Interprovinciaal Overleg
van, voor en door provincies

Handreiking digitaliseringswetgeving voor provincies

Impact Europese en Nederlandse wet- en regelgeving

8 APRIL 2026

Interprovinciaal Overleg
Gezamenlijke provincies
WWW.IPO.NL

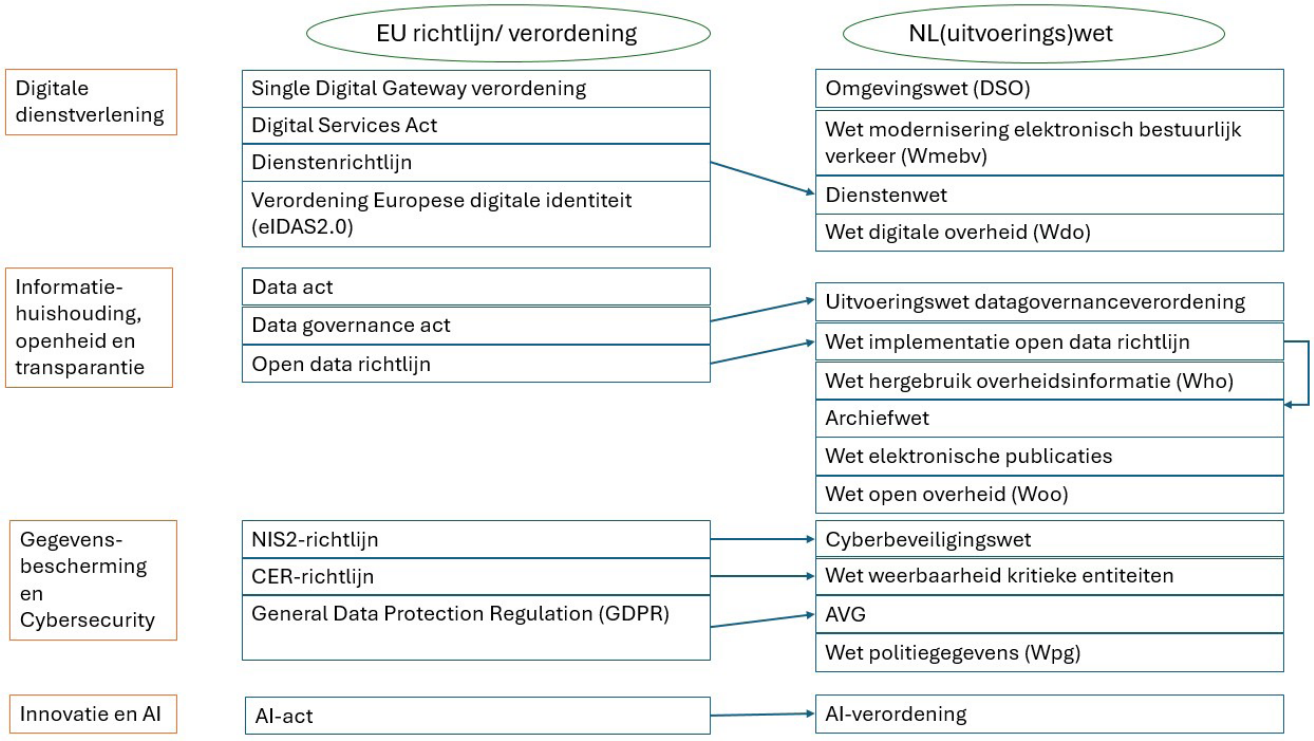
Inhoudsopgave

1. Inleiding

Om richting en kaders te geven aan de groeiende digitalisering binnen de overheid is er de afgelopen jaren een aanzienlijk aantal Europese richtlijnen en verordeningen en Nederlandse wetgeving aangenomen. De Europese Unie bestempelde het huidige decennium tot 'Digital Decade' en stelde een bijbehorende visie en strategie op. Dit vertaalt zich in verordeningen en richtlijnen, zoals de Data Governance Act, Data Act, AI-verordening, NIS2-richtlijn en de eIDAS2.0 verordening. Daarnaast zijn er ook Nederlandse wetten opgesteld op het gebied van digitalisering, zoals de Wet modernisering elektronisch bestuurlijk verkeer, de Wet digitale overheid, de Wet open overheid en de Cyberbeveiligingswet. Een groot deel van deze wetten geeft uitvoering aan Europese richtlijnen en verordeningen. Zo wordt bijvoorbeeld de NIS2-richtlijn geïmplementeerd middels de Cyberbeveiligingswet, de Dienstenrichtlijn middels de Dienstenwet en de Open data richtlijn middels de Wet hergebruik overheidsinformatie.

1.1 Samenhang digitale wetgeving

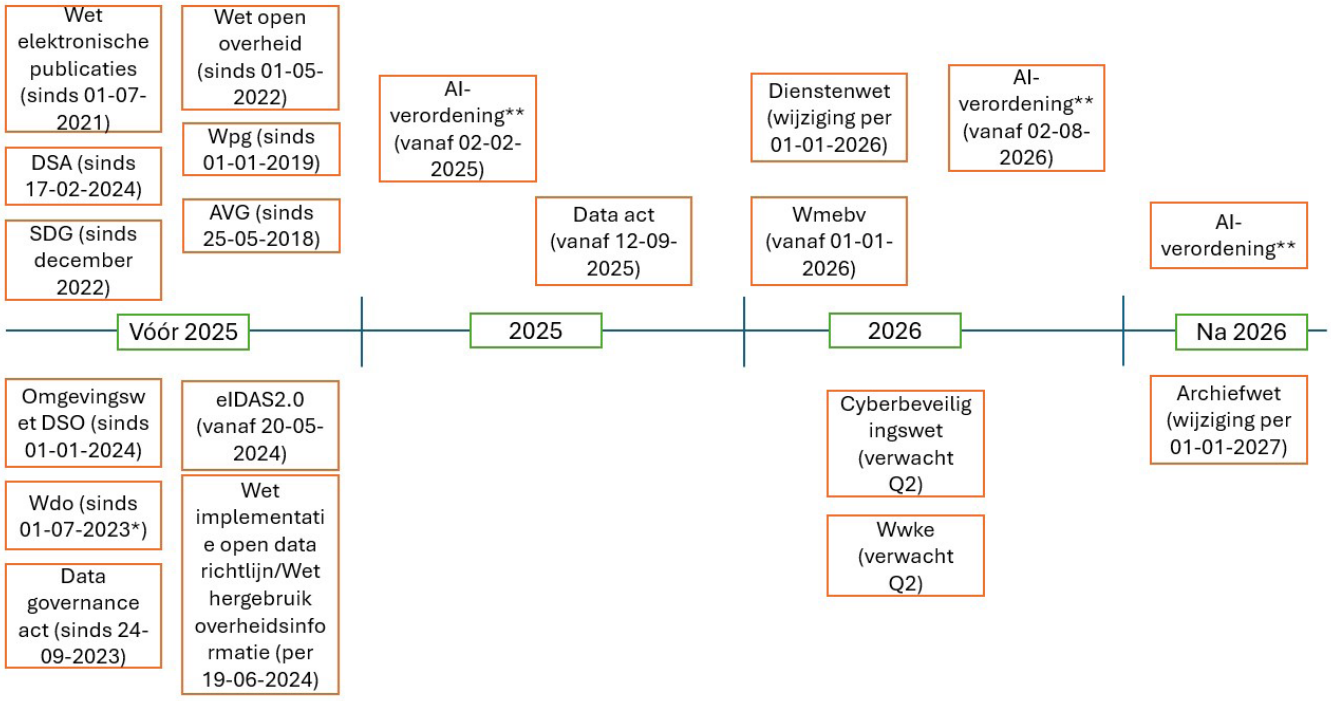
In onderstaande figuur is de samenhang tussen de EU richtlijnen en verordeningen en de Nederlandse (uitvoerings)wetten schematisch weergegeven. De richtlijnen, verordeningen en wetten zijn onderverdeeld in vier wetgevingsclusters: digitale dienstverlening, informatiehuishouding, openheid en transparantie, gegevensbescherming en cybersecurity en innovatie en AI.



Figuur 1 – Samenhang tussen de EU richtlijnen en verordeningen en de Nederlandse (uitvoerings)wetten.

1.2 Tijdlijn

De tijdlijn van inwerkingtreding van de hierboven genoemde richtlijnen, verordeningen en wetten is weergegeven in onderstaande figuur.



Figuur 2 - Tijdlijn van inwerkingtreding van de richtlijnen, verordeningen en wetten.

*met een aansluitschema per organisatie wordt bepaald vanaf wanneer een organisatie precies moet voldoen
** treedt gefaseerd in werking: 2 feb 2025: AI voor algemene doeleinden voldoet aan AI-verordening, 2 aug 2026: Nieuwe en substantieel gewijzigde AI-systemen voldoen aan AI-verordening, 2 aug 2030: Alle AI-systemen bij overheidsinstellingen voldoen aan vereisten AI-verordening

1.3 Ontwikkelingen

EU

Een actueel overzicht van ontwikkelingen vanuit de EU op het gebied van digitale wetgeving is beschikbaar via de EU-wetgevingsmonitor: https://eu-wetgevingsmonitor.realisatieibds.nl/

Ook de Tijdlijn Digitalisering van het Kenniscentrum Europa Decentraal (KED) biedt een handig overzicht van relevante wet- en regelgeving en andere initiatieven vanuit de EU: https://europadecentraal.nl/tijdlijn-digitalisering/

Nederland

Een actueel overzicht van (aankomende) Nederlandse wetgeving is te vinden in de wetgevingskalender: https://wetgevingskalender.overheid.nl/

Digitale Omnibus

De Europese Commissie presenteerde op 19 november 2025 het digitale omnibuspakket. Dit is een wetsvoorstel dat diverse EU richtlijnen en verordeningen wijzigt. Het digitale omnibuspakket is bedoeld om de EU-regelgeving te stroomlijnen en te harmoniseren, administratieve lasten te verlagen, innovatie en concurrentiepositie te bevorderen en te zorgen voor efficiëntere compliance–processen, terwijl het fundamentele beschermingsniveau behouden blijft. Als het Europees Parlement en de Europese Raad met de voorstellen hebben ingestemd, worden deze aangenomen. Dit proces wordt naar verwachting eind 2026 afgerond. Dan is er meer duidelijkheid over de exacte wijzigingen en maatregelen, die naar verwachting midden 2027 van kracht worden. Provincies kunnen op verschillende momenten reageren op raadplegingen, dit wordt vanuit het Huis van de Nederlandse Provincies (HNP) in samenwerking met IPO gecoördineerd[1].

1 Het IPO werkt daarbij ook nauw samen met de VNG.

1.4 Wetgeving als organisatieopgave

Wetgeving en het implementeren daarvan is niet enkel een juridisch vraagstuk, maar juist een onderwerp dat alle lagen van de organisatie raakt. Het is onlosmakelijk verbonden aan de core business die verschillende teams uitvoeren. Wetgeving vereist structurele aandacht, want door wijzigingen en toevoegingen is wetgeving nooit 'af' maar moet deze ook als het ware 'beheerd' worden. Dit beheer moet goed geborgd worden in de organisatie met duidelijk eigenaarschap. Het implementeren van wetgeving vraagt om interdisciplinaire samenwerking op het gebied van beleid, techniek en informatiebeheer.
Als organisatieopgave vraagt het bovendien om bestuurlijke regie en vaak is er een gedragsverandering nodig binnen de organisatie. Uit gesprekken met de provincies blijkt dat dit nog niet in alle provincies op deze manier gezien wordt, waardoor de implementatie van wetgeving vaak versnipperd is en eigenaarschap niet duidelijk ingericht is. Daardoor krijgen niet alle wetten de aandacht die nodig is om als provincie tijdig te kunnen voldoen aan de verplichtingen.

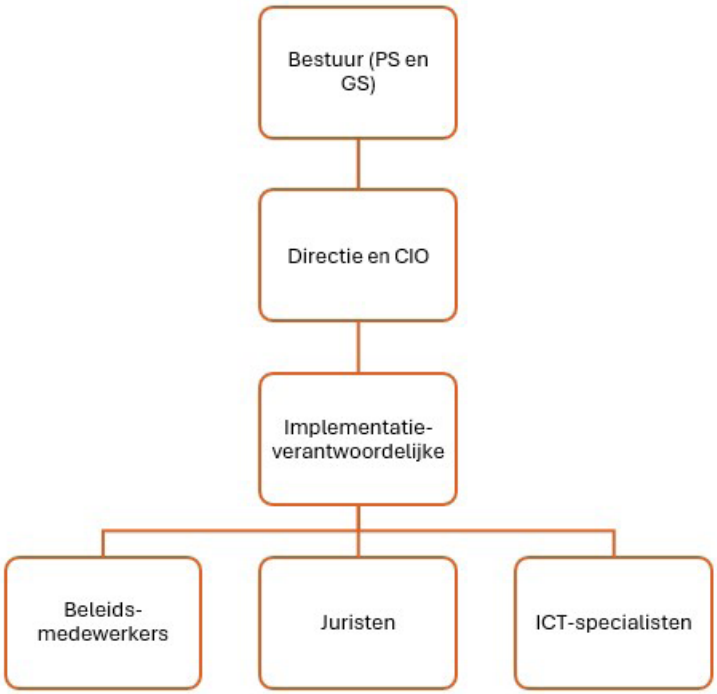
Voor het succesvol toepassen van wetgeving is het belangrijk dat het bewustzijn onder medewerkers hoog is en dat er voldoende kennis aanwezig is. Voor onderwerpen als bijvoorbeeld informatieveiligheid, het verantwoord inzetten van AI en het alert zijn op datalekken is het cruciaal dat alle medewerkers weten wat de spelregels zijn. Bij het implementeren van wetgeving moet het doel dan ook niet alleen zijn om compliant te zijn aan de regels, maar ook om ervoor te zorgen dat medewerkers een basis kennisniveau hebben dat passend is bij hun functie. Medewerkers moeten weten wat er van hen verwacht wordt en waar zij terecht kunnen met vragen.

De wetgeving waar provincies op dit moment mee te maken hebben of binnenkort gaan krijgen bestaat bovendien niet uit geheel op zichzelf staande wetten. Er is namelijk in sommige gevallen sprake van enige overlap waarbij verschillende wetten aanpassingen aan dezelfde systemen of processen kunnen vereisen. Het is dus belangrijk om deze wetten in samenhang te zien om efficiënte en effectieve implementatie mogelijk te maken. Het hoge tempo waarmee nieuwe verordeningen, richtlijnen en wetten in de Digital Decade op provincies afkomen is een andere belangrijke reden om de implementatie gestructureerd aan te pakken.

Bij het implementeren van de grote hoeveelheid wetten is een prioritering nodig. Afhankelijk van de uitgangspositie van een provincie moeten er onder andere keuzes gemaakt worden met betrekking tot het ambitieniveau (wil een provincie voorloper zijn of een volgende rol aannemen?), beschikbare capaciteit (hoeveel tijd, geld en expertise wordt er beschikbaar gesteld?), de mate waarin de risico's van het niet tijdig voldoen aan een wet geaccepteerd kunnen worden (wat is de 'risk-appetite'?) etc. Op basis van een risicoafweging kunnen keuzes in prioritering gemaakt worden op bestuurlijk- en directieniveau en kunnen er heldere opdrachten aan de organisatie gegeven worden.

1.5 Rollen en verantwoordelijkheden

Uit gesprekken met provincies komt naar voren dat niet zozeer onbekendheid met wet- en regelgeving, maar vooral gebrek aan eigenaarschap een risico vormt voor het tijdig voldoen aan wet- en regelgeving. Er is een goede governancestructuur nodig om wetten te implementeren waarbij taken en verantwoordelijkheden voor iedereen helder zijn. Afhankelijk van de wet en de activiteiten die ondernomen moeten worden kunnen verschillende rollen betrokken worden. Daarbij is het belangrijk om op te merken dat, afhankelijk van de organisatie-inrichting, bepaalde rollen andere benamingen hebben of niet aanwezig zijn in alle provincies. Ook kunnen er additionele rollen voorkomen in provincies. In de basis zal een structuur in ieder geval uit een aantal lagen bestaan. Deze lagen worden hieronder kort toegelicht. Dit overzicht is, gelet op bovenstaande kanttekeningen, geen uitputtend overzicht maar geeft een algemeen beeld van de benodigde kennis en capaciteiten:



Figuur 3 - Benodigde rollen bij de implementatie van digitaliseringswetgeving.

*De rol van implementatieverantwoordelijke kan een aparte rol zijn, maar kan ook belegd zijn bij een bestaande rol (bijvoorbeeld beleidsmedewerker, jurist of ICT-specialist)

Bestuur

De Gedeputeerde Staten nemen bestuurlijke besluiten over aanpak en prioritering en leggen hierover verantwoording af aan de Provinciale Staten. Uit de gesprekken blijkt dat de bestuurlijke aandacht op het gebied van digitaliseringswetgeving vaak onvoldoende aanwezig is. Onderwerpen als AI en Cybersecurity krijgen tegenwoordig wel meer aandacht, maar voor een groot deel van de wetten is dat niet het geval.

Directie en CIO

De mate waarin digitaliseringswetgeving op het netvlies van de directie staat verschilt per provincie. Dit heeft gevolgen voor de capaciteit en middelen die een provincie beschikbaar stelt voor de implementatie van wetgeving. De CIO bewaakt de samenhang tussen processen, beleid en informatiearchitectuur.

Implementatieverantwoordelijke

Idealiter is er voor elke wet een persoon aangewezen die het eigenaarschap voor de implementatie van die wet heeft. Dit kan een project- of programmamanager zijn of een andere medewerker bij wie deze taak belegd is. Deze persoon legt verantwoording af aan de ambtelijk opdrachtgever. Nadat een wet geïmplementeerd is, is het belangrijk dat deze in beheer blijft zodat er gereageerd kan worden op eventuele latere wijzigingen of toevoegingen. Ook hier moet een eigenaar voor aangewezen worden, die de ontwikkelingen volgt.

Juristen, ICT-specialisten en beleidsmedewerkers

Bij het implementeren van wetgeving is er expertise vanuit verschillende specialisten nodig. Juristen interpreteren wetgeving en adviseren over verplichtingen, risico's en andere juridische vraagstukken. ICT-specialisten vertalen wetgeving naar systeemaanpassingen en zorgen voor de benodigde technische aanpassingen in processen, applicaties en koppelingen. Beleidsmedewerkers vertalen wettelijke verplichtingen naar provinciaal beleid en uitvoeringskaders. Er zijn afhankelijkheden tussen deze disciplines, maar iedere groep heeft ook duidelijk zijn eigen taken. Het is belangrijk dat de samenwerking gecoördineerd wordt door de implementatieverantwoordelijke.

Andere mogelijke rollen

Naast juristen, ICT-specialisten en beleidsmedewerkers zijn er ook andere rollen die mogelijk een rol spelen bij het implementeren van een wet. Zo kunnen financiële specialisten nodig zijn voor het in kaart brengen van de financiële gevolgen van een wet. Communicatieadviseurs kunnen een rol spelen bij het informeren van interne medewerkers en externe stakeholders over de veranderingen die nieuwe wetten met zich meebrengen. Wanneer er trainingen nodig zijn over nieuwe werkwijzen kunnen HR-specialisten hier mogelijk een rol in spelen. Ook kan wetgeving impact hebben op de manier waarop informatie en data beheerd wordt, waardoor ook informatiebeheerders en data-specialisten mogelijk betrokken moeten worden. Afhankelijk van de organisatiestructuur van een provincie kunnen er nog andere rollen relevant zijn.

1.6 Over deze handreiking

De hierboven genoemde verordeningen, richtlijnen en wetten raken ook provincies. Om de impact voor provincies in kaart te brengen heeft het IPO een impactanalyse uitgevoerd. Het gaat daarbij om WAT provincies moeten doen, niet HOE ze dat moeten doen. Dat kan voor elke provincie anders zijn vanwege verschillen in organisatiestructuur, beschikbare capaciteit en middelen, uitgangssituatie en bestuurlijke keuzes die gemaakt worden (bijvoorbeeld ten aanzien van prioritering). Vanuit het IPO zijn er verschillende interprovinciale vakgroepen en werkgroepen actief die zich onder andere bezighouden met vraagstukken op het gebied van de verschillende verordeningen, richtlijnen en wetten.

De resultaten van de impactanalyse zijn in deze handreiking terug te vinden. Per richtlijn/verordening/wet is in kaart gebracht welke verplichtingen er zijn, welke recente ontwikkelingen er zijn en wat de impact van deze verplichtingen op provincies is. Deze handreiking is bedoeld voor managers, beleidsadviseurs, informatiemanagers en andere professionals binnen de provincies die zich bezig houden met het doorvertalen van wetgeving naar organisatieopgaves. Het biedt een overzicht op hoofdlijnen, dat voor provincies als startpunt kan dienen voor nadere uitwerking in bijvoorbeeld actieplannen of implementatieplannen. Bij die uitwerking is het van belang om ook juridische en technische expertise binnen de provincie te betrekken.

Er zijn al diverse impactanalyses uitgevoerd door het IPO zelf of door onderzoeksbureaus. Ook de Vereniging van Nederlandse Gemeenten (VNG), de Unie van Waterschappen (UvW) en het Kenniscentrum Europa Decentraal (KED) hebben impactanalyses uitgevoerd en producten zoals handreikingen, implementatiesteunen en checklists ontwikkeld. Voor het opstellen van deze handreiking was het dan ook niet de bedoeling om het wiel opnieuw uit te vinden, maar is er vooral gebruik gemaakt van bestaande bronnen. Per richtlijn, verordening of wet wordt verwezen naar de relevante stukken.

De richtlijnen, verordeningen en wetten kunnen worden ingedeeld in vier wetgevingsclusters: digitale dienstverlening, informatiehuishouding, openheid en transparantie, gegevensbescherming en cybersecurity en innovatie en AI. De vier wetgevingsclusters komen in de hoofdstukken hieronder aan bod. Per cluster worden de richtlijnen, verordeningen en wetten verder toegelicht volgens de hierboven beschreven methode. In hoofdstuk 6 wordt de samenhang en overlap tussen de wetten in beeld gebracht. Bijlage A bevat een lijst van alle bronnen waar in de handreiking naar verwezen wordt.

2. Digitale dienstverlening

Het wetgevingscluster digitale dienstverlening bevat de richtlijnen, verordeningen en wetten die betrekking hebben op de digitale dienstverlening van provincies. Het gaat daarbij om:

- Single Digital Gateway verordening (SDG) (EU verordening)
- Digital services act (DSA) (EU verordening)
- Dienstenwet (NL uitvoeringswet van een EU richtlijn, namelijk de Dienstenrichtlijn)
- eIDAS2.0 (EU verordening)
- Omgevingswet (DSO) (NL wet)
- Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) (NL wet)
- Wet digitale overheid (Wdo) (NL kaderwet)

2.1 Single Digital Gateway verordening (SDG)

De Single Digital Gateway verordening (SDG) is een Europese verordening met als doel om burgers en bedrijven makkelijk toegang te geven tot digitale overheidsdienstverlening in de hele Europese Unie. Het portaal (de 'gateway') Your Europe dient daarbij als centrale toegangspoort en verwijst gebruikers door naar de juiste websites in de verschillende lidstaten. Via Your Europe kunnen burgers en bedrijven op een eenvoudige manier betrouwbare informatie vinden over overheidsdiensten, -producten en -procedures in Europa. Sommige procedures kunnen ze bovendien online doorlopen. Het grootste deel van de diensten van provincies die hierdoor geraakt worden valt onder de Omgevingswet. De toegang hiervoor loopt via het DSO.

2.1.1 Verplichtingen uit de wet

De SDG-verordening bestaat uit 3 onderdelen:

- Annex 1 (Informatie): Overheidsorganisaties moeten online informatie verstrekken over diensten die relevant zijn bij grensoverschrijdende activiteiten. Denk aan reizen, werk, pensioen, voertuigen, verblijf, onderwijs, gezondheidszorg en burger- en familierechten. Deze informatie moet aan bepaalde kwaliteitseisen voldoen en beschikbaar zijn in het Nederlands en Engels.
- Annex 2 (Procedures en Once Only Technical System): Daarnaast moeten overheidsorganisaties relevante procedures voor grensoverschrijdende gebruikers digitaal toegankelijk maken. Denk aan procedures voor verhuizen, een bedrijf starten of studeren. Voor provincies heeft dit meestal met vergunningen te maken.
- Annex 3 (Hulp en ondersteuningsdiensten): Ondersteuningsdiensten moeten ook online beschikbaar zijn voor gebruikers die hulp nodig hebben bij de ontsloten informatie en procedures.

Het online verstrekken van informatie via Your Europe (annex 1) is verplicht vanaf december 2022. Het digitaal toegankelijk maken van procedures (annex 2) is verplicht vanaf 12 december 2023. De verplichtingen uit annex 3 hebben betrekking op zowel annex 1 als annex 2 en treden gelijktijdig in werking.

2.1.2 Ontwikkelingen

De VNG, het IPO en de UvW hebben elk een eigen voorziening gerealiseerd waarmee hun leden kunnen voldoen aan de eisen voor het onderdeel 'Informeren' van de SDG-verordening. Deze voorzieningen zijn momenteel gebaseerd op één open source systeem. Het IPO heeft gekozen voor een CMS-overstijgende hub: een SDG-brugfunctie. Hiermee worden teksten van het CMS en/of PDC van de verschillende provinciewebsites gekoppeld aan de nationale portalen. Daarmee voldoen provincies al sinds januari 2023 aan annex 1. Het beheer van productinformatie en de brugfunctie (annex 1) is ondergebracht bij BIJ12. Provincies voldoen nog niet aan annex 2, maar maken gebruik van een alternatieve methode totdat de technische randvoorwaarden (zoals de eID wallet en OOTS) beschikbaar komen.

2.1.3 Impact op provincies

Implementatiescenario

In de AAC Digitalisering is besloten om te kiezen voor een minimaal implementatiescenario. Hiertoe is ook een handreiking opgesteld. De invoering van de SDG heeft namelijk een beheersbare impact op provincies. Voor informeren (annex 1) is aangesloten op twee nationale portalen. Van daaruit vindt de ontsluiting plaats naar het Europese Your Europe portaal. Deze aansluiting wordt beheerd door BIJ12 in samenwerking met de Provinciale Redactieraad.

Voor annex 2 is een intakeformulier opgezet waarbij een Europees bedrijf of inwoner zijn vraag kan stellen. Als zo'n vraag binnenkomt neemt de desbetreffende provincie contact op met de aanvrager om die op deze manier optimaal te faciliteren. Een ondernemer komt binnen via het Europese Your Europe-portaal en wordt dan doorgeleid naar de website van de provincie. Deze aanpak voldoet weliswaar niet volledig aan alle SDG-eisen, maar biedt wel een werkbare oplossing totdat technische randvoorwaarden (zoals de eID wallet en OOTS) beschikbaar komen. Daarnaast hebben provincies in hun dienstverlening veelal te maken met ondernemers die vergunningen aanvragen en minder met burgers. Op Europees niveau zijn er nog weinig landen waar ondernemers met een digitaal erkend middel zijn uitgerust (zoals eHerkenning in Nederland) om digitale dienstverlening mogelijk te maken.

OOTS

De SDG-verordening geeft gebruikers de mogelijkheid overheden te vragen onderling digitaal bewijsstukken uit te wisselen: het Once-Only Principle (OOP). Hiervoor richten Europese lidstaten samen met de Europese Commissie een Once-Only Technical System (OOTS) in. Het OOTS is een veilige en betrouwbare gegevensuitwisseling tussen overheidsorganisaties. Met het systeem kunnen Europese overheidsinstanties onderling bewijsstukken zoals diploma's of geboortebewijzen uitwisselen. Een gebruiker hoeft dit bewijs dan niet zelf aan te leveren door het bijvoorbeeld op te sturen of te uploaden. Een Nederlandse student die in België wil gaan studeren kan bijvoorbeeld aangeven dat zijn diploma's via het OOTS uit het Nederlandse
diplomaregister mogen worden gehaald. Gebruikers zijn niet verplicht het OOTS te gebruiken. De kaders van het OOTS zijn vastgelegd in de Uitvoeringsverordening OOTS (augustus 2022).
Voor wat betreft de uitwisseling van bewijzen is een SDG productenlijst opgesteld. Hierin zijn de producten opgenomen die volgens de verordening onder de SDG vallen. Deze producten zijn door de provincies beoordeeld op bewijzen die provincies van andere lidstaten nodig hebben en hiervan is aangegeven dat die er niet zijn. Andersom – dus de provincie als bewijsverstrekker – is dit ook niet het geval. OOTS zal dus niet of nauwelijks worden gebruikt door provincies.

IMI

Als het OOTS niet werkt of als een gebruiker het OOTS niet wil gebruiken, kunnen bevoegde instanties het IMI (Informatiesysteem Interne Markt) gebruiken om bewijzen te verifiëren. Het IMI is een digitaal systeem waarmee nationale overheden in hun eigen taal contact kunnen opnemen met overheden in andere EU-lidstaten. Het IMI komt voort uit de Dienstenrichtlijn en Dienstenwet, waar het gebruikt wordt voor samenwerking tussen EU-lidstaten. Een deel van de provincies beschikt op dit moment over IMI, maar dat is nog niet voor alle provincies het geval.

2.1.4 Bronnen

- Single Digital Gateway (SDG) Annex II en III: Handreiking voor implementatie minimale scenario, IPO, 2024
- Memo Borging Single Digital Gateway, IPO, 2025
- Informatie over IMI: https://europadecentraal.nl/praktijkvraag/praktijkvraag-imi-functionaliteit-en-gebruik-voor-decentrale-overheid/#

2.2 Digital services act

De Digital Services Act (DSA) is een Europese verordening die regels oplegt aan online diensten, zoals sociale media, online marktplaatsen en zoekmachines. Het doel hiervan is om een veiligere en transparantere online omgeving te creëren. De wet verplicht deze platforms om illegale inhoud te bestrijden, de grondrechten van gebruikers te beschermen en processen transparanter te maken. De DSA en de AVG vullen elkaar aan. Als een digitale dienst persoonsgegevens verwerkt, dan moet deze zowel aan de AVG als aan de DSA voldoen.

2.2.1 Verplichtingen uit de wet

De DSA bevat verplichtingen op het gebied van aansprakelijkheid, zorgvuldigheid en transparantie. De verplichtingen verschillen per type aanbieder van een digitale dienst: hoe nauwer een aanbieder betrokken is bij de informatie van de afnemers, hoe meer verplichtingen er gelden.

2.2.2 Ontwikkelingen

De DSA is op 17 februari 2024 in werking getreden. Sinds 4 februari 2025 zijn de Autoriteit Persoonsgegevens (AP) en de Autoriteit Consument & Markt (ACM) bevoegd om toezicht te houden op de regels van de DSA.

2.2.3 Impact op provincies

Overheidsorganisaties vallen niet automatisch onder de DSA, tenzij zij zelf optreden als aanbieder van een online dienst die valt onder de definitie van een tussenhandeldienst. Bijvoorbeeld: Een gemeente die een online platform aanbiedt waar burgers informatie kunnen delen of publiceren, een ministerie dat een hostingdienst aanbiedt voor publieke fora of interactieve content of een overheidsinstantie die een zoekmachine of marktplaats faciliteert voor publieke diensten of producten. Voor reguliere overheidswebsites of digitale loketten die geen tussenhandeldiensten aanbieden, is de DSA niet van toepassing. Er zijn provincies die aangeven dat zij online platformen aanbieden als tussenhandeldienst, overeenkomstig de definitie en toepassingsgebied van de DSA. Dit is niet bij alle provincies het geval.

2.2.4 Bronnen

- Factsheet DSA, ICT Recht
- DSA Leidraad: Zorgvuldigheidsverplichtingen tussenhandeldiensten, ACM, 2024

2.3 Dienstenwet

De Europese Dienstenrichtlijn verplicht elk land één loket aan te wijzen waar ondernemers hun zaken kunnen regelen, wanneer zij zich in Nederland vestigen of hier tijdelijk hun diensten aanbieden. Op die manier hoeven ondernemers niet met verschillende overheden zaken te doen, maar regelen zij alles op één centrale plek. In Nederland is het Ondernemersplein dit loket. Ondernemers kunnen bij dit loket veilig informatie uitwisselen met verschillende overheidsinstanties. De Dienstenrichtlijn is vertaald in de Nederlandse Dienstenwet.

2.3.1 Verplichtingen uit de wet

Provincies krijgen in de praktijk met de Dienstenwet te maken als een dienstverlener uit een andere lidstaat zich in de provincie wil vestigen of tijdelijk een dienst wil verlenen. Er zijn vier hoofdverplichtingen die voortkomen uit de Dienstenwet:

1. **Dienstenloket:** Er moet een Dienstenloket worden ingericht, waarmee dienstverleners op één centrale plek toegang tot informatie hebben, bijstand kunnen verkrijgen en procedures en formaliteiten met een provincie moeten kunnen afwikkelen.
2. **Bescherming van afnemers:** Er gelden informatie- en bijstandsverplichtingen, waarbij informatie verstrekt moet worden en op verzoek hulp geboden moet worden over rechtsmiddelen aan afnemers van diensten (zakelijke afnemers en consumenten).
3. **Algemene voorschriften met betrekking tot vergunningstelsels:** Vergunningstelsels moeten non-discriminatoir, noodzakelijk en evenredig zijn. Bovendien stelt de Dienstenwet eisen aan de inrichting en grondslagen van het vergunningstelsel.
4. **Grensoverschrijdende administratieve samenwerking:** Lidstaten, en daarmee ook decentrale overheden, moeten elkaar wederzijdse bijstand verlenen en maatregelen nemen om doeltreffend met elkaar samen te werken bij het toezicht op dienstverleners en hun diensten.

Naast deze hoofdverplichtingen geldt er ook een Notificatieplicht. Wanneer een provincie nieuwe regels en wetten maakt of bestaande regels en wetten wijzigt moet de provincie nagaan of deze onder de reikwijdte van de Dienstenwet valt. Als dat het geval is, moet de provincie de nieuwe of gewijzigde wetten en regels melden bij de Europese Commissie. Dit verloopt via een coördinatiepunt bij het ministerie van EZK.

2.3.2 Ontwikkelingen

De Dienstenrichtlijn is in 2006 in werking getreden. De Nederlandse Dienstenwet is van kracht sinds 12 november 2009. Er is in 2020 een checklist ‘Voldoen aan de Dienstenwet’ opgesteld voor provincies.

2.3.3 Impact op provincies

De impact op provincies die voortkomt uit de hoofdverplichtingen is als volgt:

1. Provincies zijn aangesloten op het Dienstenloket, dat is ondergebracht op https://ondernemersplein.overheid.nl/. Ook zijn alle provincies aangesloten op de Berichtenbox voor bedrijven. Dienstverleners kunnen vragen stellen aan de provincie en procedures afhandelen via deze Berichtenbox.
2. Decentrale overheden moeten, net als voor de dienstverleners, informatie over de formaliteiten en procedures voor afnemers van diensten elektronisch toegankelijk maken. Deze informatie is overigens grotendeels hetzelfde als de informatie die decentrale overheden ten behoeve van dienstverleners moeten verstrekken en daarmee al via het Dienstenloket is ontsloten. Daarnaast legt de Dienstenwet de provincies een bijstandsverplichting op waarbij deze verplichting niet verder gaat dan het op verzoek verschaffen van informatie over de rechtsmiddelen die voorhanden zijn met betrekking tot de eisen en vergunningstelsels waar de betreffende decentrale overheid bij betrokken is.
3. Naast dat een vergunningstelsel non-discriminatoir, noodzakelijk en evenredig moet zijn, stellen de Dienstenrichtlijn en Dienstenwet ook eisen aan de inrichting en grondslagen van het vergunningstelsel. Zo moet een vergunning duidelijk, ondubbelzinnig, objectief, transparant en toegankelijk zijn en moet deze vooraf openbaar bekend worden gemaakt (artikel 10 Dienstenrichtlijn). Daarnaast mag een vergunning als hoofdregel niet meer voor een beperkte tijd worden verleend (artikel 11 Dienstenrichtlijn en artikel 33 Dienstenwet) en is er een juridisch kader hoe moet worden omgegaan met schaarse vergunningen (artikel 12 Dienstenrichtlijn en artikel 33 Dienstenwet). Ook mogen vergunningsvoorwaarden die gelijke of vergelijkbare eisen en controles bevatten waaraan de dienstverlener in een andere lidstaat al aan is onderworpen, elkaar niet overlappen (artikel 10 lid 3 Dienstenrichtlijn en artikel 30 Dienstenwet). Tot slot dient een ontvangstbevestiging naar aanleiding van een vergunningaanvraag zo snel mogelijk te worden verstuurd waarbij de Dienstenrichtlijn (artikel 13 lid 5) en Dienstenwet (artikel 29 en 35) eisen aan deze ontvangstbevestiging stellen.
4. Om de administratieve (internationale) samenwerking vorm te geven kunnen provincies gebruik maken van het Interne Markt Informatiesysteem (IMI). Alle medeoverheden zijn verplicht aangesloten op het IMI. Het IMI is een beveiligd, meertalig online-portaal dat de uitwisseling van informatie gemakkelijker maakt voor overheden die betrokken zijn bij de uitvoering van EU-wetgeving in de praktijk. Via IMI kan een provincie de vragen van (buitenlandse) bevoegde autoriteiten beantwoorden. Ook kan een provincie zelf vragen stellen. Verder kan een provincie bepaalde openbare documenten laten verifiëren of een verzoek indienen om een inspectie of onderzoek uit te voeren.

2.3.4 Bronnen

- De Dienstenrichtlijn: Handreiking voor decentrale overheden, BZK, 2009.
- Checklist: Voldoen aan de Dienstenwet, BZK, EZK, RVO en KED, 2020.

2.4 eIDAS2.0

De verordening Europese Digitale Identiteit (ofwel eIDAS2.0) heeft als doel om ervoor te zorgen dat burgers, bedrijven en overheden digitaal zaken kunnen doen die betrouwbaar, veilig en inclusief zijn. De eIDAS2.0 introduceert een Europese digitale identiteit-portemonnee (EUDI Wallet). De EUDI Wallet is een app die burgers kunnen gebruiken als identificatiemiddel, wanneer zij gebruik maken van digitale diensten in EU landen. Ze kunnen ermee inloggen op deze online diensten, persoonlijke en gewaarmerkte gegevens kunnen erin worden opgeslagen en gedeeld en er kan digitaal mee worden ondertekend bij overheidsinstanties.

2.4.1 Verplichtingen uit de wet

De eerste eIDAS verordening uit 2014 regelt dat nationale inlogmiddelen ook in andere lidstaten moeten kunnen worden gebruikt. De Nederlandse inlogmiddelen zijn DigiD (voor burgers) en eHerkenning (voor bedrijven). Nederlandse burgers en bedrijven moeten deze inlogmiddelen dus kunnen gebruiken om ook in andere lidstaten gebruik te maken van dienstverlening van overheidsorganisaties.

De herziene eIDAS2.0 verordening is een uitbreiding op de oorspronkelijke eIDAS verordening. Alle EU lidstaten moeten nu ook een digitale identiteit-wallet (EUDI-wallet) aanbieden aan burgers en bedrijven. Het gebruik van de wallet is op vrijwillige basis. Decentrale overheden (waaronder provincies) zijn verplicht om de EUDI-wallets te erkennen en hun dienstverlening daarop aan te passen.

2.4.2 Ontwikkelingen

Uit een evaluatie door de Europese Commissie in 2021 bleek dat de oorspronkelijke verordening uit 2014 op verschillende gebieden tekortschiet. De nieuwe eIDAS-verordening is onder andere meer toegespitst op marktveranderingen en de toenemende vraag naar nieuwe elektronische identificatiemiddelen. Momenteel ontwikkelt BZK een Nederlandse wallet, de EDI-wallet, die in alle EU landen gebruikt kan worden.

De eIDAS2.0 is in werking getreden op 20 mei 2024. Gefaseerde implementatie vindt plaats tot en met 2026–2027. Vanaf 24 december 2026 moeten alle EU lidstaten minimaal één EUDI-wallet certificeren en beschikbaar stellen aan hun burgers.

2.4.3 Impact op provincies

Er worden verschillende rollen onderscheiden in de eIDAS2.0. Provincies zijn zogenoemde 'vertrouwende partijen'. Dat houdt in dat provincies digitale identiteitsgegevens accepteren en verifiëren, aangezien zij dienstverlening aanbieden waarbij digitale identiteitsverificatie nodig is.

Provincies moeten er dus voor zorgen dat hun systemen EUDI-Wallets kunnen accepteren. Daarvoor moeten zij een koppelvlak implementeren en beheren. Ook moeten zij de Nederlandse EDI-wallet implementeren in hun eigen dienstverlening, zodat zij attributen (bijv. persoonsgegevens en diploma's) uit de EUDI wallet kunnen accepteren.

2.4.4 Bronnen

- https://europadecentraal.nl/onderwerp/digitale-overheid/digitale-samenleving/verordening-europese-digitale-identiteit-eidas2-0/
- Uitvoeringsanalyse Digital Decade eIDAS 2.0, VNG, 2025.
- Programma EDI-stelsel NL, via https://edi.pleio.nl/

2.5 Omgevingswet (DSO)

De Omgevingswet bundelt bestaande wetten en regels voor de fysieke leefomgeving met als doel om het stelsel te vereenvoudigen en daardoor snellere besluitvorming bij vergunningsaanvragen te bewerkstelligen. Ter ondersteuning van de uitvoering van de Omgevingswet is het Digitaal Stelsel Omgevingswet (DSO) ontwikkeld. Het DSO is een samenhangend stelsel van digitale voorzieningen, standaarden, gegevens, bronnen en onderlinge afspraken. Overheidsorganisaties sluiten hun eigen lokale systemen aan op onderdelen van het DSO. In het stelsel zit ook een landelijke voorziening, waar onder andere het Omgevingsloket onderdeel van uitmaakt. Via het Omgevingsloket kunnen burgers en bedrijven informatie vinden, vergunningen aanvragen en meldingen maken.

2.5.1 Verplichtingen uit de wet

Provincies moeten gegevens en documenten uitwisselen met het DSO. Het gaat om de volgende gegevens en documenten:

- **Omgevingsdocumenten:** dit zijn officiële publicaties van provincies, zoals een omgevingsplan of omgevingsverordening. Provincies publiceren deze omgevingsdocumenten via de Landelijke voorziening bekendmaken en beschikbaar stellen (LVBB), waarna ze in het DSO en het Omgevingsloket gepubliceerd worden.

- **Toepasbare regels:** dit zijn vertalingen van juridische regels in begrijpelijke taal. Provincies stellen deze toepasbare regels op en publiceren ze vervolgens in een regelbeheersysteem. Dat systeem is gekoppeld aan de Registratie toepasbare regels (RTR). Na publicatie in de RTR zijn de regels ook te zien in het Omgevingsloket.
- **Vergunningaanvragen en meldingen:** wanneer een initiatiefnemer een vergunning aanvraagt of een melding maakt, krijgt een provincie hier een notificatie van. Vervolgens kan de provincie de aanvraag of melding digitaal ophalen uit het Omgevingsloket. Voor het ontvangen van de notificaties moeten provincies hun zaak- of vergunningensysteem aansluiten op het DSO.
- **Informatieproducten:** dit zijn sets van informatie over de fysieke leefomgeving. Provincies moeten deze sets aanleveren via de Stelselcatalogus Omgevingswet, maar deze is momenteel nog in ontwikkeling.

2.5.2 Ontwikkelingen

De Omgevingswet is sinds 1 januari 2024 van kracht en ook het DSO is sinds die tijd in gebruik. In januari 2025 is er door de Evaluatiecommissie Omgevingswet een eerste tussentijdse evaluatie van het DSO gedaan. Daaruit blijkt dat het DSO nog onvoldoende functioneert en niet gebruiksvriendelijk genoeg is.

2.5.3 Impact op provincies

Provincies moeten hun systemen koppelen aan de verschillende onderdelen van het DSO om gegevens en documenten te kunnen uitwisselen zoals beschreven in 2.5.1. De Omgevingswet betekent een grote organisatieverandering die veel aanpassingen vergt. De wet schrijft het gebruik van de STOP/TPOD standaard voor, en de impact daarvan op het opstellen van Omgevingsdocumenten gaat ver. Processen moeten worden aangepast en de manier waarop men omgevingsdocumenten opbouwt in de plansoftware, vraagt specifieke kennis en vaardigheden van de opstellers. Kennis die bovendien nog schaars aanwezig is.

Een andere belangrijke verandering is dat de Omgevingswet vraagt om integrale afwegingen, waardoor verschillende domeinen meer moeten afstemmen. Tevens dient participatie te worden toegepast.

In het DSO staan omgevingsdocumenten niet op zichzelf, ze zijn allemaal aan elkaar gelinkt (d.m.v. annotaties), dus ook de consistentie tussen Omgevingsdocumenten moet worden geborgd. Het is daarmee niet alleen een IT-technische verandering, maar ook een organisatorische verandering met nieuwe rollen en aangepaste processen, en deze impact mag niet worden onderschat.

2.5.4 Bronnen

- In werking, maar onderbenut. Reflectierapport Omgevingswet 2024, Evaluatiecommissie Omgevingswet, 2025.
- Informatiepunt Leefomgeving, via https://iplo.nl/

2.6 Wmebv

De Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) regelt dat burgers en bedrijven hun zaken die ze met de overheid moeten doen, digitaal kunnen afhandelen. Zij krijgen daarmee het recht om officiële berichten, zoals aanvragen voor vergunningen en bezwaarschriften, elektronisch aan het bestuursorgaan te zenden. Ook versterkt de wet de rechten en waarborgen voor burgers en bedrijven.

2.6.1 Verplichtingen uit de wet

De Wmebv brengt verschillende verplichtingen met zich mee:

1. **Voor berichten aan de overheid geldt:**
    a. Burgers en bedrijven hebben recht op het elektronisch inzenden van een bericht in het kader van een formele (wettelijk geregelde) procedure.
    b. Burgers en bedrijven hebben recht op een ontvangstbevestiging nadat zij een elektronisch bericht hebben verstuurd.
    c. Burgers en bedrijven hebben recht op het ontvangen van een afschrift van door hen ingevoerde gegevens in een webformulier.
    d. Er is een verbod op het afdwingen in een webformulier van niet verplichte en niet noodzakelijke gegevens voor de behandeling van de aanvraag.
    e. Er geldt een verlengde indieningstermijn voor burgers en bedrijven bij storing aan de kant van het bestuursorgaan.
2. **Voor berichten van de overheid in een berichtenbox geldt:**
    a. Bestuursorganen zijn verplicht om een notificatie te sturen wanneer zij een bericht in de berichtenbox plaatsen.
    b. In die notificatie moet informatie over de aard en rechtsgevolgen van het bericht staan en moet de reactietermijn benoemd worden.
    c. Als een notificatie of ander elektronisch bericht niet kan worden bezorgd (bijv. door een gewijzigd emailadres) moet het bestuursorgaan langs een andere weg contact opnemen (bijv. schriftelijk of telefonisch) met de ontvanger.
    d. Het bestuursorgaan moet de ontvangst en verzendingen van berichten in de berichtenbox kunnen bewijzen (bijv. middels loggegevens) wanneer de burger of het bedrijf hierom vraagt.

Bovendien wijzigt de Wmebv afdeling 2.3 van de Algemene wet bestuursrecht (Awb) en artikel 2.1 van de Awb. Dit heeft voor bestuursorganen de volgende gevolgen:

> Aanpassing afdeling 2.3 van de Awb:
- Het verplicht openstellen van digitale kanalen voor ieder elektronisch formeel bericht gericht aan het bestuursorgaan.
- Het aanpassen van digitale kanalen zodat aan wettelijke eisen/waarborgen wordt voldaan.

> Aanpassing artikel 2.1 van de Awb:
    - Er geldt een zorgplicht die inhoudt dat bestuursorganen aan burgers en bedrijven passende ondersteuning moeten bieden bij bestuurlijk verkeer.

2.6.2 Ontwikkelingen

De Wmebv treedt op 1 januari 2026 in werking. In 2024 is er een quickscan uitgevoerd door IPO waarmee de stand van zaken bij de provincies in kaart is gebracht. Toen was de verwachting nog dat de wet per 1 januari 2025 in werking zou treden. 9 provincies hebben de quickscan ingevuld. 3 provincies gaven aan klaar te zijn voor inwerkingtreding per 1 januari 2025, 6 provincies gaven aan dat niet te zijn. In 2025 is er opnieuw een quickscan uitgevoerd. Deze is door 5 provincies ingevuld, waarvan 2 provincies aangaven klaar te zijn voor inwerkingtreding per 1 januari en 3 aangaven dan nog niet klaar te zijn.

2.6.3 Impact op provincies

De verplichtingen waar provincies op grond van de Wmebv aan moeten voldoen kunnen worden onderverdeeld in twee categorieën: *verplichtingen op het moment* van ontvangst van elektronische berichten en verplichtingen *na* ontvangst van elektronische berichten.

Verplichtingen op het moment van ontvangst van elektronische berichten:

1. Aanwijzen en zo nodig inrichten of aanpassen van elektronische weg voor berichten: provincies moeten voor ieder type formeel bericht dat zij kunnen ontvangen een elektronische wijze van verzenden aanwijzen. Ook moeten provincies ervoor zorgen dat reeds bestaande digitale kanalen voldoen aan de wet. Dit moet per digitaal kanaal of webformulier worden onderzocht, waarna eventuele aanpassingen gedaan moeten worden.
2. Geen onnodige belemmeringen voor verzending formeel elektronisch bericht: eventuele eisen die provincies stellen aan de manier waarop berichten verzonden moeten worden (bijv. altijd in pdf of xml formaat) mogen niet onnodig belemmerend zijn voor degene die het bericht verstuurt. Ook mogen er geen gegevens van de verzender gevraagd worden die niet noodzakelijk zijn voor de behandeling van het bericht.

Verplichtingen na ontvangst van elektronische berichten:

1. Wanneer een provincie een formeel elektronisch bericht ontvangt moet zij een ontvangstbevestiging sturen.
2. Wanneer een provincie ervoor kiest om een webformulier aan te wijzen voor het verzenden van een bericht, moeten de via dat formulier ingevoerde gegevens voor de indiener toegankelijk zijn (bijv. door een kopie van het ingevulde formulier mee te sturen in de ontvangstbevestiging).

3. Wanneer een formeel bericht verkeerd ingezonden wordt, krijgt de provincie de mogelijkheid om te volstaan met de mededeling dat het bericht onjuist is ingediend en te wijzen op de juiste manier van indienen. Dit geldt alleen voor berichten waarvoor een wijze van verzending is aangewezen door de provincie.

Bovendien gelden er aanvullende verplichtingen en regels wanneer een provincie gebruik maakt van een berichtenbox.

De Awb vereist ook dat elektronisch verkeer tussen burger en provincie 'voldoende betrouwbaar en vertrouwelijk' geschiedt. Wat daaronder verstaan moet worden, bepaalt de provincie primair zelf. De provincie regelt de betrouwbaarheidsniveaus in volgens de definities uit de Wet digitale overheid.

2.6.4 Bronnen

> Handreiking Wet Modernisering Elektronisch Bestuurlijk Verkeer, IPO, 2022.
> Handreiking implementatie Wet modernisering elektronisch bestuurlijk verkeer, BZK, 2023.

Implementatiesteun Wmebv, VNG.

2.7 Wet digitale overheid (Wdo)

De Wet digitale overheid (Wdo) heeft als doel om het inloggen voor burgers en bedrijven en hun gemachtigden bij de (semi-) overheid veilig en betrouwbaar te maken. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een substantiële of hoge mate van betrouwbaarheid. De wet verplicht dienstverleners om toegestane inlogmiddelen te accepteren, geeft regels over informatieveiligheid en privacy, biedt de grondslag om overheidsinstanties te verplichten tot het toepassen van open standaarden en bevat uitgangspunten ten aanzien van (inter-)bestuurlijk toezicht op de naleving van de wet.

2.7.1 Verplichtingen uit de wet

De Wdo bevat de volgende verplichtingen:

> Bepaalde (open) standaarden zijn verplicht in het elektronisch verkeer van de overheid
> Er zijn regels gesteld over informatieveiligheid en het verwerken van persoonsgegevens
> De verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI)

- Belangrijk onderdeel van de Wdo is de acceptatieplicht. Dit houdt in dat burgers, bedrijven en hun gemachtigden op een uniforme manier, met alle toegelaten publieke en private inlogmiddelen in kunnen loggen bij dienstverleners (zoals de provincies). Het Stelsel Toegang maakt dit technisch mogelijk. Overheidsorganisaties kunnen via één aansluitpunt burgers en bedrijven veilig toegang geven tot hun digitale dienstverlening. En als dienstverleners zijn aangesloten op het Stelsel Toegang kunnen zij automatisch alle toegelaten middelen accepteren en daarmee voldoen aan de acceptatieplicht.

2.7.2 Ontwikkelingen

De wet heette oorspronkelijk Wet generieke digitale infrastructuur. De Wdo is officieel per 1 juli 2023 in werking getreden en wordt de komende jaren gefaseerd ingevoerd. De Wdo is een zogeheten kaderwet: de wet regelt algemene principes, verantwoordelijkheden en procedures, maar geen gedetailleerde regels. De eerste tranche van de Wdo is (gefaseerd) ingegaan per 1 juli 2023 en omvat digitale toegankelijkheid, beveiligde verbindingen (HTTPS en HSTS), aansluiten op Stelsel Toegang en het accepteren van toegelaten inlogmiddelen. De tweede tranche bevat o.a. Regie op gegevens; eIDAS 2.0 en de implementatie van de Europese Digitale Identiteit (EDI-wallet).

2.7.3 Impact op provincies

Per 1 juli 2023 moeten provincies voldoen aan de eerste tranche, die bestaat uit:

- De Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening. Dit betekent dat een provincie betrouwbaarheidsniveaus moet bepalen en moet inregelen dat de dienstverlening ook volgens dat betrouwbaarheidsniveau geleverd wordt.
- Accepteren van de nu geldende officiële inlogmiddelen (DigiD, eHerkenning en eIDAS).
- Een aantal wettelijke standaarden. Op de website digitaleoverheid.nl is een overzicht gemaakt van welke standaarden exact gelden. Op Forum Standaardisatie valt na te lezen wat de verschillende verplichtingskaders inhouden:
    - Het Besluit digitale toegankelijkheid. Dit besluit is al sinds 2018 van toepassing en is nu wettelijk verankerd in de Wdo. Op 28 juni 2025 is bovendien de Europese Toegankelijkheidswet (European Accessibility Act, EAA) in werking getreden. De verplichtingen die al sinds 2018 gelden voor overheden blijven ongewijzigd door de invoering van deze EAA.
    - Het Besluit beveiligde verbindingen met overheidswebsites en webapplicaties, specifiek de HTTPS en HSTS-standaarden. Deze standaarden vallen al onder de pas-toe-leg-uit lijst en worden nu verplicht.

2.7.4 Bronnen

- Handreiking implementatie Wet digitale overheid, IPO.

3. Informatiehuishouding, openheid en transparantie

Het wetgevingscluster informatiehuishouding, openheid en transparantie omvat richtlijnen, verordeningen en wetten die betrekking hebben op de informatiehuishouding van provincies en regels stellen aan openheid en transparantie. Dit cluster omvat:

- Data governance verordening (DGA) (EU verordening)
- Data verordening (DA) (EU verordening)
- Wet hergebruik overheidsinformatie (Who) (NL wet)
- Archiefwet (NL wet)
- Wet elektronische publicaties (Wep) (NL wet)
- Wet open overheid (Woo)

3.1 Data governance verordening

De Data governance act (DGA) regelt de betrouwbaarheid, toegang en neutraliteit van data. De DGA geeft een raamwerk met de kaders en procedures om datahergebruik mogelijk te maken. Daarnaast introduceert het een regime voor databemiddelingsdiensten die commerciële relaties tot stand brengen voor het uitwisselen van gegevens en tegelijkertijd de privacy van betrokkenen garanderen. De Data verordening gaat verder en reguleert wie onder welke voorwaarden toegang moet geven tot gegenereerde data door het gebruik van een product of gerelateerde dienst.

3.1.1 Verplichtingen uit de wet

De Data Governance verordening bevat een aantal speerpunten:

- Het hergebruik van overheidsinformatie faciliteren.
- Verplichtingen voor bemiddelaars van data.
- Het stimuleren van data delen op altruïstische wijze.
- Het aanstellen van de ‘European Data Innovation Board’.

3.1.2 Ontwikkelingen

De verplichtingen in de DGA zijn met ingang van 24 september 2024 van toepassing. In Nederland zijn de regels van de DGA omgezet in nationale wetgeving middels de Uitvoeringswet datagovernanceverordening. De Uitvoeringswet wijst de Autoriteit Consument en Markt (ACM) aan als toezichthouder en bevoegde autoriteit voor databemiddelingsdiensten en data-altruïsme. De Autoriteit Persoonsgegevens (AP) adviseert over de voorwaarden uit de verordening die verband houden met de bescherming van persoonsgegevens.

3.1.3 Impact op provincies

Door de volgende factoren blijft de impact van de DGA voor provincies beperkt:

- De gegevenscategorieën waarop de DGA van toepassing is zijn gelimiteerd in aantal (hoofdstuk II, artikel 3 DGA).
- De verplichtingen en mogelijkheden in de DGA gaan uit van nationale grondslagen en kunnen zonder deze grondslagen niet uitgevoerd en benut worden. Het aantal grondslagen blijkt binnen het Nederlandse stelsel minimaal te zijn, waardoor de DGA slechts in beperkte mate kan worden toegepast (hoofdstuk II DGA).
- De verplichtingen in de DGA richten zich niet direct tot decentrale overheden. Zo zijn bijvoorbeeld de hoofdstukken omtrent data-altruïsme, databemiddelingsdiensten, de internationale toegang en doorgifte van data en als laatste het hoofdstuk omtrent het verbod op exclusieve overeenkomsten nauwelijks tot niet relevant voor decentrale overheden (dit valt buiten hergebruik van gegevens volgens hoofdstuk II, met uitzondering van exclusieve overeenkomsten).

3.1.4 Bronnen

- Data Governance Verordening: Impactanalyse, KED, 2023.

3.2 Data verordening

De Data verordening zorgt voor betere toegang tot data, voor zowel bedrijven en consumenten als overheidsorganisaties. Juridische, economische en technische obstakels worden weggenomen.

3.2.1 Verplichtingen uit de wet

De Data verordening geeft kaders voor de volgende situaties:

- Het beschikbaar stellen van gegevens door gegevenshouders aan overheidsinstanties, de Commissie, de Europese Centrale Bank en organen van de Unie, indien er sprake is van een uitzonderlijke noodzaak aan die gegevens voor de uitvoering van een specifieke taak in het algemeen belang.
- Het vergemakkelijken van het overstappen tussen dataverwerkings- en clouddiensten.
- De ontwikkeling van interoperabiliteitsnormen voor dataruimten, dataverwerkingsdiensten en slimme contracten.

3.2.2 Ontwikkelingen

De Data verordening is samen met de Data governance verordening (DGA) onderdeel van de Europese datastrategie. De Data verordening is van toepassing sinds 12 september 2025.

3.2.3 Impact op provincies

De impact van de Data verordening op provincies is beperkt:

- Provincies kunnen in uitzonderlijke gevallen data opvragen bij derde partijen voor het uitvoeren van hun wettelijke taken, bijvoorbeeld in een noodsituatie. De wet stelt eisen aan hoe zo'n dataverzoek eruit moet zien en hoe de provincie de data verwerkt en verwijdert.
- Voor provincies wordt het makkelijker om gegevens en toepassingen over te brengen van de ene cloud aanbieder naar de andere.
- De interoperabiliteitsnormen zijn geen verplichting en zijn alleen van toepassing als de provincie de rol van gebruiker heeft.

3.2.4 Bronnen

- Uitvoeringsanalyse Digital Decade: Dataregelgeving, VNG, 2024.

3.3 Wet hergebruik overheidsinformatie (Who)

De wet regelt dat openbare gegevens, meestal verwerkt door overheidsinstanties, ook voor een ander doel kunnen worden gebruikt dan waarvoor ze oorspronkelijk zijn verzameld. Met de Who kunnen burgers, journalisten, wetenschappers, bedrijven en anderen een verzoek indienen tot het verstrekken van overheidsinformatie.

3.3.1 Verplichtingen uit de wet

Naast overheidsinformatie op verzoek, bevat de Who verplichtingen tot het actief voor hergebruik beschikbaar stellen van alle openbare, algemene overheidsinformatie. Daarnaast is er ook nog de Europese INSPIRE-richtlijn. Dat is een specifieke richtlijn voor geografische/ruimtelijke gegevens. In Nederland is de INSPIRE-richtlijn grotendeels geïmplementeerd in de implementatiewet INSPIRE en het Besluit INSPIRE.

3.3.2 Ontwikkelingen

De ontwikkeling van Open data richtlijn tot Who ziet er als volgt uit: Open data richtlijn -> Wet implementatie open data richtlijn -> Wet hergebruik overheidsinformatie. De Europese Open data richtlijn is middels de Wet implementatie open data richtlijn geïmplementeerd in de Nederlandse Wet hergebruik van overheidsinformatie. Op 19 juni 2024 is de Wet implementatie open data richtlijn inwerking getreden en is daarmee de Wet hergebruik overheidsinformatie gewijzigd.

3.3.3 Impact op provincies

Provincies moesten al voldoen aan de Wet hergebruik van overheidsinformatie. Wijzigingen naar aanleiding van de herziene Who zijn:

- een verplichting om 'specifieke hoogwaardige gegevenssets' actief ter beschikking te stellen voor hergebruik
- het op verzoek beschikbaar stellen van 'dynamische gegevens'
- het actief beschikbaar stellen van onderzoeksgegevens door publiek gefinancierde onderzoeksorganisaties
- een algemene inspanningsverplichting om zoveel mogelijk te werken vanuit het principe 'open door ontwerp en door standaardinstellingen'
- een inspanningsverplichting voor overheden om de broncode van overheidssoftware (alle software die zij zelf maakt of laat ontwikkelen) vrij toegankelijk en herbruikbaar te maken (open source)

Provincies voldoen nog niet aan de Who. Vanuit het ministerie van BZK is hierover een aanmaningsbrief gestuurd. Dit is in behandeling bij de vakgroep PP-GEO, aangezien de Who vooral betrekking heeft op geo-datasets van provincies.

INSPIRE-richtlijn

De INSPIRE-richtlijn verplicht provincies tot het delen van ruimtelijke gegevens. Om ervoor te zorgen dat geo-informatie digitaal uitwisselbaar is tussen de Europese lidstaten, zijn er standaarden opgesteld. Deze standaarden zorgen ervoor dat men gegevens online kan zoeken, bekijken en downloaden. Provincies moeten deze standaarden implementeren.

3.3.4 Bronnen

- Handleiding Herziene Who nav de Wet implementatie open data richtlijn, BZK, VNG, IPO, UvW, NA, KED, 2024.

3.4 Archiefwet

Het doel van de Archiefwet is om overheidsinformatie te behouden en toegankelijk te maken, voor huidige en toekomstige generaties. Het belangrijkste verschil tussen de oude en de nieuwe Archiefwet is dat de nieuwe wet veel beter aansluit op het digitale tijdperk en strengere eisen stelt aan het beheer van digitale informatie. De nieuwe Archiefwet vraagt om een proactieve, digitale en transparante aanpak van informatiebeheer. Dit betekent investeren in mensen, processen en technologie.

3.4.1 Verplichtingen uit de wet

De Archiefwet stelt eisen aan de informatiehuishouding van overheidsorganisaties. De belangrijkste wijziging ten opzichte van de bestaande Archiefwet is dat de overbrengingstermijn van documenten naar een archiefdienst verkort wordt van 20 naar 10 jaar. Ook moet elke overheidsorganisatie verplicht een archivaris aanstellen en moet de digitale infrastructuur herzien worden om te voldoen aan de nieuwe eisen voor digitaal archiveren.

3.4.2 Ontwikkelingen

De huidige Archiefwet komt uit 1995, maar wordt momenteel gemoderniseerd in de nieuwe Archiefwet. De nieuwe Archiefwet ligt op dit moment voor aan de Eerste Kamer en treedt naar verwachting in werking per 1 januari 2027. Het ministerie van OCW heeft een implementatieprogramma opgezet, dat loopt van 1 januari 2026 tot 2030. Het IPO neemt deel aan dit implementatieprogramma, maar er zal ook actieve participatie en steun vanuit de individuele provincies nodig zijn.

3.4.3 Impact op provincies

Als onderdeel van het implementatieprogramma zijn de volgende activiteiten voor provincies van belang:

- Verkorting van de overbrengingstermijn tot 10 jaar
- Aanpassing van het proces voor het opstellen van selectiebesluiten
- Aanpassing van het openbaarheidsregime o.a. door harmonisering met de Woo
- Verplichte aanstelling van een gediplomeerde archivaris
- Uitbreiding van het toezicht op de naar de archiefdienst overgebrachte archiefbescheiden
- Vernieuwing van het toezichtskader
- Aanpassing van de archief-KPI's
- Participatie in het opstellen van kennisproducten

De impact van deze veranderingen en de tijdlijn zullen in het implementatieprogramma nader worden uitgewerkt in samenspraak met de koepels. Dan zal ook duidelijk worden wat van de provincies wordt verwacht en welke zaken eventueel op interprovinciaal niveau moeten worden georganiseerd. De eerste stap is participatie van IPO in het implementatieoverleg. Het landelijk overleg provincies archivarissen (LOPAI) en de vakgroep duurzame toegankelijkheid zijn ook betrokken bij de ontwikkelingen.

3.4.4 Bronnen

> Meerjarenplan Digitale Informatiehuishouding Provincies, IPO, 2025

3.5 Wet elektronische publicaties

Het doel van de Wet elektronische publicaties (Wep) is om burgers digitaal te informeren over besluiten van de overheidsinstellingen die impact hebben op hun leefomgeving. De besluiten zijn in te zien via www.officielebekendmakingen.nl.

3.5.1 Verplichtingen uit de wet

Met de komst van de Wep is het voor decentrale overheden verplicht om besluiten uitsluitend elektronisch bekend te maken. Papieren bekendmaking telt sindsdien niet meer als rechtsgeldige publicatie. Het bekendmaken gebeurt via de systemen van KOOP.

3.5.2 Ontwikkelingen

De Wep is op 1 juli 2021 in werking getreden. De Wep wijzigt de Bekendmakingswet.

3.5.3 Impact op provincies

De Wep heeft de volgende impact op provincies:

> Het is voor provincies verplicht om de officiële publicaties via DROP te publiceren in hun eigen publicatieblad (het Provinciaal Blad) op https://www.officielebekendmakingen.nl.
> Kennisgevingen over vergunningen dienen vanaf 1 juli 2021 ook verplicht elektronisch bekend te worden gemaakt.
> Alle nieuw vastgestelde beleidsregels dienen vanaf 1 juli 2021 volledig bekend te worden gemaakt en geconsolideerd. Vanaf 1 juli 2022 moeten alle op dat moment geldende beleidsregels geconsolideerd zijn aangeboden.
> Documenten die ter kennisgeving fysiek ter inzage in een overheidsgebouw worden gelegd, moeten vanaf 1 juli 2023 ook digitaal ter inzage worden gelegd. Deze documenten moeten geanonimiseerd zijn.

3.5.4 Bronnen

> https://www.koopoverheid.nl/voor-overheden/gemeenten-provincies-en-waterschappen/bekendmakingswet
> https://www.koopoverheid.nl/voor-overheden/gemeenten-provincies-en-waterschappen/drop/presentaties-roadshow

3.6 Wet open overheid

De Wet open overheid (Woo) regelt welke overheidsinformatie openbaar is en hoe iemand die kan aanvragen.

3.6.1 Verplichtingen uit de wet

De Woo brengt verschillende verplichtingen met zich mee:

- **Actieve openbaarmakingsplicht:** de overheid moet sommige informatie uit zichzelf openbaar maken. Er zijn 17 categorieën informatie die overheidsorganisaties actief openbaar moeten maken. Deze verplichting wordt de komende jaren stap voor stap ingevoerd.
- **Openbaarmakingsplicht op verzoek:** de overheid maakt informatie openbaar als iemand erom vraagt.
- **Informatiehuishoudingsplicht:** overheidsinformatie moet goed te vinden zijn.

3.6.2 Ontwikkelingen

De Woo is de opvolger van de Wet openbaarheid van bestuur (Wob) en is op 1 mei 2022 in werking getreden. De stand van zaken bij provincies met betrekking tot de verplichtingen van de Woo is op dit moment als volgt:

- **Actieve openbaarmaking:** de 1ste tranche met verplichte categorieën om actief openbaar te maken is ingegaan per 1 november 2024. Alle provincies voldoen vanaf die datum aan deze wettelijke eis. De planning van de inwerkingtreding van tranche 2, 3 en 4 is nog niet bekend.
- **Openbaarmaking op verzoek:** nog niet alle Woo-verzoeken worden binnen de wettelijke termijn afgehandeld door provincies. Er zijn aanzienlijke verschillen tussen provincies. De oorzaken daarvoor zijn onder andere de omvang van verzoeken, de benodigde tijd voor beoordeling, een tekort aan medewerkers en het niet op orde zijn van de informatiehuishouding.
- **Informatiehuishouding:** uit de jaarlijkse Woo-monitor blijkt dat provincies nog aanzienlijke stappen moeten zetten bij het op orde brengen van hun informatiehuishouding.

3.6.3 Impact op provincies

Provincies moeten voldoen aan de verplichtingen uit de Woo. Op grond van artikel 3.3 van de Woo moeten provincies informatiecategorieën openbaar maken. Dit gebeurt de komende jaren gefaseerd in vier tranches. Daarnaast is er ook een inspanningsverplichting (artikel 3.1) voor provincies om uit eigen beweging meer documenten actief openbaar te maken.

Provincies plaatsen de documenten op een eigen platform en publiceren de locatie hiervan op een centrale verwijsindex: de Woo-index. Aan de hand daarvan wordt de informatie opgehaald door de zogenaamde ‘harvester’ en beschikbaar gemaakt via een landelijk zoekportaal. Er zijn verschillende manieren om deze informatie aan te leveren aan de Woo-index: via de harvester, via een handmatig aanleverloket (HAL), via de Open Raadsinformatie (ORI) API en via een generieke API.

3.6.4 Bronnen

- Meerjarenplan Digitale Informatiehuishouding Provincies, IPO, 2025
- Monitor implementatie Wet open overheid Provincies 2025, IPO, 2025

4. Gegevensbescherming en cybersecurity

Dit wetgevingscluster staat in het teken van richtlijnen, verordeningen en wetten op het gebied van gegevensbescherming en cybersecurity. Daartoe behoren:

- Cyberbeveiligingswet (Cbw) (NL wet)
- Wet weerbaarheid kritieke entiteiten (Wwke) (NL wet)
- Algemene verordening gegevensbescherming (AVG) (NL wet)
- Wet politiegegevens (Wpg) (NL wet)

4.1 Cyberbeveiligingswet

De Europese Network and Information Systems (NIS2) richtlijn wordt in Nederland geïmplementeerd met de Cyberbeveiligingswet (Cbw). De Cbw heeft als doel de digitale weerbaarheid van essentiële en belangrijke sectoren te versterken. De wet is gericht op bescherming tegen digitale dreigingen zoals cyberaanvallen en datalekken. Provincies vallen, net als andere overheidsorganisaties, onder de essentiële entiteiten.

4.1.1 Verplichtingen uit de wet

De verplichtingen uit de Cbw zijn als volgt:

- **Zorgplicht:** provincies moeten 10 passende technische en organisatorische beveiligingsmaatregelen nemen, op basis van risicoanalyses.
- **Meldplicht:** ernstige cyberincidenten moeten binnen 24 uur gemeld worden.
- **Registratieplicht:** provincies moeten netwerk- en organisatiegegevens aan leveren voor het entiteitenregister bij het NCSC.

Een ander belangrijk onderdeel van de Cbw is het toezicht. Dit houdt in dat de naleving van de verplichtingen uit de wet proactief wordt gecontroleerd. Voor provincies is de Rijksinspectie voor Digitale Infrastructuur (RDI) aangewezen als toezichthouder.

BIO2 en Cbw

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle lagen van de overheid. De BIO is van kracht sinds 2019. In september 2025 is een hernieuwde versie van de BIO vastgesteld: de BIO2. Vanaf dat moment tot de inwerkingtreding van de Cbw hanteren provincies, waterschappen en het Rijk de BIO2 als verplichtende zelfregulering.
De BIO2 wordt opgenomen in de ministeriële regeling voor de sector overheid onder het Cyberbeveiligingsbesluit (AMVB), wat betekent dat het toepassen van de BIO2 vanaf dan wettelijk verplicht is voor overheden (waaronder provincies).

4.1.2 Ontwikkelingen

De Cbw wordt naar verwachting in Q2 van 2026 van kracht. Het concept Cyberbeveiligingsbesluit (AMVB) ligt momenteel bij de Tweede Kamer. Vervolgens gaat het voor akkoord naar de ministerraad, waarna het voor advies worden voorgelegd aan de Afdeling advisering van de Raad van de State. De AMVB's voor de Cbw en de Wwke treden tegelijk met de wetsvoorstellen in werking. De consultatie voor de ministeriële regeling loopt tot en met 21 december 2025. De verschillende departementen stellen elk een eigen ministeriële regeling op voor de sectoren waar zij verantwoordelijk voor zijn. Het ministerie van BZK is verantwoordelijk departement voor de sector overheid, dus deze ministeriële regeling is relevant voor provincies.

4.1.3 Impact op provincies

In 2024 is er een impactanalyse uitgevoerd voor de provincies. Daarbij is voor elke provincie een rapportage opgesteld over de verwachte impact voor die provincie. De impact van de Cbw is over het algemeen hoog voor provincies, al zijn er ook verschillen tussen de uitgangsposities van provincies. In ieder geval moeten alle provincies maatregelen nemen in het kader van de zorgplicht, de meldplicht en de registratieplicht. Ook komt er toezicht, voor provincies wordt de Rijksinspectie Digitale Infrastructuur (RDI) toezichthouder. Er is in 2025 een onderzoek uitgevoerd naar het toezicht. Omdat provincies essentiële entiteiten zijn, houdt RDI proactief toezicht. Dat betekent dat RDI op een willekeurig moment informatie kan opvragen of langs kan komen, niet alleen nadat er een incident heeft plaatsgevonden.

4.1.4 Bronnen

> Impactanalyse NIS2 voor de 12 provincies, PBLQ, 2024.
> Toezicht in het kader van de Cyberbeveiligingswet: Naar gelaagd én geslaagd toezicht, PBLQ, 2025.

4.2 Wet weerbaarheid kritieke entiteiten

De Europese Critical Entities Resilience (CER) richtlijn wordt in Nederland geïmplementeerd met de Wet weerbaarheid kritieke entiteiten (Wwke). De Wwke heeft als doel het versterken van de fysieke weerbaarheid van kritieke entiteiten. De wet is gericht op bescherming tegen fysieke dreigingen zoals sabotage, natuurrampen, pandemieën en terroristische aanvallen.

4.2.1 Verplichtingen uit de wet

De verplichtingen uit de Wwke voor kritieke entiteiten zijn als volgt:

> Het uitvoeren van een **risicobeoordeling** ten aanzien van alle relevante dreigingen die hun dienstverlening kunnen verstoren
> **Zorgplicht:** op basis van de risicobeoordelingen moeten kritieke entiteiten passende en evenredige maatregelen nemen om incidenten, die de essentiële dienstverlening kunnen verstoren, te voorkomen, de gevolgen van incidenten te beperken en zo spoedig mogelijk te kunnen herstellen als er een incident plaatsvindt

- **Meldplicht:** kritieke entiteiten moeten incidenten die de verlening van hun essentiële diensten aanzienlijk verstoren of kunnen verstoren zo spoedig mogelijk (binnen 24 uur) melden bij de bevoegde autoriteit

4.2.2 Ontwikkelingen

De Wwke wordt naar verwachting in Q2 van 2026 van kracht. Het concept Besluit weerbaarheid kritieke entiteiten (AMVB) ligt momenteel bij de Tweede Kamer. Vervolgens gaat het voor akkoord naar de ministerraad, waarna het voor advies worden voorgelegd aan de Afdeling advisering van de Raad van de State. De AMVB's voor de Cbw en Wwke treden tegelijk met de wetsvoorstellen in werking. De Wwke is vooralsnog niet van toepassing op provincies, omdat de Europese ITS-richtlijn (Intelligent Transport Systems nog geïmplementeerd moet worden in Nederlandse wetgeving. Naar verwachting is deze wetgeving medio 2026 af. Daarna hangt het ervan af of de infrastructuur van provincies wordt aangewezen als kritiek. Dit moet dan per ministeriële regeling gedaan worden, waarna de Wwke van toepassing is op provincies.

4.2.3 Impact op provincies

Wanneer de Wwke voor provincies van kracht wordt bestaat de impact uit de volgende onderdelen:

- Provincies moeten een eigen **risicobeoordeling** uitvoeren ten aanzien van alle relevante dreigingen die hun dienstverlening kunnen verstoren. De kritieke entiteit moet de risicobeoordeling periodiek uitvoeren en herzien. De eerste risicobeoordeling moet uiterlijk negen maanden nadat een organisatie is aangewezen als kritieke entiteit plaatsvinden. Vanaf dat moment is de kritieke entiteit verplicht om de risicobeoordeling ten minste om de vier jaar uit te voeren, of eerder als daar aanleiding toe is.
- **Zorgplicht:** op basis van de risicobeoordelingen moeten provincies passende en evenredige maatregelen nemen om incidenten, die de essentiële dienstverlening kunnen verstoren, te voorkomen, de gevolgen van incidenten te beperken en zo spoedig mogelijk te kunnen herstellen als er een incident plaatsvindt.
- **Meldplicht:** provincies moeten incidenten die de verlening van hun essentiële diensten aanzienlijk verstoren of kunnen verstoren zo spoedig mogelijk (binnen 24 uur) melden bij de bevoegde autoriteit.
- Binnen 10 maanden na de aanwijzing moeten de kritieke entiteiten aan zorgplicht en de meldplicht voldoen.

4.2.4 Bronnen

- Wet weerbaarheid kritieke entiteiten Informatiebrochure, NCTV, 2025.

4.3 AVG

De Algemene Verordening Gegevensbescherming (AVG) heeft als doel om de privacyrechten van personen binnen de EU te beschermen. De AVG is de Nederlandse vertaling van de General Data Protection Regulation (GDPR) van de EU. De AVG kent 6 basisprincipes, in de AVG 'beginselen' genoemd (artikel 5).

4.3.1 Verplichtingen uit de wet

Iedereen die persoonsgegevens verwerkt moet zich houden aan de 6 beginselen van de AVG: rechtmatigheid, behoorlijkheid en transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking en vertrouwelijkheid en integriteit. Dit moet ook aangetoond kunnen worden (de verantwoordingsplicht).

4.3.2 Ontwikkelingen

De AVG is van kracht sinds 25 mei 2018 en geldt voor iedereen die persoonsgegevens verwerkt. Elke EU-lidstaat moet aanvullende wetgeving maken op een aantal punten uit de AVG

4.3.3 Impact op provincies

De AVG brengt meerdere verplichtingen met zich mee voor provincies:

- Er geldt een verantwoordingsplicht, die inhoudt dat provincies moeten kunnen aantonen dat zij zich houden aan de AVG beginselen.
- Provincies zijn verplicht om een FG aan te stellen. De FG is onafhankelijk en controleert of een organisatie de AVG goed toepast en zich aan de privacyregels houdt. Ook geeft de FG advies.
- Provincies moeten DPIAs uitvoeren en maatregelen treffen.
- Provincies moeten technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen.

4.3.4 Bronnen

- https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort
- Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, JenV, 2018.

4.4 Wet politiegegevens (Wpg)

Naast de AVG is er een aparte richtlijn voor gegevensbescherming door politie en justitie (Europese Richtlijn voor gegevensbescherming bij rechtshandhaving (RGR)). Deze richtlijn is in Nederland geïmplementeerd in de Wet politiegegevens (Wpg). De Wpg geeft regels voor de verwerking van persoonsgegevens door bevoegde autoriteiten om strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, en om straffen uit te voeren.

4.4.1 Verplichtingen uit de wet

De uitgangspunten voor gegevensbescherming onder de AVG en Wpg zijn nagenoeg hetzelfde. Er zijn echter ook verschillen. Zo heeft de Wpg een verplichting tot logging, een auditverplichting en zijn er meer beperkingen en uitzonderingen voor de rechten van betrokkenen.

4.4.2 Ontwikkelingen

In Nederland is de RGR per 1 januari 2019 geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) inclusief de daaronder vallende besluiten.

4.4.3 Impact op provincies

Als boa's van provincies politiegegevens verwerken voor opsporing of strafrechtelijk onderzoek valt deze verwerking onder de Wpg. Niet alle provincies hebben boa's. Een aantal provincies geeft aan dat de boa's bij de omgevingsdiensten zijn ondergebracht. Er zijn echter ook provincies die wel zelf boa's hebben en dus aan de Wpg moeten voldoen.

4.4.4 Bronnen

> https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/politie-bijzondere-opsporing-en-justitie/privacywetgeving-voor-politie-en-justitie

5. Innovatie en AI

Het wetgevingscluster innovatie en AI bevat de AI-verordening (EU verordening).

5.1 AI-verordening

De AI verordening heeft als doel dat AI-systemen die gebruikt en ontwikkeld worden veilig zijn en fundamentele rechten respecteren. De regels gaan dus zowel over het gebruiken van AI als over het ontwikkelen van AI. De verordening geldt voor overheden, bedrijven en andere organisaties.

5.1.1 Verplichtingen uit de wet

De verplichtingen uit de wet zijn afhankelijk van het type AI-systeem dat een organisatie gebruikt. De AI-verordening typeert verschillende risicocategorieën waarin AI-systemen onderverdeeld kunnen worden. Afhankelijk van het risiconiveau gelden er per categorie andere regels, waarbij geldt dat hoe meer risico de technologie met zich meebrengt, hoe strikter de regels zijn. De categorieën zijn als volgt:

- **Onaanvaardbaar risico:** systemen met een onaanvaardbaar risico zijn verboden om aan te bieden of te gebruiken. Hieronder vallen systemen die profileren, discrimineren, manipuleren of de vrije keuze van mensen te veel inperken. Dit verbod geldt sinds 2 februari 2025.
- **Hoog risico:** systemen met een hoog risico kennen strenge verplichtingen waaraan voldaan moet worden om deze te mogen aanbieden of gebruiken. Een voorbeeld van een hoog risico systeem is een systeem dat cv's selecteert in een wervingsprocedure. Door middel van maatregelen kun hoge risico's worden voorkomen of worden teruggebracht tot een aanvaardbaar niveau. De verplichtingen voor hoog risico systemen gelden vanaf 2 augustus 2026.
- **Beperkt risico:** voor systemen met een beperkt risico, zoals chatbots en generatieve AI systemen, gelden enkele transparantieverplichtingen. Als deze systemen aangeboden worden moeten gebruikers geïnformeerd worden over het feit dat zij met AI te maken hebben. De transparantieverplichtingen gelden vanaf 2 augustus 2026.

Voor het handhaven van naleving van de AI-verordening worden toezichthouders aangewezen. De toezichthouders kunnen het aanbieden van een bepaald AI systeem verbieden en kunnen boetes opleggen. Er wordt momenteel door het kabinet gewerkt aan de precieze invulling van het toezicht, maar het is waarschijnlijk dat er meerdere toezichthouders zullen worden aangewezen voor verschillende onderdelen van de AI-verordening. De Autoriteit Persoonsgegevens (AP) wordt waarschijnlijk één van deze toezichthouders, mede vanwege haar bestaande rol als toezichthouder op de verwerking van persoonsgegevens door algoritmes.

5.1.2 Ontwikkelingen

De AI-verordening treedt stapsgewijs in werking. De eerste regels gelden sinds 2 februari 2025 in Nederland. Op 2 augustus 2027 zal de gehele wet van toepassing zijn. Het KED heeft in het kader van het UDO traject een impactanalyse van de AI-verordening voor provincies en waterschappen gedaan. Er loopt momenteel nog een analyse door PBLQ naar de kwantitatieve uitvoeringslasten van de implementatie van de AI-verordening.

5.1.3 Impact op provincies

Provincies zijn meestal gebruikers van AI-systemen. In die rol moeten zij voldoen aan bepaalde regels en verplichtingen, waaronder:

- Het uitvoeren van een grondrechteneffectbeoordeling bij systemen met een hoog risico
- Het melden van incidenten
- Het opleiden van medewerkers in AI-geletterdheid
- Het uitvoeren van risicoanalyses voor gebruikte AI-systemen
- Het uitvoeren van monitoring en logging
- Het inrichten van interne controlemechanismen
- Het aanpassen van inkoopprocessen zodat wordt voldaan aan de eisen uit de verordening

5.1.4 Bronnen

- AI-Verordening Impactanalyse voor waterschappen en provincies, KED, 2025.
- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/ai-verordening
- *Kwantificering van kosten door PBLQ volgt nog, onderzoek loopt nu*

6. Samenhang en overlap

Binnen de richtlijnen/verordeningen/wetten die in deze impactanalyse beschreven zijn zit op diverse punten overlap. Er zijn verplichtingen die in meerdere richtlijnen/verordeningen/wetten voorkomen, of die elkaar aanvullen. In dit hoofdstuk wordt er aandacht besteed aan deze samenhang en overlap.

6.1 Wdo en andere wetten

In de handreiking die door het IPO is opgesteld voor de Wdo is ook onderzocht hoe de Wdo zich verhoudt tot andere wetten. De resultaten hiervan zijn als volgt:

De Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) ofwel de nieuwe Algemene wet bestuursrecht (AWB) zegt dat burgers en bedrijven alle producten en diensten van de provincies digitaal moeten kunnen aanvragen (recht op digitaal zakendoen/ recht op elektronisch berichtenverkeer met bestuursorganen).

> De Wdo geeft vervolgens regels over de beveiliging van die toegang.

Op grond van de AWB moeten provincies dit “officieel berichtenverkeer” zo inrichten dat dit voor de aard en inhoud van een bepaald type bericht ‘voldoende betrouwbaar en vertrouwelijk’ verloopt’.

> De Wdo geeft de methode om het vereiste betrouwbaarheidsniveau vast te stellen.

De overheid mag in e-formulieren geen gegevens vragen, die zij voor het nemen van de beschikking niet nodig heeft of die zij al bezit (dataminimalisatie).

> De Wdo inventariseert welke gegevens gevraagd worden tbv het betrouwbaarheidsniveau.

De provincie moet machtigen ondersteunen zoals beschreven in artikel 2:1 lid 1 Awb.

> In de Wdo is dit uitgewerkt in art. 5 lid 6 van de Regeling betrouwbaarheidsniveaus en nader toegelicht op pag. 28 van de memorie van toelichting.

De Algemene verordening gegevensbescherming (AVG) regelt in algemene zin welke persoonsgegevens mogen worden verwerkt.

> De vereiste betrouwbaarheidsniveaus in de Wdo zijn gebaseerd op die kaders.
> Noot: Ook voor verzoeken om inzage of doorhalen van persoonsgegevens (AVG) of documenten (Woo en Who) zal door elke provincie een vereist betrouwbaarheidsniveau bepaald moeten worden.

In de Europese verordening eIDAS (29 sept 2018) worden Europese regels gesteld ten aanzien van digitale identiteit.

> De Wdo geeft de doorvertaling in Nederlandse wetgeving.

In de Europese verordening Single Digital Gateway wordt geregeld dat inwoners en bedrijven uit Europa in het Engels informatie kunnen vinden over de dienstverlening van provincies en vanaf Annex 2/3 ook producten en diensten kunnen afnemen, daarbij inloggend met hun Europees erkende inlogmiddel (erkend in de eIDAS verordening).

> De Wdo verplicht de provincies deze Europees erkende middelen te accepteren.

In de Cbw worden beveiligingsnormen voorgeschreven waar provincies aan moeten voldoen.

> De Wdo geeft regels voor de informatieveiligheid van de 'dienstverleningsprocessen'. Dit valt binnen de bredere scope van de Cbw.

De Wet elektronische publicaties schrijft voor hoe besluiten gepubliceerd moeten worden.

> Het classificatiebesluit van de betrouwbaarheidsniveaus van de (online) diensten van een provincie moet conform deze regels bekendgemaakt worden.

6.2 SDG en DSO

Het grootste deel van de door provincies geïdentificeerde producten die onder de SDG vallen, vallen onder de Omgevingswet. De Omgevingswet wordt ondersteunt door het DSO met een landelijke voorziening om deze procedures digitaal te doorlopen. Om aan de SDG verordening te voldoen is voor het Omgevingsloket een aparte Engelstalige website gemaakt: Get in Touch - Environment and Planning Portal. Hiermee kunnen initiatiefnemers met een Europees erkend inlogmiddel (eIDAS) een overleg aanvragen over een vergunningaanvraag bij Nederlandse gemeenten. Deze website is niet beschikbaar via het Omgevingsloket zelf, maar via de website van Your Europe. Initiatiefnemers kunnen niet rechtstreeks overleggen met provincies, aangezien zij voor veel Europeanen een minder herkenbare bestuurslaag zijn dan gemeenten. Gemeenten zijn verantwoordelijk voor het betrekken van provincies indien nodig en sturen verzoeken die onder de verantwoordelijkheid van provincies vallen door naar provincies.

6.3 SDG en Dienstenwet

De SDG heeft een bredere reikwijdte dan de Dienstenwet. Onder de Dienstenwet vallen verschillende producten voor ondernemers. Onder de SDG vallen nog meer producten voor ondernemers en daarnaast ook producten voor burgers. Vuistregel is dat alle producten waar verplichtingen voor gelden onder de Dienstenwet, ook onder de SDG vallen. Zowel de Dienstenwet als de SDG worden ondersteund door het IMI (Informatiesysteem Interne Markt).

6.4 DGA, Open data richtlijn en AVG

De DGA-impactanalyse van het KED trekt een vergelijking tussen de DGA, de Open data Richtlijn (in Nederland middels de Wet implementatie open data richtlijn geïmplementeerd in de Nederlandse Wet hergebruik van overheidsinformatie (Who)) en de Algemene Verordening Gegevensbescherming (AVG). De Verordeningen en de Richtlijn zijn sterk aan elkaar gerelateerd. Zo vangt de DGA een deel van de data op die buiten de Open Data Richtlijn valt en ook data die niet onder de AVG zou vallen. Daarmee vult de DGA het gat tussen de AVG en Open Data richtlijn. Om verwarring in decentrale praktijk te voorkomen, wordt in de DGA-impactanalyse uiteengezet welke data onder de Open Data Richtlijn vallen en welke onder de DGA.

6.5 Woo en Archiefwet

De Woo is van toepassing zolang documenten zich bij de overheidsorganisatie bevinden. Zodra de documenten zijn overgedragen aan het archief, geldt de Archiefwet. Wanneer een verzoek om informatie wordt gedaan op grond van de Woo maar de betreffende documenten al overgebracht zijn naar het archief, is de Woo niet van toepassing. In dat geval gelden de openbaarmakingsregels van de Archiefwet.

Er zijn ook diverse andere wetten en regels die aan de Woo of de Archiefwet raken en soms ook aanvullende eisen aan de informatiehuishouding van provincies stellen. In het meerjarenplan informatiehuishouding van het IPO worden de volgende wetten en regels genoemd:

- De Wet implementatie Open Data richtlijn implementeert de Europese Open Data richtlijn in de Wet hergebruik van overheidsinformatie. Deze wet verplicht provincies om op verzoek overheidsinformatie als open data beschikbaar te stellen voor hergebruik. Dat hergebruik kan zowel maatschappelijke als commerciële doelstellingen hebben.
- Het Besluit digitale toegankelijkheid overheid stelt eisen aan alle websites en apps inclusief content van de overheid. En dus ook aan documenten als deze op grond van de Woo gepubliceerd worden.
- De Algemene Verordening Gegevensbescherming (AVG). De AVG is complementair aan de Archiefwet en de Woo. Dat betekent dat bij het uitvoeren van de Archiefwet en de Woo rekening moet worden gehouden met de AVG.
    - Op advies van de Autoriteit Persoonsgegevens (AP) zijn de beginselen van de AVG meer geïntegreerd in de nieuwe Archiefwet. Overheidsorganisaties die zich houden aan de Archiefwet, voldoen daarbij automatisch ook aan de AVG.
    - Er is een spanningsveld tussen de Woo en de AVG. Het openbaar maken van informatie die persoonsgegevens bevat kan in strijd zijn met de AVG, terwijl het achterhouden ervan in strijd kan zijn met de Woo. Overheidsorganisaties moeten hier een juiste afweging in maken, wat een complex en tijdrovend juridisch proces kan zijn.
    - Bij het beheer van persoonsgegevens hebben overheidsorganisaties te maken met de Archiefwet én de AVG. De handout ‘Weten of vergeten’ van de KVAN (2024) geeft handvatten en aanwijzingen voor de omgang met beide, in onderlinge samenhang.

6.6 Cbw en Wwke

De Cbw richt zich op digitale (cyber)risico's voor netwerk- en informatiesystemen, de Wwke richt zich op fysieke dreigingen. Beide wetten kennen een zorgplicht op basis van risicoanalyses en een meldplicht bij incidenten.

6.7 AI-verordening, AVG en Cbw

De AI-verordening heeft een sterke relatie met andere wetgeving en richtlijnen op het gebied van informatiebeveiliging, privacy en ethiek, zoals de AVG en de Cbw. De AI-verordening, de AVG en de Cbw vormen samen een belangrijk juridisch kader voor verantwoord en veilig gebruik van digitale technologie bij overheden. Ze hebben elk een eigen focus, maar overlappen op cruciale punten.
De AI-verordening richt zich op het reguleren van het ontwikkelen, inkopen en gebruiken van AI-systemen, met nadruk op transparantie, risicobeheer en menselijk toezicht. De AVG waarborgt de bescherming van persoonsgegevens, die essentieel is bij AI-systemen die vaak grote hoeveelheden data verwerken. De Cbw richt zich op cyberbeveiliging en continuïteit van data, digitale systemen en infrastructuren. AI-systemen vallen daar ook onder, maar hebben bijzondere eigenschappen en risico's waarmee rekening moet worden gehouden.

Er zijn verschillende situaties waarin er raakvlakken zijn:

- AI-systemen die persoonsgegevens verwerken, moeten voldoen aan eisen van zowel de AI-verordening als de AVG, denk aan dataminimalisatie, rechtmatigheid en uitlegbaarheid van algoritmes.
- De verplichtingen rond risicobeheer en beveiliging uit de AI-verordening sluiten direct aan bij de Cbw-eisen voor cyberbeveiliging en incidentmanagement.
- Transparantie en verantwoordingsplicht zijn in alle drie de wetten terug te vinden; samenhang en consistentie in governance, processen, documentatie en audits is dus belangrijk.

Bijlage A: Bronnenlijst

- Single Digital Gateway (SDG) Annex II en III: Handreiking voor implementatie minimale scenario, IPO, 2024
- Memo Borging Single Digital Gateway, IPO, 2025
- Informatie over IMI: https://europadecentraal.nl/praktijkvraag/praktijkvraag-imi-functionaliteit-en-gebruik-voor-decentrale-overheid/#
- Factsheet DSA, ICT Recht
- DSA Leidraad: Zorgvuldigheidsverplichtingen tussenhandeldiensten, ACM, 2024
- De Dienstenrichtlijn: Handreiking voor decentrale overheden, BZK, 2009.
- Checklist: Voldoen aan de Dienstenwet, BZK, EZK, RVO en KED, 2020.
- https://europadecentraal.nl/onderwerp/digitale-overheid/digitale-samenleving/verordening-europese-digitale-identiteit-eidas2-0/
- Uitvoeringsanalyse Digital Decade eIDAS 2.0, VNG, 2025.
- Programma EDI-stelsel NL, via https://edi.pleio.nl/
- In werking, maar onderbenut. Reflectierapport Omgevingswet 2024, Evaluatiecommissie Omgevingswet, 2025.
- Informatiepunt Leefomgeving, via https://iplo.nl/
- Handreiking Wet Modernisering Elektronisch Bestuurlijk Verkeer, IPO, 2022.
- Handreiking implementatie Wet modernisering elektronisch bestuurlijk verkeer, BZK, 2023.
- Implementatiesteun Wmebv, VNG.
- Handreiking implementatie Wet digitale overheid, IPO.
- Data Governance Verordening: Impactanalyse, KED, 2023.
- Uitvoeringsanalyse Digital Decade: Dataregelgeving, VNG, 2024.
- Handleiding Herziene Who nav de Wet implementatie open data richtlijn, BZK, VNG, IPO, UvW, NA, KED, 2024.
- https://www.koopoverheid.nl/voor-overheden/gemeenten-provincies-en-waterschappen/bekendmakingswet
- https://www.koopoverheid.nl/voor-overheden/gemeenten-provincies-en-waterschappen/drop/presentaties-roadshow
- Meerjarenplan Digitale Informatiehuishouding Provincies, IPO, 2025
- Monitor implementatie Wet open overheid Provincies 2025, IPO, 2025
- Impactanalyse NIS2 voor de 12 provincies, PBLQ, 2024.
- Toezicht in het kader van de Cyberbeveiligingswet: Naar gelaagd én geslaagd toezicht, PBLQ, 2025.
- Wet weerbaarheid kritieke entiteiten Informatiebrochure, NCTV, 2025.
- https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/politie-bijzondere-opsporing-en-justitie/privacywetgeving-voor-politie-en-justitie
- Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, JenV, 2018.

- https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/politie-bijzondere-opsporing-en-justitie/privacywetgeving-voor-politie-en-justitie
- AI-Verordening Impactanalyse voor waterschappen en provincies, KED, 2025.
- https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/ai-verordening
- Weten of vergeten? hand-out Archiefwet & AVG, KVAN, 2024 via https://www.kvan.nl/nieuws/hand-out-weten-of-vergeten-avg-archiefwet-verschenen/

E-mail: digitalisering@ipo.nl

Den Haag
Herengracht 23