemeente fungeert zelf als platform of maakt daar gebruik van. Rol van de gemeente: de gemeente als aanbieder van een platform.
- De gemeente maakt gebruik van platformtechnologieën bij de ontwikkeling van de stad naar een *smart city* door IoT en AI gebaseerde platforms in te zetten in de openbare ruimte. Rol van de gemeente: gebruiker van een platform van een private aanbieder.
- De gemeente wordt geconfronteerd met de met de effecten van private platforms (zoals Uber, AirBNB, Lime etc) op haar grondgebied. Rol van de gemeente: overheid die moet reageren op maatschappelijke ontwikkelingen.
- De gemeente oefent bestaande wettelijke taken uit t.a.v. een platform. Denk bijvoorbeeld aan het gebruiken van bevoegdheden op grond van de Wet personenvervoer richting Uber. (heeft mogelijk betrekking op gerelateerde wetgeving en niet de DSA. Dan kan het nog steeds relevant zijn als gerelateerde wetgeving die samenhangt met de DSA).

De gemeente als aanbieder van een platform.
In de eerste plaats kan een gemeente zelf als platform fungeren of platforms gebruiken. Daarbij maakt een gemeente gebruik van sociale media en cloud- en datagebaseerde systemen voor gedeelde dienstverlening[30]. Dit betekent dat de gemeente zich bij het uitvoeren van deze activiteiten zelf aan de regels van de DSA moet houden.

De gemeente als gebruiker van private platforms
In dat geval moeten private platforms (waaronder de zeer grote als Google en Facebook) zich aan de DSA houden.
Gemeenten gaan steeds meer samenwerkingsverbanden aan met private techpartners om hun smart city ambities te verwezenlijken. Voorbeelden[31]: een gemeente biedt voor haar medewerkers en inwoners een 'mobility as a service' platform aan, een andere gemeente heeft een digital twin van de haven op haar grondgebied laten ontwikkelen door een private partner.

Maatschappelijke effecten van de activiteiten van platforms.
In het position paper van de VNG worden een aantal problemen / uitdagingen geschetst die met het functioneren van platforms samenhangen. Platforms veroorzaken maatschappelijke effecten, denk aan overlast door verhuur van woningen aan toeristen, verandering van de taximarkt door Uber, distributielocaties op locaties waar ze overlast geven, etc. Een oproep van rivaliserende voetbal-supporters om elkaar op een bepaalde locatie te treffen noopt de overheid tot optreden. Zo zouden

29 Position Paper VNG Digital Service Act NL_541943486
30 Position Paper VNG Digital Service Act NL_541943486
31 Afkomstig uit Position Paper VNG Digital Service Act NL_541943486

er nog tal van andere effecten te benoemen zijn. Dat geldt natuurlijk niet alleen voor platforms, digitalisering verandert de manier waarop we leven ingrijpend op tal van terreinen[32].
De platforms veroorzaken deze problemen wel, maar zijn er niet aansprakelijk voor. Omdat platforms anders functioneren dan andere bedrijven waardoor bestaande handhavingsinstrumenten ontoereikend zijn. Hier kan van belang zijn dat de DSA de platforms verplichtingen oplegt (bijvoorbeeld transparantie verplichtingen) die een gemeente helpen bij het verminderen van ongewenste maatschappelijke effecten van de activiteiten van platforms.

Het uitoefenen van bestaande wettelijke bevoegdheden richting platforms.
De juridische status van platforms kan op twee manieren van belang zijn. Enerzijds is er discussie wat de juridische status van platforms is en welke regels voor een platform gelden. Dergelijke discussies maken het lastig en kostbaar om de naleving van regels af te dwingen[33]. Veel hangt er daarbij vanaf wat de transparantie verplichting precies inhoudt en hoe eenvoudig / bewerkelijk het is om de gegevens te verkrijgen en gebruiken.
Anderzijds kan Europese regelgeving, waaronder de DSA en/ of de gerelateerde e-commerce richtlijn een platform juist een bepaalde juridische status geven waar een gemeente rekening mee moet houden. Een voorbeeld is dat een platform onder de Richtlijn inzake elektronische handel (verder te noemen de e commerce richtlijn) soms kan worden gekwalificeerd als een 'dienst van de informatiemaatschappij'.[34] Dat betekent dat ze vallen onder de regels van de e commerce richtlijn. Wanneer een gemeente bijvoorbeeld haar bevoegdheden op grond van de Wet personenvervoer wil uitoefenen om Uber te reguleren dient ze hiermee rekening te houden.

2.4.2. Verordening inzake Digitale Markten (Digital Markets Act)

Doel

De DMA moet zorgen voor een goed functionerende Europese interne markt door concurrentie te stimuleren op digitale markten en moet ertoe leiden dat poortwachtersplatforms zich eerlijk gedragen tegenover ondernemers die hun producten of diensten via een platform aanbieden.
De DMA is een belangrijk onderdeel van een pakket (nieuwe) Europese regelgeving gericht op het goed functioneren van de digitale economie en is samen met de Wet inzake digitale diensten ('Digital Services Act') gepubliceerd.

De DMA benoemt een set nauw gedefinieerde objectieve criteria om een groot online platform als een zogenaamde 'poortwachter' te kwalificeren. Alleen poortwachters zullen moeten voldoen aan de do's en don'ts die de DMA specificeert[35].

- onlinetussenhandelsdiensten(onder meer marktplaatsen, appstores en onlinetussen-handelsdiensten in andere sectoren zoals mobiliteit, vervoer of energie),
- onlinezoekmachines,
- sociale netwerken,
- videoplatformdiensten,
- nummeronafhankelijke interpersoonlijke communicatiediensten,
- besturingssystemen,
- clouddiensten
- advertentiediensten, waaronder advertentienetwerken, advertentie-uitwisselingsdiensten en andere advertentietussenhandelsdiensten, indien deze advertentiedienstenverband houden met een of meer van de andere bovenvermelde kernplatformdiensten[36].

32 "Digitale en fysieke wereld komen samen in gemeenten" - Digitale Overheid, interview met Nathan Ducastel
33 Position Paper VNG Digital Service Act NL_541943486, deze stellingen worden niet nader uitgewerkt.
34 https://europadecentraal.nl/onderwerp/digitale-overheid/digitale-samenleving/e-commerce/#:~:text=In%20december%202020%20werd%20de%20Digital%20Services%20Act,elektronische%20handel%20te%20actualiseren%20en%20deze%20te%20vervangen.
35 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN
36 Ontleend aan: Motivering en doel van het wetsvoorstel.

Status

De DMA is in november in de Raad van de EU goedgekeurd en eveneens door het Europees Parlement (EP). In de eerste helft van 2022 werd nog onderhandeld tussen Raad, EP en EC over de eindtekst. Politieke overeenstemming daarover werd bereikt in maart 2022. De eindtekst (PDF) is in mei 2022 gepubliceerd, en op 5 juli 2022 aanvaard door het EP. Er volgt nog een laatste akkoord van de Raad, waarna deze officieel wordt gepubliceerd. De DMA zal dus in 2022 gereed zijn en zal na een verschoningstijd van 6 maanden per het tweede kwartaal 2023 uiterlijk van kracht zijn.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

Deze wet raakt gemeenten niet direct.

2.4.3. Urban air mobility

Doel[37]

Het betreft de volgende verordeningen:

- GEDELEGEERDE VERORDENING (EU) 2019/945[38]VAN DE COMMISSIE van 12 maart 2019 inzake onbemande luchtvaartuigsystemen en uit derde landen afkomstige exploitanten van onbemande luchtvaartuigsystemen

- UITVOERINGSVERORDENING (EU) 2019/947[39] VAN DE COMMISSIE van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen. Deze verordening is in Nederland geïmplementeerd via de Regeling onbemande luchtvoertuigen.

- UITVOERINGSVERORDENING (EU) 2021/664[40] VAN DE COMMISSIE van 22 april 2021 inzake een regelgevingskader voor U-space.

- UITVOERINGSVERORDENING (EU) 2021/665[41] VAN DE COMMISSIE van 22 april 2021 tot wijziging van Uitvoeringsverordening (EU) 2017/373 wat betreft de eisen voor verleners van luchtverkeers-beheers-/luchtvaartnavigatiediensten en andere netwerkfuncties voor luchtverkeersbeheer in het U-spaceluchtruim dat is aangewezen in het gecontroleerde luchtruim.

- UITVOERINGSVERORDENING (EU) 2021/666[42] VAN DE COMMISSIE van 22 april 2021 tot wijziging van Verordening (EU) nr. 923/2012 wat betreft eisen voor bemande luchtvaart in U-spaceluchtruim

De eerste twee verordeningen zorgen voor een veilige uitvoering van de gewenste operatie. 947 richt zich op deze veilige operatie. 945 richt zich specifiek op de technische eisen aan drones die operaties met een laag risico uitvoeren (open categorie en deels specifieke categorie). Op basis van de operationele regels (open) of afgegeven vergunning (specifiek) mag de operator de gewenste operatie uitvoeren.

De andere 3 verordeningen voorzien in een verkeersleidingssysteem voor drones in een deel van het luchtruim waar deze extra begeleiding noodzakelijk is voor een veilige operatie. Dit kan bijvoorbeeld komen doordat er veel drones tegelijk vliegen of om reden van privacy, omgevingshinder of security.

De bestaande Air Traffic Managementsystemen (ATM's) voor bemande luchtvaartuigen zijn gebaseerd op menselijke communicatie. Voor onbemande luchtvaartuigen die geen piloot aan

37 Bron: Aanzet voor een visie op U-space. Rapport Deloitte in opdracht van het Ministerie van Infrastructuur en Waterstaat. Juli 2021
38 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R0945
39 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R0947&from=SK
40 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32021R0664
41 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0665
42 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32021R0666

boord hebben (Unmanned Aircraft Systems of UAS) zijn systemen op basis van geautomatiseerde communicatie (UAS Traffic Management systemen (UTM) nodig.

De laatste drie verordeningen samen geven invulling aan het Europese concept van een U-space waarin veilig vliegverkeer gewaarborgd is. U-space is de Europese versie van UTM. Landen zijn verantwoordelijk voor het aanwijzen van U-space luchtruim. De criteria voor deze aanwijzing staan in de vorige twee paragrafen. Daarnaast moeten landen ook zorgen dat de Common Information Service voor dit luchtruim aanwezig is. Dienstverleners van de verplichte diensten die gecertificeerd zijn voor het leveren van deze diensten (op nationaal of EU-niveau) mogen in dit luchtruim de diensten leveren aan operators die deze diensten van de dienstverlener willen afnemen (markt-werking voor de dienstverleners).

Status

De uitvoeringsverordening inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen is van toepassing met ingang van 1 juli 2020. Deze verordening is in Nederland geïmplementeerd via de Regeling onbemande luchtvaartuigen. Deze regeling is 31 december 2020 in werking getreden.

De drie andere uitvoeringsregelingen zijn in werking getreden in mei 2021. Zij zijn van toepassing met ingang van 26 januari 2023. Op dat moment kan de Nederlandse overheid U-space luchtruim aanwijzen waarbinnen een aantal verplichte diensten geleverd moeten worden: een geobewust-zijnsdienst, verkeersinformatiedienst, Unmanned Aircraft System (UAS)-vluchtvergunningsdienst, netwerkidentificatiedienst en Common Information Service (CIS).

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

De gemeente wordt geraakt in meerdere rollen: als gebruiker van drones, mogelijk kan de gemeente een rol hebben bij de aanwijzing van U-space luchtruim en als overheid die geconfronteerd wordt met de maatschappelijke gevolgen van het toegenomen aantal drones.

Het ministerie van Infrastructuur en Milieu verwachtte in 2017 dat het gebruik en de toepassings-mogelijkheden van drones in Europa en in Nederland snel zal toenemen[43]. Dat betekent dat er meer drones in het luchtruim boven gemeenten gaan vliegen. In één van de verordeningen[44] wordt genoemd dat daardoor risico's ontstaan voor veiligheid, beveiliging, privacy en milieu. De verordeningen bevatten maatregelen om de veiligheidsrisico's voor het vliegverkeer te beperken, maar niet om de andere (maatschappelijke) risico's te beheersen. Die risico's doen zich in het gemeentelijk domein voor en bij een groei van het aantal drones zal de gemeente daar in toenemende mate mee gecon-fronteerd worden.

De EU regelgeving raakt de gemeenten ook in hun rol van eigenaar van drones en opdrachtgever voor vluchten met drones. Dat komt bijvoorbeeld steeds vaker voor in verband met de bijhouding van basisregistraties zoals de BAG en de BGT. Camerabeelden die met behulp van drones worden gemaakt worden onder meer gebruikt om mutaties te signaleren. Wanneer de gemeente opdrachtgever is heeft ze indirect met de EU regelgeving te maken: in dat geval zullen de bedrijven die ingehuurd worden door de gemeente onder de EU regelgeving vallen en zich aan de veiligheidsvoorschriften moeten houden.

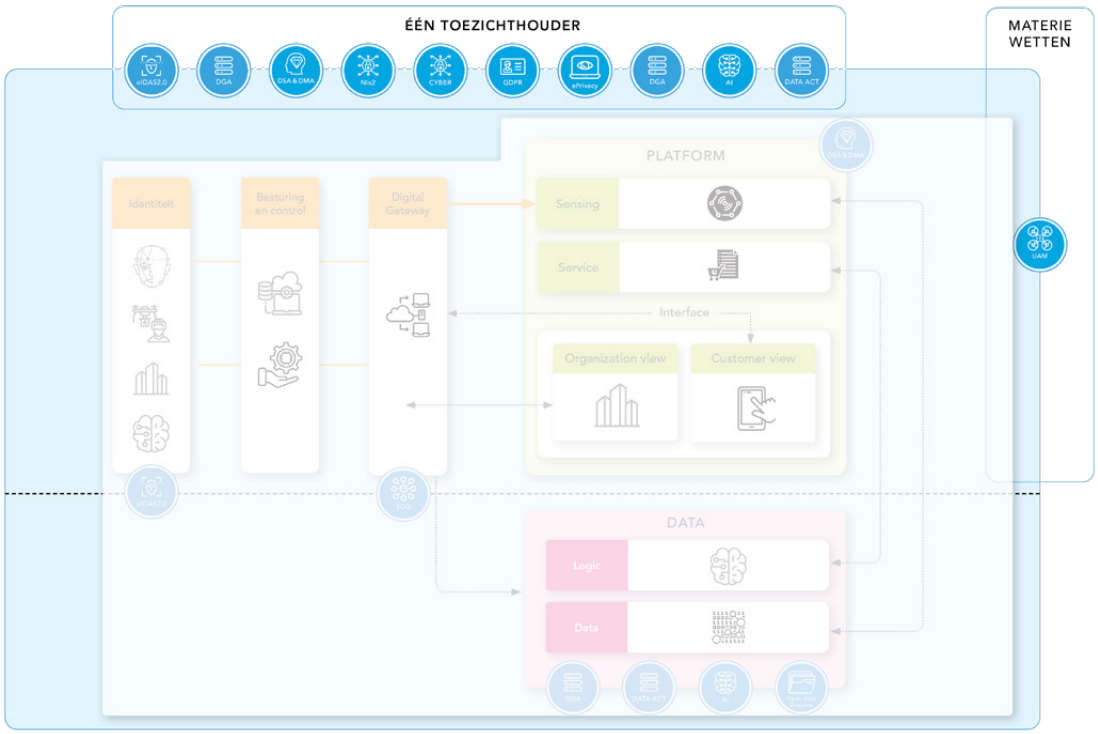
43 Kansen voor drones – Visie op de inzet van drones, Ministerie van Infrastructuur en Milieu, 2017
44 De uitvoeringsverordening inzake een regelgevingskader voor U-space

2.5. Privacy en Security

De EU-strategie voor cyberbeveiliging heeft tot doel weerbaarheid tegen cyberdreigingen op te bouwen en ervoor te zorgen dat burgers en bedrijven profiteren van betrouwbare digitale technologieën.
De regulering zal betrekking hebben op drie actiegebieden van de EU:[45]

1. veerkracht, technologische soevereiniteit en leiderschap;
2. operationele capaciteit om te voorkomen, af te schrikken en te reageren;
3. samenwerking om een mondiale en open cyberspace te bevorderen.

In het kader van privacy bepaalt het Handvest van de grondrechten van de EU dat EU-burgers recht hebben op bescherming van hun persoonsgegevens. De AVG[46] (ook bekend onder de Engelse afkorting GDPR) versterkt de grondrechten van de burgers in het digitale tijdperk en bevordert het handelsverkeer door de regels voor bedrijven in de digitale eengemaakte markt te verduidelijken. Dit gemeenschappelijke stel regels heeft een einde gemaakt aan de versnippering die het gevolg was van uiteenlopende nationale systemen, en voorkomt administratieve rompslomp. De verordening is op 24 mei 2016 in werking getreden en is sinds 25 mei 2018 van toepassing.



2.5.1. Cyberbeveiligingsverordening

Doel

Dit wetsvoorstel strekt tot uitvoering van Verordening (EU) nr. 2019/881 van het Europees Parlement en de Raad van 17 april 2019. De cyberbeveiligingsverordening versterkt het mandaat van Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging) en introduceert een Europees kader op het gebied van cyberbeveiligingscertificering. Het doel van de verordening is om door middel van een geharmoniseerde certificatiesystematiek de cyberbeveiliging in de Europese Unie te vergroten

45 https://digital-strategy.ec.europa.eu/nl/node/9690
46 Omdat de AVG al in werking is wordt deze niet meer apart beschreven in dit hoofdstuk. Deze wet is overkoepelend geldig voor alle andere wetten waar persoonsgegevens onderwerp van regulering zijn.

en de (digitale) interne markt te versterken. Deze verordening biedt een kader om op Europees niveau regelingen op het gebied van cyberveiligheidscertificering te ontwikkelen en uit te voeren.

Met de inwerkingtreding van de cyberbeveiligingsverordening wordt certificering van cyberbeveiliging in het publieke domein gebracht. Het betreft een nieuw beleidsterrein, waarvoor nog geen nationale wet- en regelgeving is. Er is daarom gekozen voor de uitvoering van de cyberbeveiligingsverordening vorm te geven in een nieuwe nationale wet: de Uitvoeringswet cyberbeveiligingsverordening.

Het doel van de verordening is:

- Het versterken van de interne marktwerking voor ICT-producten, diensten en -processen te ondersteunen door middel van een geharmoniseerde systematiek voor cyberbeveiligingscertificering.
- Verhogen van de digitale weerbaarheid binnen de EE. De verwachting is dat door een toegenomen vraag naar een hoger cyberbeveiligingsniveau van ICT-producten, -diensten en -processen meer en meer aanbieders voor certificeringen zullen kiezen.
- Verhogen van het vertrouwen in de beveiliging van ICT-producten, -diensten en -processen middels verstrekking van EU cyberbeveiligingscertificaten.

Status

De verordening is op 27 juni 2019 in werking getreden
De Uitvoeringswet cyberbeveiligingsverordening is op 9 april 2022 in werking getreden.[47]

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

De cyberbeveiligingsverordening maakt het mogelijk om cyberbeveiligingscertificeringsregelingen te ontwerpen voor alle ICT-producten, -diensten en -processen. De verordening heeft betrekking op alle aanbieders van ICT-producten, -diensten en -processen met commerciële activiteiten op het grondgebied van de Europese Unie, nu en in de toekomst. Gemeenten zullen in de toekomst bij aanschaf van ICT-producten, -diensten en -processen moeten verifiëren of aanbieders voldoen en blijven voldoen.

2.5.2. Network and Information Systems (NIS) directive 2

Doel

De oorspronkelijke NIS- directive regelt de beveiliging van netwerk- en informatiesystemen van aanbieders van essentiële diensten (AED's) en van digitale dienstverleners (DSP's), onder meer door hen te laten voldoen aan een zorg- en meldplicht. Deze AED's dienen door de lidstaten zelf te worden aangewezen. Met de Wet beveiliging netwerk- en informatiesystemen (Wbni) wettelijke verplichtingen (Wbni) heeft Nederland de NIS-richtlijn geïmplementeerd. De Commissie constateert dat sinds het vaststellen van de NIS-richtlijn in 2016 de digitalisering van de eengemaakte markt is toegenomen en dat het dreigingsbeeld zich verder heeft ontwikkeld. Beide ontwikkelingen zijn verder versterkt door de COVID-19 crisis. Daarnaast is er in opdracht van de Commissie een evaluatie van de NIS-richtlijn uitgevoerd, die een aantal knelpunten in het functioneren van de richtlijn identificeert. Op basis van deze ontwikkelingen en de uitkomsten van deze evaluatie heeft de Commissie besloten om een voorstel te doen om de huidige richtlijn te vervangen, voortbouwend op de huidige richtlijn, de NIS directive 2.
In deze richtlijn worden maatregelen vastgesteld om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie te waarborgen.

47 https://vng.nl/wetsvoorstellen/uitvoeringswet-cyberbeveiligingsverordening

Met het oog hierop worden in deze richtlijn:
(a) verplichtingen voor de lidstaten vastgesteld om nationale strategieën voor cyberbeveiliging vast te stellen en om bevoegde nationale autoriteiten, centrale contactpunten en computer security incident response teams (CSIRT's) aan te wijzen;
b) verplichtingen vastgesteld inzake risicobeheer en rapportage op het gebied van cyberbeveiliging voor entiteiten van een type dat wordt aangeduid als essentiële entiteiten en als belangrijke entiteiten;
(c) verplichtingen vastgesteld met betrekking tot het delen van informatie op het gebied van cyberbeveiliging.

Het nieuwe voorstel regelt via centrale aanwijzing welke entiteiten binnen de reikwijdte van de richtlijn vallen. Naast de sectoren die al onder de huidige richtlijn vallen, worden nieuwe sectoren in het toepassingsgebied opgenomen, waaronder telecommunicatie, chemicaliën, levensmiddelen, post- en koeriersdiensten, bepaalde industrieën, overheidsdiensten, platforms voor sociale netwerken, ruimtevaart, afvalbeheer en afvalwaterbeheer. Verder zullen entiteiten van het openbaar bestuur van centrale overheden onder NIS2-richtlijn vallen, en kunnen lidstaten besluiten om het toepassingsgebied uit te breiden tot soortgelijke entiteiten op regionaal en lokaal niveau.

Status

De NIS directive 2[48] is voorgesteld in december 2020. Na de goedkeuring van het voorlopige akkoord door het Europees Parlement zal de nieuwe NIS2-richtlijn naar verwachting dit najaar worden gepubliceerd, waarna deze vanaf medio 2024 in nationale wetgeving kan worden omgezet.[49]

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?

Voor gemeenten die als AED worden aangemerkt:
- Gelden verplichtingen inzake risicobeheer, maatregelen en rapportage op het gebied van cyberbeveiliging
- Gelden Europese cyberbeveiligingscertificeringsregelingen (zie ook Uitvoeringswet cyberbeveiligingsverordening)
- Moeten zich aanmelden bij het Europees register
- Moeten onderling relevante informatie over cyberbeveiliging uitwisselen om incidenten te voorkomen, te bestrijden of te beperken en daarmee de cyberbeveiliging te verhogen.

Voor het beheersorgaan van de gemeente geldt dat:
- Goedkeuring moet worden gegeven op de maatregelen
- Toezicht moet worden gehouden op uitvoering van genomen maatregelen en verantwoordelijk zijn voor de niet-naleving door de entiteiten van de verplichtingen.
- Specifieke opleidingen moet worden gevolgd om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.

2.5.3. ePrivacy verordening

Doel

Bij deze verordening worden regels vastgesteld betreffende de bescherming van de fundamentele rechten en vrijheden van rechtspersonen bij het aanbieden en gebruiken van de elektronische-communicatiediensten, en met name hun recht op eerbiediging van communicatie. De ePrivacy Verordening is een aanvulling op de Algemene verordening gegevensbescherming (AVG).
Deze verordening is van toepassing op:
- de verwerking van elektronische-communicatie inhoud en van elektronische-communicatiemeta-gegevens in verband met het aanbieden en gebruiken van elektronische-communicatiediensten;

48 https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf
49 https://www.government.nl/latest/news/2022/06/23/cybersecurity-measures-in-more-sectors-will-improve-digital-security-in-the-netherlands-and-

- informatie over apparatuur van eindgebruikers;
- het aanbieden van een openbaar toegankelijke gids van eindgebruikers van elektronische apparatuur voor communicatiediensten;
- het verzenden van direct marketingcommunicatie naar eindgebruikers.

De belangrijkste punten in de conceptverordening zijn:
- Elektronische-communicatiegegevens zijn vertrouwelijk. Elke interferentie met elektronische-communicatiegegevens, met inbegrip van het afluisteren, aftappen, opslaan, monitoren, scannen of andere vormen van onderschepping, bewaking en verwerking van elektronische-communicatie-gegevens, door iemand anders dan de betrokken eindgebruikers, is verboden, behalve wanneer dit op grond van deze verordening is toegestaan. Het gaat niet alleen om email en sms, maar alle vormen van elektronische communicatie, ook het internet der dingen, internet-telefonie (zoals Skype), wifi tracking services (als beweging van personen, hotspots) en de diensten van internetproviders
- Het gebruik van cookies en metadata is toegestaan, indien de doeleinden verenigbaar zijn met het oorspronkelijke doel
- De aanbieder van de elektronische-communicatiedienst wist de inhoud van de elektronische communicatie of maakt deze gegevens anoniem wanneer dit niet langer nodig is voor de verwerking
- Het gebruik van verwerkings- en opslagcapaciteit van eindapparatuur en het verzamelen van informatie uit de eindapparatuur van eindgebruikers, met inbegrip van de software en hardware ervan, anders dan door de betrokken eindgebruiker, is verboden, behalve wanneer dit op grond van deze verordening is toegestaan
- Het voorstel bevat ook regels over lijnidentificatie, openbare telefoongidsen, of meer algemeen een openbare toegankelijke gids van eindgebruikers van elektronische apparatuur voor communicatiediensten. Onder openbaar beschikbare telefoongidsen wordt verstaan elke telefoon-gids of dienst die informatie bevat over eindgebruikers van op nummers gebaseerde interpersoon-lijke communicatiediensten, zoals naam, telefoonnummers (met inbegrip van mobiele telefoon-nummers), e-mailadres, thuisadres, waarvan de belangrijkste functie erin bestaat dergelijke eind-gebruikers te kunnen identificeren.
- Tot slot bevat het regels over ongevraagde en direct marketing.

Status

De ePrivacy verordening zal de ePrivacy Richtlijn vervangen. De ePrivacy Richtlijn is in Nederland omgezet in de Telecommunicatiewet. Het Europese wetsproces van de verordening is in 2017 van start gegaan en nog steeds in gang.[50] Lidstaten konden het niet eens worden over cruciale punten in de regelgeving, waaronder de bepalingen omtrent cookies. Op 10 februari 2021 heeft de Raad haar standpunt over de ePrivacy-conceptverordening bepaald.

Nu de Raad een gezamenlijk standpunt heeft bereikt, is in mei 2021 de zogeheten 'triloog' begonnen. Hierbij onderhandelt een vertegenwoordiging van de Raad met een vertegenwoordiger van het Parlement en de Commissie over de definitieve tekst van de verordening. Zoals bij Europese wetgeving gebruikelijk is, krijgen de lidstaten daarna nog een bepaalde periode de tijd voor de nieuwe regels van toepassing worden. In het huidige voorstel is dat een periode van 2 jaar.

Waar gaat de wet in hoofdlijnen over in de gemeentelijke context?[51]

Het startpunt is de AVG, maar in de specifieke gevallen waarin een organisatie te maken heeft met elektronische communicatiegegevens zal de ePrivacy verordening leidend zijn.

Gemeenten als aanbieders van openbare elektronische communicatiediensten komen in aanraking met de verordening als:

50 https://europadecentraal.nl/onderwerp/digitale-overheid/privacy/eprivacy-verordening/
51 https://europadecentraal.nl/onderwerp/digitale-overheid/privacy/eprivacy-verordening/

- Ze cookiegegevens ophalen van bezoekers op hun websites of via sociale mediakanalen, zij zullen het cookiebeleid moeten aanpassen aan de eisen in de verordening (specifieke en geïnformeerde toestemming verwerken door middel van transparante en gebruiksvriendelijke instellingen);
- Het gebruik en verzamelen van (metadata) van elektronische-communicatiegegevens moet voldoen aan de privacy en beveiligingseisen uit de verordening en gemeenten moeten deze gegevens wissen indien ze niet meer nodig zijn in de verwerking. Dit geldt bijvoorbeeld voor hotspots (wifi-tracking) in openbare ruimte en ook voor sensoren (internet of things)

3. Impact op hoofdlijnen

Zoals in hoofdstuk 1 is aangegeven beperkt deze impactanalyse zich tot de impact op hoofdlijnen van Europese digitale wetgeving op gemeenten. Daar komt bij dat de in hoofdstuk 2 beschreven wetten vaak nog in een fase zijn van voorstel wetgeving en/of op onderdelen nog ruimte bieden voor interpretatie en/of de Europese Commissie en Nederland nog inrichtingskeuzes moeten maken, waardoor deze impactbepaling een verkennend karakter heeft.

In dit hoofdstuk verkennen we daarom wat de Europese digitale wetgeving op hoofdlijnen betekent voor gemeenten. Dit doen we langs verschillende aspecten van de uitvoering bij gemeenten:

- Security (beveiliging/ privacy)
- Communicatie (met burgers/ bedrijven/ dienstverlening)
- Organisatie (besturing en control)
- Personeel (personeelsbestand)
- Administratieve organisatie (processen)
- Financiën (geldstromen)[52]
- Informatievoorziening (informatie en technologie)
- Juridisch (wet- en regelgeving/ juridische voorwaarden/ overeenkomsten)
- Technologie (zie: informatievoorziening)

In de volgende paragrafen wordt per aspect verkennend de impact op hoofdlijnen beschreven. Niet alle wetten worden specifiek genoemd dit komt omdat de wet nog niet voldoende is uitgewerkt waardoor een impactbeschrijving nog niet mogelijk is of voor een wet is ingeschat dat een specifiek aspect niet tot noemenswaardige impact leidt.

Deze wijze van beschrijving geeft een tweede manier van samenhang, namelijk een ordening van Europese digitale wetten langs bedrijfsvoeringscomponenten. Op deze manier is het mogelijk om vanuit 1 aspect inzicht te krijgen wat op hoofdlijnen de impact is.

3.1. Security (beveiliging/ privacy)

In het algemeen geldt dat alle wetten die gaan over persoonsgegevens moeten voldoen aan de AVG en dat de Baseline Informatiebeveiliging Overheid (BIO) wordt toegepast om informatiebeveiligings-risico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. Gemeenten verantwoorden zich over informatiebeveiliging en kwaliteit middels ENSIA.[53] Dat staat voor Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen

ePrivacy verordening: Gemeenten moeten inspanning leveren om te zorgen dat het gebruik en verzamelen van (metadata) van elektronische-communicatiegegevens door hen voldoet aan de privacy en beveiligingseisen uit de verordening. Dit geldt bijvoorbeeld voor hotspots (wifitracking) in openbare ruimte en ook voor sensoren (internet of things).

DGA: Gemeenten moeten technische randvoorwaarden inrichten die privacyvriendelijke analyses van databanken met persoonsgegevens mogelijk maken, zoals anonimisering, pseudonimisering, generalisering, onderdrukking en randomisering. De toepassing van deze privacybevorderende technologieën, in combinatie met een omvattende aanpak op het gebied van gegevensbescherming, moet het veilige hergebruik van persoonsgegevens en commercieel vertrouwelijke bedrijfsgegevens

52 Deze analyse heeft niet tot doel om de impact te becijferen. Daarom wordt dit aspect hier niet apart beschreven. De andere aspecten beschrijven een mate van inspanning, wat kwalitatief een inzicht geeft in het financiële aspect.
53 https://vng.nl/projecten/ensia

voor onderzoeks-, innovatie- en statistische doeleinden waarborgen. In veel gevallen betekent dit dat gegevens alleen mogen worden gebruikt en hergebruikt binnen een beveiligde verwerkingsomgeving die is gecreëerd door en onder toezicht staat van een gemeenten.
Bovendien moet een gemeente als data altruïsme organisatie voldoen aan een zogenoemde rulebook (uiterlijk 18 maanden na de inwerkingtreding ervan), waarin informatievereisten, technische en beveiligingsvereisten, communicatiestappenplannen en aanbevelingen inzake interoperabiliteitsnormen zullen worden vastgelegd. Het rulebook zal worden ontwikkeld door de Commissie, in nauwe samenwerking met organisaties voor gegevensaltruïsme en andere relevante belanghebbenden.

DA: Gemeenten moeten bij verzoek om data op grond van uitzonderlijke noodzaak zorgen dat ze:
- de data die ze hiervoor gebruiken verenigbaar is met het doel waarvoor zij zijn gevraagd;
- technische en organisatorische maatregelen treffen, voor zover de verwerking van persoonsgegevens noodzakelijk is, die de rechten en vrijheden van de betrokkenen waarborgen;
- de data vernietigen zodra zij niet langer nodig zijn voor het aangegeven doel en de datahouder daarvoor in kennis stellen dat de data zijn vernietigd.

Open data richtlijn: Privacy als leidraad te nemen voor het verzamelen van data ('privacy by design ', zodat het achteraf anonimiseren van data niet nodig is.

Europese digitale identiteit verordening: Gemeenten moeten om veilig en betrouwbaar te identificeren en authentiseren zorgen dat het inloggen op digitale diensten op het juiste betrouwbaarheidsniveau wordt beveiligd. Een grote inspanning wordt verwacht omdat voor alle digitale diensten deze inschaling moet worden gemaakt en worden beheerd.

NIS2: Elke lidstaat moet een nationale cyberbeveiligingsstrategie vaststellen waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden gedefinieerd om een hoog niveau van cyberbeveiliging te bereiken en te handhaven:

Voor gemeenten die als AED zijn aangemerkt geldt dat ze inspanningen moeten leveren om te voldoen aan (hieronder nader uitgewerkt):
- Maatregelen voor het beheer van cyberbeveiligingsrisico's
- Rapportageverplichtingen
- Certificeringsverplichtingen
- Regelingen voor informatie-uitwisseling op het gebied van cyberbeveiliging

De mate van impact is afhankelijk van in hoeverre gemeenten als AED organisaties worden aangemerkt en op welke wijze het nu algemeen informatieveiligheidsbeleid plaats moet krijgen in toekomstige wetgeving. Dit geldt onder andere voor de Baseline Informatie Overheid (BIO) die mogelijk van een wettelijke grondslag worden voorzien.[54]

Maatregelen voor het beheer van cyberbeveiligingsrisico's
De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten bij het verlenen van hun diensten gebruiken, te beheren. Rekening houdend met de stand van de techniek zorgen deze maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op het aanwezige risico. De bedoelde maatregelen omvatten ten minste het volgende:

a) risicoanalyse en beleid inzake de beveiliging van informatiesystemen;
b) incidentenbehandeling (preventie en opsporing van en respons op incidenten);
c) bedrijfscontinuïteit en crisisbeheer;
d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar leveranciers of dienstverleners, zoals leveranciers van diensten op het gebied van gegevensopslag en -verwerking of beheerde beveiligingsdiensten;

54 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/wet-en-regelgeving/

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f) beleid en procedures (testen en audits) om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g) het gebruik van cryptografie en encryptie.

Rapportageverplichtingen
De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten de bevoegde autoriteiten of het CSIRT onverwijld in kennis stellen van elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten. In voorkomend geval stellen deze entiteiten de ontvangers van hun diensten onverwijld in kennis van incidenten die een nadelige invloed kunnen hebben op de verlening van die dienst. De lidstaten zorgen ervoor dat deze entiteiten onder meer alle informatie rapporteren die de bevoegde autoriteiten of het CSIRT in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen.

Mogelijke certificeringsverplichtingen
Lidstaten kunnen eisen dat essentiële en belangrijke entiteiten bepaalde ICT-producten, ICT- diensten en ICT-processen certificeren in het kader van specifieke Europese cyberbeveiligingscertificerings-regelingen.
Regelingen voor informatie-uitwisseling op het gebied van cyberbeveiliging
Gaat om relevante informatie over cyberbeveiliging uitwisselen met inbegrip van informatie over cyberbedreigingen, kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen

NIS2: Om de convergente uitvoering van het voorstel te bevorderen, moedigen de lidstaten, zonder het gebruik van een bepaald type technologie op te leggen of te bevoordelen, het gebruik aan van Europese of internationaal aanvaarde normen en specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen.
Het Enisa stelt in samenwerking met de lidstaten adviezen en richtsnoeren op over de technische gebieden die in aanmerking moeten worden genomen, alsmede over de reeds bestaande normen, met inbegrip van de nationale normen van de lidstaten, die het mogelijk maken deze gebieden te bestrijken.

3.2. Communicatie (met burgers/ bedrijven/ dienstverlening)

DGA: Om potentiële hergebruikers te helpen relevante informatie te vinden over welke gegevens door welke overheidsinstanties worden bewaard, moeten de lidstaten één informatiepunt (logisch lijkt dat dit data.overheid.nl is) oprichten. Gemeenten moeten hierop aansluiten. De Commissie zal een Europees centraal toegangspunt opzetten (met een doorzoekbaar register van de door de nationale centrale informatiepunten samengestelde informatie) om het hergebruik van gegevens op de interne markt en daarbuiten verder te vergemakkelijken.

DGA: De gemeente als erkende datadeeldienst kan het label voeren "in de Unie erkende aanbieder van gegevensbemiddelingsdiensten" in haar schriftelijke en gesproken communicatie, evenals het gemeenschappelijke logo. Dit geldt ook voor de gemeente als data-altruisme-organisatie. Gemeenten kunnnen het voor dit doel ontworpen gemeenschappelijke logo gebruiken en kunnen ervoor kiezen om te worden opgenomen in het openbare register van data-altruïsme-organisaties. De Commissie zal ter informatie een register op EU-niveau van erkende datadeeldienten en gegevens-/altruïsmeorganisaties opzetten.

Open data richtlijn: Open data via data.overheid.nl (het uploaden op data.overheid.nl is niet verplicht maar facultatief)

54 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/wet-en-regelgeving/

SDG:[55] In de communicatie met burgers en bedrijven willen gemeenten voldoen aan het onderliggende doel van de verordening namelijk gelijkschakeling van dienstverlening voor Europeanen en dat hoeft niet per se door het inzetten van een digitaal kanaal. Vanuit ervaringen met de doelgroepen expats en ondernemers hebben gemeenten afgeleid dat persoonlijk contact het meest gewaardeerd wordt en bovendien effectiever is. Hierdoor is het digitale kanaal ook voor Nederlandse klanten niet altijd volledig ontwikkeld. Door in te zetten op accountmanagement en zoekende Europeanen toe te leiden naar een loket dat in samenhang antwoord kan geven, wordt het onderliggende doel van de verordening (gelijkschakeling van dienstverlening) bereikt. Gemeenten zien daarom een interpretatie van de verordening die meer aansluit bij de dienstverleningspraktijk als zeer wenselijk om op een juiste en (kosten-) verantwoorde manier aan de slag te gaan met de aansluiting op de Single Digital Gateway.

Europese Digitale Identiteit verordening: Zoveel mogelijk burgers en ondernemers moeten gebruik kunnen maken van wallets op een gebruiksvriendelijke en toegankelijke manier. Ook mensen met een beperking of die digitaal minder vaardig zijn, moeten mee kunnen doen als ze dat willen. Gemeenten moeten binnen de kaders (veillig en betrouwbaar identificeren) voor al hun digitale processen in interactie met burgers en ondernemers steeds de afweging maken tussen veilig en betrouwbaar enerzijds en gebruiksvriendelijke en toegankelijk anderzijds. We hebben als VNG bij de SDG impactanalyse is geconstateerd (zie hierboven) dat er naar proportionaliteit en haalbaarheid in de interpretatieruimte gezocht moet worden. Datzelfde zou kunnen gelden voor de Digitale identiteit, de nuance die hierin zit zal in verder uitwerking van de Europese digitale verordening in Nederland en een daarop volgende verdiepende impactanalyse duidelijk moeten worden.

AI-act: Publieke waarden moeten voorop staan bij de ontwikkeling en inzet van AI, en deze moeten gediend worden door de AI-verordening. Hierbij is de innovatie geen doel op zich; het mag nooit belangrijker zijn dan waarden en mensenrechten en de fundamentele constitutionele beginselen van de rechtsstaat moeten gewaarborgd blijven. Deze afweging moeten gemeenten steeds maken.

3.3. Organisatie

Besturing en Control

DGA: Als gemeenten als gegevensbemiddelingsdienst optreden dan moeten zij zorgen dat belangenconflicten worden voorkomen door een structurele scheiding tussen de gegevensbemiddelingsdienst en alle andere geleverde diensten (d.w.z. dat ze wettelijk gescheiden moeten zijn). Ook mogen de commerciële voorwaarden (met inbegrip van de prijsstelling) voor het aanbieden van bemiddelingsdiensten niet afhankelijk zijn van de vraag of een potentiële gegevenshouder of gegevensgebruiker andere diensten gebruikt. Alle verkregen gegevens en metagegevens kunnen alleen worden gebruikt om de gegevensbemiddelingsdienst te verbeteren.

Op grond van de DGA moeten gemeenten als gegevensbemiddelaars de bevoegde autoriteit in kennis stellen van hun voornemen om dergelijke diensten te verlenen. De bevoegde autoriteit ziet erop toe dat de kennisgevingsprocedure niet-discriminerend is en de mededinging niet verstoort en bevestigt dat de aanbieder van gegevensbemiddelingsdiensten de kennisgeving met alle vereiste informatie heeft ingediend.

AI-act: Gemeenten zullen kosten moeten maken voor het uitvoeren van de aanvullende verplichtingen wanneer zij zelf AI-systemen, die onder dit voorstel vallen, ontwikkelen, als distributeur aanbieden aan medeoverheden en/of zelf gebruiken. Daarnaast is in het voorstel onder meer voorzien in een verplichte conformiteits-beoordeling voor hoog risico AI-systemen en in een autorisatieprocedure teneinde toestemming te verkrijgen voor het inzetten van specifieke hoog risico AI-systemen. Deze procedures vergen van gemeenten aanpassing van werkwijze, aanvullende verplichtingen en extra capaciteit en specifieke kennis en expertise t.a.v. de huidige situatie. Gezien de reikwijdte van de verordening, de gehanteerde definitie van AI, opgenomen verplichtingen en het benodigde toezicht

55 https://vng.nl/sites/default/files/2022-04/impactanalyseSingleDigital%20Gateway.pdf

hierop, kan gesteld worden dat de implicaties voor de uitvoering en handhaving aanzienlijk kunnen zijn. Omdat nog niet voldoende duidelijk is welke AI-systemen onder dit voorstel vallen, kunnen bij een brede reikwijdte van het voorstel de kosten voor conformiteitsbeoordelingen van hoog-risicosystemen binnen gemeenten mogelijk aanzienlijk zijn.[56] Het is belangrijk dat de administratieve lasten voor gemeenten in verhouding staan tot het doel van de AI-verordening, de bescherming van publieke waarden, en waar nodig ondersteuning te bieden.[57] Gemeenten werken met beperkte budgetten en capaciteit. Zeker waar het om moderne innovaties gaat als AI, en zeker de kleinere gemeenten. In elke vorm zal de komst van de AI-act grote impact hebben op uitvoeringsorganisaties en toezichthouders. Zelfs een kant-en-klaar product zal ingebed moeten worden in een systeem van registratie en governance. En mogelijk zullen ook bestaande systemen met bewezen staat van dienst te maken krijgen met extra administratieve lasten. Hierin zit een aanzienlijk risico van concentratie van macht bij grote spelers die al vooroplopen in de ontwikkeling van AI. In plaats van concurrentie te bevorderen, werpt de AI-verordening dan barrières op die voor grote bedrijven te overzien zijn, maar voor gemeenten en kleinere spelers torenhoog blijken.

NIS2: Voor gemeenten die als AED zijn aangemerkt geldt dat:

- De beheersorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het risicobeheer op het gebied van cyberbeveiliging goedkeuren, toezicht moeten houden op de uitvoering ervan en zijn verantwoordelijk zijn voor de niet-naleving door de entiteiten van de verplichtingen uit hoofde van dit artikel.
- De leden van het beheersorgaan regelmatig specifieke opleidingen moeten volgen om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.

Europese Digitale Identiteit verordening: Gemeenten moeten verantwoording afleggen over de veilige en betrouwbare inzet van wallets. De vraag is of dit op soortgelijke wijze gaat als bij DigiD.

DSA:

2. Cumulative obligations by platform	IS	HS	OP	VLOP
Transparency reporting	✔	✔	✔	✔
Requirements on terms of service due account of fundamental rights	✔	✔	✔	✔
Cooperation with national authorities following orders	✔	✔	✔	✔
Points of contract and, where necessary, legal representative	✔	✔	✔	✔
Notice and action and obligation to provide information to users		✔	✔	✔
Complaint an redress mechanism and out of court dispute settlement			✔	✔
Trusted flaggers			✔	✔
Measures against abusive notices and counter-notices			✔	✔
Know your Business Customer (KYBC)			✔	✔
User-facing transparency of online advertising			✔	✔
Reporting criminal offences			✔	✔
Risk management obligations and compliance officer				✔
External risk auditing and public accountability				✔
Transparency of recommender systems and enhanced advertising transparency				✔
Data sharing with authorities and researchers				✔
Codes of conduct				✔
Crisis response cooperation				✔

Voor online platforms gelden nieuwe verplichtingen, daar moet de gemeente zich aan houden wanneer ze zelf een platform aanbiedt[58]

56 https://www.rijksoverheid.nl/documenten/vergaderstukken/2021/05/31/fiche-2-verordening-betreffende-kunstmatige-intelligentie
57 https://vng.nl/sites/default/files/2022-04/VNG%20Position%20paper%20Kunstmatige%20intelligentie%20%28AI%29_0.pdf
58 Overgenomen van https://ddma.nl/legal/wetgeving/digital-service-markets-act/

Urban Air mobility: Het eerste wat hier nodig lijkt is het opdoen van basale kennis door gemeenten. Dat begint met een vertaling van de Europese regels naar de praktijk in afstemming met I&W. Vanuit de ruimtelijke ordening moet gekeken worden op welke rol Urban Air Mobility gaat spelen bij de inrichting van de mobiliteit in de stad. Een gemeente moet afwegen welke onderdelen van Urban Air Mobility ze zelf uitvoert (en in welke mate) en welk aan andere overheidslagen en/of marktpartijen. Een aantal kernverantwoordelijkheden zullen binnen de gemeentelijke organisatie belegd moeten worden.

Sancties:
De toezichthoudende autoriteiten hebben onderzoeks- en correctiebevoegdheden, met inbegrip van de bevoegdheid om overeenkomstig artikel 23 administratieve geldboeten op te leggen, die overeen kunnen komen met de geldboetes uit de Avg. (administratieve boeten van ten minste 20.000.000 EUR of ten hoogste 4 % van de totale wereldwijde jaaromzet van de onderneming, afhankelijk van welk bedrag hoger is).

DGA: Het voorstel vereist dat lidstaten één of meerdere autoriteiten aanwijzen voor toezicht en handhaving op datatussenpersonen en data-altruïsme organisaties.

Sancties:
De lidstaten stellen de regels vast betreffende de sancties die van toepassing zijn op inbreuken tegen de verplichtingen inzake doorgifte van niet-persoonsgebonden gegevens aan derde landen op grond van artikel 5, lid 14, en artikel 31, de meldingsplicht voor aanbieders van databemiddelingsdiensten op grond van artikel 11, de voorwaarden voor het verlenen van databemiddelingsdiensten op grond van artikel 12 en de voorwaarden voor de registratie als een erkende organisatie voor data-altruïsme op grond van de artikelen 18, 20, 21 en 22, en nemen alle nodige maatregelen om ervoor te zorgen dat die sancties worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. In hun sanctieregels houden de lidstaten rekening met de aanbevelingen van het Europees Comité voor gegevensinnovatie. De lidstaten stellen de Commissie uiterlijk op 24 september 2023 in kennis van die regels en maatregelen en delen haar onverwijld alle latere wijzigingen daarvan mee.
DA: In iedere Lidstaat wordt een bevoegde autoriteit aangewezen en belast met de handhaving van de DA. Deze kan administratieve boetes opleggen, en iedereen kan een klacht of verzoek indienen. De Autoriteit Persoonsgegevens heeft een rol voor zover persoonsgegevens aan de orde zijn, en ook sectorale autoriteiten behouden hun zeggenschap.

DA: Het voorstel vereist dat een bevoegde autoriteit wordt aangewezen en belast met de handhaving van de DA. Sectorale autoriteiten kunnen hun zeggenschap behouden. De Autoriteit Persoonsgegevens heeft een rol voor zover persoonsgegevens aan de orde zijn.

Sancties:
De boetes kunnen door de Lidstaat zelf worden opgesteld, voor sommige gevallen verplicht in lijn met de sanctieregels in de AVG.

AI-act: Het voorstel creëert een systeem voor toezicht dat ziet op de toepassing en naleving van de in het voorstel opgenomen vereisten en verplichtingen. Elke lidstaat dient een nationale toezichthouder aan te wijzen of in te stellen die verantwoordelijk is voor het toezicht op de verordening in algemene zin. Daarnaast wordt het bestaande toezicht uitgebreid door het instellen van een 'Europees Artificial Intelligence Board' (bestaande uit de hoofden van de toezichthouders van de lidstaten en de European Data Protection Supervisor). Volgens het voorstel is de Commissie zelf onderdeel als voorzitter (en doet voorbereiding meetings en ondersteuning), ook kunnen externe deskundigen en waarnemers worden uitgenodigd. Lidstaten moeten verder toezichthouders aanwijzen, afhankelijk van de sector waar een AI-systeem in gebruik wordt genomen. Toezichthouders kunnen boetes uitdelen als organisaties zich niet aan de eisen van deze verordening houden. Verder krijgen toezichthouders de mogelijkheid om de gebruikte datasets en de verplichte documentatie, die providers van hoog-risico AI-systemen moeten produceren, in te zien. Wanneer deze documentatie ontoereikend is om te bepalen of Unie-verplichtingen zijn geschonden die fundamentele rechten beogen te beschermen, kunnen de systemen worden getest door de markt-toezichthouder. Er gelden verder bepalingen met betrekking tot vertrouwelijkheid van de informatie die wordt ingezien.

Het voorstel introduceert daarnaast een EU-brede database waar providers van hoog-risico AI-systemen zich moeten aanmelden.

Sancties:

- Overeenkomstig de voorwaarden van deze AI-act stellen de lidstaten de voorschriften voor sancties vast, waaronder administratieve geldboeten, die van toepassing zijn op inbreuken op deze verordening en nemen zij alle nodige maatregelen om ervoor te zorgen dat deze naar behoren en doeltreffend worden uitgevoerd. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn. Hierbij wordt met name rekening gehouden met de belangen van kleine aanbieders en start-ups en hun economische levensvatbaarheid.
- De lidstaten stellen de Commissie van die voorschriften en maatregelen in kennis en delen haar onverwijld alle latere wijzigingen daarvan mee.
- Voor de volgende inbreuken gelden administratieve geldboeten tot 30.000.000 EUR of, als de overtreder een onderneming is, tot 6 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, als dat hoger is:
  (a) niet-naleving van het verbod van de in artikel 5 vermelde praktijken op het gebied van artificiële intelligentie;
  (b) non-conformiteit van het AI-systeem met de in artikel 10 neergelegde voorschriften.
- Voor de non-conformiteit van het AI-systeem met voorschriften of verplichtingen krachtens deze verordening, uitgezonderd die bepaald in de artikelen 5 en 10, gelden administratieve geldboeten tot 20 000 000 EUR of, als de overtreder een onderneming is, tot 4 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, als dat hoger is.
- Voor de verstrekking van onjuiste, onvolledige of misleidende informatie aan aangemelde instanties en nationale bevoegde autoriteiten naar aanleiding van een verzoek, gelden administratieve geldboeten tot 10.000.000 EUR of, als de overtreder een onderneming is, tot 2 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, als dat hoger is.
- Bij het bepalen van het bedrag van de administratieve geldboete in elk individueel geval worden alle relevante omstandigheden van de specifieke situatie in aanmerking genomen en wordt terdege rekening gehouden met het volgende:
  - de aard, ernst en duur van de inbreuk en de gevolgen ervan;
  - of administratieve geldboeten reeds door andere markttoezichtautoriteiten voor dezelfde inbreuk op dezelfde exploitant zijn toegepast;
  - de omvang en het marktaandeel van de exploitant die de inbreuk pleegt.

NIS2:

- Elke lidstaat wijst een of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor cyberbeveiliging en toezichthoudende taken. De lidstaten kunnen daartoe een of meer bestaande instanties aanwijzen. De lidstaten zorgen ervoor dat de bevoegde autoriteiten effectief toezicht houden op de naleving van deze richtlijn, en nemen daartoe de nodige maatregelen.
- De bevoegde autoriteiten werken nauw samen met de gegevensbeschermingsautoriteiten bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens.
- Elke lidstaat wijst een of meer CSIRT's aan en verantwoordelijk zijn voor de incidentenbehandeling volgens een welbepaald proces.

In de huidige situatie is de Wet beveiliging netwerk- en informatiesystemen (afgekort Wbni) van toepassing. Agentschap Telecom is toezichthouder op deze wet. De Wbni is de Nederlandse implementatie van de Europese Netwerk- en Informatiebeveiliging Richtlijn (afgekort de NIB-Richtlijn).

Sancties:

De lidstaten stellen regels vast voor de sancties die van toepassing zijn op inbreuken op de krachtens deze richtlijn vastgestelde nationale bepalingen en nemen alle nodige maatregelen om ervoor te zorgen dat deze worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn.

Europese Digitale Identiteit verordening:
eIDAS toezicht blijft van toepassing en is geregeld in de Telecomwet[59], toezichthouder is het agentschap Telecom dat valt onder het ministerie van Economische zaken en Klimaat. De Autoriteit Persoonsgegevens heeft een rol voor zover persoonsgegevens aan de orde zijn.

- het verlenen van vertrouwensdiensten door in Nederland gevestigde verleners van vertrouwensdiensten als geregeld in hoofdstuk III van de eidas-verordening, met inbegrip van de bijlagen waarnaar in dat hoofdstuk wordt verwezen, en de artikelen 18.15a, voor zover het Onze Minister aangaat, 18.15b tot en met 18.15e, en 18.18 van deze wet;
- De bij besluit van de Autoriteit persoonsgegevens aangewezen ambtenaren zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de artikelen 11.3a en 11.5b en, voor zover het een inbreuk op de veiligheid of het verlies van integriteit betreft die of dat aanzienlijke gevolgen heeft voor persoonsgegevens, het bepaalde bij en krachtens artikel 18.15a van deze wet en artikel 19, tweede lid van de eidas-verordening.

Het is nog onbekend of met de aanpassing van de eIDAS verordening, de toezichthoudende rol op soortgelijke wijze blijft ingericht.

Sancties:
De lidstaten stellen regels vast voor de sancties die van toepassing zijn op inbreuken op deze verordening. De sancties moeten doeltreffend, evenredig en afschrikkend zijn.

DSA:
De lidstaten duiden een of meer bevoegde autoriteiten aan als verantwoordelijke voor de toepassing en uitvoering van de DSA ("bevoegde autoriteiten"). De lidstaten duiden een van de bevoegde autoriteiten aan als hun coördinator voor digitale diensten. De coördinator voor digitale diensten is verantwoordelijk voor alle kwesties die verband houden met de toepassing en handhaving van deze verordening in die lidstaat, tenzij de betrokken lidstaat bepaalde specifieke taken of sectoren aan andere bevoegde autoriteiten heeft toegewezen. De coördinator voor digitale diensten is in elk geval verantwoordelijk voor de coördinatie op nationaal niveau in verband met deze kwesties en voor het bijdragen tot de doeltreffende en consistente toepassing en handhaving van deze verordening binnen de hele EU.

Sancties:
- De lidstaten stellen de voorschriften vast inzake de sancties die in geval van inbreuk op deze verordening door onder hun rechtsmacht vallende aanbieders van tussenhandelsdiensten van toepassing zijn en nemen de nodige maatregelen om ervoor te zorgen dat de sancties in overeenstemming met artikel41 worden toegepast.
- De sancties zijn doeltreffend, evenredig en afschrikkend. De lidstaten stellen de Commissie van die voorschriften en maatregelen in kennis en delen haar onverwijld alle latere wijzigingen daarvan mede.
- De lidstaten zorgen ervoor dat het maximumbedrag van de sancties die worden opgelegd voor niet-naleving van de in deze verordening vastgestelde verplichtingen, niet meer bedraagt dan 6% van de jaarlijkse inkomsten of de omzet van de betrokken aanbieders van tussenhandelsdiensten. Sancties voor het verstrekken van onjuiste, onvolledige of misleidende informatie, het niet beantwoorden of corrigeren van onjuiste, onvolledige of misleidende informatie en het niet onderwerpen aan een inspectie ter plaatse mogen niet meer bedragen dan 1 % van de jaarlijkse inkomsten of de omzet van de betrokken dienstverlener.
- De lidstaten zorgen ervoor dat het maximumbedrag van een dwangsom niet meer bedraagt dan 5 % van de gemiddelde dagelijkse omzet van de betrokken aanbieder van tussenhandelsdiensten in het voorgaande boekjaar, berekend vanaf de in het desbetreffende besluit vermelde datum.

59 https://wetten.overheid.nl/BWBR0009950/2022-05-01/#Hoofdstuk18_Artikel18.15a

Mogelijke rechtsgevolgen voor gemeenten als een gemeente niet aan de regels van een Europese verordening voldoet

Als een gemeente niet aan de regels van een Europese verordening voldoet, zijn er drie mogelijke gevolgen:

1. Sancties – EU niveau

Een van de taken van de Europese Commissie is om de juiste toepassing van het EU-recht te waarborgen. Wanneer een lidstaat bepaalde verplichtingen niet nakomt, is de Commissie bevoegd om via een zogeheten inbreukprocedure een zaak aanhangig te maken bij het Europees Hof van Justitie. Dit staat in artikel 258 VWEU. Het Hof beslist dan welke sancties aan de lidstaat worden opgelegd. Meer informatie over deze procedure staat ook op de website van Europa Decentraal.
Een inbreukprocedure wordt slechts in het uiterste geval gestart. De Commissie zal altijd eerst in overleg gaan met de betrokken lidstaat om via dialoog tot een oplossing te komen.

2. Sancties – lid statelijk niveau

Ook wanneer de inbreuk is gepleegd door een decentrale overheid is de centrale overheid verantwoordelijk. Om zo'n inbreukprocedure te voorkomen heeft Nederland daarom de Wet naleving Europese regelgeving publieke entiteiten ingesteld (Wet NERpe). Deze wet biedt de rijksoverheid instrumenten om de naleving van Europese regelgeving af te dwingen jegens organen en instanties ('publieke entiteiten') die het Europese recht niet – of niet juist – naleven. Deze instrumenten zijn de aanwijzingsbevoegdheid en het verhaalsrecht. In deze notitie staat hier meer informatie over. Wanneer een overheidsinstantie niet op tijd voldoet aan de verplichtingen van een EU-verordening, kan de rijksoverheid op grond van deze wet dus maatregelen nemen.

Net als bij de inbreukprocedure wordt de Wet NERpe in de praktijk alleen in het uiterste geval gebruikt.

3. Sancties - particulieren

Naast de acties die door de EU en de lidstaten genomen kunnen worden, moet er ook rekening mee worden gehouden dat particulieren via de nationale rechter naleving kunnen proberen af te dwingen als zij rechten kunnen ontlenen aan de wet die niet nageleefd wordt. Ook bestaat de mogelijkheid dat er een klacht wordt ingediend bij de Europese Commissie door de betrokken partij.

Samenvattend handhaving en sanctieregimes

Uit bovenstaande blijkt dat er verschillende toezichthouders en handhavingsregimes voor de digitaliseringsopgaven worden voorgesteld. De vraag is hoe dit uitgewerkt wordt in Nederland. Voor gemeenten is het belangrijk dat dit zoveel als mogelijk integraal gebeurd om te voorkomen dat gemeenten met een verscheidenheid aan toezichthouders en handhavingsmechanismen te maken krijgen en daarmee worden opgezadeld met een grote administratieve last. In de volgende tabel zijn samenvattend de toezichthoudende instanties en sancties van nieuwe Europese digitale wetgeving weergegeven.

	Belangrijkste onderwerp	Toezichthoudende instantie	Sancties
ePrivacy verordening	Bescherming van persoonsgegevens rond elektronische communicatie	In Nederland is het toezicht op de ePrivacyrichtlijn en de AVG nu nog gescheiden. De Autoriteit Consument en Markt (ACM) ziet toe op de ePrivacyrichtlijn, de Autoriteit Persoonsgegevens (AP) op de AVG. De ePrivacy verordening poogt een betere samenhang met de AVG te garanderen.	Tot 20.000.000 EUR of ten hoogste 4 % van de totale wereldwijde jaaromzet
DGA	Kaders voor: • Hergebruik van beschermde overheidsgegevens • Datadeeldiensten • Data altruïsme • Europees Comité gegevensinnovatie	Het voorstel vereist dat lidstaten één of meerdere autoriteiten aanwijzen voor toezicht en handhaving op datatussen-personen en data-altruïsme organisaties.	De boetes kunnen door de Lidstaat zelf worden opgesteld. In hun sanctieregels houden de lidstaten rekening met de aanbevelingen van het Europees Comité voor gegevensinnovatie.
DA	Kaders voor: • delen van data tussen bedrijven en consumenten (B2C) en tussen bedrijven en bedrijven (B2B) • Beschikbaarstellen data bij een uitzonderlijk behoefte/situatie • Dataportabiliteit • Interoperabiliteit	Het voorstel vereist dat een bevoegde autoriteit wordt aan-gewezen en belast met de hand-having van de DA. Sectorale autoriteiten kunnen hun zeggen-schap behouden. De Autoriteit Persoonsgegevens heeft een rol voor zover persoonsgegevens aan de orde zijn.	De boetes kunnen door de Lidstaat zelf worden opgesteld, voor sommige gevallen verplicht in lijn met de sanctieregels in de AVG
AI-act	Kaders voor AI-systemen: • Grondrechten en waarden • Rechtszekerheid garanderen om investeringen en innovatie te vergemakkelijken; • Beheer en handhaving bestaande wetgeving inzake grondrechten en veiligheids-voorschriften • Ontwikkeling eengemaakte markt vergemakkelijken en voorkomen van markt-versnippering • Conformiteitsbeoordelingen van hoog-risicosystemen met AI	Elke lidstaat dient een nationale toezichthouder aan te wijzen of in te stellen die verantwoordelijk is voor het toezicht op de verordening in algemene zin. Lidstaten moeten verder toezicht-houders aanwijzen, afhankelijk van de sector waar een AI-systeem in gebruik wordt genomen.	Tot 20.000.000 EUR of ten hoogste 4 % van de totale wereldwijde jaaromzet
NIS 2	Verplichtingen • Om nationale strategieën voor cyberbeveiliging vast te stellen en om bevoegde nationale autoriteiten, centrale contact-punten en computer security incident response teams (CSIRT's) aan te wijzen;	• Elke lidstaat wijst een of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor cyber-beveiliging en toezichthoudende taken. De lidstaten kunnen daar-toe een of meer bestaande instanties aanwijzen.	De lidstaten stellen regels vast voor de sancties die van toepassing zijn op inbreuken op de krachtens deze richt-lijn vastgestelde nationale bepalingen

Tabel $$$: Toezichthoudende instanties en sancties van nieuwe Europese digitale wetgeving

	Belangrijkste onderwerp	Toezichthoudende instantie	Sancties
	• Inzake risicobeheer en rapportage • Tot delen van informatie op het gebied van cyberbeveiliging. Voor gemeenten die als AED zijn aangemerkt geldt, dat het beheersorgaan: • Genomen maatregelen voor het risicobeheer op het gebied van cyber-beveiliging goedkeuren, toezicht moeten houden op de uitvoering ervan en zijn verantwoordelijk voor de niet-naleving door de entiteiten van de verplichtingen. • Specifieke opleidingen moet volgen om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.	• De bevoegde autoriteiten werken nauw samen met de gegevensbeschermingsautoriteiten bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens. • Elke lidstaat wijst een of meer CSIRT's aan en verantwoordelijk zijn voor de incidentenbehandeling	nemen alle nodige maatregelen om ervoor te zorgen dat deze worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn.
Europese Digitale Identiteit verordening	Regulering van: • Elektronische identificatiemiddelen (eID's) • Elektronische vertrouwensdiensten • Elektronische attestatie van attributen • Wallet	eIDAS Toezicht blijft van toepassing en is geregeld in de Telecomwet: toezichthouder is het agentschap Telecom dat valt onder het ministerie van Economische zaken en Klimaat. De Autoriteit Persoonsgegevens heeft een rol voor zover persoonsgegevens aan de orde zijn. Het is nog onbekend of met de aanpassing van de eIDAS verordening, de toezichthoudende rol op soortgelijke wijze blijft ingericht.	De lidstaten stellen regels vast voor de sancties die van toepassing zijn op inbreuken op deze verordening. De sancties moeten doeltreffend, evenredig en afschrikkend zijn.
DSA	Vier categorieën partijen waarvoor verschillende regels gelden: 1. Tussenhandelsdiensten die netwerkinfrastructuur aanbieden: internetproviders, domeinnaamregistrators, waaronder ook:	De lidstaten duiden een of meer bevoegde autoriteiten aan: • als verantwoordelijke voor de toepassing en uitvoering van de DSA • als hun coördinator voor digitale diensten en is verantwoordelijk voor alle kwesties die verband houden met de toepassing	Tot ten hoogste 6 % van de jaarlijkse inkomsten of omzet van betrokken aanbieders van

Tabel $$$: Toezichthoudende instanties en sancties van nieuwe Europese digitale wetgeving

	Belangrijkste onderwerp	Toezichthoudende instantie	
	2.Hostingdiensten zoals cloud- en webhostingdiensten, waaronder ook: 3.Onlineplatforms waar verkopers en consumenten samenkomen, zoals online-marktplaatsen, appstores, deeleconomieplatforms en sociale media platforms 4. Zeer grote onlineplatforms vormen een bijzonder risico wat betreft de verspreiding van illegale inhoud en het toebrengen van schade aan de maatschappij. Er zijn specifieke regels vastgesteld voor platforms die meer dan 10% van de Europeanen (dus 45 miljoen gebruikers) bereiken.	en handhaving van deze verordening in die lidstaat, tenzij de betrokken lidstaat bepaalde specifieke taken of sectoren aan andere bevoegde autoriteiten heeft toegewezen.	

3.4. Personeel (personeelsbestand)

In het kort gezegd is een grote inspanning voorzien in vergroten van leiderschap, kennis en uitvoeringscapaciteit om de Europese digitale wetgeving te implementeren. Dit geldt op alle niveaus van de gemeentelijke organisatie waar aandacht is voor zowel de dagelijkse operatie als innovatie. Door de vaardigheden dient het adaptief vermogen om om te gaan met verandering vergroot te worden. Om dit in te richten dienen op bestuurlijk, directie en ambtelijk niveau de bewustwording, competenties en vaardigheden aanwezig te zijn om om te kunnen gaan met de transformaties en de inhoudelijke kennis die nodig is om technologie en digitalisering te kunnen sturen.

Inhoudelijke kennis
De kaders uit de EU helpen in het reguleren van de veranderende machtsstructuren in de data (platform) economie, maar het vergt leiderschap om de waarde van de Europese digitale (data) strategie te kunnen voorstellen en deze te vertalen naar wat dit betekent voor de gemeentelijk uitvoering en inwoners en bedrijven. Dit leiderschap vraagt een mindset waarin een data (platform) economie en daarbij behorende mechanismes een belangrijke strategische rol spelen. Het gaat om het daadwerkelijk doorgronden van de betekenis van digitale identiteiten, data(platformen), artificiële intelligentie (AI), cybersecurity etc. voor het uitvoeren van de gemeentelijk taken en het zichtbaar uitdragen van de mogelijkheden van deze digitale identiteiten, data, AI, en het verantwoord inzetten hiervan en dit te vertalen naar commitment, urgentie, financiering en organisatieverandering.

Ethiek en bewustwording
Gemeenten hebben hierbij niet alleen te maken met een juridische werkelijkheid, gebaseerd op normatieve kaders (hoe het zou moeten zijn), of een technische werkelijkheid (cloudinfrastructuren, wallets, vertrouwensdiensten, federatieve datastelsels, datastructuren, api's, biometrie, machine learning, etc) maar ook met hoe ze verantwoord invulling kunnen geven aan de gemeentelijke taakopvatting (ethiek en ambitie). Het nadenken over ethiek roept allerlei vragen op over (democratische) verantwoordelijkheden en transparantie over de afweging. Nieuwe technologieën waarvoor uit Europa kaders komen als digitale identiteit, artificiële intelligentie, de werking van algoritmes, cybersecurity en de nog onbekendheid hierover vormen hierbij een extra uitdaging. Deze uitdaging moet bovendien plaatsvinden gelijktijdig met de enorme opgave die gemeenten hebben bij de uitvoering van de maatschappelijke opgaven zowel in het sociale als fysieke domein.

Transformatieve vaardigheden
De digitale transformatie is 90% cultuur waarin technologie verandering helpt versnellen. De transformaties kunnen alleen succesvol worden geïmplementeerd als de organisatie de vaardigheden heeft om op te kunnen gaan met de hoeveelheid verandering en in staat is het proces met haar inwoners goed te voeren. De vaardigheden in veranderkunde en de aanpassingen in bestaande structuren zal om flexibiliteit en snelheid vragen van leiders, managers en medewerkers vragen in alle niveaus van de organisatie.

3.5. Administratieve organisatie (processen)

eIDAS2.0:
Open data richtlijn: Er geldt een primaire beslistermijn van maximaal vier weken om de gevraagde data te verstrekken, die met twee weken verdaagd kan worden de richtlijn laat ruimte om de informatie 'zo spoedig mogelijk' te verstrekken, 'maar in ieder geval binnen een termijn die het mogelijk maakt het potentieel van de informatie volledig te benutten'. De impact van de Open data richtlijn kan worden benaderd vanuit de letter van de wet, waarbij de impact vrij beperkt is (huidige Who voortzetten); en de geest van de wet, waarbij de impact aanzienlijk hoger is. In tegenstelling tot de letter van de wet ademt de geest van de wet economisch en maatschappelijk potentieel uit en vraagt de richtlijn om zoveel mogelijk belemmeringen in hergebruik van overheidsinformatie weg te nemen.[60]

DGA: Gemeenten moeten beschermde data die via exclusieve overeenkomsten worden gedeeld ook beschikbaar stellen aan andere partijen. Daarvoor moeten ze nodige juridische, technische en communicatieve voorbereidingen treffen. Daarnaast moeten deze gemeenten of een bevoegde autoriteit die is aangewezen om openbare lichamen te ondersteunen maatregelen nemen om ervoor te zorgen dat data die wordt overgedragen naar derde landen voldoen aan de voorwaarden die zijn gesteld in de verordening.

DGA: Verzoeken tot hergebruik van gegevens moeten binnen een redelijke termijn, en in elk geval binnen twee maanden na de datum van het verzoek, worden ingewilligd of afgewezen door gemeenten.

DGA: Gemeenten mogen vergoedingen in rekening brengen voor het toestaan van hergebruik, zolang die vergoedingen niet hoger zijn dan de noodzakelijke gemaakte kosten. Daarnaast moeten gemeenten het hergebruik voor wetenschappelijk onderzoek en andere niet-commerciële doeleinden, alsook door kleine en midden grote ondernemeingen en start-ups stimuleren door de heffingen te verlagen of zelfs uit te sluiten.

DGA: Indien een gemeente geen toegang kan verlenen tot bepaalde gegevens voor hergebruik, moet het de potentiële hergebruiker helpen bij het vragen van toestemming van de betrokkene om zijn persoonsgegevens te hergebruiken of de toestemming van de houder van de gegevens wiens rechten of belangen door het hergebruik kunnen worden aangetast. Bovendien kan vertrouwelijke informatie (bijv. bedrijfsgeheimen) alleen met die toestemming of toestemming voor hergebruik worden bekend-gemaakt.

DGA: Gemeenten moeten een proces inrichten zodat degenen die hun gegevens delen (in geval van data-altruisme), gemakkelijk hun toestemming kunnen geven en intrekken.
AI-act: Gemeenten moeten hun AI-systemen risicogericht inventariseren en voor deze systemen vervolgens de verplichtingen uitvoeren en inbedden in hun uitvoeringsprocessen om aan de eisen voldoen. Daarnaast biedt AI ook een kans om processen verder te optimaliseren en administratieve lasten te verlagen

SDG: De activiteiten die gemeenten moeten ontplooien om conform de Verordening valt uiteen in twee onderdelen: informatie en transacties. In december 2022 zullen de eerste gemeentelijke informatieproducten ('Annex I') beschikbaar moeten zijn conform de eisen die de Verordening aan informatieverstrekking stelt:

- gebruiksvriendelijk
- duidelijke structuur en presentatie
- actueel, accuraat en volledig en in duidelijke en begrijpelijke taal;
- de geboden informatie omvat verwijzingen naar specificaties, de procedures, de naam van de dienstverlener en de contactgegevens
- in ten minste één andere Europese taal

60 https://vng.nl/nieuws/impactanalyse-eu-open-datarichtlijn

Er zijn 82 SDG producten vastgesteld. Het vraagt gemiddeld 1 uur per product om de (Nederlandse en Engelse) standaardteksten te controleren, aan te vullen met gemeente specifieke informatie en te publiceren in de invoervoorziening. Daarna moeten gemeenten de informatie zelf onderhouden.[61]

Per 12 december 2023 zal vervolgens aan het transactionele deel van de verordening ('Annex II') voldaan moeten zijn door de voorgeschreven producten volledig online af te handelen, van aanvraag tot en met het resultaat (vaak een 'besluit'). Hier kan alleen van afgeweken worden als er dwingende redenen zijn die vereisen dat de gebruiker in persoon verschijnt. Deze redenen moeten dan goed gemotiveerd zijn en gebaseerd zijn op openbare veiligheid, volksgezondheid of fraudebestrijding.

Voor deze onlineprocedures wordt verder vereist dat een grensoverschrijdende gebruiker:

- Op een gebruikersvriendelijke manier door de procedure geleid wordt, zodanig dat alle procedure-vereisten ingevuld worden.
- De benodigde gegevens kan verstrekken, ook als structuur of inhoud verschilt van de Nederlandse situatie (bijvoorbeeld de wijze van adresnotatie)
- Zich elektronisch kan identificeren en authentiseren; documenten kan ondertekenen en verzegelen conform de eIDAS verordening. Dit betekent dat alle EU-erkende middelen geaccepteerd moeten worden. Indien het voor een procedure nationaal is toegestaan een kopie van identificatiedocument te leveren, dan mogen grensoverschrijdende gebruikers dit ook.
- Elektronisch bewijs kan aanleveren, overal waar dit ook voor nationale gebruikers mogelijk is of deze op laten vragen bij bevoegde instantie (*Once Only Principle*). Dit betekent dat volgens het eenmaligheidsbeginsel burgers niet gedwongen mogen worden om informatie aan autoriteiten te verstrekken als een andere autoriteit die informatie al in elektronische vorm bezit.
- Automatisch een ontvangstbewijs ontvangt, tenzij het resultaat van de procedure meteen wordt geleverd.
- Elektronisch kan betalen met algemeen beschikbare grensoverschrijdende betaaldiensten. Landelijke betaalmiddelen zoals iDeal voldoen daar dus niet aan.

De instructies om de procedure te kunnen doorlopen, moeten vertaald zijn in het Engels. De formulieren/invulvelden zelf hoeven niet vertaald te worden, noch de output.

ePrivacy verordening:
Gemeenten moeten het toestemmingsproces rond cookies inrichten volgens de eisen genoemd in de verordening.
Gemeenten moeten als aanbieder van de elektronische-communicatiedienst de inhoud van de elektronische communicatie wissen of deze gegevens anoniem maken wanneer dit niet langer nodig is voor de verwerking.

61 https://werkenaaneenoverheid.pleio.nl/groups/view/ed87e451-f6fc-49b0-aec4-41f2358426f7/single-digital-gateway/wiki/view/09fa2d17-dc94-4c5f-ab8f-875a9fb5e701/veelgestelde-vragen-over-single-digital-gateway-voor-gemeenten

3.6. Informatievoorziening (informatie en technologie)

Waar moeten/kunnen gemeenten op aansluiten?

DGA: De lidstaten wijzen een of meer bevoegde organen aan, die sectoraal kunnen zijn, om de openbare lichamen te ondersteunen bij het verlenen van toegang tot het hergebruik van de van toepassing zijnde data. De bedoelde steun omvat, indien nodig:

- Technische steun, door een beveiligde verwerkingsomgeving voor het verlenen van toegang tot gegevens met het oog op hergebruik ter beschikking te stellen;
- Technische steun bij de toepassing van beproefde technieken die garanderen dat de gegevensverwerking plaatsvindt op een wijze die garandeert dat de privacy van de informatie in de gegevens waarvoor hergebruik wordt toegestaan, behouden blijft, met inbegrip van technieken voor pseudonimisering, anonimisering, veralgemening en randomisering van persoonsgegevens;

DGA: Een centraal informatiepunt waar alle relevante informatie van hergebruik ter beschikking zijn. Logisch lijkt dat dit data.overheid.nl wordt. Zie hieronder bij Open data richtlijn.

Open data richtlijn[62]: Gemeenten kunnen gegevens als 'open data' aanbieden via een portaal, website of API, of facultatief via data.overheid.nl

Data ruimten: In lijn brengen door Nederland en gemeenten van bestaande of in ontwikkeling zijnde dataruimten (zoals basisregistraties of voorziene gefedereerde basisregistratgies als mobiliteitsdata, gegevensuitwisselingsmechanisme binnen GDI/Common Grond) met de Europese dataruimten. De Commissie investeert in de ontwikkeling van infrastructuur voor gegevensverwerking, instrumenten voor het delen van gegevens, architecturen en governancemechanismen voor een uitwisseling van gegevens en voor de federatie van energie-efficiënte en betrouwbare cloudinfrastructuren en aanverwante diensten.
Voorts voorziet het DIGITAL werkprogramma[63] in financiering voor de oprichting en exploitatie van een ondersteuningscentrum voor gegevensruimten. Een in het kader van DIGITAL gefinancierde coördinatie- en ondersteuningsactie (CSA) zal alle relevante acties op het gebied van sectorale gegevensruimten coördineren en (blauwdruk)architecturen en vereisten voor de gegevensinfrastructuur beschikbaar stellen, met inbegrip van mogelijke technologieën, processen, normen en instrumenten die hergebruik van gegevens in verschillende sectoren door de publieke sector en Europese bedrijven mogelijk maken.

Voor de cloud opslag zal de Europese Commissie gebruik maken van GAIA-X zodat de interoperabiliteit van de 'data spaces' gegarandeerd kan worden op basis van de Europese waarden.

Europese Digitale Identiteit verordening: Het voorstel voorziet nu in een verplichting voor lidstaten om binnen twee jaar na adoptie een nationale wallet gerealiseerd of erkend te hebben die werkt voor grensoverstijgend gebruik, terwijl juridische, beleidsmatige, organisatorische, procesmatige en technische aspecten om dit mogelijk te maken eerst uitwerking behoeven op EU- en nationaal niveau. Volgens het kabinet is van belang dat het voorstel ruimte laat voor gefaseerde invoering, waarbij begonnen wordt met de verplichte invoering en koppeling van eID-componenten, dat wil zeggen de identificatiefunctie in de wallet. Wanneer dit gerealiseerd is, kunnen lidstaten stapsgewijs attributen hieraan koppelen en in een wallet invoeren. Daarbij dienen lidstaten in gezamenlijkheid de prioritering en het tijdspad te kunnen bepalen, ook met het oog op de benodigde aanpassingen in nationale wet- en regelgeving.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) ontwikkelt, beheert en exploiteert de generieke digitale infrastructuur voor grensoverstijgend gebruik van eID-middelen ter uitvoering van de huidige eIDAS-verordening, en ondersteunt dienstverleners bij het aansluiten op en gebruik van de nationale eIDAS-voorzieningen. De huidige eIDAS-infrastructuur en -voorzieningen kunnen geïntegreerd worden in en/of gekoppeld worden aan het nieuwe raamwerk voor Europese digitale identiteiten. Voor de Europese digitale identiteit verordening is recent door BZK een uitwerking

62 https://vng.nl/nieuws/impactanalyse-eu-open-datarichtlijn
63 https://digital-strategy.ec.europa.eu/en/activities/digital-programme

gemaakt[64]. De staatssecretaris voor Koninkrijksrelaties en Digitalisering is bezig met het opzetten van een programma dat de inrichting, het toezicht en de governance voor de Nederlandse invulling van het Europese Digitale Identiteit raamwerk zal vormgeven. De inrichting zal bestaan uit voorzieningen en afspraken om wallets aan burgers en bedrijven uit te kunnen geven, ze te kunnen vullen met gegevens uit overheidsregisters, wallets uit andere EU-lidstaten te kunnen accepteren en andere voorzieningen die de goede en veilige werking van het stelsel faciliteren.

Om te zorgen dat alle burgers en bedrijven, volgens de doelstelling van de EU- verordening, in 2025 gebruik kunnen maken van een hoogwaardige wallet zal dit programma een eerste versie van een Nederlandse open source wallet neerzetten. Daarnaast lopen er trajecten om de digitale identiteit verder te ontwikkelen:

- 'Verkenning eWallets (speelveldanalyse)'[65] bevat een onderzoek naar de omschrijving van en eisen voor een wallet, zoals beschreven in het voorstel tot herziening van de eIDAS-verordening. Ook is gekeken naar de relatie met de huidige eID-middelen, zoals DigiD en eHerkenning. Verder is het huidige speelveld van wallets in Nederland uiteengezet en de bredere context van een stelsel voor wallets beschreven: wat is er al geregeld en wat moet er verder onderzocht en geregeld worden?;
- Een Maatschappelijke Kosten-Baten Analyse (MKBA). Het doel van de MKBA (oplevering najaar 2022) is om op basis van scenario's en use cases de directe en indirecte kosten en baten van de EDI-wallet in kaart te brengen en te kwantificeren. Dit draagt bij aan het duidelijk krijgen van het nut en de noodzaak van wetgeving. Ook zal het meer inzicht geven in de risico's en kansen die wallets met zich meebrengen; wat levert een wallet burgers, bedrijven en overheid op?;
- In oktober 2022 moet de eerste versie van de Toolbox (instrument van de Europese digitale identiteit, zie hoofdstuk 2) met technische uitwerkingen gereed zijn. Nederland neemt actief deel in alle werkgroepen en in Europese pilots om de voorgestelde inrichting te bespreken en beproeven, maar zeker ook om de nodige invloed uit te oefenen op de technische en organisatorische inrichting;
- De Europese Commissie heeft op 10 juni 2022 een aanbesteding gepubliceerd voor de ontwikkeling van een referentie-wallet, ondersteunende software voor het ecosysteem en implementatie-ondersteuning. Dit moet lidstaten helpen bij het realiseren van hun nationale wallets en de grensoverschrijdende werking daarvan.

Ten opzichte van de huidige situatie, zullen de uitwisseling van attributen en het ontsluiten van vertrouwensdiensten in de wallet extra aanpassingen en investeringen vragen van de dienstverleners, voor sommige meer dan voor andere, afhankelijk van de hoeveelheid attributen die dienen te worden verwerkt. De hierboven genoemde MKBA zal meer inzicht geven in de kosten en baten van de gevolgen van de Europese Digitale Identiteit verordening.

Europese Digitale Identiteit verordening en SDG: Het Once-Only Technical System (OOTS) maakt het mogelijk om informatie te delen tussen overheidsdiensten over de grenzen tussen EU-landen heen. Deze technische voorziening kan gezien worden als Het is sectoroverschrijdend en kan worden uitgebreid tot buiten het huidige toepassingsgebied van levensgebeurtenissen zoals uiteengezet in de SDG of voor de attestatie benodigd voor de wallets. Het ondersteunt het eenmaligheidsbeginsel technisch, dat bepaalt dat burgers niet mogen worden gedwongen om informatie aan autoriteiten te verstrekken als een andere autoriteit die informatie al in elektronische vorm bezit.

AI: Om Artificial Intelligence (en onderliggende algortimes) op een transparante en uitlegbare manier te kunnen gebruiken is het noodzakelijk op landelijk niveau te komen tot de identiteit van het algoritme via een algoritme register. Wanneer een algoritme marktplaats beschikbaar komt kan dat gemeenten helpen om effectief gebruik te maken van algoritmes in de digitale dienstverlening.

Urban Air Mobility: Door de ontwikkeling rondom Urban Air Mobility zullen gemeenten regie moeten gaan nemen over het luchtruim boven steden. Dat stelt eisen aan een 'Geo Spatial Infrastructure' die gemeenten in staat moet stellen om hun verantwoordelijkheid voor Urban Air Mobility waar te kunnen maken.

64 https://www.rijksoverheid.nl/documenten/kamerstukken/2022/08/17/kamerbrief-voortgang-europese-digitale-identiteit
65 https://www.rijksoverheid.nl/documenten/rapporten/2022/01/11/verkenning-ewallets-speelveldanalyse

Wat moeten gemeenten zelf inrichten?

DGA: Eventueel een beveiligde verwerkingsomgeving inrichten om hergebruik van gegevens mogelijk te maken: de fysieke of virtuele omgeving en organisatorische middelen om de mogelijkheid te bieden gegevens te hergebruiken op een wijze die de exploitant van de beveiligde verwerkingsomgeving in staat stelt alle gegevensverwerkingsactiviteiten, met inbegrip van het weergeven, opslaan, downloaden en exporteren van de gegevens en het berekenen van afgeleide gegevens door middel van computeralgoritmen, te bepalen en er toezicht op uit te oefenen.

DA: Gemeenten als mogelijke exploitanten van dataruimten voldoen aan de volgende essentiële eisen om de interoperabiliteit van data, mechanismen en diensten voor data-uitwisseling te vergemakkelijken:

- De inhoud van de dataset, gebruiksbeperkingen, licenties, dataverzamelingsmethoden, datakwaliteit en onzekerheid worden voldoende beschreven om de ontvanger in staat te stellen de data te vinden, te raadplegen en te gebruiken;
- De datastructuren, dataformaten, vocabularia, classificatieschema's, taxonomieën en codelijsten worden op een voor het publiek toegankelijke en consistente wijze beschreven;
- De technische middelen om toegang te krijgen tot de data, zoals applicatieprogramma-interfaces, en de gebruiksvoorwaarden en de kwaliteit van de dienstverlening worden voldoende beschreven om automatische toegang tot en overdracht van data tussen partijen mogelijk te maken, ook continu of in realtime in een machineleesbaar formaat;
- Er wordt voorzien in de middelen om de interoperabiliteit van slimme contracten binnen hun diensten en activiteiten mogelijk te maken.

Open data richtlijn[66]: De wijziging betreffende de bevordering van beschikbaarstelling van dynamische en realtime data met gebruik van API's heeft een aanzienlijke impact op gemeenten. Op dit moment bieden gemeenten nauwelijks (sensor)data aan door middel van API's. Wel wordt door alle ondervraagde gemeenten aangegeven dat er in meer of mindere mate sensordata verzameld wordt. Hoewel de aangepaste richtlijn ruimte laat voor minder ingrijpende technische alternatieven op de korte termijn, zal de data op de lange termijn via API's aangeboden moeten worden. Vanuit technisch oogpunt moet er vooral aandacht besteed worden aan de manier waarop individuele gemeenten API's zullen gaan inzetten voor het ontsluiten van de dynamische gegevens (bijv. door gebruik te maken van een'Internet of Things module' bij een dataplatformleverancier). Bestaande software modules kunnen hier een passende uitkomst bieden. Daarnaast is het van belang om mee te geven dat de er in de richtlijn voldoende ruimte gelaten is om onevenredige inspanning aan de kant van de gemeenten, als het draait om het beschikbaar stellen van dynamische data via API's, niet verplicht te stellen.

De wijziging betreffende de vaststelling van een gemeenschappelijke Europese HVDL is op dit moment nog lastig in te schatten, omdat de uitvoeringsrichtlijn waarin de exacte datasets en het proces benoemd worden, nog niet gereed is. Als gemeenten data moeten aanleveren die ze al beschikbaar hebben, dan lijkt dat geen grote impact te hebben. Echter, als vanuit de Europese HVDL gevraagd wordt om data aan te leveren die de gemeente nog niet zelf verzameld, dan is de impact veel groter.

SDG: Gemeenten hoeven zelf géén oplossing te regelen voor de eerste stap: het ontsluiten van informatie over producten en diensten. Het bestuur van de VNG heeft ervoor gekozen om een centrale oplossing te realiseren voor alle gemeenten. Hiermee kunnen gemeenten efficiënt en optimaal voldoen aan alle eisen van de eerste stap van de verordening. Deze oplossing bestaat uit:

- de SDG Invoervoorziening
- standaardteksten in Nederlands en Engels

De tweede stap van Single Digital Gateway (Annex II) is dat EU-burgers en bedrijven toegang hebben tot online procedures. Ook krijgen burgers en bedrijven het recht om overheden toestemming te geven om onderling digitaal bewijsstukken uit te wisselen. De deadline hiervoor is

66 https://vng.nl/nieuws/impactanalyse-eu-open-datarichtlijn

december 2023. Op dit moment wordt onderzocht in hoeverre dit ook op een centrale manier kan worden ingericht. De volgende technische activiteiten zijn hier te zien: Het ontwerpen bouwen, koppelen en plaatsen van een online transactie kent aanzienlijke kosten. In lijn met de eerdere kostenraming uit de impactanalyse eIDAS,[67] dient er bij prijsbepaling rekening gehouden te worden met meer dan alleen de kosten voor de formulierenleverancier. Het betreft hier onder andere kosten voor het geschikt maken van het formulier voor internationale bezoekers (vertaalkosten) internationale betaling (alternatieve betaalmogelijkheden bieden, naast iDeal) en authenticatie (aansluiten op het juiste koppelvlak eHerkenning, om daarmee via het eIDAS stelsel Europese eID middelen te kunnen accepteren). Daarnaast dient het formulier ingebed te worden in de website en ontsloten te worden via Samenwerkende Catalogi (redactiecapaciteit) en gekoppeld te worden aan het juiste behandelsysteem, om de afhandeling geen vertraging te laten oplopen en de vereiste ontvangstbevestiging en het eindresultaat digitaal te kunnen verzenden Het ondernemersdeel is, in potentie een veelvoud van de hierboven genoemde kosten. Het aantal ondernemersproducten kan sterk verschillen tussen gemeenten, onder andere vanwege het verschil in reikwijdte van de APV.

ePrivacy verordening: Aanbieders van software worden aangemoedigd om in hun software instellingen op te nemen waarmee eindgebruikers op een gebruiksvriendelijke en transparante manier de toestemming voor de opslag van en toegang tot opgeslagen gegevens in hun eindapparatuur kunnen beheren door eenvoudig witte lijsten in te stellen en te wijzigen en hun toestemming op elk moment in te trekken. In het licht van de zelfbeschikking van de eindgebruiker moet de toestemming die rechtstreeks door een eindgebruiker wordt uitgedrukt, altijd prevaleren boven de software-instellingen. Elke toestemming die door een eindgebruiker aan een dienst wordt gevraagd en gegeven, moet zonder verdere vertraging rechtstreeks worden geïmplementeerd door de toepassingen van de terminal van de eindgebruiker. Indien de opslag van informatie of de toegang tot reeds in de eindapparatuur van de eindgebruiker opgeslagen informatie is toegestaan, moet hetzelfde gelden.

Europese Digitale Identiteit verordening: Gemeenten moeten kunnen aansluiten en gebruik kunnen maken van de wallet, de uitwisseling van attributen uit authentieke bronnen en vertrouwensdiensten. In het impact assessment heeft de Commissie de financiële consequenties daarvan voor alle lidstaten gezamenlijk geraamd op bijna 1 miljard euro. Hierbij moet in het achterhoofd gehouden worden dat nog niet alle gemeenten zijn aangesloten op de huidige eIDAS verordening.
Ten opzichte van de huidige eIDAS-verordening zal dit voorstel naar verwachting tot meer inspanning en lasten leiden voor het beheer van en het toezicht op eID-stelsel en -middelen, omdat deze oplossingen (zoals wallets) meer functionaliteiten en gegevens dan alleen identiteitsgegevens en meer aanbieders en gebruikers ervan zullen bevatten. Die verruiming van de reikwijdte en het gebruik zal ook van uitvoerende instanties vragen op termijn hun digitale processen en producten aan te passen. Op basis van het voorstel is het voor gemeenten niet mogelijk om te bepalen wat de implicaties zijn van de implementatie van de verordening voor de uitvoering. De voorlopige inschatting is dat gemeenten aanzienlijke aanpassingen moeten doen in hun digitale infrastructuur en processen om de wallet en nieuwe vertrouwensdiensten te ontsluiten en te incorporeren in hun dienstverlening. Er is door Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) een speelveldanalyse gemaakt van ontwikkelingen rondom eWallets in Nederland en Europa[68]. Een conclusie uit deze analyse is dat het geheel complex en veelomvattend is – zowel technisch, organisatorisch als juridisch – en de voorgestelde tijdspanne voor realisatie is kort. De aanbevelingen in dit rapport geven al een eerste indicatie van de grote impact die deze verordening heeft. De precieze impact en uitvoerbare doorlooptijd voor gemeenten zal verder moeten worden onderzocht.

67 Impactanalyse eIDAS-verordening – KING, oktober 2017
68 https://www.rijksoverheid.nl/documenten/rapporten/2022/01/11/verkenning-ewallets-speelveldanalyse

3.7. Juridisch (wet- en regelgeving/ juridische voorwaarden/ overeenkomsten)

DGA: Een gemeenschappelijk Europees toestemmingsformulier voor gegevensaltruïsme zal het mogelijk maken om gegevens in alle lidstaten in een uniform formaat te verzamelen, zodat degenen die hun gegevens delen, gemakkelijk hun toestemming kunnen geven en intrekken. Het zal ook rechtszekerheid bieden aan onderzoekers en bedrijven die gegevens op basis van altruïsme willen gebruiken. Dit zal een modulaire vorm zijn, die kan worden afgestemd op de behoeften van specifieke sectoren en doeleinden.

DGA: De lidstaten wijzen een of meer bevoegde organen aan, die sectoraal kunnen zijn, om de openbare lichamen te ondersteunen bij het verlenen van toegang tot het hergebruik van de van toepassing zijnde data. De bedoelde steun omvat, indien nodig:

- Bijstand aan de openbare lichamen, indien nodig, om hergebruikers te helpen instemming of toestemming te krijgen voor het hergebruik voor altruïstische en andere doeleinden die in de lijn liggen van specifieke beslissingen van de gegevenshouders, onder meer ook met betrekking tot het rechtsgebied of de rechtsgebieden waarin de gegevensverwerking zal plaatsvinden;
- Bijstand aan openbare lichamen met betrekking tot de toereikendheid van de overeenkomstig aangegane verbintenissen van een hergebruiker.

DA:

- De opgevraagde data mag alleen voor het tevoren geformuleerde doel worden gebruikt, niet voor opsporingsdoeleinden.
- Dataverstrekking door bedrijven is in beginsel gratis, en hooguit tegen marginale kosten plus een redelijke marge mits dit tevoren o.b.v. kostenberekeningen transparant is gemaakt.
- Opgevraagde gegevens mogen voor statistiekdoeleinden en voor non-profit onderzoek worden doorgeleverd door de overheid. De datahouder wordt hierover geïnformeerd.

Open data richtlijn[69]: Vanuit juridisch oogpunt speelt het thema data-eigendom, oftewel: van wie zijn bijvoorbeeld de sensordata die worden ingewonnen? Er moet worden voorkomen dat gemeenten er pas ná het plaatsen van de sensoren achter komen dat de data eigendom is van het bedrijf dat de sensoren geplaatst heeft. Dit betekent dat er vóór het plaatsen van de sensoren goede afspraken gemaakt moeten worden over data-eigendom. Zonder deze afspraken kunnen gemeenten tegen (onverwachte) problemen aanlopen op het moment dat zij de betreffende sensordata als open data beschikbaar willen stellen.

De wijziging betreffende de verdere beperking van exclusieve overeenkomsten bij beschikbaarstelling van data en de bijbehorende publicatieverplichting lijkt een beperkte impact op gemeenten te hebben. Dit heeft grotendeels te maken met het feit dat alle ondervraagde gemeenten aangeven dat er momenteel geen exclusieve overeenkomsten afgesloten zijn. Dit kan echter veranderen als deze overeenkomsten in deze toekomst wel afgesloten worden of als blijkt dat er wel exclusieve overeenkomsten zijn die nu door gemeenten niet onder die noemer geschaard worden. Denk hierbij aan data van sensoren die door een andere partij namens de gemeente wordt verzameld.

De wijziging betreffende de uitbreiding van de reikwijdte van het begrip open data naar onderzoeksdata heeft een redelijke impact op gemeenten. Dit komt vooral door het mogelijk moeten aanpassen van contracten met externe onderzoeksbureaus, zodat de verplichting om de gebruikte onderzoeksdata terug te leveren aan de gemeente in deze contracten kan worden opgenomen. Veel onderzoeksdata bij gemeenten wordt immers verzameld door externe onderzoeksbureaus die voor een specifieke onderzoeksopdracht benaderd zijn. Tevens moeten alle gemeentelijke vakafdelingen van deze eis op de hoogte zijn en hun werkwijze bij het laten uitvoeren van onderzoek hierop aanpassen. Voor gemeenten die nu al gebruik maken van bet VNG Model Algemene Inkoopvoorwaarden voor leveringen en diensten bij het afsluiten van contracten met onderzoeksbureaus is de impact beperkt.

69 https://vng.nl/nieuws/impactanalyse-eu-open-datarichtlijn

De vraag dringt zich op waarom de Open datarichtlijn in een gewijzigde Wet hergebruik van overheidsinformatie (Who) wordt geïmplementeerd in plaats van in de Wet open overheid (Woo). Weliswaar is er sprake van complementariteit, maar vanuit oogpunt van overzichtelijkheid is het wenselijk dat de Woo het gezamenlijke kader voor openbaarheid en hergebruik van overheidsinformatie biedt. Is dit niet mogelijk op de korte termijn vanwege de deadline voor implementatie van Europese regelgeving, dan zou dat in de nabije toekomst kunnen plaatsvinden.[70]

AI-act: *Duidelijkheid over de rolverdeling tussen leveranciers en gebruikers van AI-technologie, in lijn met de geest van de wet dat 'de ontwikkelaar betaalt'.*[71]
Gemeenten zijn van nature geneigd de verantwoordelijkheid naar zich toe te trekken om hun inwoners te beschermen. Ze willen dit niet aan private partijen overlaten. Toch mag dat geen vrijbrief zijn voor leveranciers om zich te beperken tot het leveren van een technisch functioneel product zonder aandacht voor de juridische en ethische aspecten. Gemeenten willen een veilig en volledig product inkopen. Daarbij willen ze erop kunnen vertrouwen dat de leverancier binnen de kaders werkt en een correcte conformiteitsbeoordeling heeft gedaan. Ook moet de inkopende gemeente door onduidelijkheden in de verordening niet onbedoeld in de rol van leverancier komen, en opgezadeld zitten met de administratieve lasten die eigenlijk bij de productontwikkelaar horen. De VNG ondersteunt gemeenten daarbij met de ontwikkeling van o.a. inkoop- en kwaliteitsvoorwaarden en informatiemodellen en standaarden, om leveranciers duidelijkheid te bieden over de eisen die zij stellen qua veiligheid, publieke waarden en mensenrechten.

Europese Digitale Identiteit verordening: Nationale uitvoeringsregelgeving is nodig vanwege de brede werkingssfeer van het voorstel. Basis hiervoor zou moeten vormen de tweede tranche van de Wdo die momenteel wordt voorbereid. Het betreft aanpassingen die digitale transacties met nationale eID-middelen in het private domein mogelijk moeten maken, die gegevensuitwisseling onder regie van de burger faciliteren, die naast identificerende ook andere typen gegevens reguleren en die maatregelen voor inzage, correctie en bescherming van gebruikers, certificering, elektronische archivering, toezicht en handhaving verder uitwerken. Tot slot zullen voor eID-middelen de Paspoortwet en de Wegenverkeerswet en voor vertrouwensdiensten de Telecommunicatiewetwet en onderliggende regelingen en besluiten in lijn moeten worden gebracht met het voorstel. Het voorstel is in lijn met de AVG. Daarnaast bevat het voorstel specifieke waarborgen om te voorkomen dat leveranciers van eID-middelen en van attributen de gegevens van gebruikers combineren en aanwenden voor andere diensten. Ook verplicht het voorstel tot gescheiden opslag van gegevens. Essentieel is voorts dat gebruikers bepalen welke data met wie gedeeld wordt en dat gebruikers geïnformeerd moeten worden over de benodigde attributen en gegevens voor afname van een concrete dienst, die alleen gedeeld mogen worden als dit in overeenstemming is met nationaal recht en niet meer dan voor het gebruik van een bepaalde dienst noodzakelijk is.

70 https://vng.nl/sites/default/files/2022-02/Brief%20aan%20BZK%20Consultatie%20wetsvoorstel%20Open%20data%20richtlijn.pdf
71 https://vng.nl/sites/default/files/2022-04/VNG%20Position%20paper%20Kunstmatige%20intelligentie%20%28AI%29_0.pdf

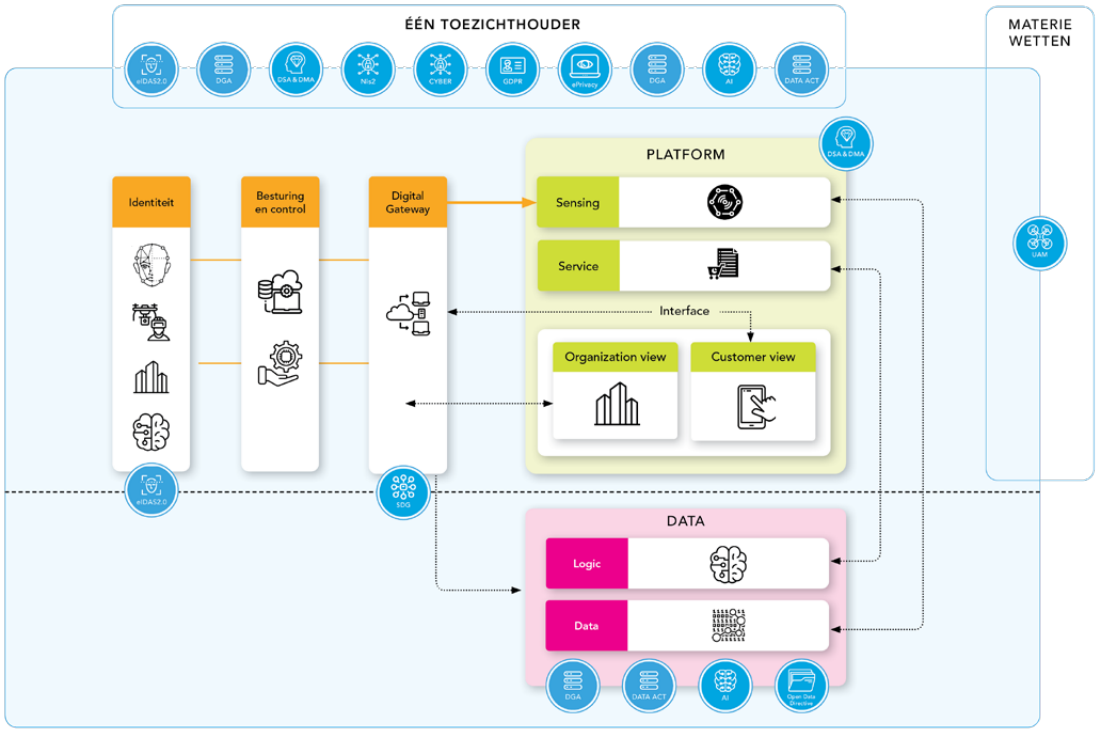
4. Conclusies en aanbevelingen

Hieronder geven we antwoord op de onderzoeksvragen op basis van de beschrijving uit de voorafgaande hoofstukken.

4.1. Beantwoording onderzoeksvragen

1. Wat is op hoofdlijnen de samenhang tussen de relevante bestaande en nieuwe Europese digitale wetten vanuit de bedoeling van de wet? Betrek hierbij ook relevante Nederlandse digitale wetgevingsinitiatieven.

Om meer samenhang te brengen in Europese digitale wetten voor gemeenten is het belangrijk om overzicht te creëren van welke wetten en regels en onderliggende normen nu daadwerkelijk relevant zijn voor gemeenten. Het geven van overzicht kan zorgen voor meer (be)grip en urgentie en het tijdig kunnen inschatten van de impact van de wetten. De wetten zijn daarom samenhangend geclusterd overkoepelende onderwerpen, nl. Identiteit, Besturing en Contro, Digital gateway, Data, Platform en Privacy, zie hiervoor figuur 4. Vervolgens is binnen deze samenhang het doel en de status van de specifieke wetten beschreven en is een beschrijving gegeven over waar de wet over gaat in de gemeentelijke context (zie hoofdstuk 2). In onderstaande figuur 4 is ook het beoogde tijdspad van de verschillende wetten beschreven.



Figuur 4 Samenhang Europese Digitale wetgeving

Wet	Jaar publicatie voorstel	Jaar van kracht	Jaar van kracht, geschat	Jaar ingaan verplichting	Jaar ingaan verplichting geschat
DGA		2022		2023	
DA	2022	onbekend		onbekend	
ePrivacy verordening					
Open data richtlijn		2019		2021	
Europese digitale identiteit verordening	2021		2023		2025
SDG		2018		2023	
AI-act	2021		2023		2025
Data ruimten	2020	nvt		nvt	
NIS2		2023		2024	
Urban air mobility		2021		2023	
DSA		2022		2024	
DMA		2022		2023	
Cyberbeveiligings-verordening		2019		2022	

Figuur 3 – Overzicht Europese digitale wetten in de tijd

2. Wat wijzigt er op hoofdlijnen in de werkwijze van de gemeente door deze Europese digitale wetten als deze in samenhang worden beschouwd?

		Belangrijkste onderwerp
Identiteit	**eIDAS 2.0**	Regulering van: • Elektronische identificatiemiddelen (eID's) • Elektronische vertrouwensdiensten • Elektronische attestatie van attributen Wallet
Digital gateway	**SDG**	Eén digitale toegangspoort voor informatie, procedures en diensten
Data	**DGA**	Kaders voor: • Hergebruik van beschermde overheidsgegevens • Datadeeldiensten • Data altruïsme • Europees Comité gegevensinnovatie
	DA	Kaders voor: • delen van data tussen bedrijven en consumenten (B2C) en tussen bedrijven en bedrijven (B2B) • Beschikbaarstellen data bij een uitzonderlijk behoefte/situatie • Dataportabiliteit • Interoperabiliteit
	Open data richtlijn	1. Beschikbaar stellen realtime data 2. High Value Data Sets 3. Data beschikbaar maken die publiek belang dienen 4. Verdere beperking van exclusieve overeenkomsten bij beschikbaarstelling van data

		Belangrijkste onderwerp
	Data Spaces	De eerste dataspaces: • Gezondheid • Mobiliteit • Industrie • Financiële diensten • Energie • Landbouw • Green Deal • Overheid • Vaardigheden (onderwijs en arbeidsmarkt)
	AI-act	Kaders voor AI-systemen: • Grondrechten en waarden • Rechtszekerheid garanderen om investeringen en innovatie te vergemakkelijken; • Beheer en handhaving bestaande wetgeving inzake grondrechten en veiligheidsvoorschriften • Ontwikkeling eengemaakte markt vergemakkelijken en voorkomen van marktversnippering • Conformiteitsbeoordelingen van hoog-risicosystemen met AI
Platform	**DSA**	Vier categorieën partijen waarvoor verschillende regels gelden: 1. Tussenhandelsdiensten die netwerkinfrastructuur aanbieden: internetproviders, domeinnaamregistrators, waaronder ook: 2. Hostingdiensten zoals cloud- en webhostingdiensten, waaronder ook: 3. Onlineplatforms waar verkopers en consumenten samenkomen, zoals onlinemarktplaatsen, appstores, deeleconomieplatforms en sociale media platforms 4. Zeer grote onlineplatforms vormen een bijzonder risico wat betreft de verspreiding van illegale inhoud en het toebrengen van schade aan de maatschappij. Er zijn specifieke regels vastgesteld voor platforms die meer dan 10% van de Europeanen (dus 45 miljoen gebruikers) bereiken.
	Urban air mobility	Regulering van onbemande voertuigen: • veilige uitvoering van de gewenste operatie • technische eisen • verkeersleidingssysteem waar noodzakelijk
Privacy en Security	**Cyberbeveiligings-verordening**	Europees kader op het gebied van cyberbeveiligingscertificering
	NIS 2	Voor gemeenten die als AED zijn aangemerkt geldt, dat het beheers-orgaan: • Genomen maatregelen voor het risicobeheer op het gebied van cyber-beveiliging goedkeuren, toezicht moeten houden op de uitvoering ervan en zijn verantwoordelijk voor de niet-naleving door de entiteiten van de verplichtingen. • Specifieke opleidingen moet volgen om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.
	ePrivacy verordening	Bescherming van persoonsgegevens rond de elektronische communicatie

3. Wat betekenen deze veranderingen[72] voor de gemeentelijke organisatie op hoofdlijnen?

Impact op hoofdlijnen

De impact van de bestaande en nieuwe digitale Europese wetten op de uitvoering van gemeenten is groot. Het aantal nieuwe wetten is zo groot dat er een strategie nodig op lokaal niveau waarin integraal gekeken wordt naar de digitale infrastructuur, beleidsdomeinen en organisatie. Volgens de geldende Europese planning moeten alle wetten eind 2026 geïmplementeerd zijn.

Bij de implementatie zijn er ook een aantal belangrijke afhankelijkheden waar een gemeente afhankelijk is van landelijke voorzieningen (vb digital identiteit en/of kenregistraties). Dit vraagt daarom om een interbestuurlijke strategie waarin helder is welke voorzieningen op EU, nationaal, regionaal en lokaal niveau beschikbaar komen.

In de verkenning wat de Europese digitale wetgeving op hoofdlijnen betekent voor gemeenten is, naast een analyse per wet, langs verschillende aspecten van de bedrijfsvoering gekeken naar de impact bij gemeenten. Hieronder is per organisatie-onderdeel kort in beeld gebracht wat de effecten zijn op de uitvoering.

Privacy en beveiliging
De eisen die gesteld worden veranderen niet, er zijn wel tal van nieuwe toepassingen bij waarvoor gegarandeerd moet zijn dat ze aan de gestelde eisen voldoen. Voorbeelden:

- Hotspots (wifitracking)
- Sensoren en algoritmes die transparant en uitlegbaar zijn conform de doelbinding van de GDPR/AVG
- Publiek private datadeling waardoor de inwoner regie krijgt over het zijn/haar datagebruik.
- Een beveiligde werkomgeving om het veilige hergebruik van persoonsgegevens en commercieel vertrouwelijke bedrijfsgegevens voor onderzoeks-, innovatie- en statistische doeleinden mogelijk te maken
- Afhandelen van verzoeken om data op grond van uitzonderlijke noodzaak
- Een rol als erkende datadeeldienst
- Het gebruik van wallets om mensen regie te geven over eigen gegevens.

Communicatie
Het grote aantal vernieuwingen dat het gevolg zal zijn van de Europese wetten vragen communicatie-inspanningen van de gemeenten. Het betreft zowel communicatie binnen de gemeente over de noodzakelijke veranderingen als communicatie naar inwoners en bedrijven. Hergebruik van gegevens is onderdeel van een aantal EU wetten, de invulling daarvan vraagt ethische afwegingen en politieke besluitvorming. Belangrijke onderwerpen voor de communicatie zijn:

- Praktisch: het cookie beleid, dat moet worden aangepast
- Communiceren over nieuwe mogelijkheden (regie op gegevens, uitbreiding digitale dienstverlening aan inwoners Europa bijvoorbeeld)
- Verantwoording richting toezichthouders over de gehele digitale infrastructuur.
- Urgentie en bewustwording vanuit het leiderschap (bestuurlijk en ambtelijk) van de gemeente gevraagd wordt.

Personeel
Een grote inspanning is voorzien in vergroten van leiderschap, kennis en uitvoeringscapaciteit om de Europese digitale wetgeving te implementeren, nieuwe technologie te begrijpen en in te kunnen kopen en de markt te kunnen sturen. Dit geldt op alle niveaus van de gemeentelijke organisatie. Het gaat om het daadwerkelijk doorgronden van de betekenis van digitale identiteiten, data(platformen), artificiële intelligentie (AI), cybersecurity en interoperabiliteit voor het uitvoeren van de gemeentelijk taken en het zichtbaar uitdragen ervan.

72 Hierbij wordt zowel gekeken naar de primaire processen als naar de bedrijfsvoeringsaspecten (security, communicatie, organisatie, personeel, administratieve organisatie, financiën, informatievoorziening, juridisch, technologie, huisvesting)

Administratieve organisatie
De administratieve organisatie moet worden aangepast om:
- De potentie van een integrale digitale infrastructuur effectief te implementeren (minder administratieve lasten)
- Aan een aantal nieuwe verplichtingen rond het delen van gegevens te kunnen voldoen (Data act, AI Act)
- Er nieuwe functionaliteiten zullen ontstaan zoals bijvoorbeeld nieuwe kernregistraties (AI en sensoren register),
- Om aan de informatieverplichtingen van SDG te voldoen (Engelstalige documenten op de website zetten)
- Voldoen aan het transactionele deel van SDG en data act
- Ook voldoen aan verplichtingen m.b.t. privacy en beveiliging (bijvoorbeeld transparantie, informatie verstrekken op basis van logging en bewaren / wissen van gegevens) kan aanpassingen van de administratieve organisatie vergen.

Informatievoorziening
De Europese agenda raakt de complete informatievoorziening van de gemeenten. Concreet zijn aanpassingen nodig om:
- Aan te sluiten op een aantal centrale voorzieningen
- Identificatie en authenticatie op alle betrouwbaarheidsniveaus te kunnen bieden
- De benodigde data uitwisseling tussen applicaties te faciliteren via standaarden en inkoopkaders
- Het applicatielandschap drastisch te vereenvoudigen en vervangen op basis van een adaptieve architectuur
- Effectieve inkoop om de markt te kunnen sturen.
- Integratie en beheer van sensoren en algoritmes onder regie van gemeenten te krijgen om de maatschappelijke rol te borgen.

Dat is nodig om gegevens (persoonsgegevens en andere gegevens) voor hergebruik beschikbaar te kunnen stellen en (grensoverschrijdend) digitale dienstverlening op een hoog kwaliteitsniveau te kunnen bieden. Het is zeer de vraag of dit realiseerbaar is door het aanpassen van het bestaande applicatielandschap, dat sterk langs de lijn van taakapplicaties (silo's) is georganiseerd. In dat landschap zijn koppelingen tussen applicaties die voor de Europese ambities op grote schaal gerealiseerd moeten worden bewerkelijk, weinig flexibel en duur, waarbij de realisatie lange doorlooptijden vraagt en het resultaat kwalitatief niet voldoende is om de Europese ambities waar te kunnen maken. Digitale dienstverlening staat, vergeleken met de ambities die bijvoorbeeld uit SDG annex 2 blijken, nog in de kinderschoenen.

Juridische aspecten
Het betreft wet- en regelgeving, juridische voorwaarden, overeenkomsten. Er zijn op een aantal punten aanpassingen nodig in de contracten die gemeenten hanteren: de inkoopcontracten met leveranciers om EU compliance en open standaarden (ten behoeve van interoperabiliteit) te borgen.

Daarnaast moet de toezichthoudende rol op nationaal niveau goed en eenduidig worden ingericht zodat gemeenten op een effectieve en efficiënte manier aan hun verantwoordingsverplichtingen kunnen voldoen.

4.2. Aanbevelingen

Dit onderzoek heeft een eerste verkennend beeld opgeleverd van de grote impact van relevante Europese digitale wetgeving op gemeenten. Het is van belang dat de VNG met voldoende daadkracht de benodigde inspanning en complexiteit om aan de wettelijke verplichtingen te voldoen voor het voetlicht brengt bij zowel het rijk als gemeenten. Het is nodig dat bewustwording, kennis en urgentie wordt gecreëerd, financiële middelen worden vrijgemaakt en gemeenten concreet geholpen worden om de Europese digitale wetgeving te implementeren en uit te voeren. Dit leidt tot de volgende aanbevelingen:

- Blijf de Europese wetten vanuit samenhang benaderen en zorg voor integratie met nationale kaders zoals de Werkagenda Waardengedreven Digitalisering van BZK.
- Zorg voor een verdieping op dit onderzoek door per wet een uitvoeringstoets uit te voeren op basis van de samenhang.
- Zorg voor een bewustwordingscampagne onder de leden om te borgen dat gemeenten zich bewust worden van de nieuwe Europese kaders en de deadline (2026) wanneer die geïmplementeerd moeten zijn.
- Ga in gesprek met het kabinet om de financiering voor de implementatie van de nieuwe Europese kaders te borgen. Beschikbaarheid van de benodigde financiële middelen is randvoorwaardelijk om gemeenten in staat te stellen aan hun verplichtingen te voldoen.
- Ontwikkel een instrumentarium, bijvoorbeeld een toolbox met menukaart voor gemeenten dat gemeenten helpt om zelf de nieuwe Europese kaders te implementeren.

Bewustwording, kennis en urgentie

De gemeenten staan voor de uitdagende taak om de komende jaren digitale identiteiten, data-(platformen), artificiële intelligentie (AI), cybersecurity en nieuwe technische infrastructuren verantwoord in te zetten en dit te vertalen naar commitment, urgentie, financiering en organisatieverandering. Gemeenten hebben hierbij niet alleen te maken met een juridische werkelijkheid, gebaseerd op normatieve kaders (hoe het zou moeten zijn), of een technische werkelijkheid (zoals cloudinfrastructuren, wallets, vertrouwensdiensten, federatieve datastelsels, datastructuren, api's, biometrie, machine learning) maar ook met hoe ze verantwoord invulling kunnen geven aan de gemeentelijke taakopvatting en het perspectief van de inwoner (ethiek en ambitie). Het nadenken over ethiek roept allerlei vragen op over (democratische) verantwoordelijkheden en transparantie over de afweging. Nieuwe technologieën waarvoor uit Europa kaders komen als digitale identiteit, artificiële intelligentie, de werking van algoritmes, cybersecurity en de nog onbekendheid hierover vormen hierbij een extra uitdaging. Deze uitdaging moet bovendien plaatsvinden gelijktijdig met de enorme opgave die gemeenten hebben bij de uitvoering van de maatschappelijke opgaven zowel in het sociale als fysieke domein. Het gaat niet meer om het sec implementeren van techniek en de waarborgen daarbij, maar om het transformeren van de gemeentelijk organisatie in de 'Digital Decade', waarbij het sociale, fysieke, bedrijfsvoerende en digitale samenkomt en integraal moet worden aangestuurd en uitgevoerd.

Opvolging van dit verkennend onderzoek

De beschrijvingen in dit rapport geven op hoofdlijnen een eerste kwalitatieve indicatie van de grote impact die de Europese digitale wetgeving op gemeenten heeft. De precieze impact en uitvoerbare doorlooptijd voor gemeenten zal verder moeten worden onderzocht per wet (o.a middels een uitvoeringstoets) en zeker ook in samenhang met elkaar en met de staande (digitaliserings) opgaven voor gemeenten. Daarnaast zijn de onderhandelingen van een aantal wetsvoorstellen nog in de beginnende fase en vinden er op moment van schrijven nog discussies plaats over fundamentele vraagstukken in de wet, bijvoorbeeld over de definitie van AI. Dit kan bepalend zijn voor de uiteindelijke wet, implementatie in Nederland en de impact op gemeenten.

Het structureel in beeld brengen van de (samenhangende) impact van relevante Europese digitale wetgeving kan helpen om op tijd bewustwording, urgentie, geld, tijd en prioriteit te organiseren bij gemeenten. Deze taak lijkt binnen VNG nu versnipperd te zijn, het is nodig om deze taak beter in te richten zodat dit onderzoek geen eenmalig karakter heeft. Hier ligt ook een mogelijkheid om via een meer integrale aanpak met voldoende daadkracht de gemeentelijke belangen in te brengen (samen met het rijk) in de vormgeving van de Europese digitale wetten.

Versterking middelen uitvoering

Gemeenten staan zoals gezegd voor grote complexe verandering: enerzijds de verplichtingen uit de Europese digitale wetgeving implementeren en anderzijds een digitale transformatie waarbij gemeenten opereren in een wereld van platformen, data-economie en digitale identiteiten. Dit is een complex traject. Dit legt een druk op de gemeentelijke middelen. Het is randvoorwaardelijk dat deze middelen voor gemeenten beschikbaar zijn.

Implementatie strategie en instrumenten om gemeenten te helpen

Het is nodig de Europese digitale wetgeving verplichtingen in lijn te brengen met de landelijke visie en Werkagenda waardengedreven digitalisering en te zorgen dat het voor gemeenten inzichtelijk wordt waar landelijk gezamenlijk aan gewerkt wordt en niet iedere individuele gemeenten het wiel zelf hoeft uit te vinden. En aan de andere kant ook instrumenten ter beschikking stellen die gemeenten helpen om bepaalde onderdelen zelf te implementeren.

Bijlage A: Gesprekspartners

Organisatie	Naam
Gemeente Den Haag	Evelyn Leiva Deantonio Michel Stam
Gemeente Amsterdam	Brit Stenberg
Gemeente Enschede	Wouter Asveld
VNG	Berend Alberts-de Gier Caspar Sluiter Dirk van Brederode Janneke de Zwaan Jonas Onland Kato Vierbergen Kim de Vries Maurice van Erven Max Tiemessen Minke van Velzen Sophie van Velzen Tim Kies

Bijlage B
Verkennende lijst met Europese digitale wetten

ePrivacy verordening
Cybersecurity Act
NIS Directive (Network & Information Systems)
NIS Directive 2
Single Digital Gateway
Open Data Directive
Data Governance Act
Data Act
AI Regulation (AI act)
Digital Services Act
Digital Markets Act
e-IDAS Regulation
e-IDAS 2.0 Regulation verordening inzake de Europese digitale identiteit
Urbain air mobility regulation

Bijlage C: Samenvatting impact

4.8. Samenvattend: Belangrijkste kostencompenten per bedrijfsvoeringsaspect

Bedrijfsvoeringsaspect	Op hoofdlijnen: Kostencomponenten
Privacy en Security	Elektronische communicatiegegevens beveiligen (bijv voor hotspots (wifitracking) in openbare ruimte en ook voor sensoren (internet of things)
	Zorgen voor veilige verwerkingsomgeving voor data-analyses met her te gebruiken persoonsgegevens en commercieel vertrouwelijke bedrijfsgegevens voor onderzoeks-, innovatie- en statistische doeleinden.
	Inzetten van privacy bevorderende technologieën (als anonimisering, pseudonimisering, generalisering, onderdrukking en randomisering)
	Omvattende aanpak op het gebied van gegevensbescherming inrichten en beheren (aanvullende (tov AVG) technische en organisatorische maatregelen treffen)
	Inrichten en beheren beveiligingsniveaus met nieuwe toegangsmiddelen en vertrouwensdiensten
	Als aanbieder van essentiële diensten (AED) risicoanalyse en extra maatregelen uitvoeren voor het beheer van cyberbeveiligingsrisico's
	Voldoen aan Europese of internationaal aanvaarde normen en specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen
Communicatie	EU-cyberbeveiligingscertificaten inzetten
	Recht op eerbiediging van communicatie waarborgen door het gebruik van cookies inrichten met specifieke en geïnformeerde toestemming
	Transparant zijn over AI-inzet
	Gebruik van data bevorderen en verzekeren dat de waarde uit data gelijkwaardiger wordt verdeeld
	Online zaken regelen mogelijk maken door identificatie en authenticatie middelen voor burgers en bedrijven in te zetten
	Burgers en bedrijven regie geven in het delen van informatie voor bepaalde diensten als dat nodig is
	Gericht op EU-inwoners en bedrijven: • Informatie verstrekken over de regels, procedures en diensten (in het Engels) • Volledig online de voorgeschreven procedures aanbieden (in het Engels)

Bedrijfsvoeringsaspect	Op hoofdlijnen: Kostencomponenten
Organisatie (Besturing en control)	Conformiteitsbeoordelingen van hoog-risicosystemen met AI
	Voor gemeenten die als AED zijn aangemerkt geldt, dat het beheersorgaan: • Genomen maatregelen voor het risicobeheer op het gebied van cyber-beveiliging goedkeuren, toezicht moeten houden op de uitvoering ervan • Specifieke opleidingen moet volgen om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.
	Voor het beheersorgaan van de gemeente geldt dat: • Goedkeuring moet worden gegeven op de maatregelen • Toezicht moet worden gehouden op uitvoering van genomen maatregelen en verantwoordelijk zijn voor de niet-naleving door de entiteiten van de verplichtingen. • Specifieke opleidingen moet worden gevolgd om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.
	Gemeenten moeten verantwoording afleggen over de veilige en betrouwbare inzet van eID middelen
	Gemeenten als gegevensbemiddelingsdienst moeten structurele scheiding tussen deze dienst en alle andere geleverde diensten organiseren
	Voor online platforms gelden nieuwe verplichtingen, dat moet een gemeenten organiseren wanneer ze zelf een platform aanbiedt
	Er worden verschillende toezichthouders en handhavingsregimes voor de digitaliseringsopgaven voorgesteld. De vraag is hoe dit uitgewerkt wordt in Nederland. Voor gemeenten is het belangrijk dat dit zoveel als mogelijk integraal gebeurd om te voorkomen dat gemeenten met een verscheidenheid aan toezichthouders en handhavingsmechanismen te maken krijgen en daarmee worden opgezadeld met een grote administratieve last.
Personeel	Een grote inspanning is voorzien in vergroten van leiderschap, kennis en uitvoeringscapaciteit om de Europese digitale wetgeving te implementeren. Dit geldt op alle niveaus van de gemeentelijke organisatie. De kaders uit de EU helpen in het reguleren van de veranderende machtsstructuren in de data (platform) economie, maar het vergt leiderschap om de waarde van de Europese digitale (data) strategie te kunnen voorstellen en deze te vertalen naar wat dit betekent voor de gemeentelijk uitvoering en inwoners en bedrijven. Dit leiderschap vraagt een mindset waarin een data (platform) economie en daarbij behorende mechanismes een belangrijke strategische rol spelen. Het gaat om het daadwerkelijk doorgronden van de betekenis van digitale identiteiten, data(platformen), artificiële intelligentie (AI), cybersecurity etc. voor het uitvoeren van de gemeentelijk taken en het zichtbaar uitdragen van de mogelijkheden van deze digitale identiteiten, data, AI, en het verantwoord inzetten hiervan en dit te vertalen naar commitment, urgentie, financiering en

Bedrijfsvoeringsaspect	Op hoofdlijnen: Kostencomponenten
	organisatieverandering. Gemeenten hebben hierbij niet alleen te maken met een juridische werkelijkheid, gebaseerd op normatieve kaders (hoe het zou moeten zijn), of een technische werkelijkheid (cloudinfrastructuren, wallets, vertrouwensdiensten, federatieve data-stelsels, datastructuren, api's, biometrie, machine learning, etc) maar ook met hoe ze verantwoord invulling kunnen geven aan de gemeente-lijke taakopvatting (ethiek en ambitie). Het nadenken over ethiek roept allerlei vragen op over (democratische) verantwoordelijkheden en transparantie over de afweging. Nieuwe technologieën waarvoor uit Europa kaders komen als digitale identiteit, artificiële intelligentie, de werking van algoritmes, cybersecurity en de nog onbekendheid hierover vormen hierbij een extra uitdaging.
Administratieve organisatie (processen)	Processen zodanig inregelen dat voor hergebruik geschikte gegevens eenvoudig beschikbaar komen, zoals: • Zorgen dat verzoeken tot hergebruik van gegevens binnen gestelde termijn worden afgehandeld • Inregelen dat exclusieve overeenkomsten die moeten worden gedeeld ook beschikbaar komen voor andere partijen • Potentiële hergebruikers helpen bij het vragen van toestemming van de betrokkene om zijn persoonsgegevens te hergebruiken • Proces inrichten zodat degenen die hun gegevens delen (in geval van data-altruisme), gemakkelijk hun toestemming kunnen geven en intrekken
	AI-systemen risicogericht inventariseren en voor deze systemen vervolgens de verplichtingen uitvoeren en inbedden in uitvoeringsprocessen om aan de eisen voldoen.
	Voor 82 SDG producten de (Nederlandse en Engelse) standaard-teksten controleren, aan te vullen met gemeente specifieke informatie en te publiceren in de invoervoorziening Daarna moeten gemeenten de informatie zelf onderhouden.
	Voor transactionele deel van de SDG ('Annex II') zorgen dat de voorgeschreven producten volledig online af te handelen zijn van aanvraag tot en met het resultaat (vaak een 'besluit')
	Toestemmingsproces rond cookies inrichten
	Als aanbieder van de elektronische-communicatiedienst de inhoud van de elektronische communicatie wissen of deze gegevens anoniem maken wanneer dit niet langer nodig is voor de verwerking.
Informatievoorziening	Aansluiten op (mogelijke) generieke voorzieningen • Verwerkingsomgeving voor data-analyses • Centraal data informatiepunt (data.overheid.nl) • Federatief (basis) registraties netwerk (dataruimten) • Eu Once-Only Technical System (OOTS): technische ondersteuning eenmaligheidsbeginsel (burgers mogen niet gedwongen worden om informatie aan autoriteiten te verstrekken als een andere autoriteit die informatie al in elektronische vorm bezit) • Aansluiten op eID middelen (zoals als wallet) • Aansluiten op de SDG voorziening

Bedrijfsvoeringsaspect	Op hoofdlijnen: Kostencomponenten
	Verwerkingsomgeving inrichten en beheren om hergebruik van gegevens mogelijk te maken
	Voldoen aan de eisen voor hergebruik van data als portabiliteit, interoperabiliteit, standaardisatie.
	API's voor hergebruik (realtime) data inzetten en beheren
	Extra data beschikbaar maken (als (beschermde binnen wettelijke kaders) overheidsgegevens, uitzonderlijke situaties, highvalue lijst) via data.overheid.nl en/of gemeentelijke data portalen
	Online afhandelen van procedures voor EU burgers en bedrijven mogelijk maken
	Elektronisch betalen mogelijk maken met algemeen beschikbare grens-overschrijdende betaaldiensten
	Inrichten en beheren specifieke en geïnformeerde toestemming voor-ziening voor verwerken elektronische communicatie gegevens (als cookies)
	Digitale producten en processen aanpassen eID middelen (als wallet en OOTS)
	Verzamelen en verwerken van altruïstische gegevens inclusief (opvragen en intrekken van) toestemmingsproces
	Gegevens als 'open data' aanbieden via een portaal, website of API, waarmee verzoeken om hergebruik in velerlei gevallen automatisch kunnen worden afgehandeld
Juridisch (wet- en regelgeving/ juridische voorwaarden/ overeenkomsten)	Inkoopvoorwaarden aanpassen/opstellen zodat aan leveranciers eisen en wensen gesteld worden over informatiemodellen en standaarden, privacy, veiligheid, publieke waarden en mensenrechten
	Vastleggen in contracten dat de opgevraagde data alleen voor het tevoren geformuleerde doel mag worden gebruikt, niet voor opsporings-doeleinden.
	Opgevraagde gegevens mogen voor statistiekdoeleinden en voor non-profit onderzoek worden doorgeleverd door de overheid. De datahouder wordt hierover geïnformeerd
	Zorgen dat het mogelijk wordt dat gebruikers bepalen welke data met wie gedeeld wordt en dat gebruikers geïnformeerd moeten worden over de benodigde attributen en gegevens voor afname van een concrete dienst, die alleen gedeeld mogen worden als dit in overeenstemming is met nationaal recht en niet meer dan voor het gebruik van een bepaalde dienst noodzakelijk is.
	Data-eigendom regelen in overeenkomsten met leveranciers
	Bij exclusieve overeenkomsten bij beschikbaarstelling van data, de bijbehorende publicatie/ hergebruik verplichting afspreken

Bedrijfsvoeringsaspect	Op hoofdlijnen: Kostencomponenten
	Aanpassen van contracten met externe onderzoeksbureaus, zodat de verplichting om de gebruikte onderzoeksdata terug te leveren aan de gemeente in deze contracten kan worden opgenomen.
	Voldoen aan gemeenschappelijk Europees toestemmingsformulier voor gegevensaltruïsme

Bijlage D: Gebruikte bronnen

Rapporten en studies

VNG: AI position paper VNG, april 2022 [74]
Impactanalyse eIDAS-verordening, 2017 [75]
Single Digital Gateway, april 2019 [76]
GDI meerjarenvisie, februari 2022 versie 0.8 [77]
Position Paper VNG Digital Service Act NL_541943486
Aanzet voor een visie op U-space. Rapport Deloitte in opdracht van het Ministerie van Infrastructuur en Waterstaat. Juli 2021
Kansen voor drones – Visie op de inzet van drones, Ministerie van Infrastructuur en Milieu, 2017
Verkenning ewallets en speelveld analyse, januari 2022 [78]
Interbestuurlijke datastrategie, oktober 2021 [79]

Internetsites geraadpleegd in periode juni-augustus 2022

ePrivacy verordening
- https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf
- https://europadecentraal.nl/onderwerp/digitale-overheid/privacy/eprivacy-verordening/
- https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained
- Europese data strategie: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_nl en COM(2020)66: A European strategy for data: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

Data Governance Act
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
- https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
- https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114

Data act
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN
- Wet implementatie Open data richtlijn: https://www.internetconsultatie.nl/wetimplementatieopendatarichtlijn/b1
- https://vng.nl/nieuws/impactanalyse-eu-open-datarichtlijn
- https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces
- https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en

AI-act
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Cyberbeveiligingsverordening
- https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32019R0881
- https://vng.nl/wetsvoorstellen/uitvoeringswet-cyberbeveiligingsverordening
- NIS2: https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf
- https://www.government.nl/latest/news/2022/06/23/cybersecurity-measures-in-more-sectors-will-improve-digital-security-in-the-netherlands-and-the-eu

74 https://vng.nl/sites/default/files/2022-04/VNG%20Position%20paper%20Kunstmatige%20intelligentie%20%28AI%29_0.pdf
75 https://vng.nl/sites/default/files/2022-06/Impactanalyse-eIDAS-verordening-2017.pdf
76 https://vng.nl/kennisbank-impactanalyse?term=sdg&sort_bef_combine=created_DESC
77 https://pgdi.nl/file/download/76e7b281-9905-4848-95b6-0c79eadf9a5a/20220309-kggo-05-meerjarenvisie-gdi.pdf
78 https://www.rijksoverheid.nl/documenten/rapporten/2022/01/11/verkenning-ewallets-speelveldanalyse
79 https://www.rijksoverheid.nl/documenten/rapporten/2021/10/31/nl-digitaal-interbestuurlijke-datastrategie-nederland

SDG
- https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX%3A32018R1724

eIDAS verordening
- https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32014R0910&from=RO

Europese digitale identiteit verordening
- https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0281
- https://www.rijksoverheid.nl/documenten/kamerstukken/2022/08/17/kamerbrief-voortgang-europese-digitale-identiteit
- https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

DSA
- https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN
- https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_nl
- "Digitale en fysieke wereld komen samen in gemeenten" - Digitale Overheid, interview met Nathan Ducastel
- DMA: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN
- https://ec.europa.eu/competition-policy/sectors/ict/dma_en

Urban air mobility
- https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R0945
- https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R0947&from=SK
- https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32021R0664
- https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52021PC0665
- https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32021R0666
- Mvt: https://www.internetconsultatie.nl/wetimplementatieopendatarichtlijn/b1
- https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/wet-en-regelgeving/
- https://geonovum.github.io/eu_regelingen_datastrategie/
- https://www.rijksoverheid.nl/documenten/publicaties/2020/11/25/fiche-2-verordening-data-governance-act
- https://www.rijksoverheid.nl/documenten/publicaties/2022/02/23/fiche-1-dataverordening
- https://www.rijksoverheid.nl/documenten/vergaderstukken/2021/05/31/fiche-2-verordening-betreffende-kunstmatige-intelligentie
- https://www.eerstekamer.nl/eu/behandeling/20210709/brief_van_de_minister_van
- https://www.rijksoverheid.nl/documenten/richtlijnen/2020/12/16/fiche-5-herziening-richtlijn-netwerk-en-informatiebeveiliging-nib-richtlijn
- https://www.eerstekamer.nl/eu/behandeling/20170217/brief_regering_fiche_vervanging/info

Besluit sturing van de digitale overheid:
- https://zoek.officielebekendmakingen.nl/stcrt-2022-18861.html
- https://wetten.overheid.nl/BWBR0009950/2022-05-01/#Hoofdstuk18_Artikel18.15a
- https://vng.nl/sites/default/files/2022-02/Brief%20aan%20BZK%20Consultatie%20wetsvoorstel%20Open%20data%20richtlijn.pdf
- https://werkenaaneenoverheid.pleio.nl/groups/view/ed87e451-f6fc-49b0-aec4-41f2358426f7/single-digital-gateway/wiki/view/09fa2d17-dc94-4c5f-ab8f-875a9fb5e701/veelgestelde-vragen-over-single-digital-gateway-voor-gemeenten
- https://vng.nl/sites/default/files/2022-04/impactanalyseSingleDigital%20Gateway.pdf
- https://ddma.nl/legal/wetgeving/digital-service-markets-act/
- https://digital-strategy.ec.europa.eu/en/activities/digital-programme
- https://www.noraonline.nl/wiki/GDI-Architectuur_(GA)