

September 2026

Onderzoeksrapport

Verkenning van wet- en regelgeving over
informatiehuishouding van de overheid

Inhoudsopgave

<i>Managementsamenvatting</i>	5
Aanleiding en urgentie.....	5
Opdracht, onderzoeksvraag en doel.....	5
Beoordelingskader.....	5
Belangrijkste bevindingen.....	6
Conclusie voor besluitvorming.....	10
Inleiding	12
<i>Kern van dit rapport</i>	14
<i>De vijf pijlers</i>	14
1. Pijler 1: Coherente sturing en governance	16
1.1. <i>Antwoord op de kernvraag</i>	16
1.1.1. Digital Decade als sturingsmechanisme.....	16
1.1.2. Juridisch bindend.....	18
1.1.3. Gewenste informatiehuishouding van de overheid.....	20
1.1.4. Staats- en bestuursrechtelijke structuur.....	22
1.1.5. Concluderend.....	22
1.2. <i>Mandaat</i>	23
1.2.1. Toelichting deelvraag.....	23
1.2.2. Concluderend.....	24
1.3. <i>Interbestuurlijke werking</i>	25
1.3.1. Toelichting deelvraag.....	25
1.3.2. Concluderend.....	28
1.4. <i>Planning, controle en rapportage</i>	28
1.4.1. Toelichting deelvraag.....	28
1.4.2. Concluderend.....	29
1.5. <i>Toezicht en handhaving</i>	30
1.5.1. Toelichting deelvraag.....	30
1.5.2. Concluderend.....	32
2. Pijler 2: Semantische en technische interoperabiliteit	33
2.1. <i>Antwoord op de kernvraag</i>	33
2.2. <i>Begrippen</i>	34
2.2.1. Toelichting deelvraag.....	34
2.2.2. De verhouding tussen begrippen.....	35
2.2.3. Strategische analyse.....	37
2.2.4. Concluderend.....	40
2.3. <i>Technische standaarden</i>	41
2.3.1. Toelichting deelvraag.....	41
2.3.2. Technische standaarden.....	43
2.3.3. Handhaving.....	47
2.3.4. Concluderend.....	47
2.4. <i>Keteninteroperabiliteit</i>	48
2.4.1. Toelichting deelvraag.....	48
2.4.2. Concluderend.....	50

2.5. EU-interoperabiliteit.....	50
3. Pijler 3: Integrale kwaliteit en zorgplicht.....	51
3.1. Antwoord op de kernvraag.....	51
3.1.1. De behoefte aan eenduidige kaders en invulling.....	51
3.1.2. Afstemming en begeleiding.....	53
3.1.3. Concluderend.....	54
3.2. Generieke zorgplicht.....	54
3.2.1. Juridische afdwingbaarheid.....	57
3.2.2. Concluderend.....	58
3.3. Informatiebeveiliging, privacy en governance.....	59
3.3.1. UAVG.....	64
3.3.2. Namen, termen en definities die de lading dekken.....	65
3.3.3. Terug naar de kern.....	65
3.3.4. Concluderend.....	66
3.4. Monitoring en kwaliteit.....	66
3.4.1. Concluderend.....	67
4. Pijler 4: Maatschappelijke functionaliteit.....	67
4.1. Antwoord op de kernvraag.....	68
4.2. Burgerrechten.....	69
4.2.1. Toelichting deelvraag.....	69
4.2.2. Openbaarheid.....	70
4.2.3. Toegang, correctie en inzicht.....	70
4.2.4. Navolgbaarheid.....	71
4.2.5. Concluderend.....	72
4.3. Proactieve en passende dienstverlening.....	72
4.3.1. Toelichting deelvraag.....	72
4.3.2. Proactief.....	73
4.3.3. Grenzen van proactieve dienstverlening.....	74
4.3.4. Concluderend.....	75
4.4. Transparantie.....	75
4.4.1. Toelichting deelvraag.....	75
4.4.2. Concluderend.....	77
5. Pijler 5: Oplossend en lerend vermogen.....	78
5.1. Antwoord op de kernvraag.....	78
5.1.1. Gegevensdeling.....	79
5.1.2. Datakwaliteit.....	79
5.1.3. Standaardisatie.....	80
5.1.4. Concluderend.....	80
5.2. Knelpuntenmechanismen en escalatie.....	80
5.2.1. Toelichting deelvraag.....	80
5.2.2. CIO Rijk.....	83
5.2.3. Concluderend.....	83
5.3. Lerend vermogen.....	83
5.3.1. Toelichting deelvraag.....	83
5.3.2. Basisregistraties.....	84
5.3.3. AVG.....	84

5.3.4.	Archiefwet.....	85
5.3.5.	BIO	85
5.3.6.	Concluderend.....	85
5.4.	<i>Innovatie en experiment</i>	85
5.4.1.	Toelichting deelvraag.....	85
5.4.2.	Wdo.....	86
5.4.3.	Participatiewet.....	86
5.4.4.	Wgds.....	86
5.4.5.	Europees niveau.....	87
5.4.6.	Concluderend.....	87
5.5.	<i>Professionalisering en vakmanschap</i>	88
5.5.1.	Toelichting deelvraag.....	88
5.5.2.	Functionaris gegevensbescherming.....	88
5.5.3.	Archiefprofessionals	89
5.5.4.	Chief Information Officer	89
5.5.5.	Chief Information Security Officer	89
5.5.6.	AI-verordening	89
5.5.7.	Concluderend.....	89
Concluderend		90
<i>Inzicht door overzicht: technologische basis en juridische analyse per sector</i>		<i>92</i>
Afkortingenlijst.....		94
Bijlagen.....		96
<i>Bijlage 1: Overzicht begrippen 'informatieobject'</i>		<i>96</i>
<i>Bijlage 2: Overzicht van zorgplichten bij Pijler 3</i>		<i>102</i>
	Internationale verdragen	102
	Europese verordeningen	103
	Europese richtlijnen	105
	Nederlandse (uitvoerings)wetten.....	105
	Lagere nationale uitvoeringsregels.....	109

Managementsamenvatting

Aanleiding en urgentie

Een goed functionerende informatiehuishouding van de overheid is essentieel om de rechten van burgers in de praktijk te brengen. Daarnaast is het fundamenteel voor een goed werkend bestuur en om de democratische rechtsstaat in de digitaliserende wereld te kunnen ondersteunen. Het belang van een goed functionerende informatiehuishouding is herhaaldelijk benadrukt: in het actieplan 'Open op Orde' (2021), in de daaropvolgende programma's en in het coalitieakkoord van januari 2026.

Tegelijkertijd blijkt dat de huidige informatiehuishouding van de overheid onvoldoende aansluit bij deze ambities. Ondanks diverse initiatieven ontbreekt het aan samenhang, sturing en uitvoerbaarheid. De groeiende digitalisering en toenemende afhankelijkheid van burgers van digitale overheidsdiensten vergroten de urgentie om deze knelpunten structureel aan te pakken.

Opdracht, onderzoeksvraag en doel

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verzocht ICTRecht om een onderzoek en rapportage om inzicht te bieden in het huidige landschap aan (data)wet- en regelgeving in verband met de verbetering van de informatiehuishouding. Dit in relatie tot het voorstel van de Algemene informatiewet overheid (Aiw).

In de voorbereiding van deze opdracht creëerden BZK en ICTRecht een toetsingskader van pijlers en bijbehorende criteria. Deze pijlers illustreren de gewenste benodigdheden om tot een verbeterde informatiehuishouding van de overheid te komen. De Aiw heeft ook ten doel de informatiehuishouding van de overheid te verbeteren en ambieert (deels) dezelfde doelstellingen als geïllustreerd met de pijlers.

De kernvraag luidt: in hoeverre bestaande wet- en regelgeving ten aanzien van informatieobjecten de verbetering van de informatiehuishouding (belegd in de vijf pijlers) al realiseert of kan realiseren, ten opzichte van de conceptversie van de Aiw en de bedoelingen hierachter?

Door op basis van deze afgestemde structuur inzicht te bieden in het huidige landschap aan datawet- en regelgeving, illustreert het rapport in hoeverre de huidige status quo (zonder een geldende Aiw) al opties biedt ter verbetering van de informatiehuishouding.

Zo dient dit rapport als hulpstuk in de verdere besluitvorming over het verbeteren van de informatiehuishouding dan wel over het aannemen van een Aiw en het faciliteren van veilige en verantwoorde gegevensuitwisseling binnen de overheid.

Beoordelingskader

Dit rapport is opgebouwd uit vijf pijlers.

Pijler 1: Coherente sturing en governance. In hoeverre biedt het bestaande wettelijke en beleidsmatige instrumentarium een bindend overheidsbreed sturingsmechanisme voor de gewenste informatiehuishouding?

Pijler 2: Semantische en technische interoperabiliteit. In welke mate faciliteren bestaande kaders uniforme begrippen, standaarden en technische interoperabiliteit die noodzakelijk zijn voor vrij verkeer van gegevens (of informatieobjecten)?

Pijler 3: Integrale kwaliteit en zorgplicht. In hoeverre waarborgen huidige kaders de generieke kwaliteit, toegankelijkheid en veiligheid van overheidsinformatie gedurende de gehele levenscyclus van informatie?

Pijler 4: Maatschappelijke functionaliteit. In welke mate ondersteunen bestaande juridische kaders de informatieverhouding overheid-burger en dragen zij bij aan transparante, proactieve en toegankelijke publieke dienstverlening?

Pijler 5: Oplossend en lerend vermogen. In hoeverre maken bestaande juridische instrumenten het mogelijk om structurele knelpunten in gegevensdeling, kwaliteit en standaardisatie tijdig te signaleren en duurzaam op te lossen?

Belangrijkste bevindingen

Pijler 1: Coherente sturing en governance

Het Europese beleidsprogramma voor het digitale decennium (de Digital Decade) van de Europese Unie (EU) is een belangrijk sturingsmechanisme voor de Nederlandse overheid. De Digital Decade is gericht op het realiseren van een mensgerichte, duurzame en inclusieve digitale transformatie. Digitalisering van overheidsdiensten is een van de vier prioriteiten waarbinnen de doelstellingen van de Digital Decade gegroepeerd zijn. De stip aan de horizon is dat Europa in 2030 volledig digitaal functioneert en dat alle Europese burgers toegang hebben tot digitale overheidsdiensten via veilige identificatie- en authenticatieoplossingen.

Er bestaat een samenwerkingscyclus tussen de EU en de lidstaten ten aanzien van de uitvoering van de Digital Decade. De uitwerking van de Digital Decade bestaat uit onder meer verordeningen en richtlijnen van de EU. Deze zijn juridisch afdwingbaar.¹ Zo is de sturing vanuit de EU voor de Nederlandse overheid belangrijk en bepalend. Er zijn de afgelopen jaren diverse voorstellen geïntroduceerd voor nationale uitvoeringswetten bij verordeningen en implementatiewetten bij richtlijnen. Een aantal daarvan is al definitief aangenomen en een aantal nog niet.²

Nederland kent de Nederlandse Digitaliseringsstrategie (NDS) en diverse programma's, commissies, adviesorganen en colleges die allemaal ten doel hebben de informatiehuishouding van de overheid te verbeteren. Denk aan de Nationale Technologiestrategie, het Federatief Datastelsel, de Interbestuurlijke Datastrategie (IBDS), het programma Open op Orde, de Centrale Commissie Gegevensgebruik, de Adviesfunctie Verantwoord Datagebruik en het Overheidsbreed Beleidsoverleg Digitale Overheid. Hoewel de diverse programma's en initiatieven allemaal gericht zijn op het bijdragen aan de gewenste informatiehuishouding, is nog niet duidelijk in hoeverre de NDS en andere genoemde programma's juridisch afdwingbaar zijn en hoe zij nu precies samenhangen. Wenselijk is om de samenhang tussen de verschillende

¹ Zowel het naleven van verordeningen als het implementeren van richtlijnen.

² De implementatiewet voor de NIS2-richtlijn moest in oktober 2024 worden aangenomen maar is (aanzienlijk) vertraagd. Hier loopt Nederland een risico op sancties vanuit de EU.

programma's en projecten en de samenwerkingscyclus met de EU zoveel mogelijk te verduidelijken en te verbeteren.

Pijler 2: Semantische en technische interoperabiliteit

De tweede pijler van dit rapport duikt in de semantiek van verschillende wetten en de technische interoperabiliteit. Het woord 'informatieobject' is een centrale term. Daarmee wordt in conceptvoorstellen van Nederlandse wetgeving een overkoepelende term geïntroduceerd. Er zijn allerlei termen die in wetgeving over informatiehuishouding worden behandeld, die óf onder de term informatieobject vallen óf als gelijk hieraan kunnen worden beschouwd. Denk hierbij aan document, data, gegevens of archiefbescheiden.

Die objecten worden allemaal beheerst door een eigen stelsel van regels.³ Hoewel de ambitie van de Nederlandse overheid ten aanzien van de verbetering van de informatiehuishouding (enigszins) centraal volgt uit overkoepelende programma's, kennen de begrippen die terugkomen in de uitvoering (wetgeving) geen eenduidige semantiek.

De moeilijk overzichtelijk te maken hoeveelheid wetgeving die er al is, leidt er bovendien toe dat het steeds complexer wordt om bij het maken van nieuwe wetgeving onbedoelde inconsistenties of interacties met bestaande wetgeving te vermijden.

De Europese structuur van terminologie wijkt op sommige vlakken af van de Nederlandse structuur. De Europese wetgever reguleert 'gegevens', daar waar in de huidige situatie Nederlandse wetten juist ook de vorm waarin gegevens gevat zijn reguleren, zoals een document of archiefbescheiden. De Europese wetgever verwijst in haar wetgeving naar andere stukken voor definities en erkent een gelaagdheid van definities, zoals uitgebeeld in de verhouding van metagegevens tot andere termen in het voorbeeld hieronder:

Gegevens	
Persoonsgegevens	Niet-persoonsgebonden gegevens
Metagegevens	

In de huidige Nederlandse regelgeving is er nog geen overkoepelende definitie van 'informatieobject' of een object dat daaronder valt. Het is logisch dat de Aiw daarom met een voorstel voor de definitie komt. Definities ten aanzien van informatieobject zijn in Nederlandse wetgeving gespecificeerd op het doel van de wet, zoals het archiveren of publiek beschikbaar stellen van gegevens. Daardoor kent eenzelfde woord ('document') verschillende definities uit verschillende stukken wetgeving. Er bestaan daarnaast definities naast elkaar, die onderdeel van elkaar kunnen zijn (zoals 'gegevens' die onderdeel zijn van een 'document'). Tussen die definities is er geen duidelijke hiërarchie of heldere verhouding (zie voorbeeld hieronder), hoewel deze in de praktijk overlappen.

Informatieobject				
Archiefbescheiden	Document	Document 2	Gegevens	Publieke informatie

³ Bijvoorbeeld de Archiefwet, de Wet open overheid (Woo) of de Dataverordening.

Uit Europese en nationale wetgeving volgen technische vereisten voor overheidsorganen, zoals machineleesbaarheid, open formats, interoperabiliteit, beveiliging, anonimisering en soms overige maatregelen die (nog) niet zijn vastgesteld. Ten aanzien van beveiligingsvereisten gelden verschillende eisen die zich kunnen opstapelen voor eenzelfde situatie of overheidsorgaan. Denk hierbij aan de Algemene verordening gegevensbescherming (AVG) (alleen bij persoonsgegevens, open norm), de Baseline Informatiebeveiliging Overheid 2, de Cyberbeveiligingswet, de (Uitvoeringswet) Cyberbeveiligingsverordening en eventueel zelfs de (Uitvoeringswet) Verordening cyberweerbaarheid. Veel van de cyberbeveiligingseisen zijn juridisch afdwingbaar, maar uitvoering en toezicht moeten grotendeels nog worden ingeregeld.

Pijler 3: Integrale kwaliteit en zorgplicht

De derde pijler gaat in op integrale kwaliteit en zorgplichten. Een zeer omvangrijk thema. Een zorgplicht kan algemeen worden omschreven als een plicht om zorgvuldig te handelen en de belangen van anderen te beschermen, of om schade aan mens en milieu te voorkomen. Zorgplichten voor de overheid om juistheid, veiligheid en privacy van informatie te borgen volgen uit verschillende Europese en nationale wetten en besluiten.

Er is veel sectorale wetgeving die specifiek invulling geeft aan zorgplichten. Hoewel dit logisch lijkt bij de opzet van een sectorale wet, is er hierdoor ook een gebrek aan integrale samenhang van dergelijke plichten. Dit leidt tot tegenstrijdigheden en onduidelijkheden en beperkt interoperabiliteit als bedoeld in de vorige pijler. De samenhang en consistentie hiervan moeten verbeterd worden.

De wettelijke regels over de informatiehuishouding en de zorgplichten voor het borgen van de informatiekwaliteit door de overheid zouden eenduidig antwoord moeten kunnen geven op onder andere de volgende vragen:

- Wie mag of moet welke rechten hebben om de betreffende gegevens te verwerken (zoals aanmaken, inzien, aanpassen, doorgeven, verwijderen)?
- In welke (ICT- en/of AI-)systemen mag of moet de informatie worden verwerkt?⁴
- Hoe lang moeten de gegevens worden bewaard en wanneer vernietigd?
- Wat zou er bij het verwerken van de gegevens fout kunnen gaan; wie lijdt er hoeveel schade of ander (ernstig) nadeel als de gegevens onjuist zijn of de beveiliging wordt aangetast?
- Wat moeten we redelijkerwijs doen of laten (ter invulling van onze zorgplicht) om de kans en impact daarvan tot een acceptabel niveau terug te dringen?
- Hoe zien we erop toe dat de maatregelen die we hebben geselecteerd ook goed zijn geïmplementeerd en hoe evalueren we periodiek of onze inschatting van de risico's en de reductie daarvan door onze maatregelen (nog steeds) juist is?

Een significant probleem voor de feitelijke uitvoerbaarheid, toepasbaarheid en onderlinge consistentie en interoperabiliteit van de huidige kaders en zorgplichten is dat diverse wetten en regels aan de ene kant een risicogebaseerde benadering

⁴ Deze vraag vormt een kern van de zorgplicht die het voorstel voor de Aiw introduceert in art. 7, namelijk de plicht voor ieder overheidsorgaan om te zorgen 'dat de door haar gebruikte informatiesystemen geschikt zijn voor het verkeer van informatieobjecten binnen, tussen en met overheidsorganen'.

voorschrijven maar aan de andere kant specifieke bepalingen bevatten die juist afbreuk kunnen doen aan de mogelijkheid om risico's optimaal in samenhang of integraal in te schatten en te beperken. De grote hoeveelheid specifieke (zorg)plichten die tegelijkertijd op dezelfde gegevens en (ICT- en AI-)systemen van toepassing kunnen zijn, maakt het toepassen van de huidige kaders om antwoorden te geven op concrete vragen als hierboven omschreven, complex en tijdrovend.

Aan te raden is om een begrijpelijke maar paradoxale reflex te bedwingen. Die reflex is om het probleem dat er (te) veel wetgeving naast elkaar van toepassing is op dezelfde gegevens, die moeilijk met elkaar te verenigen en integraal toe te passen zijn, aan te pakken met nóg weer een nieuwe wet. In dit verband kan verbetering eerder worden gezocht in het gericht schrappen van onduidelijke wetgeving en het verbeteren van de coherentie en consistentie van lagere wet- en regelgeving met hogere.

Pijler 4: Maatschappelijke functionaliteit

De vierde pijler gaat in op de juridische waarborgen op het gebied van transparantie. Op het gebied van toegang, correctie en inzicht kent de privacywetgeving stevige juridische waarborgen zoals de AVG en de Wet politiegegevens (Wpg). Toegang krijgen tot gegevens is mogelijk zowel via de Wet open overheid (Woo) als via privacywetgeving. De Woo reguleert allerhande gegevens, terwijl privacywetgeving uitsluitend de gegevens beheerst die zijn te classificeren als persoons- of politiegegevens. Ten aanzien van het correctierecht is het belangrijk te erkennen dat de waarborging daarvan binnen het overheidsdomein als lastig wordt ervaren.

Ook openbaarheid als onderdeel van burgerrechten is in de Woo stevig verankerd. De Woo borgt een verruimde proactieve plicht (ten opzichte van haar voorganger, de Wet openbaarheid van bestuur) tot openbaarmaking door overheidsorganen. De digitale infrastructuur die deze proactieve openbaarmaking moet borgen, komt echter moeilijk van de grond. Dit heeft mede te maken met de technische architectuur en afhankelijkheden van stakeholders.

Navolgbaarheid van beslissingen, als onderdeel van burgerrechten, is minder expliciet verankerd in de wet, hoewel besluitvorming juist gemotiveerd en gevolgd moet kunnen worden. Navolgbaarheid volgt wél impliciet uit principes van motivering en transparantie (Algemene wet bestuursrecht, Awb). De komst en het gebruik van kunstmatige intelligentie (AI) zetten navolgbaarheid, en daarmee het kunnen motiveren van besluiten, echter onder druk.

Dienstverlening van de overheid is breder dan uitsluitend het bieden van transparantie over gegevens; het gaat ook om het actief informeren van burgers over hun rechten. Dit wordt met name bemoeilijkt door privacywetgeving, zoals al is gebleken bij de totstandkoming van de Wet proactieve dienstverlening SZW en andere wetten. Als een gegeven geen persoons- of politiegegevens bevat, is het openbaar maken daarvan minder strikt gereguleerd. De lastigheid zit hem dan in de wettelijke kaders die bevoegdheden tot het delen van gegevens legitimeren, die niet altijd even expliciet zijn.

De Wpg en de AVG kennen informatierechten aan personen toe op het gebied van transparantie en verantwoording. De Wpg kent een strenger informatierecht door

de aard van de betrokken gegevens: politietaken kunnen immers bemoeilijkt worden als bepaalde informatie (vroegtijdig) bekend wordt. Dit voorbeeld illustreert de moeilijkheid om gegevens qua juridische terminologie gelijk te moeten, willen of kunnen trekken. Zelfs dezelfde soort gegevens in de vorm van persoonsgegevens kunnen immers afhankelijk van hun gebruikscontext aan verschillende vormen van transparantie onderworpen worden. De mate waarin de inzage en uitleg gegeven dienen te worden, is echter anders per wet.

De huidige inrichting van de overheid ondersteunt een proactieve en responsieve dienstverlening richting burgers nog onvoldoende. Hoewel bestaande juridische kaders, zoals de Grondwet, Woo, Awb, Archiefwet en privacywetgeving, een stevig fundament bieden voor transparantie, openbaarheid en burgerrechten, ontbreekt het aan samenhang en praktische uitvoerbaarheid. Burgerrechten zoals toegang, inzage en correctie zijn juridisch goed geborgd, maar navolgbaarheid en de vertaling naar de praktijk blijven complex door versnippering van systemen, gegevens en regelgeving. Voor proactieve dienstverlening is het juridische kader minder ontwikkeld. Hierdoor draagt de informatiehuishouding nog onvoldoende bij aan een toegankelijke en begrijpelijke overheid.

Pijler 5: Oplossend en lerend vermogen

De vijfde en laatste pijler gaat in op het juridisch kader om knelpunten in de informatiehuishouding te detecteren. Het huidige juridische kader voor gegevensdeling, datakwaliteit en standaardisatie wordt gekenmerkt door sterke fragmentatie. Een veelheid aan Europese en nationale wetten, sectorale regelingen en beleidsinstrumenten bevat zowel overlappende als tegenstrijdige bepalingen, waardoor het lastig is om knelpunten tijdig te signaleren en structureel op te lossen. Bovendien kunnen signalen uit allerlei invalshoeken en richtingen komen, wat het opvangen daarvan op een centraal punt bemoeilijkt. Het huidige juridische instrumentarium is ten aanzien van het tijdig signaleren en oplossen van knelpunten in gegevensdeling, kwaliteit en standaardisatie onvoldoende. Hoewel er binnen de huidige juridische kaders bepalingen te vinden zijn die omgang met knelpunten reguleren, is deze omgang hoofdzakelijk gericht op reactief handelen, in plaats van stelselmatige preventieve monitoring.

Voor datakwaliteit en standaardisatie bestaan deels expliciete juridische waarborgen, met name binnen het privacydomein en specifieke registers, maar deze zijn veelal gericht op individuele correcties en niet op structurele kwaliteitsverbetering. Toezicht en monitoring vinden bovendien slechts beperkt en niet stelselmatig plaats. Op het gebied van standaardisatie zijn wel stappen gezet, maar de toepassing en reikwijdte blijven vooralsnog beperkt. Al met al biedt het huidige stelsel onvoldoende basis voor proactieve, overheidsbrede sturing. Een samenhangend en wettelijk verankerd kader, zoals beoogd met de Aiw, kan bijdragen aan structurele verbetering en betere beheersing van deze knelpunten.

Conclusie voor besluitvorming

De doelen van de Aiw vinden brede steun in Europese en nationale wet- en regelgeving, met name ten aanzien van het vrije verkeer van informatieobjecten en het wegnemen van belemmeringen voor gegevensdeling. De uitwerking van deze doelen is in het huidige juridische landschap te breed, te complex en te gefragmenteerd. Dit zorgt ervoor dat het voor overheidsorganisaties in de praktijk te complex is om consequent helder antwoord te kunnen geven op de vraag of informatieobjecten of gegevens gedeeld moeten of mogen worden. Aanvullende

inspanningen zijn nodig om binnen het huidige landschap van beleid en wet- en regelgeving de informatiehuishouding van de overheid structureel te kunnen verbeteren. Elke alternatieve oplossing in het huidige landschap die informatiehuishouding kan verbeteren, is afhankelijk van het bestaande landschap van wetgeving. Daarom is (sectoraal) inzicht in de huidige stand van zaken onmisbaar en aanvullend een analyse of alle facetten gewenst zijn en bijdragen aan de doelen uit de nationale en Europese programma's. Op basis daarvan moeten volgende stappen worden bepaald. Zonder inzicht blijft het antwoord op de simpele kernvraag uit de praktijk, "mag ik dit delen?", continu verschuiven.

Inleiding

*"Voor het goed functioneren van onze democratische rechtsstaat is het essentieel dat de rijksoverheid haar informatiehuishouding op orde heeft."*⁵

Een informatiehuishouding op orde draagt bij aan volledigheid en betrouwbaarheid van overheidsinformatie en dient zodoende de democratische verantwoording. Daarom is in 2021 het actieplan 'Open op Orde' aangeboden aan de Tweede Kamer. Na dit actieplan zijn diverse andere plannen gepresenteerd die streven naar een toegankelijke overheid met een gedegen informatiehuishouding.⁶ Het belang van al deze plannen is nog eens benadrukt in het coalitieakkoord 'Aan de slag' dat in januari 2026 is gepresenteerd. Het akkoord spreekt de ambitie uit om Nederland koploper in de digitale wereld te maken.⁷ Digitaal betrouwbaar, toegankelijk, efficiënt en weerbaar. Zo moet de overheid er volgens het coalitieakkoord uitzien.

In 2024 heeft het onafhankelijke Adviescollege Openbaarheid en Informatiehuishouding (ACOI) in zijn rapport 'Alles is *niets*'⁸ geconcludeerd dat de meerjarenplannen⁹ enerzijds zorgen voor het op gang brengen van een goede beweging, maar anderzijds door een veelheid aan losse plannen en gebrek aan samenhang onvoldoende effectief zijn. Het advies van het ACOI is dan ook om te komen tot een nationale aanpak.

De Nederlandse Digitaliseringsstrategie (NDS) 'Samen versnellen' is zo'n aanpak. In dat kader heeft de overheid de behoefte om data onderling uit te wisselen. Ruw gezegd is dit noodzakelijk om aan haar taken te kunnen voldoen. Op dit moment beantwoordt de informatiehuishouding van de overheid niet aan deze behoefte, mede door complexe en strenge wet- en regelgeving die zichzelf lijkt tegen te spreken. De initiatiefnemer van de voorgestelde Algemene informatiewet overheid (Aiw) wil hier een oplossing voor bieden, door een kader voor informatieobject-uitwisseling op te zetten.

De Europese Unie (EU) publiceerde in 2022 haar beleidsprogramma voor het digitale decennium van Europa (dat vooral onder de Engelstalige benaming bekend is en aangeduid wordt met 'Digital Decade'). Dit beleidsprogramma moet ervoor zorgen dat Europa in 2030 digitaal concurrerend, veilig en inclusief is via meetbare doelstellingen voor (1) vaardigheden, (2) infrastructuur, (3) digitaal zakendoen en (4) digitale overheidsdiensten.¹⁰ De Europese regelgeving die uit de Digital Decade voortvloeit, betreft de digitale (data)huishouding van de EU en kent daarom veel overlap met alle hierboven genoemde stukken Nederlands beleid en regelgeving. Voor de analyse van de huidige en gewenste informatiehuishouding van de

⁵ Zie *Kamerstukken II* 2020/21, 29362, nr. 291, p. 1.

⁶ Zie onder andere 'Meerjarenplan Digitale informatiehuishouding 2026-2030' en 'Meerjarenplan Openbaarheid en Informatiehuishouding Rijksoverheid 2026-2030' en het herijkte actieplan 'Open Overheid 2023-2027'.

⁷ Zie 'Aan de slag, Bouwen aan een beter Nederland', Coalitieakkoord 2026-2030, D66, VVD en CDA, p. 58.

⁸ Zie 'Alles is *niets*', Advies over meerjarenplannen van de overheid voor de digitale informatiehuishouding, Adviescollege Openbaarheid en Informatiehuishouding (ACOI), 2024.

⁹ Het gaat om meerjarenplannen van de overheid voor de digitale informatiehuishouding.

¹⁰ Zie bijvoorbeeld <https://digital-strategy.ec.europa.eu/nl/policies/europes-digital-decade>.

Nederlandse overheid is het meenemen van de Digital Decade en de regelgeving die daaruit volgt essentieel.

Naarmate de digitalisering van overheid en samenleving verder toeneemt, groeit ook het belang van een solide informatiehuishouding. Onze maatschappij draait op een digitale infrastructuur. Die digitale laag is zo ingebakken dat die inmiddels onmisbaar is. Burgers zijn logischerwijs steeds meer gewend aan en afhankelijk van digitale processen, die efficiënt, veilig en met respect voor privacy moeten worden ingericht en uitgevoerd. Gebreken in de informatiehuishouding van de overheid zijn voor burgers al snel voelbaar en frustrerend door vertraging, fouten en onnodige of onevenredige inspanningen die van burgers zelf worden gevraagd. Een gebrekkige dienstverlening als gevolg van een gebrekkige informatiehuishouding kan al snel grote schade berokkenen, zowel direct als indirect, en het vertrouwen van burgers aantasten.¹¹

Het handelen van de overheid en de informatiehuishouding die daarbij een essentiële rol speelt worden enerzijds beheerst door wet- en regelgeving en anderzijds door ICT- en AI-systemen waar informatie mee wordt verwerkt. De hoeveelheid en complexiteit van zowel wet- en regelgeving als ICT- en AI-systemen nemen alsmaar toe, waardoor een heldere samenhang steeds moeilijker te vinden is. Bijvoorbeeld waar de Wet open overheid (Woo), de Archiefwet en de Algemene verordening gegevensbescherming (AVG) elkaar raken en op gespannen voet met elkaar kunnen staan, ontstaat al snel behoefte aan verheldering of verduidelijking. Het voorstel voor versimpeling vanuit Europa – de zogeheten Digital Omnibus-regelgeving – heeft ten doel de ‘regeldruk’ van de AVG en zo’n tien andere Europese wetten te verminderen, bijvoorbeeld door één loket voor meldplichten onder al die wetgeving in te voeren. Verheldering, via een wet dan wel via uitleg door gezaghebbende autoriteiten, is gewenst. Een belangrijke vraag hierbij is hoeveel ruimte er kan bestaan voor een nieuwe nationale wet in formele zin, tegen de achtergrond van bestaande internationale, Europese en grondwettelijke kaders. Bovendien is onduidelijk of er nu eerder wetten nodig zijn, of verheldering en begeleiding.

Uit de memorie van toelichting (MvT) bij de concept-Aiw blijkt dat de Aiw de informatiehuishouding van de overheid beoogt te reguleren en structureren door meer samenhang te brengen in de reeds bestaande informatiewetten. Uit het actieplan ‘Open op Orde’ volgt onder meer de actielijn “*Heldere besturing van de informatiehuishouding en passende planning en control*”. De Aiw zou ervoor moeten zorgen dat de informatiehuishouding als eenheid wordt beschouwd. Het is een voorstel tot een funderende wet die verschillende aspecten van de informatiehuishouding van de overheid in samenhang regelt. Daarbij focust de Aiw op de inrichting van de informatiehuishouding.¹²

Uit de toelichting van de Regeringscommissaris Informatiehuishouding volgt dat het verbeteren van de informatiehuishouding van de overheid met behulp van de

¹¹ Zie bijvoorbeeld het verslag van de Parlementaire ondervragingscommissie Kinderopvangtoeslag met de titel ‘Ongekend onrecht’, https://www.tweedekamer.nl/sites/default/files/atoms/files/20201217_eindverslag_parlementaire_ondervragingscommissie_kinderopvangtoeslag.pdf.

¹² Zie memorie van toelichting Algemene informatiewet overheid, p. 1 en 5.

Aiw geen doel op zich is maar een middel. Een kerndoel is: *"Een overheid die naast de burger staat, betrouwbaar is en zich inzet om mensen verder te helpen."*¹³

Kern van dit rapport

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verzocht ICTRecht om een onderzoek en rapportage om inzicht te bieden in het huidige landschap aan (data)wet- en regelgeving in verband met de verbetering van de informatiehuishouding. Dit in relatie tot het voorstel van de AiW.

In de voorbereiding van deze opdracht creëerden BZK en ICTRecht een toetsingskader van pijlers en bijbehorende criteria. Op voorhand is in overleg met BZK gekeken naar de behoefte aan verbetering van de informatiehuishouding en het faciliteren van veilige uitwisseling van informatieobjecten. Welke eigenschappen een verbeterde informatiehuishouding moet hebben en welke behoefte de overheid kent ten aanzien van die verbetering, wordt geïllustreerd door vijf pijlers.

De pijlers illustreren de gewenste benodigdheden om tot een verbeterde informatiehuishouding van de overheid te komen. De AiW heeft ook ten doel de informatiehuishouding van de overheid te verbeteren en ambieert (deels) dezelfde doelstellingen als geïllustreerd met de pijlers.

De kernvraag luidt: in hoeverre bestaande wet- en regelgeving ten aanzien van informatieobjecten de verbetering van de informatiehuishouding (belegd in de vijf pijlers) al realiseert of kan realiseren, ten opzichte van de conceptversie van de AiW en de bedoelingen hierachter?

Door op basis van deze afgestemde structuur inzicht te bieden in het huidige landschap aan datawet- en regelgeving, illustreert het rapport in hoeverre de huidige status quo (zonder een geldende AiW) al opties biedt ter verbetering van de informatiehuishouding. In hoeverre realiseert de bestaande wet- en regelgeving ten aanzien van informatieobjecten de verbetering van de informatiehuishouding (belegd in de vijf pijlers) al? En kan het gerealiseerd worden binnen dit landschap?

Zo dient dit rapport als hulpstuk in de verdere besluitvorming over het verbeteren van de informatiehuishouding dan wel over het aannemen van een AiW en het faciliteren van veilige en verantwoorde gegevensuitwisseling binnen de overheid. Bovendien biedt deze analyse inzicht in de vraag of er obstakels zijn om aan de doelen van de AiW te kunnen voldoen.

De vijf pijlers

In overleg met BZK zijn vijf fundamentele pijlers opgesteld. Deze pijlers illustreren de behoefte waaraan een sterk fundament van informatiehuishouding zou moeten voldoen. Elke pijler kent een kernvraag en deelvragen.

Bij elk van de pijlers is de centrale vraag in hoeverre bestaande of nieuwe wettelijke instrumenten bijdragen aan het realiseren van het bijbehorende doel. Dit rapport gaat per pijler in op de deelvragen, beantwoordt de kernvraag en vormt zo een conclusie.

¹³ Zie <https://www.open-overheid.nl/over-open-overheid/regeringscommissaris-informatiehuishouding>.

- Pijler 1: Coherente sturing en governance
- Pijler 2: Semantische en technische interoperabiliteit
- Pijler 3: Integrale kwaliteit en zorgplicht
- Pijler 4: Maatschappelijke functionaliteit
- Pijler 5: Oplossend en lerend vermogen

Dit onderzoeksrapport behandelt ieder van deze vijf pijlers hieronder uitgebreid. In deze fase van het onderzoek is aandacht geweest voor de inhoudelijke documentatie van BZK, publiek beschikbare documenten, beleidsstukken, programma's, wet- en regelgeving en inhoudelijke (vak)literatuur.

1. Pijler 1: Coherente sturing en governance

Een terugkerend probleem is dat overzicht, samenhang en centrale sturing ontbreken. Het streven moet een samenhangende, overheidsbrede sturing op de informatiehuishouding zijn die de traditionele kokers van organisaties en beleidsdomeinen doorbreekt.

De wens bestaat om versnipperde bevoegdheden te doorbreken en een rijksbreed fundament te leggen voor een gedegen informatiehuishouding. De Aiw is bedoeld om hieraan bij te dragen. Deze pijler gaat over de mate waarin sturing, coördinatie en verantwoordingsstructuren wettelijk en beleidsmatig geborgd zijn.

Om dat te onderzoeken kent deze eerste pijler de volgende kernvraag:

In hoeverre biedt het bestaande wettelijke en beleidsmatige instrumentarium een bindend overheidsbreed sturingsmechanisme voor de gewenste informatiehuishouding?

Om deze kernvraag adequaat te kunnen behandelen, komen in het onderzoeksrapport de volgende criteria aan bod:

- Mandaat en juridische basis: is er een wettelijke grondslag om rijksbrede kaders, standaarden en voorzieningen bindend te maken?
- Interbestuurlijke werking: in welke mate kunnen Rijk, gemeenten, waterschappen, provincies en zelfstandige bestuursorganen (ZBO's) verplicht worden tot uniforme toepassing?
- Planning, controle en rapportage: zijn er verplichtingen voor informatieplannen, meerjarenprogramma's en voortgangsrapportages die sturing structureel borgen?
- Toezicht en handhaving: is toezicht belegd en bestaan er effectieve interventiemogelijkheden bij niet-naleving?

1.1. Antwoord op de kernvraag

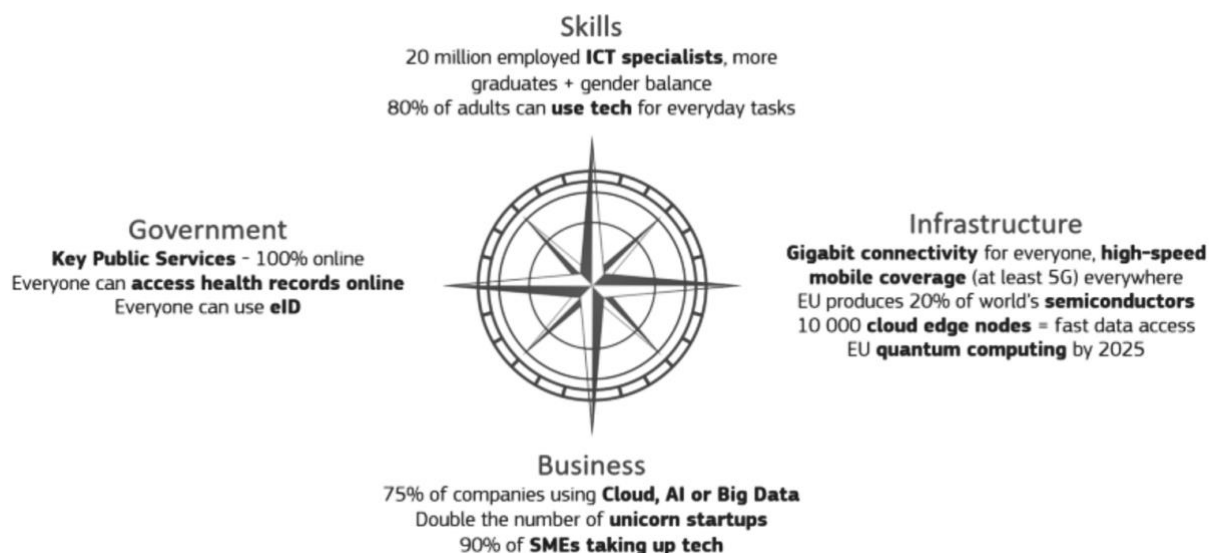
De Digital Decade en de NDS vormen een overheidsbreed sturingsmechanisme. De Europese en nationale wet- en regelgeving die daaronder wordt aangenomen, is juridisch bindend. Enerzijds ondersteunen ze het bereiken van de gewenste informatiehuishouding, anderzijds is nog steeds meer consistentie en samenhang tussen verschillende wet- en regelgeving en toepassingsgebieden wenselijk. Dit wordt hieronder toegelicht.

1.1.1. Digital Decade als sturingsmechanisme

Een belangrijk overheidsbreed sturingsmechanisme voor de gewenste informatiehuishouding wordt op EU-niveau gevormd door het beleidsprogramma voor de Digital Decade en op nationaal niveau is er de NDS.

De Digital Decade is gericht op het realiseren van een mensgerichte, duurzame en inclusieve digitale transformatie. Digitalisering van overheidsdiensten is een van de vier prioriteiten waarbinnen de doelstellingen van de Digital Decade gegroepeerd zijn. De stip aan de horizon is dat Europa in 2030 volledig digitaal moet functioneren en dat alle Europese burgers toegang moeten hebben tot digitale overheidsdiensten via veilige identificatie- en authenticatieoplossingen.

De EU heeft het volgende kompas gepubliceerd met de vier hoofddoelstellingen voor de Digital Decade.¹⁴



Afbeelding 1: Hoofddoelstellingen voor de Digital Decade.

De Digital Decade is er uitdrukkelijk op gericht Europese waarden en fundamentele rechten te verankeren in het digitale tijdperk en te vertalen naar concrete digitale systemen en oplossingen. De focus op fundamentele digitale rechten is bijvoorbeeld tot uitdrukking gebracht in de Europese verklaring over digitale rechten en beginselen voor het digitale decennium.¹⁵ Hoewel deze verklaring zelf niet rechtstreeks juridisch bindend is, vormt deze uitdrukkelijk wel een sturingsinstrument voor de richting waarin digitalisering en de digitale (data)huishouding binnen de EU moeten worden vormgegeven. In deze verklaring is bijvoorbeeld een aantal ethische beginselen geformuleerd die de EU moeten leiden bij haar aanpak voor digitale transformatie, zoals het recht op privacy, non-discriminatie en gendergelijkheid, consumentenbescherming, technologische neutraliteit en netneutraliteit, betrouwbaarheid en inclusiviteit. Als zodanig vormt de verklaring een belangrijk sturingsmechanisme om te borgen dat de digitale transformatie in de EU iedereen ten goede komt. Daarnaast zorgt de verklaring er in juridische zin voor dat iedereen in de EU toegang heeft tot digitale diensten en infrastructuur die veilig zijn en die de privacy, autonomie en menselijke waardigheid van mensen ondersteunen.

De Europese Commissie (EC) voorziet jaarlijks in een verslag over 'de staat van het digitale decennium', waarin zowel per lidstaat¹⁶ als EU-breed¹⁷ inzicht wordt verschaft in de voortgang in het bereiken van de doelstellingen. In het landenrapport van 2025 voor Nederland wordt bijvoorbeeld verwezen naar de NDS

¹⁴ Zie <https://digital-strategy.ec.europa.eu/nl/policies/digital-decade-policy-programme>.

¹⁵ Zie Europese verklaring over digitale rechten en beginselen voor het digitale decennium, 2023/C 23/01.

¹⁶ Zie het landenrapport van Nederland voor 2025, <https://ec.europa.eu/newsroom/dae/redirection/document/116918>.

¹⁷ Zie het EU-brede rapport van 2025, <https://ec.europa.eu/newsroom/dae/redirection/document/116741>.

en de Nationale Technologiestrategie¹⁸. Ook voor de eerdergenoemde verklaring over digitale rechten is op EU-niveau voorzien in monitoring.¹⁹ Uit het rapport van 2025 bleek overigens wel dat er nog het nodige te verbeteren is wat betreft de perceptie en het vertrouwen onder burgers in de beschikbaarheid, kwaliteit, duurzaamheid en privacyvriendelijkheid van digitale diensten. Minder dan de helft van de respondenten gaf bijvoorbeeld aan zich goed beschermd te voelen in de digitale ruimte.²⁰

De EU heeft voor het realiseren van de Digital Decade een samenwerkingscyclus tussen lidstaten en de EU voorzien, die als volgt grafisch is weergegeven.²¹



Afbeelding 2: Samenwerkingscyclus tussen lidstaten en de EU.

Ook deze samenwerkingscyclus kan worden beschouwd als een belangrijk sturingsmechanisme om tot een coherente uitvoering te komen van het Digital Decade-beleidsprogramma.

1.1.2. Juridisch bindend

Onderdeel van de kernvraag in deze pijler is in hoeverre er een overheidsbreed sturingsmechanisme is dat juridisch bindend is. De juridische verbindendheid van het Digital Decade-beleidsprogramma wordt gevormd door de verordeningen en richtlijnen die de EU onder dit programma vaststelt en die binnen de lidstaten uitgevoerd of geïmplementeerd moeten worden in nationale wet- en regelgeving. Ook van belang is dat veel van de kernwaarden die in de Digital Decade centraal staan en in de praktijk moeten worden gebracht, bindende kracht hebben in de vorm van fundamentele Europese rechten of grondrechten, zoals vervat in

¹⁸ De Nationale Technologiestrategie is gepubliceerd op <https://open.overheid.nl/documenten/67b0a9e1-135b-483f-9ed9-3aade270dbce/file>.

¹⁹ Zie bijvoorbeeld <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-declaration-digital-rights-and-principles-monitoring-report-2025>.

²⁰ Zie bijvoorbeeld de paragraaf 'Citizens' perceptions' op p. 5 en verder en op p. 12.

²¹ Zie <https://digital-strategy.ec.europa.eu/nl/policies/digital-decade-policy-programme>.

bijvoorbeeld het Handvest van de grondrechten van de EU en het Europees Verdrag voor de Rechten van de Mens.²²

Een EU-richtlijn kan op zichzelf ook als een juridisch bindend sturingsmechanisme worden beschouwd voor de lidstaten. Wanneer een lidstaat een EU-richtlijn niet tijdig heeft omgezet in nationale wetgeving en de nationale implementatiewetgeving niet tijdig heeft doorgegeven aan de EC, kan de Commissie een inbreukprocedure tegen de lidstaat aanhangig maken. Daarbij kan zowel een boete als een last onder dwangsom worden gevorderd tegen de lidstaat.²³ In dit opzicht loopt Nederland bijvoorbeeld een risico zolang de NIS2-richtlijn nog niet definitief is omgezet in nationale wetgeving, terwijl dit in oktober 2024 al gebeurd had moeten zijn. Kort na het verlopen van deze termijn, eind november 2024, heeft de EC al aangekondigd inbreukprocedures te openen tegen de 23 lidstaten die op dat moment te laat waren.²⁴ In de NIS2 implementation tracker van de European Cyber Security Organisation is te zien dat in maart 2026 inmiddels 21 van de 27 lidstaten de NIS2-richtlijn hebben geïmplementeerd, maar Nederland, Frankrijk, Spanje, Ierland, Luxemburg en Estland nog niet.²⁵

De mate waarin of de manier waarop de NDS als sturingsmechanisme ook juridisch bindend is of zou kunnen zijn, is minder duidelijk dan voor de Europese Digital Decade. In de online publicatie van de NDS²⁶ wordt ten aanzien van bindende afspraken en standaarden verwezen naar het Federatief Datastelsel (FDS), dat tot stand is gebracht onder de Interbestuurlijke Datastrategie (IBDS) en het programma Realisatie IBDS. Een praktisch hulpmiddel dat onder de IBDS tot stand is gebracht, is bijvoorbeeld de EU Wetgevingsmonitor, een overzicht waarin meer dan 475 Europese wetgevingstrajecten zijn ondergebracht op het gebied van digitale dienstverlening, data, cybersecurity, digitale identiteit, elektronische communicatie en de informatiesamenleving.²⁷ Realisatie IBDS kent overigens ook de Adviesfunctie Verantwoord Datagebruik om eigenaren van maatschappelijke dataprojecten te ondersteunen met gezaghebbend advies en praktische handvatten.²⁸ Daarnaast is de Centrale Commissie Gegevensgebruik (CCG) opgericht om doorbraken te faciliteren bij knelpunten op het vlak van gegevensgebruik.²⁹ Dergelijke adviesorganen sluiten aan bij de opzet van de Aiw tot oprichting van een adviescollege en kunnen mede fungeren als sturingsmechanisme, al zijn de adviezen niet juridisch bindend.

Op basis van de NDS, met als subtitel 'Samen versnellen', en het IBDS Jaarplan 2026 richt het programma Realisatie IBDS zich op het maken van bindende afspraken en standaarden. In de NDS wordt het al dan niet aansluiten op het FDS als te vrijblijvend beschouwd. Voor het wettelijk verplichten van standaarden wordt verwezen naar artikel 3 van de Wet digitale overheid (Wdo). In lijn met de doelstelling voor het komen tot bindende afspraken heeft het Overheidsbreed

²² In pijler 3 wordt de juridische verbindendheid van de zorgplichten die uit fundamentele rechten voortvloeien nog nader behandeld.

²³ Zie bijvoorbeeld de zaak tegen Spanje van 25 februari 2021 (C-658/19) waar zowel een boete van 15 miljoen euro is opgelegd als een last onder dwangsom van 89.000 euro per dag, <https://>.

²⁴ Zie https://ec.europa.eu/commission/presscorner/detail/en/inf_24_5988.

²⁵ Zie <https://ecs-org.eu/activities/nis2-directive-transposition-tracker/>.

²⁶ Zie <https://www.digitaleoverheid.nl/document/de-nederlandse-digitaliseringsstrategie-nds/>.

²⁷ Zie <https://eu-wetgevingsmonitor.realisatieibds.nl/>.

²⁸ Zie <https://realisatieibds.nl/page/view/f896fe3b-f93f-450e-a107-e280cbe8ecf6/adviesfunctie>.

²⁹ Zie <https://realisatieibds.nl/groups/view/56d3fbd7-fd82-4869-93e1-7530114c037c/centrale-commissie-gegevensgebruik-ccg>.

Beleidsoverleg Digitale Overheid in februari 2026 het Afsprakenstelsel FDS formeel vastgesteld. Geopolitieke ontwikkelingen en een behoefte aan Europese en nationale soevereiniteit spelen een uitdrukkelijke rol in de versnelling die wordt gezocht in de uitvoering van de digitalisering en het maken van bindende afspraken daarover.

1.1.3. Gewenste informatiehuishouding van de overheid

Tot dusver is in dit rapport de term 'informatiehuishouding' al meerdere malen gebruikt zonder nader te verkennen wat daarmee wordt bedoeld. Aangezien het in de kernvraag van deze pijler draait om de 'gewenste informatiehuishouding', is het relevant om nader te bespreken wat hieronder kan worden verstaan. Op de website [digitaleoverheid.nl](https://www.digitaleoverheid.nl) wordt het begrip 'informatiehuishouding' als volgt omschreven:

Informatiehuishouding is het geheel aan regels, structuren, processen en voorzieningen gericht op het gebruik en het beheer van informatie. Denk aan het creëren, opslaan, ordenen, bewaren, ontsluiten, verstrekken en vernietigen van informatie.³⁰

Uit de bovenstaande omschrijving zijn de volgende elementen te distilleren die samen de informatiehuishouding vormen:

- alle wet- en regelgeving over informatieverwerking,
- de staats- en bestuursrechtelijke structuur waarbinnen wet- en regelgeving tot stand komt,
- de processen waarbij informatie wordt verwerkt en gebruik wordt gemaakt van (fysieke of digitale) systemen, en
- de fysieke of digitale (ICT- en/of AI-)systemen waarmee of waarin informatie wordt verwerkt.

In verband met diverse onderzoeken en initiatieven zoals besproken in de inleiding kan de informatiehuishouding van de overheid globaal gezien als 'gewenst' worden beschouwd wanneer die faciliteert dat de overheid goede diensten levert aan burgers en hen effectief helpt. De Digital Decade kleurt dat nader in als een mensgerichte, duurzame en inclusieve digitalisering, waarbij fundamentele rechten als vrijheid en veiligheid, privacy, gelijke behandeling en vrijheid van meningsuiting en informatiegaring actief tot uitdrukking worden gebracht in digitale diensten en systemen.

Om een informatiehuishouding als 'gewenst' te kunnen beschouwen, moet deze ook een coherent en logisch geheel vormen, zo overzichtelijk mogelijk zijn en geen innerlijke tegenstrijdigheden bevatten. Een gewenste informatiehuishouding bevat bijvoorbeeld geen tegenstrijdige verplichtingen ten aanzien van dezelfde (soorten of categorieën) informatie, zoals bewaren of juist vernietigen, openbaar maken of juist afschermen. Waar verschillende verplichtingen en belangen wel op gespannen voet staan, moet een goede balans vindbaar en concreet uitvoerbaar zijn of duidelijk zijn welke verplichting voorgaat en waarom.

Dit onderzoek richt zich op de wet- en regelgeving die deel uitmaakt van en bepalend is voor de informatiehuishouding van de overheid. Belangrijke wettelijke

³⁰ Zie <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatiehuishouding/>.

verplichtingen voor overheden in verband met informatieverwerking zijn bijvoorbeeld om:

- overheidsinformatie te bewaren en archiveren volgens de Archiefwet³¹,
- overheidsinformatie (actief) openbaar te maken volgens de Woo,
- digitale overheidsdiensten beschikbaar te maken volgens de Wdo,
- overheidsinformatie herbruikbaar te maken volgens de Wet hergebruik van overheidsinformatie (Who) en/of de Datagovernanceverordening (DGV) en de Uitvoeringswet Datagovernanceverordening,
- persoonsgegevens en privacy te beschermen volgens de AVG en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG),
- informatie en systemen te beveiligen volgens de (aankomende) Cyberbeveiligingswet (Cbw) en Baseline Informatiebeveiliging Overheid (BIO),
- AI-systemen en algoritmen voor (gedeeltelijke) automatische besluitvorming in te richten en te gebruiken volgens de AI-verordening en de AVG, en
- mensen gelijk te behandelen ongeacht hun godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat volgens de Algemene wet gelijke behandeling (Awgb).

Voor diverse van bovenstaande verplichtingen zijn specifieke toezichthouders, adviescolleges en handhavingssystemen ingericht. Denk aan:

- de Inspectie Overheidsinformatie en Erfgoed (IOE) en het ACOI voor de Archiefwet en Woo,
- de Rijksinspectie Digitale Infrastructuur (RDI) voor de Wdo (en Logius voor ICT-beveiligingsassessments voor DigiD en het naleven van de Voorwaarden DigiD³²) en Cbw,
- de Autoriteit Persoonsgegevens (AP) voor de AVG en UAVG, en
- het College voor de Rechten van de Mens voor de Awgb (oordelen zijn niet juridisch bindend maar wel gezaghebbend).

Voor andere verplichtingen geldt in het algemeen het passieve toezicht door de rechter, die in actie komt wanneer iemand bijvoorbeeld een procedure aanhangig maakt in verband met een vermeende schending. In andere pijlers van dit onderzoek worden diverse van deze wetten, verplichtingen en handhavingssystemen nader behandeld.

Een klacht die in verband met de informatiehuishouding in diverse rapporten naar voren is gekomen, betreft de omvang, complexiteit en schijnbare tegenstrijdigheid van de wet- en regelgeving.³³ Ook uit dit onderzoek blijkt dat de hoeveelheid wettelijke regels in verband met digitalisering sterk toeneemt en dat de verplichtingen en de toepassingsgebieden op basis van de wetgeving niet altijd eenvoudig zijn vast te stellen of uit te leggen. De hoeveelheid verplichtingen die tegelijkertijd van toepassing kunnen zijn op dezelfde digitale producten, diensten

³¹ Sinds 2021 wordt gewerkt aan een nieuwe Archiefwet. Op moment van schrijven is de verwachting dat de nieuwe Archiefwet 1 januari 2027 in werking zal treden.

³² Zie bijvoorbeeld <https://www.logius.nl/onze-dienstverlening/toegang/digid/ict-beveiligingsassessments-digid/wie-doet-wat>.

³³ Zie bijvoorbeeld 'Open op Orde', Generiek actieplan informatiehuishouding Rijksoverheid, p. 18.

en aanbieders neemt ook toe. In dit verband heeft het Adviescollege toetsing regeldruk een belangrijke rol om te helpen borgen dat de wet- en regelgeving die deel uitmaakt van de informatiehuishouding niet tot disproportionele inspanning leidt om deze toe te passen. In de samenwerkingscyclus met de EU voor de uitvoering van de Digital Decade is van belang dat de Nederlandse overheid blijft wijzen op knelpunten, inconsistenties en onvolkomenheden in EU-wetgevingsinstrumenten die het bereiken van de kerndoelstellingen eerder in de weg kunnen zitten dan deze te helpen bereiken.

1.1.4. Staats- en bestuursrechtelijke structuur

Het Nederlandse staatsrechtelijke bestel kent een scheiding, of op sommige aspecten meer een spreiding³⁴, van machten binnen de overheid tussen de wetgevende, uitvoerende en rechtsprekende machten, bekend als *trias politica*. Al deze machten maken deel uit van de overheid en de informatiehuishouding van ieder van hen maakt deel uit van de informatiehuishouding van de overheid. Verder is de bestuurlijke structuur van Nederland nog altijd gebaseerd op het 'Huis van Thorbecke', waar gemeenten, provincies en de rijksoverheid ieder een bestuurslaag vormen die elk hun eigen (gedeeltelijke) autonomie kennen en waar ook de waterschappen hun eigen plek innemen. In de NDS wordt er in dit verband op gewezen dat het voor burgers zelf minder van belang is met welke specifieke overheidsorganisatie zij te maken hebben, maar vooral dat hun informatie correct wordt verwerkt en beschermd en dat zij de diensten en voorzieningen krijgen die ze nodig hebben en waar ze recht op hebben.³⁵ In verband met digitalisering en het sturen op een goede informatiehuishouding blijft wel van belang dat de balans tussen verschillende machten en bestuurslagen goed wordt bewaard en vooral ook dat de machtsbalans tussen overheid en burger niet wordt gekanteld in het nadeel van de burger.³⁶

Boven het Nederlandse Huis van Thorbecke vormt de EU een hogere bestuurslaag, die steeds nadrukkelijker sturing geeft met het oog op harmonisatie van de Europese interne markt. Daarmee wordt ook de ruimte steeds meer beperkt om nationale wetgeving aan te nemen die de (volledige) informatiehuishouding integraal zou (kunnen) reguleren. Voor de informatiehuishouding van de Nederlandse overheid is het steeds meer de Europese Digital Decade die de richting bepaalt. De kwaliteit en effectiviteit waarmee de Nederlandse overheid daar invulling en uitvoering aan geeft, blijft echter van onverminderd belang voor burgers en de Nederlandse maatschappij als geheel. Dat geldt ook voor initiatieven als de NDS, het FDS, de EU Wetgevingsmonitor en diverse adviesfuncties en colleges die samen de gewenste informatiehuishouding dichterbij brengen.

1.1.5. Concluderend

Een samenspel van Europese en nationale wetgeving is kaderstellend voor de gewenste informatiehuishouding. Binnen deze kaders dient bewogen te worden. De toenemende omvang en complexiteit van wet- en regelgeving is, en blijft

³⁴ Ten aanzien van de dubbele taak van de regering in Nederland, die zowel wetgevende als uitvoerende taken heeft, wordt bijvoorbeeld gesproken van een spreiding van machten in plaats van een strikte scheiding. Zie bijvoorbeeld <https://www.denederlandsegrondwet.nl/de-trias-politica-de-nederlandse-grondwet>.

³⁵ Zie de Nederlandse Digitaliseringsstrategie, <https://>.

³⁶ Het wordt wel gesteld dat digitalisering een gevaar oplevert dat de machtsbalans te veel naar de uitvoerende macht verschuift. Zie bijvoorbeeld het artikel 'Digitalisering en de (dis)balans binnen de trias politica', Ars Aequi oktober 2020, <https://>.

voorlopig, een aandachtspunt. Het is zaak om de machtsbalans tussen overheid en burger daarbij te blijven waarborgen.

1.2. Mandaat

1.2.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“is er een wettelijke grondslag om rijksbrede kaders, standaarden en voorzieningen bindend te maken?”* centraal.

Om te komen tot de gewenste informatiehuishouding is in dit onderzoeksrapport onderzocht in hoeverre bestaande wet- en regelgeving grondslagen biedt om rijksbrede kaders, standaarden en voorzieningen rondom de informatiehuishouding bindend te maken. Daarbij is gekeken naar thans geldende wetgeving. Zonder een diepgaande en gedetailleerde bestuursrechtelijke analyse uit te voeren, is vastgesteld dat er bestuursrechtelijk voldoende ruimte en mandaat is om rijksbrede regels te stellen aan informatiehuishouding en gegevensdeling.

De reikwijdte van een mandaat begint in dit geval bij een solide basis. Die basis is gevormd in de Grondwet. Daarin zijn bevoegdheden binnen het Rijk gereguleerd.³⁷ Ministeries staan onder leiding van een minister en die minister is politiek verantwoordelijk voor het betreffende beleidsgebied, waarmee ook ruimte wordt gecreëerd voor interne sturing van een ministerie en alle organisatievormen die daaronder vallen.

Een minister kan als bestuursorgaan beleidsregels maken voor zover dat past binnen de verantwoordelijkheden van de betreffende minister, of voor zover dat bij wettelijk voorschrift is bepaald.³⁸ Dergelijke beleidsregels zijn in beginsel bindend voor het betreffende ministerie.³⁹ Hoewel beleidsregels niet gezien moeten worden als wet in formele zin, kunnen het wel degelijk bindende kaders zijn voor informatiehuishouding en gegevensdeling. Het basisprincipe van verantwoordelijke ministers en daaronder hangende ministeries is van belang om te bepalen in hoeverre er een mandaat en juridische basis is om rijksbreed wet- en regelgeving te maken die kaders, standaarden en voorzieningen schept voor een gezonde informatiehuishouding en rechtmatige gegevensdeling.

Naast deze benadering per ministerie bevat de Grondwet uiteraard ook een route om in een breder kader wet- en regelgeving te maken. Dat gebeurt in dat geval niet op ministerieel niveau door middel van beleidsregels, maar via de regering en de Staten-Generaal samen.⁴⁰

Juridisch is er ruimte om op ministerieel niveau gedecentraliseerde kaders en beleidsregels te maken via de hierboven beschreven route. Juridisch is er ook ruimte om meer centraal regels te stellen door middel van de wetgevingsprocedure via de regering en Staten-Generaal.

³⁷ Zie art. 42 e.v. Grondwet.

³⁸ Zie art. 4:81 Algemene wet bestuursrecht.

³⁹ Zie art. 4:84 Algemene wet bestuursrecht, waarin ook uitzonderingen worden genoemd die voor dit onderzoeksrapport niet relevant zijn.

⁴⁰ Zie art. 81 Grondwet.

Er is momenteel echter geen geldende wetgeving die dient als één wettelijke centrale basis om rijksbrede kaders op het gebied van informatiehuishouding en gegevensdeling bindend te maken. Daarvoor is de term informatiehuishouding te veel versplinterd in verschillende wetten opgenomen. Wel zijn er daardoor diverse wetten die direct of indirect bepalingen bevatten die de informatiehuishouding raken. De wetgeving bevat per domein grondslagen die de informatiehuishouding en gegevensdeling raken. Zo bevat de Archiefwet een constructie om regels te stellen over de inrichting en uitvoering van archivering⁴¹, bevat de Woo ruimte om regels te stellen over hoe bestuursorganen uitvoering geven aan de Woo⁴², en daarmee deels aan informatiehuishouding, en bevat de Wdo een grondslag om standaarden voor elektronisch verkeer toe te passen.⁴³ Archivering, openheid en digitalisering kennen zo hun eigen wettelijke grondslagen, grondslagen die binnen het eigen domein reguleren of en hoe de informatiehuishouding wordt geraakt, maar die tegelijkertijd ook geen algemene basis bevatten voor het verbindend verklaren van standaarden, kaders of voorzieningen. Dat deze wetten de informatiehuishouding direct raken, heeft ook gevolgen voor het delen van gegevens binnen de overheid. Immers, als wetten bepalingen bevatten over de vorm en de manier waarop gegevens opgeslagen en verwerkt moeten worden, zijn dat bepalingen die direct van invloed zijn op het verder delen van deze gegevens. Wanneer vereisten inzake de technische opslag en het operationeel verwerken van gegevens juridisch of beleidsmatig zijn vastgelegd, kan dat het verder delen van diezelfde gegevens vergemakkelijken of bemoeilijken.

In verband met het mandaat om rijksbrede kaders, standaarden en voorzieningen juridisch bindend te maken, kan ook specifiek worden gewezen op artikel 3 van de Wdo. Op basis van lid 2 kan een standaard bij algemene maatregel van bestuur (AMvB) worden aangewezen die:

noodzakelijk en proportioneel is gelet op de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronische verkeer, dan wel noodzakelijk is ter uitvoering van verdragen of bindende besluiten van volkenrechtelijke organisaties.

Op basis van de memorie van toelichting bij de Wdo kan worden geconcludeerd dat het begrip 'elektronisch verkeer' breed wordt bedoeld en in de praktijk alle digitale uitwisseling van informatie kan omvatten. Standaarden zijn ook van belang voor interoperabiliteit bij het delen en uitwisselen van informatie, zoals in Pijler 2 nader wordt behandeld. Als het de bedoeling is om, zoals gesteld in de NDS, het FDS (geheel of gedeeltelijk) juridisch bindend te maken op grond van artikel 3 van de Wdo, dient wel te worden voldaan aan de eisen die in dat artikel worden gesteld. Lid 3 vereist bijvoorbeeld vastlegging in de AMvB van het functionele toepassingsbereik van de standaard, de organen waarvoor de verplichting geldt om de standaard toe te passen en de datum waarop de verplichting ingaat.

1.2.2. Concluderend

De staats- en bestuursrechtelijke structuur en de verdeling van machten en bevoegdheden maken deel uit van de informatiehuishouding van de overheid. Hoewel er beperkingen kunnen bestaan ten aanzien van de inrichting van

⁴¹ Zie art. 21 Archiefwet 1995.

⁴² Zie art. 8.7 Wet open overheid.

⁴³ Zie art. 3 Wet digitale overheid.

handhaving en toezicht, waarbij ervoor moet worden gezorgd dat er geen belangenconflicten ontstaan, bestaat er een juridische basis en mandaat om rijksbrede regels vast te stellen over informatiehuishouding en gegevensdeling binnen de overheid. Daar kan gebruik van gemaakt worden als dat nodig en wenselijk wordt geacht. Daarbij moet de inhoud van nationale wet- en regelgeving wel binnen de kaders blijven van de geldende EU-regelgeving.

1.3. Interbestuurlijke werking

1.3.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“in welke mate kunnen Rijk, gemeenten, waterschappen, provincies en ZBO’s verplicht worden tot uniforme toepassing?”* centraal.

Het instrument om verplichtingen op te leggen aan het Rijk, gemeenten, waterschappen, provincies en ZBO’s is het vaststellen van wet- en regelgeving waaraan deze instanties zich dienen te houden.

Rechters en toezichthouders die tot taak hebben om de naleving van wet- en regelgeving af te dwingen, kunnen door middel van rechtspraak, toezichtbesluiten of richtlijnen ondersteuning bieden voor een gelijke of uniforme uitleg en toepassing van wet- en regelgeving. Denk hierbij in het kader van de AVG bijvoorbeeld aan de richtlijnen van de AP en de European Data Protection Board (EDPB). Bij het naleven van de AVG en UAVG dienen het Rijk en alle andere overheidsorganen op alle niveaus rekening te houden met de richtlijnen die de toezichthouders daarvoor hebben uitgevaardigd. Voor uniforme toepassing van EU-recht kunnen nationale rechters bijvoorbeeld ook prejudiciële vragen stellen aan het Hof van Justitie van de Europese Unie. Uitspraken van het Hof van Justitie van de Europese Unie moeten worden gevolgd en dragen als zodanig bij aan uniforme toepassing van Europees recht. Richtlijnen en best practices van organen als de EDPB zijn in het algemeen niet juridisch bindend maar wel gezaghebbend.

Uniforme toepassing van wetten in formele zin kan worden bevorderd door lagere regelgeving, zoals algemene maatregelen van bestuur en ministeriële regelingen. De staats- en bestuursrechtelijke hiërarchie van wet- en regelgeving moet daarbij wel in acht worden genomen. Wetten in formele zin moeten in lijn zijn met de Grondwet en met hoger EU-recht en internationale verdragen die Nederland heeft geratificeerd. Lagere regelgeving zoals een AMvB of ministeriële regeling mag niet in strijd zijn met wetgeving in formele zin.

Waar het de bedoeling is dat *alle* overheidsorganen in Nederland zich tegelijkertijd op dezelfde manier ergens aan houden, kan bijvoorbeeld een wet in formele zin worden aangenomen die van toepassing is op alle overheidsorganen. De Archiefwet geeft bijvoorbeeld een brede definitie van de term overheidsorgaan, waar het Rijk, gemeenten, waterschappen, provincies en zelfstandige bestuursorganen onder vallen.⁴⁴ De Woo is van toepassing op bestuursorganen en een aantal specifiek bij naam genoemde organen die geen bestuursorgaan vormen in de zin van de Algemene wet bestuursrecht (Awb), zoals de Eerste en Tweede

⁴⁴ Zie art. 1 sub b Archiefwet 1995.

Kamer.⁴⁵ De AVG en UAVG gelden ook voor alle overheidsorganisaties tegelijk, voor zover zij persoonsgegevens verwerken.⁴⁶

De moeilijkheid of complexiteit in verband met uniforme toepassing lijkt echter juist vooral te zijn dat verschillende wetten, zoals de Woo, Archiefwet, (U)AVG en (aankomende) Cbw gericht zijn op verschillende belangen en in verschillende richtingen kunnen wijzen als het gaat om de vraag wat er precies moet of mag gebeuren met concrete, specifieke informatie. Bijvoorbeeld ten aanzien van de vraag hoe lang informatie mag of moet worden bewaard. Daarbij kunnen de Archiefwet en de (U)AVG verschillende kanten op wijzen. De Archiefwet verplicht tot lang of zelfs oneindig bewaren, terwijl de (U)AVG juist verplicht tot niet langer bewaren dan noodzakelijk. De vraag is dan wat noodzakelijk is en welke maatregelen ter bescherming van privacy genomen moeten worden, zoals pseudonimisering of anonimisering en op welk moment. Als verschillende wetten verplichtingen bevatten die met elkaar in strijd zijn of die verschillende kanten op kunnen wijzen, moet ofwel (a) beslist worden welke verplichting voorgaat, ofwel (b) een redelijke balans of redelijk midden worden gevonden. In sommige gevallen bevat wetgeving daar zelf een specifieke oplossing voor, maar niet altijd.

In de huidige Archiefwet⁴⁷ is wel verwezen naar de UAVG⁴⁸ en is een grondslag opgenomen om bijzondere en strafrechtelijke persoonsgegevens te verwerken in verband met archiefbeheer. Daarbuiten bevatten de Archiefwet en de (U)AVG zelf weinig specifiek of concreet houvast om in concrete gevallen de tegengestelde belangen van de Archiefwet en de (U)AVG af te wegen en daarbij steeds te komen tot de juiste balans en behandeling of verwerking van persoonsgegevens. De AP erkent de spanning tussen beide wetten en geeft ook aan dat een belangenafweging plaats moet vinden maar bepaalt niet specifiek wat de uitkomst van die afweging moet zijn.⁴⁹ Het voorstel voor de aankomende, nieuwe Archiefwet bevat enkele additionele verwijzingen naar de (U)AVG en specifieke bepalingen over de behandeling van persoonsgegevens en bevat daarnaast ook een beoogde wijziging voor de (U)AVG. Dergelijke wijzigingen lijken vooralsnog vooral de terminologie te betreffen, zoals vervanging van de term 'archiefbescheiden' door 'document' en 'archiefbewaarplaats' door 'archiefdienst', maar brengen geen specifieke duidelijkheid over wat de uitkomst van de belangenafweging tussen Archiefwet en (U)AVG in specifieke gevallen dient te zijn.⁵⁰

⁴⁵ Als zodanig zit er veel overlap tussen de organen die onder de Archiefwet en de Woo vallen. In elk geval de waterschappen, provincies, gemeenten en zelfstandige bestuursorganen vallen onder zowel de Archiefwet als de Woo. Wellicht dat er nog bepaalde organen binnen het Rijk of binnen de genoemde organen kunnen bestaan die wel kwalificeren als overheidsorgaan volgens de Archiefwet maar niet als bestuursorgaan en de specifieke bij naam genoemde andere organen in de Woo. Zelfs bijvoorbeeld de AIVD valt onder de Archiefwet en de Woo, al zal die zich meer kunnen beroepen op uitzonderingsgronden dan andere overheidsorganen.

⁴⁶ De AVG spreekt zelf van 'overheidsinstanties' en 'overheidsorganen', zonder een specifieke definitie van deze begrippen vast te leggen. Dit helpt voorkomen dat een definitie in een EU-verordening als de AVG in strijd zou raken met specifieke definities van dergelijke termen in nationaal recht van de lidstaten. In de NIS2-richtlijn is in art. 2 lid 2 sub f omschreven wat daar met een 'overheidsinstantie' wordt bedoeld.

⁴⁷ Zie art. 2a Archiefwet 1995.

⁴⁸ Zie paragraaf 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming.

⁴⁹ Zie <https://www.autoriteitpersoonsgegevens.nl/themas/overheid/archivering-door-de-overheid/voorwaarden-archivering-van-persoonsgegevens>.

⁵⁰ Zie het gewijzigde voorstel van wet van 18 februari 2025, p. 1, p. 2, p. 11 en p. 20, <https://>.

In deze situatie kan iedere bestuurslaag, zoals Rijk, provincie, gemeenten, waterschappen en zelfstandige bestuursorganen, eigen conclusies trekken over de juiste balans tussen verschillende wetten die vanuit verschillende belangen een tegengestelde richting op wijzen wat betreft de verwerking van informatie. Dat beperkt de onderlinge 'interoperabiliteit' en bemoeilijkt gegevensuitwisseling tussen de verschillende bestuurslagen. De vraag hierbij kan zijn of dat wenselijk is of juist niet. Of, om in ICT-termen te spreken: "Is het een feature of een bug?" Enerzijds kan worden gesteld dat in deze situatie de eigen autonomie van verschillende bestuurslagen bewaard blijft en het belang van privacy beter beschermd kan zijn doordat gegevensdeling de facto moeilijker is. Anderzijds kan het inefficiëntie en willekeur veroorzaken. De discussie tussen centraal en decentraal in verband met opslag en verwerking van gegevens speelt bijvoorbeeld in verband met elektronische patiëntendossiers al meer dan tien jaar. De verordening voor de European Health Data Space (EHDS) voegt daar een extra dimensie aan toe.⁵¹

Een verplichting tot uniforme toepassing van wet- en regelgeving over verschillende bestuurslagen impliceert al snel dat het detailniveau van de verplichtingen toeneemt of moet toenemen. Het detailniveau van wet- of regelgeving moet blijven passen bij enerzijds de democratische legitimering van het orgaan dat dit vaststelt en anderzijds de snelheid en efficiëntie waarmee dat orgaan de regels weer kan aanpassen. In verband met de snelheid waarmee technische ontwikkelingen plaatsvinden, kunnen er al snel problemen ontstaan als wetten in formele zin veel specifieke technische details bevatten. De wet kan dan al verouderd en niet goed toepasbaar meer zijn voordat de inkt bij wijze van spreken droog is. Wetten in formele zin worden daarom vaak zo techniekonafhankelijk mogelijk geformuleerd. Het invullen van de technische details wordt aan lagere regelgeving overgelaten of als vrij te bepalen voor de diverse overheids- of bestuursorganen op diverse lagen.

Het reguleren van de eigen informatiehuishouding per laag van de overheid is één ding. Het vervolgens zo inrichten dat de informatie per laag ook zo is opgeslagen en verwerkt dat uitwisseling tussen de verschillende overheden mogelijk is, is een ander ding.

Deze diversiteit aan wet- en regelgeving wordt in de memorie van toelichting van de Aiw aangehaald⁵²:

"Maar, er ontbreekt overzicht over het geheel en inzicht in de samenhang of juist het onderscheid tussen al de bestaande informatiewetten. De inrichting van de informatiehuishouding houdt onvoldoende rekening met de wettelijke voorschriften die aan die informatiehuishouding worden gesteld. Ook de diversiteit in de activiteiten van overheidsorganen maakt het ingewikkeld om uitvoering te geven aan deze informatiewetten."

en

⁵¹ Zie <https://www.datavoorgezondheid.nl/onderwerpen/w/wegiz/uitleg-over-de-wet/de-wegiz-in-relatie-tot-europa-european-health-data-space>.

⁵² Zie memorie van toelichting Algemene informatiewet overheid, p. 1 en 5.

"Hoewel de Grondwet dus ook de basis geeft voor de informatiecomponent, wordt een funderende wet, die de verschillende aspecten van de informatiehuishouding van de overheid (op alle bestuurslagen) in samenhang regelt, gemist."

Gelet op het huidige juridische stelsel is deze stelling uit de memorie van toelichting correct. Via onder andere de Woo bestaat de bevoegdheid en verplichting om meerjarenplannen op te stellen. Maar, zo werd door het ACOI in 2024 gesteld⁵³:

"Meerjarenplannen van de afzonderlijke bestuurslagen volstaan niet, nodig is een nationale aanpak."

In de NDS is dit probleem onderkend. Er wordt daarin gesproken over de tientallen sectorale wetten die toezien op de datahuishouding van overheden, het op hoog tempo moeten implementeren van (Europese) wetgeving en het daarvoor benodigde overzicht, de benodigde kennis en het bundelen van juridische expertise. Daarmee wordt direct verwezen naar het ontbreken van goede interbestuurlijke werking die nodig is voor het realiseren van een goede informatiehuishouding.⁵⁴

1.3.2. Concluderend

Dat iets beleidsmatig wenselijk is en wordt onderschreven in de NDS en de adviezen van het ACOI, betekent nog niet dat er ook een solide wettelijke grondslag is om de interbestuurlijke werking te realiseren. Versnippering van huidige wet- en regelgeving op dit vlak bemoeilijkt een goede en efficiënte interbestuurlijke werking.

1.4. Planning, controle en rapportage

1.4.1. Toelichting deelvraag

In deze paragraaf staat de vraag *"zijn er verplichtingen voor informatieplannen, meerjarenprogramma's en voortgangsrapportages die sturing structureel borgen?"* centraal.

Er bestaan wettelijke aanknopingspunten voor structurele sturing, maar deze zijn niet overal even expliciet of uniform vormgegeven.

De basis voor planning en verantwoording rond informatiehuishouding ligt in algemene zorgplichten. Zowel de Archiefwet als de Woo bevatten normen die bestuursorganen verplichten hun informatie in goede, geordende en toegankelijke staat te brengen en te houden. Deze zorgplichten impliceren dat organisaties hun informatiehuishouding actief moeten organiseren en beheersen. De wet schrijft echter doorgaans niet voor op welke wijze dit moet worden vertaald in interne planningsdocumenten of rapportagecycli. De norm is verplichtend, maar de bestuurlijke vertaling ervan in concrete informatieplannen of periodieke voortgangsrapportages wordt in beginsel aan het bestuursorgaan zelf overgelaten.

⁵³ Zie 'Alles is niets', Advies over meerjarenplannen van de overheid voor de digitale informatiehuishouding, Adviescollege Openbaarheid en Informatiehuishouding, mei 2024, p. 6.

⁵⁴ Zie 'De Nederlandse Digitaliseringsstrategie Samen versnellen', juni 2025, p. 4.

De Woo legt de minister van BZK een systeemverantwoordelijkheid op die thans onvoldoende is geoperationaliseerd. Deze verplichting rust echter niet op ieder afzonderlijk bestuursorgaan, maar expliciet op de minister van BZK, in overeenstemming met de minister van Onderwijs, Cultuur en Wetenschap. De systeemverantwoordelijkheid moet uitgewerkt worden in een meerjarenplan. Dit meerjarenplan wordt aan de Staten-Generaal gezonden en bevat langetermijndoelen en kortetermijnmaatregelen. Met deze constructie is op stelselniveau voorzien in een instrument voor meerjarige planning en politieke verantwoording. De wet bevat evenwel geen algemene verplichting voor alle bestuursorganen om zelfstandig een dergelijk meerjarenprogramma vast te stellen of daarover periodiek te rapporteren.

Voor de Rijksdienst geldt een verdergaande institutionele inbedding van planning en monitoring. Binnen het CIO-stelsel Rijksdienst is voorzien in de verplichting tot het opstellen van een meerjarig informatieplan per ministerie. Daarnaast is voorzien in rijksbrede monitoring en rapportage, waaronder een jaarrapportage over digitalisering en informatievoorziening. Hierdoor ontstaat binnen de Rijksdienst een herkenbare plan-do-check-act-structuur waarin informatiehuishouding periodiek wordt gepland, gevolgd en bestuurlijk besproken. Deze verplichtingen zijn gebaseerd op interne rijksbrede kaders en besluiten en hebben daarmee een bindend karakter binnen de Rijksdienst.

Voor andere bestuursorganen is een dergelijke uniforme verplichting tot het opstellen van informatieplannen of het uitbrengen van specifieke voortgangsrapportages over informatiehuishouding niet in algemene zin wettelijk voorgeschreven. Wel bestaan er op grond van de Archiefwet verplichtingen ten aanzien van zorg, toezicht en verantwoording, vaak nader uitgewerkt in archiefverordeningen en toezichtarrangementen. Deze vormen een bestuurlijk kader voor controle en toezicht, maar leiden niet automatisch tot een vaste, wettelijk voorgeschreven meerjarige plannings- en rapportagecyclus vergelijkbaar met die binnen de Rijksdienst.

De wettelijke verankering van planning, controle en rapportage rond informatiehuishouding is daarmee gelaagd. Op het niveau van normen en zorgplichten is sprake van een brede en dwingende basis. Op het niveau van concrete instrumenten is de verankering sterker binnen de Rijksdienst dan bij andere bestuursorganen. Voor medeoverheden en andere bestuursorganen is de structurele borging in grotere mate afhankelijk van de eigen inrichting van de planning- en controlcyclus en van de wijze waarop algemene wettelijke zorgplichten intern worden vertaald naar concrete sturingsinstrumenten.

1.4.2. Concluderend

Er kan worden geconcludeerd dat de sturing op informatiehuishouding juridisch is gefundeerd en op onderdelen structureel is ingebed, maar dat de mate van expliciete, uniforme en wettelijk voorgeschreven planning en rapportage verschilt tussen de Rijksdienst en andere bestuursorganen. De verankering is aanwezig, maar niet overal in dezelfde mate geformaliseerd.

1.5. Toezicht en handhaving

1.5.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“is toezicht belegd en bestaan er effectieve interventiemogelijkheden bij niet-naleving?”* centraal.

Waar het opleggen van verplichtingen juridisch mogelijk is, rijst direct een vervolgvraag. Opgelegde verplichtingen zijn daadwerkelijk effectief als ze worden uitgevoerd, als daar adequaat toezicht op wordt gehouden en als adequaat handhavend wordt opgetreden wanneer blijkt dat verplichtingen niet worden nageleefd.

Verantwoord, veilig en efficiënt gebruik van data is een van de prioriteiten in de NDS. *“Op het juiste moment over de juiste gegevens beschikken om sneller betere besluiten te kunnen nemen”*⁵⁵ is voor de overheid noodzakelijk. De huidige situatie wordt in de NDS⁵⁶ omschreven als te vrijblijvend:

“Standaarden en implementatietermijnen zijn te vrijblijvend en wetgeving wordt hiervoor nog niet ingezet; Regie en ondersteuning op de implementatie van verplichte standaarden ontbreekt.”

Dat is juist waarom toezicht en handhaving een belangrijk instrument zijn. Dit wordt onderkend in het coalitieakkoord, waarin meer ruimte aan toezichthouders wordt toebedeeld om zich te versterken met talent, te innoveren en op deze manier bestaande wetgeving effectief te handhaven.⁵⁷

Er is geen centrale toezichthouder die belast is met het toezien op de nationale informatiehuishouding van de overheid. Het toezicht is ingericht op specifieke onderdelen van de informatiehuishouding.

De AP is de toezichthouder op het gebied van verwerking van persoonsgegevens, de IOE is de toezichthouder voor de Archiefwet en de Auditdienst Rijk (ADR) houdt zich bezig met het onafhankelijk auditen van de rijksoverheid. Hoewel deze drie instanties actief bezig zijn met de informatiehuishouding van de overheid, doen ze dit alle drie binnen de kaders van hun eigen domeinen.

De ADR geeft in haar Strategische Auditagenda 2025-2028 aan onderzoek te doen naar rijksbrede digitalisering van onder andere de informatiehuishouding⁵⁸. De IOE heeft recent de Militaire Inlichtingen- en Veiligheidsdienst aangesproken⁵⁹, omdat bleek dat de informatiehuishouding daar niet op orde is,⁶⁰ waardoor de dienst niet voldeed aan de verplichtingen uit de Archiefwet.

De AP geeft in haar jaarplan 2026 aan verantwoord gebruik en gegevensuitwisseling te willen stimuleren.⁶¹ Dit zijn drie voorbeelden van

⁵⁵ Zie ‘De Nederlandse Digitaliseringsstrategie Samen versnellen’, juni 2025, p. 6.

⁵⁶ Zie ‘De Nederlandse Digitaliseringsstrategie Samen versnellen’, juni 2025, p. 6.

⁵⁷ Zie ‘Aan de slag, Bouwen aan een beter Nederland’, Coalitieakkoord 2026-2030, D66, VVD en CDA, p. 59.

⁵⁸ Zie ‘Strategische Auditagenda 2025-2028’, ADR, p. 7.

⁵⁹ Zie bijvoorbeeld <https://www.inspectie-oe.nl/actueel/nieuws/2026/02/19/mivd-moet-stappen-zetten-in-verbetering-informatiehuishouding>.

⁶⁰ ABRvS 21 augustus 2024, ECLI:NL:RVS:2024:3398.

⁶¹ Zie ‘Jaarplan 2026’, AP, p. 3.

toezichthouders die zich actief bemoeien met de informatiehuishouding van de overheid.

De domeinen van de sectorspecifieke toezichthouders betreffen de vraag "wat mag je wel of niet delen?" of "wat moet je delen?". De domeinen van de toezichthouders zien minder op toezicht op de gehele structuur van de informatiehuishouding. De vraag wat er wel of niet gedeeld moet of mag worden, is juist de vraag waarmee in de voorbereiding van de Aiw wordt geworsteld.

De handhaving draagt mogelijk bij aan een betere informatiehuishouding, maar kan niet gezien worden als een centraal gecoördineerde toezichtagenda om informatiehuishouding en gegevensuitwisseling binnen de overheid te stimuleren en controleren. Deze organen hebben wel allemaal interventiemogelijkheden in de vorm van audits, toezicht, het uitdelen van berispingen of boetes die effectief kunnen zorgen voor naleving van gefragmenteerde wettelijke verplichtingen.

Vanuit de EU wordt gekeken naar het kader van gegevensdeling. De EU wil immers (ook) al lang het delen (hergebruik) van overheidsinformatie stimuleren. Zij richtte met verschillende wetten een kader voor gegevensdeling op, waarvan een aantal specifiek geënt is op overheidsinformatie. Zo is er:

1. de DGV en Nederlandse Uitvoeringswet DGV die voorwaarden en standaarden neerleggen voor het hergebruiken van beschermde (door regels) overheidsinformatie,
2. de Dataverordening (DV) en Uitvoeringswet DV die de mogelijkheid bieden voor overheidsinstanties bij uitzonderlijke noodzaak (persoons)gegevens op te vragen bij derde partijen (inclusief andere overheidsorganisaties),
3. de Verordening Interoperabel Europa (VIE) die een kader introduceert waarbinnen overheden samen gegevens moeten kunnen delen voor het leveren van (grensoverschrijdende) overheidsdiensten. Nieuw beleid moeten zij volgens de VIE toetsen op die compatibiliteit en drempel voor interoperabiliteit, en
4. de Who die de Open Data-richtlijn (ODR) implementeert. Deze wet verplicht overheden overheidsinformatie (mits niet verboden bij wet) te delen in een bepaald format.⁶²

De toezichthouder voor de DGV is de Autoriteit Consument en Markt (ACM) in samenwerking met de AP.⁶³ Dit toezicht richt zich vooral op de organisaties die de DGV in het leven roept om hergebruik te stimuleren, niet op de overheidsorganisaties zelf. De toezichthouder voor de DV is de AP.⁶⁴ De VIE en Who kennen geen specifieke toezichthouder. De focus van deze wetgeving ligt op het opbouwen van een kader voor gegevensdeling.

Met de beoogde Aiw wordt geen nieuwe toezichthouder in het leven geroepen. De Aiw gaat uit van het centraal beleggen van stelselverantwoordelijkheid bij de minister van BZK en diens verplichting om een visie op de informatiehuishouding van de overheid te ontwikkelen.⁶⁵

⁶² Zie <https://data.overheid.nl>.

⁶³ Zie art. 2 lid 6 Uitvoeringswet Datagovernanceverordening.

⁶⁴ Zie art. 3 lid 1-3 Uitvoeringswet Dataverordening; de ACM is alleen toezichthouder voor de vergoeding bij opvragen van gegevens bij uitzonderlijke noodzaak.

⁶⁵ Zie memorie van toelichting Algemene informatiewet overheid, p. 9.

De Aiw introduceert een adviescollege.⁶⁶ Hoewel dit adviescollege geen toezichthoudende functie heeft, kan zijn adviserende functie wél bijdragen aan effectieve naleving van de wettelijke verplichtingen van overheidsorganen.

De bestaande toezichthouders, met de toezichtinstrumenten die tot hun beschikking staan, zullen vanuit hun eigen domein moeten bijdragen aan de goede informatiehuishouding van de overheid. De ACM als toezichthouder van de DGV en de AP als toezichthouder van de DV zien als enige toe op het kader van gegevensdeling, en of dat juist wordt opgezet.

1.5.2. Concluderend

De tweeledige vragen bij het kunnen delen van gegevens zijn ten eerste of er (technische) middelen zijn om gegevens te delen en ten tweede of die gegevens vervolgens gedeeld mogen of moeten worden.

De moeilijkheid zit hem vooral in de vraag of gegevens gedeeld mogen, of moeten, worden. De huidige regulering betreft meer welke gegevens gedeeld moeten (Woo, Archiefwet, Who), of mogen worden (AVG), dan een verplicht gegevensdelingskader. Europese regelgeving legt wel een basis voor een gegevensdelingskader. Deze zien, behalve de VIE en Who, echter meer op het opzetten van intermediairs dan technische verplichtingen.

Het handhavend toezicht is gecentreerd op de vraag welke gegevens gedeeld moeten of mogen worden en beperkt zich tot de AP die nagaat of persoonsgegevens juist worden behandeld. De overige regelgeving die gaat over het moeten delen van gegevens wordt niet gehandhaafd door een toezichthouder, behoudens de ADR-audit op naleving van de Archiefwet. Controle is er via instanties die auditen of de informatiehuishouding domeinspecifiek op orde is. Deze instanties wijzen overheidsorganen op niet-naleving en bewegen hen richting naleving. Dit is weinig concreet.

Hoewel er regelgeving is die verplichtingen oplegt over technische en organisatorische middelen voor gegevensdeling (in specifieke situaties), bestaat daar dan weer geen expliciet handhavend toezicht op.

⁶⁶ Zie art. 15 en 16 Algemene informatiewet overheid.

2. Pijler 2: Semantische en technische interoperabiliteit

Op taal- en architectuurniveau zijn wetten niet altijd geharmoniseerd. Terminologie wijkt af en systematiek is niet altijd op elkaar afgestemd. Het faciliteren van vrij verkeer van informatie moet het streven zijn door het vestigen van een eenduidig begrippenkader en het (verplicht) toepassen van standaarden en architecturen.

Deze pijler behandelt de voorwaarden om informatie vrij en foutloos binnen en tussen overheden te laten stromen. De Aiw beoogt conflicterende begrippen en standaarden te harmoniseren.

Om dat te onderzoeken kent deze tweede pijler de volgende kernvraag:

In welke mate faciliteren bestaande kaders uniforme begrippen, standaarden en technische interoperabiliteit die noodzakelijk zijn voor vrij verkeer van gegevens (of informatieobjecten)?

Om deze kernvraag adequaat te kunnen behandelen, komen in het onderzoeksrapport de volgende criteria aan bod:

- Begrippen: in hoeverre worden in relevante stukken wet- en regelgeving overheidsbreed dezelfde begrippen en definities gebruikt voor informatie?
- Technische standaarden: worden standaarden juridisch of beleidsmatig verplicht voorgeschreven en zijn deze verplichtingen afdwingbaar?
- Keteninteroperabiliteit: wordt ketenoverstijgende interoperabiliteit juridisch ondersteund of juist niet?
- Aansluiting op EU-interoperabiliteit: sluit de nationale juridische inrichting aan op Europese standaarden en verplichtingen?

2.1. Antwoord op de kernvraag

Bestaande kaders faciliteren in beperkte mate uniforme begrippen, standaarden en technische interoperabiliteit die noodzakelijk zijn voor vrij verkeer van informatieobjecten.

Op Europees niveau is sprake van een relatief samenhangend systeem. Definities kennen gelaagdheid en stukken regelgeving bevatten onderlinge consistentie ten aanzien van definities. Zo ontstaat een onderling verbonden begrippenkader. In nationale wetgeving ontbreekt deze systematiek. Dit komt mede door het feit dat dezelfde woorden andere definities kennen afhankelijk van de functionaliteit binnen de desbetreffende wet en er geen inzicht is in alle wetten die van toepassing zijn en hoe die moeten worden toegepast. Dit belemmert het opzetten van een uniform kader, dat noodzakelijk is voor vrij verkeer van gegevens.

Voor technische standaarden geldt dat zowel Europese als nationale normen dezelfde waarden ambiëren te vervullen, maar de invulling daarvan gefragmenteerd gebeurt. Door sector- en situatieafhankelijke verplichtingen te hanteren, is het onduidelijk welke standaard wanneer van toepassing is, wat een infrastructuur voor vrij verkeer van informatieobjecten bemoeilijkt. Bovendien zijn bestaande technische standaarden en normen niet altijd juridisch afdwingbaar.

Keteninteroperabiliteit is een ambitie van zowel de EU als Nederland. Het is momenteel echter onduidelijk via welk mechanisme interoperabiliteit afdwingbaar is en in welke vorm de overheidsorganisaties hieraan moeten voldoen. Bovendien zijn de meeste overheidsorganisaties in de praktijk gebonden aan rijksbrede beslissingen over IT-infrastructuur, waardoor zij niet individueel aan dergelijke vereisten (kunnen) voldoen. Hiervoor zijn overeenstemming en begeleiding op technisch vlak noodzakelijk.

2.2. Begrippen

2.2.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“in hoeverre worden in relevante stukken wet- en regelgeving overheidsbreed dezelfde begrippen en definities gebruikt voor informatie?”* centraal. Om deze vraag te beantwoorden, is een overzicht nodig van alle wetten en regels die ‘informatie’ betreffen.

In het kader van dit onderzoeksrapport en het verbeteren van de informatiehuishouding van de overheid, betreft ‘informatie’ de definitie ‘informatieobject’ zoals voorgesteld in de Aiw⁶⁷:

“gestructureerd of ongestructureerd identificeerbaar gegeven of geheel van gegevens, daaronder mede begrepen gegevens die kenmerken van dat gegeven of geheel van gegevens beschrijven”

Zo kan een informatieobject een naam zijn, de combinatie van naam, telefoonnummer en adres, een verstuurd brief, maar ook een algoritme of een document.⁶⁸

In Nederland worden informatieobjecten gereguleerd door verschillende stukken nationale en Europese wet- en regelgeving. Er zijn allerlei begrippen die in de wetgeving worden gebruikt en gelijk zijn aan of onder ‘informatieobject’ vallen. Een overzicht van deze begrippen is nodig om zowel overlap als discrepantie tussen die begrippen inzichtelijk te maken. Dit overzicht is beperkt tot wetgeving die dergelijke begrippen bevat én betrekking heeft op de informatiehuishouding van de overheid. Dit overzicht is te vinden in bijlage 1 van dit onderzoeksrapport.

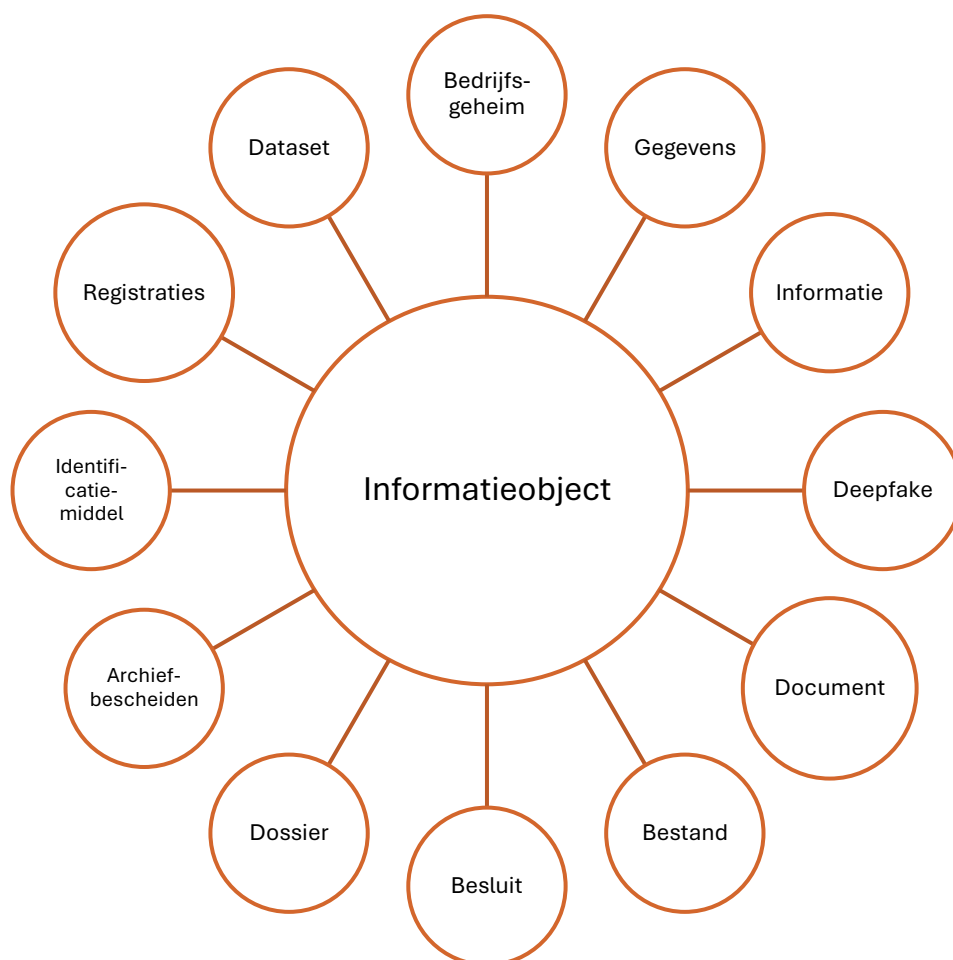
Specifiek betreft het wetgeving over het delen van gegevens binnen de overheid of de openbaarmaking van overheidsinformatie. Business-to-business (B2B) gegevensdeling, of gegevensdeling waarbij een overheidsinstantie een rol speelt in het faciliteren van gegevensdeling tussen partijen (zowel business-to-government als B2B), is hierin niet meegenomen.⁶⁹

⁶⁷ Zie art. 1 Algemene informatiewet overheid.

⁶⁸ Zie Concept MvT Algemene informatiewet overheid, p. 1.3 (c).

⁶⁹ Zie ook

https://www.noraonline.nl/wiki/Wettelijke_kaders_en_regelgeving_gegevensmanagement voor een overzicht van wetten t.a.v. gegevensmanagement van NORA.



Afbeelding 3: Verschillende verschijningsvormen van informatieobject.

De overkoepelende begrippen (bijvoorbeeld 'persoonsgegevens' valt onder 'gegevens') die in deze stukken wetgeving voorkomen, zijn geïllustreerd in afbeelding 3.⁷⁰ Allereerst volgt een analyse van de terminologie en bijbehorende definities van de betrokken begrippen en de verhouding daartussen. Daarna volgt een meer strategische analyse over de overkoepelende systematiek die de begrippen illustreren binnen de Europese en nationale wetgeving.

2.2.2. De verhouding tussen begrippen

Tussen deze begrippen bestaat een verhouding in zowel juridische terminologie als de praktijk. Zo kunnen gegevens onderdeel zijn van een bedrijfsgeheim (Wet bescherming bedrijfsgeheimen) en kan een bestand (AVG en 'gegevensbestand' in de Wet justitiële en strafvorderlijke gegevens (Wjsg)) een dataset (EHDS) bevatten en andersom.

Veel data of gegevens specifiek gedefinieerd in deze wetten kunnen vallen onder andere overkoepelende termen. 'Gegevens', een breed gebruikte term in de praktijk, is in de DV gedefinieerd: "elke digitale weergave van handelingen, feiten of informatie en elke compilatie van dergelijke handelingen, feiten of informatie, ook in de vorm van geluids-, visuele of audiovisuele opnames". Daarmee is de

⁷⁰ Europese richtlijnen zijn niet opgenomen in dit overzicht, omdat richtlijnen geen directe werking hebben.

term beperkt tot digitale gegevens. Hoewel in de praktijk een 'document' (onder de Who of Woo) gegevens kan bevatten, bevat een geprint 'dossier' (Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en Wjsg) geen 'gegevens'.⁷¹ Andere specifieke data, bijvoorbeeld testdata, inputdata, validatiedata (AI-verordening), vallen dan weer wel onder 'gegevens' (DV) en gegevens kunnen tegelijkertijd ook input-, test- of validatiedata zijn.

'Inputdata' (AI-verordening) kan andersom ook weer 'persoonsgegevens' (AVG) bevatten, maar ook 'niet-persoonsgebonden gegevens' (DV), 'persoonsgegevens van strafrechtelijke aard' of 'milieu-informatie' (Who).

De term 'document' is zowel in de Who als in de Woo gedefinieerd. In de Who is de definitie breder dan in de Woo (zie hieronder), omdat er ook bijvoorbeeld stukken van overheidsondernemingen onder vallen.

Document in de Who	Document in de Woo
a. door een met een publieke taak belaste instelling opgemaakt of ontvangen schriftelijk stuk of ander geheel of deel van vastgelegde gegevens, dat naar zijn aard verband houdt met de publieke taak van die instelling; b. door een overheidsonderneming opgemaakt of ontvangen schriftelijk stuk of ander geheel of deel van vastgelegde gegevens, dat naar zijn aard verband houdt met de dienstverlening in het algemeen belang van die overheidsonderneming; of c. door een publiek gefinancierde onderzoeksorganisatie opgemaakt of ontvangen schriftelijk stuk of ander geheel of deel van vastgelegde gegevens, dat naar zijn aard verband houdt met de geheel of gedeeltelijk publiek gefinancierde activiteiten van die onderzoeksorganisatie.	Een door een orgaan, persoon of college als bedoeld in <u>art. 2.2, eerste lid</u>, opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college. De in artikel 2.2 lid 1 genoemde bestuursorganen zijn: a. bestuursorganen; b. de Kamers en de verenigde vergadering der Staten-Generaal; c. de Raad voor de rechtspraak en het College van afgevaardigden; d. de Raad van State, tenzij de Raad het koninklijk gezag uitoefent, en met uitzondering van de Afdeling bestuursrechtspraak; e. de Algemene Rekenkamer; f. de Nationale ombudsman en de substituut-ombudsmannen als bedoeld in art. 9, eerste lid, van de Wet Nationale ombudsman, en ombudsmannen en ombudscommissies als bedoeld in art. 9:17, onderdeel b, van de Algemene wet bestuursrecht.

'Documenten' kunnen op hun beurt weer 'informatie betreffende het beheer van rechten' (Databankenwet), 'persoonsgegevens van strafrechtelijke aard' (UAVG) bevatten en 'dynamische gegevens' (Who).

Een aantal in de praktijk veel gebruikte termen is in wetten specifiek gedefinieerd. Zo is 'informatie' in de Woo gebruikt in samenstelling met 'publieke informatie'⁷², in de Wet gegevensverwerking door samenwerkingsverbanden bestaat 'informatie betreffende het beheer van rechten' en de Databankenwet heeft het over 'sturingsinformatie'. Dat terwijl het woord 'informatie' an sich een veel gebruikte term is.

⁷² Zie artikel 2.1 Wet open overheid: *informatie neergelegd in documenten die berusten bij een orgaan, persoon of college als bedoeld in art. 2.2, eerste lid.*

Niet al deze wetten zijn per definitie altijd van toepassing. Het toepassingsbereik hangt af van de organisatie of de situatie. Dit is de materiële reikwijdte van een wet. Van de lastigheid die hierboven is geïllustreerd is pas sprake als al die wetten op dezelfde situatie van toepassing zijn.

Als de situatie niet onder de materiële reikwijdte van een wet valt, valt er mogelijk een aantal definities af. Zo is de Who alleen van toepassing op 'informatie die niet openbaar is op grond van de wet'.⁷³ Dat lijkt een simpele analyse, maar of informatie openbaar is op grond van de wet kent ook weer een juridische analyse. Onder de Woo moet een bestuursorgaan immers uit eigen beweging de bij hem berustende informatie voor eenieder openbaar maken.⁷⁴ Maar als 'document' onder de Woo een specifiekere definitie heeft dan de Who, en de Who alleen van toepassing is op informatie die openbaar is (wat bepaald is onder de Woo), is het onduidelijk hoe die verbreding van de term zich verhoudt tot de toepasselijkheid van de Woo.

De bovenstaande verhoudingen en definities illustreren de lastigheid in de praktijk voor overheidsorganisaties om helderheid te hebben over wanneer zij welke informatie op welke wijze mogen delen.

2.2.3. Strategische analyse

Deze paragraaf behandelt de strategische analyse over de overkoepelende systematiek van de begrippen in Europese en nationale wetgeving. Achtereenvolgens wordt daarbij ingegaan op de duiding van woorden uit definities, het verschil in aggregatieniveau van definities, de impact van context waarbinnen definities worden gebruikt en de vorm van de definities.

2.2.3.1. Individuele gegevens en informatieverzamelingen

Het overzicht uit de bijlage⁷⁵ toont onderscheid tussen het door de wetgever willen reguleren van individuele gegevens en gestructureerde verzamelingen van informatie. Sommige regelgeving richt zich op afzonderlijke gegevens, terwijl andere regelgeving juist definities introduceert voor verzamelingen van gegevens, zoals datasets, bestanden of databanken. Hierdoor kan een individueel gegeven tegelijkertijd onderdeel zijn van een dataset, een databank of een dossier. De regelgeving overlapt hier doordat zij dezelfde informatie reguleert, maar op verschillende niveaus van aggregatie. Als voorbeeld is de term 'persoonsgegeven' in de AVG gedefinieerd als afzonderlijk gegeven, terwijl een persoonsgegeven onder de Wet gemeentelijke schuldhelpverlening (Wgs) op een hoger aggregatieniveau wordt gedefinieerd onder de noemer van 'gegevens'.

2.2.3.2. Functionele en generieke definities van informatie

In sommige wetten wordt informatie gedefinieerd vanuit het doel waarvoor zij wordt gebruikt, bijvoorbeeld in de context van kunstmatige intelligentie, opsporing, communicatie of zorg. Hierdoor wordt informatie niet primair gedefinieerd als object, maar vanuit haar rol binnen een bepaald proces of systeem. Dit leidt tot overlappende definities waarin dezelfde informatie afhankelijk van de context onder verschillende juridische regimes kan vallen.

⁷³ Zie art. 2 Wet hergebruik van overheidsinformatie.

⁷⁴ Zie art. 3.1 lid 1 Wet open overheid.

⁷⁵ Zie bijlage 1.

Zo is de definitie van een 'document' in de Woo afhankelijk van de aard van de opsteller: een met een publieke taak belaste instelling, een overheidsonderneming of een onderzoeksorganisatie. De definitie van 'document' in de Woo focust zich naast de hiervoor genoemde specificatie op de aard van de gegevens: het moet verband houden met de publieke taak belegd bij de instantie. 'Contactgegevens' definieert de Wet basisregistratie personen (Wet BRP) als "telefoonnummer en e-mailadres van de niet-ingezetene".⁷⁶ De toevoeging 'niet-ingezetene' toont de specificatie op het doel van de regulering: registratie van personen.

Deze afbakening doet zich vooral voor in Nederlandse wetten. De EU gebruikt over het algemeen dezelfde definities. Die definities worden per wet vervolgens toegelicht. Het begrip 'persoonsgegevens' in de AVG komt vervolgens als 'gegevens over gezondheid', of 'inputdata' terug in de AI-verordening. Er is een relatie tussen de gegevens. Inputdata kunnen persoonsgegevens zijn, maar ze definiëren niet hetzelfde object op een andere wijze. Soms sluiten Nederlandse wetten wel aan bij Europese begrippen, zoals de Wjsg bij de definitie van de AVG voor gegevens over gezondheid.

In een dergelijke functionele definitie wordt de toepassing van de wet beperkt. De intentie van de wet wordt zo al duidelijk door de definitie van 'document' (*"een door een orgaan, persoon of college als bedoeld in art. 2.2, eerste lid, opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college"*⁷⁷).

Dit kan de bescherming van persoonsgegevens waarborgen, maar kan het tegelijkertijd complexer maken om op nationaal niveau regels te stellen over het hergebruik van bepaalde soorten informatieobjecten, zoals biometrische gegevens. De definitie van een biometrisch gegeven is in de AVG, Wjsg en AI-verordening op detailniveau verschillend. Dat lijkt te maken te hebben met de initiële doelstellingen van ieder stuk wetgeving.

Het is juist gebruikelijk om de toepassing van de wet te beperken in andere artikelen, die gaan over het toepassingsgebied. Zo zou dat in de Woo bijvoorbeeld beperkt kunnen worden door aan de reikwijdte toe te voegen dat deze wet alleen van toepassing is op documenten die verband houden met de publieke taak van dat orgaan, die persoon of dat college. Zo wordt voorkomen dat generieke termen als 'document', 'informatie' en 'gegevens' op dezelfde wetgevingslaag op verschillende manieren worden uitgelegd.

Een dergelijke aanpak zou ruimte bieden voor een overkoepelende definitie waaraan gerefereerd kan worden in specifieke wetten, waarvan de reikwijdte wordt beperkt door de materiële reikwijdte.

2.2.3.3. Inhoud en vorm

Een belangrijke discrepantie in de regelgeving is dat sommige wetten informatie definiëren op basis van de inhoud van de informatie, terwijl andere uitgaan van de vorm waarin informatie is vastgelegd. Gegevensbeschermingswetgeving richt zich als voorbeeld op specifieke typen informatie, zoals persoonsgegevens of

⁷⁶ Zie art. 1.1 sub aa Wet basisregistratie personen.

⁷⁷ Zie art. 2.1 Wet open overheid.

gezondheidsgegevens, ongeacht de vorm waarin deze voorkomen. Transparantie- en archiefwetgeving daarentegen definieert informatie als vastgelegde gegevens in documenten of bescheiden. Hierdoor kan dezelfde informatie juridisch gelijktijdig worden gekwalificeerd als een document, een dataset en een persoonsgegeven. Dit kwam in de vorige paragraaf ook al naar voren.

2.2.3.4. Data versus document

Een tweede discrepantie ligt in het onderscheid tussen data en documenten. Europese regelgeving hanteert doorgaans brede definities van gegevens als digitale representaties van feiten of informatie. Nationale bestuursrechtelijke wetgeving gebruikt daarentegen het begrip document of archiefbescheiden voor vastgelegde informatie. Dit verschil weerspiegelt twee verschillende benaderingen: een datagerichte benadering waarin informatie op elementniveau wordt gezien en een documentgerichte benadering waarin informatie primair wordt beschouwd als een samenhangend geheel.

2.2.3.5. Digitale en vormneutrale informatie

Daarnaast bestaat een verschil tussen regelgeving die zich uitsluitend op digitale informatie richt en regelgeving die vormneutraal is. Europese dataregelgeving definieert gegevens doorgaans expliciet als digitale informatie. In nationale transparantie- en archiefwetgeving wordt informatie daarentegen vormneutraal gedefinieerd, zodat zowel digitale als analoge informatie onder de betreffende wet kan vallen. Hierdoor ontstaat overlap, maar ook een verschil in reikwijdte tussen digitale dataregimes en bredere informatiebegrippen.

2.2.3.6. Sectorspecifieke gegevensuitwisseling

Afhankelijk van de sector kennen Nederland en de EU specifieke wetgeving over gegevensuitwisseling. De overheid opereert in verschillende sectoren en is daarom onderhevig aan allerlei sectorspecifieke wetgeving. In de analyse of gegevens gedeeld moeten of mogen worden, is ook deze wetgeving relevant, zoals de Invorderingswet 1990, die regels bevat over gegevensuitwisseling bij schulden.

Een voorbeeld van een dergelijke sector is de zorgsector. Nederland kent specifiek in de zorgsector veel wetten die de veiligheid van de uitwisseling van gegevens waarborgen. De overheid speelt een rol in het leveren van zorg aan burgers, of verwerkt gegevens over zorg in verband met de maatschappelijke rol die zij vervult. De overheid kan ook de rol van zorgverlener aannemen, bijvoorbeeld bij de gemeentelijke GGD of jeugdgezondheidszorg. Denk hierbij aan het toekennen van subsidies of andere maatschappelijke ondersteuning.

Niet alle wetgeving ten aanzien van specifieke situaties is meegenomen in de analyse en het schema in bijlage 1. Het overzicht betreft de meest generiek voorkomende toepassingen van de wet voor meer algemene situaties waarin wensen zijn om gegevens te delen.

Voor een gedetailleerde analyse of gegevens over zorg of in een andere sector (zoals justitie) gedeeld mogen worden, is meer wet- en regelgeving relevant.

2.2.3.7. Lopende initiatieven

Vanuit de overheid zijn er initiatieven om het gebruik van begrippen te stroomlijnen en discrepantie daartussen te verhelpen. Het NORA Begrippenkader is een dergelijk initiatief, dat ook raakt aan het onderwerp van dit rapport. Dit kader betreft de begrippen die nodig zijn om architecturen te beschrijven die relevant zijn voor de Nederlandse overheid.

Deze begrippen zijn beschreven volgens de NL-SBB, de afgesproken nationale standaard voor begrippenbeschrijving. Deze standaard heeft ook ten doel begrijpelijkheid te bevorderen en samenhang te verhelderen.

Data, gegeven, informatieobject en bestand zijn gedefinieerd in dit begrippenkader. Hoewel dit kader niet primair ontworpen is voor wetgeving, maar voor interne organisatie, is het desalniettemin relevant om dit perspectief mee te nemen. In de praktijk is het namelijk zo dat de definities op de werkvloer, en de definities uit de wet, door elkaar worden gebruikt.

Begrip	Definitie
Data	Een vastgelegde waarneming of bewering over een eigenschap van een object.
Informatieobject	Een op zichzelf staand geheel van gegevens met een eigen identiteit
Persoonsgegevens	<i>Gelijk aan definitie AVG</i>
Bestand	Geordende verzameling van gegevens in elektronische vorm, die door een elektronisch apparaat met een naam kan worden behandeld en aangesproken

2.2.4. Concluderend

Op Europees niveau is er gelaagdheid in de definities betreffende 'informatieobject'. Het betreft de data zelf, de inhoud, of de toepassing van de data. Het uitgangspunt bij regulering uit de EU is een generieke definitie van 'gegevens' en 'persoonsgegevens', die de Europese wetgever overneemt in andere stukken wetgeving zodat het gegevensdelingskader voor dezelfde objecten een kader creëert. Alleen in specifieke situaties worden er specifieke definities binnen een wet aan toegevoegd, zoals 'testdata' in de AI-verordening. In die wetten is dan uitgelegd dat de hiërarchie van die wetten zo is, dat de specifieke definities gelden als *lex specialis* ten opzichte van een *lex generalis*. Zo ontstaat er gelaagdheid in de definitie. Bovendien volgt uit de wet de relatie tussen bepaalde definities. Zie hiervoor een voorbeeld van een aantal gegevens in de tabel hieronder.

Gegevens	
Persoonsgegevens	Niet-persoonsgebonden gegevens
Metagegevens	

In Nederlandse regelgeving is er nog geen overkoepelende definitie van 'informatieobject' of een object dat daaronder valt. Het is logisch dat de Aiw daarom met een voorstel voor de definitie komt. Definities in wetgeving zijn gespecificeerd op het doel van de wet, zoals het archiveren of publiek beschikbaar stellen van gegevens. Daardoor kent eenzelfde woord ('document') verschillende definities in verschillende stukken wetgeving. Een overlappend gegevensdelingskader voor 'document' is daarom lastig te bewerkstelligen (zie

tabel hieronder). Bovendien definieert de wetgever in verschillende stukken wetgeving hetzelfde woord op een andere manier. Er staan daarom verschillende definities naast elkaar die ofwel gelijk zijn aan 'informatieobject' ofwel daaronder vallen. Tussen die definities is er geen duidelijke hiërarchie of heldere relatie (zie tabel hieronder).

Informatieobject				
Archiefbescheiden	Document	Document 2	Gegevens	Publieke informatie

Het voorgestelde Aiw-begrip 'informatieobject' introduceert een generieke term die deze verschillende regimes conceptueel met elkaar verbindt. Een overkoepelende definitie die boven alle definities hangt, kan het gemakkelijker maken om een generiek gegevensdelingskader op te stellen. Desalniettemin is het zo dat, zolang de sectorale wetten hun eigen functionele definities behouden, er onvermijdelijk overlappende kwalificaties van hetzelfde informatieobject blijven bestaan die voor onduidelijkheid zorgen in de praktijk. De discrepantie binnen het gereguleerde onderwerp verergert de ongelijke definiëring.

Op het moment van schrijven van dit rapport wordt onder het FDS aandacht besteed aan de discrepantie in de semantiek. Zoals genoemd is er ook het NORA Begrippenkader om gebruik van begrippen en samenhang intern te verhelderen. Idealiter vindt het wetgevingskader qua definities aansluiting bij intern gebruikte terminologie.

2.3. Technische standaarden

2.3.1. Toelichting deelvraag

De consistentie tussen begrippen zoals in de vorige paragraaf uiteengezet is een belangrijk aspect van een sterke informatiehuishouding. Technische standaarden waarbinnen informatie wordt uitgewisseld zijn andere, minstens zo belangrijke, aspecten. In deze paragraaf staat de vraag *"worden standaarden juridisch of beleidsmatig verplicht voorgeschreven en zijn deze verplichtingen afdwingbaar?"* centraal. Deze paragraaf biedt inzicht in de relevante vormverplichtingen voor de overheid ten aanzien van haar informatiehuishouding.

Een van de doelen van het eerdergenoemde Digital Decade-programma is de *"waarborging van de digitale open soevereiniteit van de Unie, met name met behulp van een beveiligde en toegankelijke digitale infrastructuur en gegevensinfrastructuur die enorme hoeveelheden gegevens doeltreffend kunnen opslaan, doorsturen en verwerken"*.⁷⁸ Met verschillende stukken wetgeving wenst de EU een geharmoniseerd kader voor gegevensuitwisseling op te zetten. De DV, de DGV en de VIE vormen de basis van dit gegevensuitwisselingskader. Met specifieke dataruimten, zoals de EHDS, worden regels gemaakt ten aanzien van bepaalde soorten gegevens.⁷⁹

De DGV, de Open Data-richtlijn en de VIE zien specifiek op overheidsdata. De regulering die hieronder wordt omschreven is van toepassing op overheidsdata in specifieke gevallen.

⁷⁸ Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030.

⁷⁹ Geldend als een lex specialis op een lex generalis.

Naast Europese regels die standaarden introduceren voor de vorm van informatie, kent Nederland op nationaal niveau ook een aantal wetten die standaarden neerleggen voor informatie. Hieronder is uiteengezet wat elke wet verplicht ten aanzien van technische standaarden.⁸⁰

Regeling	Kern van de wet	Kader met betrekking tot technische standaarden voor overheidsdata
Datagovernance-verordening en Uitvoeringswet	Creëert een Europees kader voor betrouwbare datadeling en hergebruik van (beschermde) data.	Stimuleert interoperabele standaarden voor datadeling en hergebruik; introduceert tussenpersonen 'databemiddelingsdiensten' voor commerciële relaties; geen directe standaardisatieplicht voor overheden, wel beveiligde verwerkingsomgevingen en mogelijkheid tot nadere technische eisen via uitvoeringshandelingen.
Dataverordening en Uitvoeringswet	Regelt eerlijke toegang tot en het delen van data tussen bedrijven, gebruikers en overheden.	Verplicht data in begrijpelijk en machineleesbaar formaat beschikbaar te stellen bij verbonden producten; overheden kunnen gegevens opvragen bij uitzonderlijke noodzaak; bevordert interoperabiliteit; Commissie kan geharmoniseerde Europese normen laten ontwikkelen.
Open Data-richtlijn en Wet implementatie open data richtlijn	Verplicht overheden data actief beschikbaar te stellen voor hergebruik.	Overheidsinformatie moet machineleesbaar en in open, gangbare formaten worden ontworpen en vervaardigd (https://data.overheid.nl/); high-value datasets via API en bulkdownload; gebruik van open standaarden verplicht.
Verordening Interoperabel Europa	Versterkt de interoperabiliteit van digitale overheidsdiensten binnen de EU.	Gebruik en hergebruik van interoperabiliteitsoplossingen bij grensoverschrijdende diensten; gebaseerd op open specificaties en het Europees Interoperabiliteitskader (EIF).
NIS2-richtlijn	Verhoogt het niveau van cybersecurity binnen de EU voor essentiële en belangrijke entiteiten.	Toepassing van passende technische en organisatorische beveiligingsmaatregelen; verwijst naar Europese/internationale beveiligingsnormen, geen specifieke datastandaarden.
Cyberbeveiligingswet (nog niet in werking getreden)	Implementeert de NIS2-richtlijn en verbetert beveiliging.	Vereist structurele beveiligingsmaatregelen voor netwerk- en informatiesystemen en verplicht incidentmelding.
Digitaaldiensten-verordening	Versterkt toezicht en verantwoordelijkheid van online platforms. Relevant voor overheidsdata op platforms.	Verplicht gestructureerde datatoegang voor toezichthouders en onderzoekers; technische uitwerking mogelijk via uitvoeringshandelingen.
Algemene verordening gegevensbescherming	Beschermt persoonsgegevens en harmoniseert gegevensbescherming binnen de EU.	Passende technische en organisatorische beveiligingsmaatregelen.
Wet beveiliging netwerk- en informatiesystemen	Verplicht aanbieders van essentiële diensten en digitale dienstverleners om netwerk- en informatiesystemen te beveiligen en ernstige incidenten te melden.	Vereist risicobeheer en passende technische beveiligingsmaatregelen voor informatiesystemen die data verwerken.

⁸⁰ Daarbij opgemerkt dat dit geenszins een uitputtend overzicht is, maar een weergave die hoog over de belangrijkste wet- en regelgeving weergeeft. Besluiten en regelingen die op hun beurt weer gebaseerd zijn op de weergegeven wet- en regelgeving zijn voor het overzicht bewust uit deze tabel gelaten.

Archiefwet	Zorg voor archiefbescheiden.	Vereist dat informatieobjecten duurzaam toegankelijk blijven en eist vernietiging wanneer de bewaartermijn is verlopen.
Wet open overheid	Openbaarmaking van overheidsinformatie.	Overheidsinformatie moet digitaal vindbaar en toegankelijk worden gemaakt.
Wet hergebruik van overheidsinformatie	Hergebruik van overheidsinformatie.	Overheidsdata moeten waar mogelijk beschikbaar worden gesteld in open, machineleesbare en gangbare formaten. Verplicht gebruik van open standaarden, API's en interoperabele datamodellen voor hergebruik van datasets.
Wet digitale overheid	Betrouwbare toegang tot elektronische dienstverlening.	Verplicht gebruik van erkende open standaarden en generieke digitale infrastructuur voor gegevensuitwisseling tussen overheid, burgers en bedrijven. Biedt tevens mogelijkheid tot het aanwijzen van nieuwe standaarden.

Tabel 1: Overzicht regelgeving voor technische standaarden.

Al deze wetten bevatten verplichtingen ten aanzien van de standaarden waarin informatie gedeeld mag worden. De volgende paragraaf gaat daar nader op in en behandelt de voorwaarden waaronder gegevens gedeeld mogen worden en technische standaarden die worden opgelegd.

2.3.2. Technische standaarden

Tabel 2 biedt een overzicht van alle wettelijke technische vereisten om data te delen opgelegd vanuit de verschillende datareguleringen uit tabel 1. Let wel, een deel van deze vereisten moet nog worden vastgesteld, zoals bij de DGV waarin publieke organen de beveiligingsvoorwaarden (deels nog moeten) vastleggen voor hergebruik van overheidsdata.⁸¹ Dit is aangeduid als "*nadere technische specificatie mogelijk*".

Regeling	Machineleesbaar formaat	Open format ⁸²	Interoperabiliteit	API	Beveiligingsnormen	Overige vereisten mogelijk	Anonimiseren
Datagovernance-verordening	Nee	Nee	Ja	Nee	Ja	Ja	Ja
Dataverordening	Ja	Nee	Ja	Nee	Ja	Ja	Ja
Open Data-richtlijn/Wet hergebruik van overheidsinformatie	Ja	Ja	Ja	Ja	Nee	Ja	Bij AMvB
Verordening Interoperabel Europa	Nee	Ja	Ja	Nee	Nee	Ja	NVT
NIS2-richtlijn	Nee	Nee	Nee	Nee	Ja	Ja	Ja
Digitaledienstenverordening	Ja	Nee	Nee	Nee	Ja	Ja	Nee
AVG	Ja	Nee	Nee	Nee	Ja	Beperkt	Ja

Tabel 2: Overzicht technische vereisten voor datadelen per dataregulering.

De veelvoorkomende verplichtingen zijn het opleveren van gegevens of documenten in machineleesbaar formaat, een open format, verplichte beveiligingsnormen en anonimisering (in bepaalde gevallen). Al de genoemde

⁸¹ Zie art. 5 lid 2 Datagovernanceverordening.

⁸² Dit houdt in dat de regeling voorschrijft dat overheidsdata moeten worden verstrekt in een formaat dat gebaseerd is op open standaarden in plaats van gesloten standaarden.

technische standaarden zijn in specifieke situaties verplicht. De DGV is van toepassing op hergebruik (gebruik voor een ander doel dan het primaire doel van verzameling) van data die anderszins beschermd is (zoals door de AVG) via databemiddelingsdiensten of data-altruïsme. De ODR ziet bijvoorbeeld niet op informatie die niet openbaar is op grond van de wet of auteursrechtelijk beschermde werken. Zo kent elke wet een eigen toepassingsgebied. De technische standaarden uit tabel 2 zijn dus niet in iedere situatie verplicht.

Technische verplichtingen mogen naleving van andere wetten niet in de weg staan. De Digitaledienstenverordening (bekend onder de Engelse afkorting DSA) is relevant als overheidsinformatie via platforms wordt verspreid of gepubliceerd, of als de overheid zelf optreedt als aanbieder van een dienst die onder de DSA kan vallen. De technische standaarden mogen niet in strijd zijn met verplichtingen onder de DSA, zoals de verplichting om als onrechtmatig aangemerkte informatie offline te halen.

Naast wettelijke verplichtingen zijn er vanuit het FDS ook standaarden ontwikkeld om gegevensdeling te bevorderen. Deze zien op:

- inzicht creëren in het data-aanbod,
- het ontsluiten van data (API's voor data-uitwisseling, het koppelen van services), en
- verantwoord datagebruik.⁸³

Deze standaarden zijn niet wettelijk verplicht, maar kunnen via artikel 3 van de Wdo wel verplicht worden gesteld. Het sentiment dat tijdens het opstellen van dit rapport is geconstateerd, is op dit moment dat dat niet nodig zou zijn voor eenduidige toepassing van de standaarden.

Hieronder zijn interoperabiliteit, beveiligingseisen en hergebruik verder toegelicht.

2.3.2.1. Interoperabiliteit

De VIE verplicht lidstaten om bij relevante nieuwe of ingrijpend gewijzigde digitale overheidsoplossingen vooraf een interoperabiliteitsbeoordeling uit te voeren. Die beoordeling ziet op de mate waarin een oplossing aansluit bij bestaande standaarden, herbruikbaar is en uitwisseling met andere overheden mogelijk maakt. Die beoordeling moet plaatsvinden in de ontwerpfase, voordat besluitvorming over ontwikkeling of implementatie plaatsvindt.

Het EIF biedt een inhoudelijk referentiekader dat verduidelijkt hoe deze interoperabiliteit kan worden vormgegeven op juridisch, organisatorisch, semantisch en technisch niveau. De VIE geeft hieraan een bindend *governance*kader en verplicht tot interoperabiliteitsbeoordeling bij relevante digitale overheidsoplossingen, waardoor het EIF kan worden benut als inhoudelijke leidraad bij de uitvoering daarvan.

Dit biedt ruimte om interoperabiliteit (binnen nationale wetgeving) concreter te maken, bijvoorbeeld als technische norm of standaardverplichting bij de inrichting van informatiesystemen. Het Europese kader schrijft niet exact voor welke technische standaarden moeten worden gebruikt, maar verlangt wél dat aansluiting bij bestaande (Europese) kaders en hergebruik systematisch worden meegewogen.

⁸³ <https://federatief.datastelsel.nl/kennisbank/standaarden/>.

De verordening verplicht dus niet tot één specifieke technische standaard, maar creëert wel een juridische context waarin het verdedigbaar is om interoperabiliteit nationaal concreter en technischer te normeren.

2.3.2.2. Beveiligingsvereisten en -standaarden

Om van interoperabiliteit te kunnen spreken in verband met beveiligingsvereisten, is het van belang dat dezelfde of compatibele vereisten gelden voor dezelfde soorten gegevens (of informatieobjecten) en de systemen waarbinnen zij worden verwerkt. Praktisch gesproken: zijn de beveiligingsvereisten voor systeem A en systeem B gelijkwaardig, en kan hun beveiligingsniveau eenvoudig worden getoetst op geschiktheid voor de uit te wisselen gegevens?

Zorgplichten in verband met beveiliging van gegevens die de overheid verwerkt, worden uitgebreider behandeld in Pijler 3. Zoals daar nader is toegelicht, kunnen er diverse verplichtingen (of zorgplichten) voor informatiebeveiliging tegelijkertijd van toepassing zijn op dezelfde (ICT- en AI-)systemen en de gegevens die daarin worden verwerkt. Hierdoor is een analyse van verschillende stukken wet- en regelgeving noodzakelijk om te bepalen of een informatiesysteem geschikt en passend beveiligd is om ingezet te worden bij specifieke overheidstaken. In deze tweede pijler gaat het over interoperabiliteit en standaarden die ervoor zorgen dat verschillende systemen op elkaar aangesloten kunnen worden om gegevens uit te wisselen en daarbij ook passend beveiligd zijn voor de gegevens die er worden verwerkt en uitgewisseld.

Voor persoonsgegevens gelden de beveiligingsplichten uit de AVG, terwijl de BIO is vastgesteld om voor de gehele overheid een basisniveau van informatiebeveiliging te bepalen voor alle verwerkte gegevens. Sinds september 2025 is versie 2 van de BIO van kracht, die gebaseerd is op en op diverse plaatsen verwijst naar de NEN-EN-ISO/IEC-normen 27001 en 27002. De combinatie van de (aankomende) Cbw, Cyberbeveiligingsbesluit, BIO 2 en de genoemde NEN/ISO-normen moet ertoe leiden dat informatiebeveiligingsmaatregelen van overheidssystemen goed op elkaar aansluiten.

Toepassing van deze regels heeft als doel dat de overheid informatiesystemen gebruikt waarvan de beveiligingsmaatregelen geschikt zijn voor de gegevens die daarin worden verwerkt. Dit komt in grote lijnen overeen met de zorgplicht van de voorgestelde Aiw⁸⁴, die voorschrijft dat binnen de overheid gebruikte informatiesystemen geschikt zijn voor het verkeer van informatieobjecten binnen, tussen en met overheidsorganen.

De vraag welke (ICT- of AI-)systemen geschikt zijn voor welke soorten informatie en welke beveiligingsmaatregelen passend zijn, hangt samen met het doel dat wordt beoogd. Informatie die onder de Archiefwet valt, zal bijvoorbeeld dusdanig moeten worden beveiligd dat deze duurzaam toegankelijk blijft voor zo lang als de Archiefwet daartoe verplicht. Dit impliceert ook dat de informatie wordt beschermd tegen verlies, aantasting en ongeautoriseerde wijziging. In informatiebeveiligingstermen zijn voor naleving van de Archiefwet vooral de aspecten beschikbaarheid en integriteit van belang. In de risicobeoordeling die op basis van bijvoorbeeld de BIO 2 moet worden uitgevoerd, zal dit moeten worden meegenomen.

⁸⁴ Zie art. 7 Algemene informatiewet overheid.

Ook vanuit een andere hoek dient er rekening gehouden te worden met beveiligingsvereisten en standaarden. De Uitvoeringswet Verordening cyberweerbaarheid operationaliseert de Europese Verordening cyberweerbaarheid en stelt eisen aan de beveiliging van producten met digitale elementen zoals software en de hardware waar de software op draait. De eisen gelden gedurende de levenscyclus van de producten en omvatten onder andere het registreren en melden van kwetsbaarheden, het beschikbaar stellen van beveiligingsupdates en eisen voor veilige ontwikkeling en onderhoud. Voor overheidsorganisaties werkt dit vooral door in de inkoop en het gebruik van digitale systemen, omdat zij bij aanbestedingen en het sluiten van inkoopovereenkomsten moeten controleren of leveranciers aan deze beveiligingseisen voldoen en structureel updates en kwetsbaarheidsmeldingen leveren.⁸⁵ Specifiek voor veilig aanbesteden en inkopen zijn de Inkoopseisen Cybersecurity Overheid (ICO) opgesteld. Daarnaast is er een hulpmiddel (ICO-wizard) om eisenpakketten samen te stellen die aansluiten op verschillende typen aan te besteden of in te kopen producten en/of diensten.⁸⁶

De Cyberbeveiligingsverordening en de bijbehorende Uitvoeringswet Cyberbeveiligingsverordening zijn relevant in verband met interoperabiliteit en informatiebeveiliging in zoverre hiermee een geharmoniseerd kader is opgezet voor vrijwillige cyberbeveiligingscertificering van ICT-producten, -diensten en -processen. Certificering biedt mogelijkheden om op een efficiëntere wijze de nodige zekerheid ('assurance') te verkrijgen dat de toeleveringsketens voldoen aan relevante eisen voor informatiebeveiliging.

De verordening voor electronic IDentification, Authentication and trust Services (eIDAS) kan bij uitstek worden beschouwd als een beveiligingstechnisch hulpmiddel voor interoperabiliteit. Deze verordening zorgt er in de eerste plaats voor dat alle 27 EU-lidstaten elkaars aangemelde stelsels voor elektronische identificatie wederzijds erkennen. De eIDAS-verordening hanteert drie niveaus van betrouwbaarheid voor elektronische identificatie, namelijk laag, substantieel en hoog. De eisen aan beveiliging corresponderen daarmee. De aanbieders van 'vertrouwensdiensten' zoals digitale certificatedienstverleners moeten op grond van eIDAS voldoen aan specifieke beveiligingseisen die zijn vervat in diverse standaarden van het European Telecommunications Standards Institute. Door het vaststellen van eIDAS 2.0 in 2024 is het voor elke EU-lidstaat vanaf eind 2026 verplicht om een EUDI⁸⁷-wallet gratis voor burgers beschikbaar te stellen. Daarin kunnen burgers diverse persoonsgegevens en bewijzen opslaan, zoals persoonsgegevens uit de BRP en diploma's en vergunningen. Het gebruik van een dergelijke wallet is voor burgers vrijwillig en niet verplicht. Er is inmiddels een GitHub-pagina gepubliceerd waarin de NL Wallet wordt ontwikkeld, beheerd en open source beschikbaar gesteld.⁸⁸ Op die pagina is ook de verwachting uitgesproken dat de app in 2027 klaar zal zijn.

2.3.2.3. Hergebruik van overheidsinformatie

⁸⁵ Het kan de vraag zijn of bepaalde digitale producten van de overheid, zoals DigiD, zelf ook rechtstreeks onder de Cyberweerbaarheidsverordening vallen. Daar wordt nader op ingegaan in pijler 3.

⁸⁶ Zie bijvoorbeeld <https://www.bio-overheid.nl/category/producten/icoproducten>.

⁸⁷ EDI staat voor electronic data interchange.

⁸⁸ Zie <https://github.com/MinBZK/nl-wallet>.

De Who is een kernregulering als het gaat om inrichting van de informatiehuishouding. De Who ziet namelijk op bestaande, openbaar gemaakte informatie waarover een bestuursorgaan beschikt in het kader van zijn publieke taak en verplicht in beginsel tot hergebruik. De regel daarbij is 'open, tenzij'. De tenzij wordt daarbij ingevuld door omschrijvingen van informatie "*die niet openbaar is op basis van de wet*"⁸⁹ of informatie waarover een derde auteursrechthebbende is.⁹⁰

De informatie die beschikbaar moet zijn voor hergebruik moet machineleesbaar en in open, gangbare formaten worden verstrekt. Voor high-value datasets geldt dat beschikbaarstelling via API, bulkdownload en open standaarden moeten worden toegepast.

Technische keuzes, zoals het verplicht stellen van open standaarden en gestandaardiseerde gegevensmodellen, versterken de uitvoerbaarheid van de Who en faciliteren data-uitwisseling. Tegelijkertijd vergroot dit de reikwijdte en feitelijke toegankelijkheid van overheidsdata, wat expliciete afwegingen vergt ten aanzien van doelbinding, beveiliging en vertrouwelijkheid en van directe invloed is op de inrichting van de informatiehuishouding.

Op dit moment is echter onduidelijk voor overheidsorganen welke gegevens wel of niet gedeeld mogen worden onder de huidige wet- en regelgeving. Doordat de Who haar toepassingsbereik daarvan afhankelijk maakt, verheldert de Who dit niet, maar verplaatst zij dezelfde vraag naar de analyse of de Who van toepassing is. Wanneer aan deze technische voorwaarden voldaan moet worden, kan dus niet helemaal helder zijn.

2.3.3. Handhaving

Niet alle verplichtingen die de overheid kent ten aanzien van technische en overige standaarden voor de informatiehuishouding zijn afdwingbaar. Er zijn verschillende toezichthouders die handhaven op de naleving van voornamelijk beveiligingsverplichtingen. Zo is dat voor de AVG de AP, voor de Wet beveiliging netwerk- en informatiesystemen, Uitvoeringswet Cyberbeveiligingsverordening en Cbw (concept) de RDI en voor de Archiefwet de IOE.

Verder is het zo dat de rechtspraak hier ook een rol speelt ten aanzien van welke gegevens de overheid openbaar zou moeten maken op basis van de Woo. Regelmatig zijn er rechtszaken tegen overheidsinstanties waarin een burger beweert dat er stukken ofwel niet zijn gedeeld ofwel onterecht zijn zwartgelakt terwijl dat volgens de standaarden van de overheid (open, tenzij) wel had moeten.

Specifieke handhaving op de standaarden (die niet zien op beveiliging of openbaarheid van gegevens, zoals interoperabiliteit en vrij verkeer van gegevens) van de generieke informatiehuishouding van de overheid gebeurt weinig. De Wdo, die bepaalde technische standaarden verplicht stelt, kent bijvoorbeeld geen toezichthouder.

2.3.4. Concluderend

⁸⁹ Zie art. 2 lid 1 sub a Wet hergebruik van overheidsinformatie.

⁹⁰ Zie art. 2 lid 1 sub b Wet hergebruik van overheidsinformatie.

Nationale en Europese wet- en regelgeving schrijft verschillende standaarden voor, in specifieke en algemene context. In sommige gevallen zijn er toezichthouders die hierop handhaven.

De verbeterde informatiehuishouding voorgesteld via de Aiw bevat:

1. vrij verkeer van informatieobjecten,
2. informatiesystemen geschikt voor verkeer van informatieobjecten binnen, tussen en met overheidsorganen ter uitvoering van publieke taken, en
3. afgestemde standaarden en architectuur.

Het vrij verkeer faciliteren binnen informatiesystemen sluit aan bij verplichtingen onder meer uit de VIE en de Who. Voorgestelde architectuur en standaarden moeten overeenkomen met verplichtingen die reeds liggen voor de overheid, zoals de BIO-normen. Omdat verplichtingen uit wetgeving situatie- en sectorspecifiek kunnen zijn, is het noodzakelijk te voorkomen dat een standaard of architectuur verplichtingen oplegt die naleving van andere wet- en regelgeving tegenwerken. Dit kan door bij het opstellen van standaarden en architectuur aan te sluiten bij verplichte standaarden, en tegelijkertijd ruimte te laten voor de naleving van specifieke verplichtingen.

2.4. Keteninteroperabiliteit

2.4.1. Toelichting deelvraag

In de vorige paragraaf werd al aandacht besteed aan technische interoperabiliteit als standaard voor informatiehuishouding. Hieruit blijkt dat interoperabiliteit vanuit de EU tot aan nationale wet- en regelgeving gedragen wordt. De huidige stand van zaken ten aanzien van keteninteroperabiliteit is noodzakelijk om de status van de informatiehuishouding te begrijpen.

In deze paragraaf staat daarom de vraag *“wordt ketenoverstijgende interoperabiliteit juridisch ondersteund of juist niet?”* centraal. Deze paragraaf biedt inzicht in de mate waarin keteninteroperabiliteit juridisch is vastgelegd.

Keteninteroperabiliteit in de context van dit rapport betekent een systeem creëren waarbinnen informatieobjecten kunnen vloeien tussen verschillende overheidsorganen. In de vorige paragraaf kwam interoperabiliteit als technische standaard al terug. Interoperabiliteit ziet echter ook op de wetten, afspraken, voorwaarden en vorm waarin gedeeld wordt. Veel wetten, zowel Europees als nationaal, hebben als doel de interoperabiliteit, of het vrije verkeer van gegevens, te bevorderen. Zie ook tabel 2 hierboven onder ‘interoperabiliteit’.

Keteninteroperabiliteit heeft een prominente positie in de NDS gekregen. Na de cloudstrategie is de datastrategie de tweede prioriteit van de NDS. Keteninteroperabiliteit wordt praktisch als volgt omschreven⁹¹:

“We moeten de schotten tussen overheidsorganisaties weghalen: gegevens blijven bij de bron en worden op een gelijke manier georganiseerd, waardoor gegevens beter vindbaar, (her)bruikbaar en uitwisselbaar zijn. We spreken heldere regels af over hoe gegevens verantwoord gebruikt kunnen worden over grenzen van organisaties heen, met waarborgen voor verantwoord gebruik.”

⁹¹ Zie ‘De Nederlandse Digitaliseringsstrategie Samen versnellen’, juni 2025, p. 6.

en

"We pakken problemen met het delen van gegevens aan. Gegevens kunnen beter gebruikt worden over de grenzen van overheidsorganisaties heen om burgers en ondernemers beter te helpen en maatschappelijke problemen op te lossen."

In de NDS wordt dit omschreven als FDS. Dit lijkt een streven waar veel voorstanders voor te vinden zijn. Het sluit aan bij de initiatieven van Europa ten aanzien van interoperabiliteit (zie de vorige paragraaf), zoals de VIE, de ODR en de (meer specifieke) DGV en DV.

De vraag is echter in hoeverre deze wens en behoefte een juridisch solide basis kent. Om tot die juridische basis te komen, is het relevant om te analyseren onder welke voorwaarden het mogelijk is 'wat' (object) te delen, en in welke vorm ('hoe'). Er zijn stukken wet- en regelgeving die hier restricties opleggen.

Er zijn regels voor de omgang met specifieke soorten gegevens. De belangrijkste bronnen zijn de AVG en de Wet politiegegevens (Wpg). Zodra de uit te wisselen gegevens persoonsgegevens zijn zoals bedoeld in de AVG⁹², of politiegegevens zoals bedoeld in de Wpg⁹³, werpen de AVG en de Wpg drempels op. Het verwerken, en daarmee ook delen, van deze gegevens is aan strikte voorwaarden verbonden en in sommige gevallen daardoor niet toegestaan. Deels is er 'hoe'-wetgeving gemaakt om deze strikte voorwaarden op te rekken of meer te duiden. De Wet gegevensverwerking door samenwerkingsverbanden (Wgds) is daar een voorbeeld van.

Hoewel deze voorbeelden ketenoverstijgende interoperabiliteit kunnen bemoeilijken, is het noodzakelijk om de ratio achter deze regels te begrijpen. De essentie betreft het beschermen van grondrechten van burgers. De toeslagenaffaire toonde wat er kan gebeuren als gegevens verzameld voor het ene doel daarna onrechtmatig gebruikt worden voor een ander doel.⁹⁴

De Wdo stimuleert interoperabiliteit op digitaal vlak en maakt het inrichten en onderhouden van een goede digitale infrastructuur verplicht in bepaalde situaties. De Wdo bevat geen generieke verplichting voor het gehele overheidsdomein, maar bevat gerichte scenario's om digitale infrastructuur op orde te brengen zonder te spreken over ketenoverstijgende interoperabiliteit.⁹⁵

De Aiw ambieert keteninteroperabiliteit te reguleren, maar met inachtneming van wetgeving die deze interoperabiliteit om legitieme redenen blokkeert. Informatieobjecten moeten zich vrij binnen en tussen overheidsorganen kunnen bewegen, behoudens wettelijk vastgestelde beperkingen daarvan.⁹⁶ Maar niet alleen wettelijk vastgestelde beperkingen kunnen in de ogen van de Aiw gezien worden als blokkerende factor voor gegevensuitwisseling binnen en tussen overheidsorganen. De Aiw stelt ook dat het vrije verkeer van informatieobjecten

⁹² Zie art. 4 lid 1 Algemene verordening gegevensbescherming.

⁹³ Zie art. 1 onder a Wet politiegegevens.

⁹⁴ Zie boetebesluit Belastingdienst zwarte lijst FSV, AP, 12 april 2022.

⁹⁵ Zie art. 5 Wet digitale overheid.

⁹⁶ Zie art. 3 lid 1 Algemene informatiewet overheid.

beperkt kan worden door technische beperkingen van systemen en voorzieningen van de informatiehuishouding.⁹⁷ Daarbij wordt opgemerkt dat deze technische beperkingen met een reden kunnen bestaan. Bijvoorbeeld omdat het delen van informatie niet wenselijk of toegestaan is. Hiermee balanceert ook de Aiw op een dun koord als het gaat om keteninteroperabiliteit. Delen moet juridisch en technisch mogelijk zijn, maar er zijn ook situaties denkbaar waarbij dit juridisch niet is toegestaan en daarom technisch onmogelijk gemaakt moet (kunnen) worden.

2.4.2. Concluderend

Er is juridische ruimte om ketenoverstijgende interoperabiliteit op 'hoe-niveau' mogelijk te maken. Die juridische ruimte wordt echter wel ingekaderd door wet- en regelgeving ten aanzien van het delen van gegevens, waardoor ketenoverstijgende interoperabiliteit wordt beperkt. Dit is voornamelijk ten behoeve van het grondrecht op bescherming van persoonsgegevens en de persoonlijke levenssfeer.

2.5. EU-interoperabiliteit

In deze paragraaf staat de vraag *"sluit de nationale juridische inrichting aan op Europese standaarden en verplichtingen?"* centraal. Om zoveel mogelijk overzicht te bewaren over de verschillende verplichtingen is zowel het nationale als het Europese landschap ten aanzien van interoperabiliteit in de voorgaande paragrafen behandeld.

Wat daaruit volgt is dat conceptueel gezien de nationale visie aansluit bij de ambitie van Europa om een vrij verkeer van gegevens te realiseren. Let wel, de Aiw heeft een bredere focus dan Europa. Regelgeving vanuit Europa bekijkt interoperabiliteit vanuit het concept van 'gegevens', behalve in de VIE. Dat betreft de interoperabiliteit van overheidssystemen en -systematiek. Verder stelt Europa regels over wanneer welke gegevens gedeeld mogen worden. Dit beperkt het vrije verkeer van gegevens ten behoeve van het recht op bescherming van persoonsgegevens en ten dele ten behoeve van een spreiding van de marktmacht en het voorkomen van monopolies ten aanzien van data. Deze regels gelden ook voor de overheid.

Hoewel conceptueel de nationale juridische inrichting aansluit op de eerder behandelde Europese standaarden en verplichtingen, schuurt dit in de praktijk daarom in specifieke situaties.

⁹⁷ Zie MvT Algemene informatiewet overheid, p. 8.

3. Pijler 3: Integrale kwaliteit en zorgplicht

De derde pijler concentreert zich op het beperkte vermogen om informatie goed te beheren, gemakkelijk terug te vinden en op het feit dat de inrichting van de informatiehuishouding mogelijk onvoldoende rekening houdt met de wettelijke voorschriften. Een goede informatiehuishouding moet streven naar kwaliteitsborging, duurzame toegankelijkheid en betrouwbaarheid van informatie door een expliciete, afdwingbare zorgplicht bij overheidsorganen.

Deze pijler gaat over de structurele borging van informatiekwiteit: juistheid, vindbaarheid, duurzame toegankelijkheid, beveiliging en volledigheid. De Aiw introduceert hiervoor een generieke wettelijke zorgplicht.

Om de juridische passendheid van deze zorgplicht te onderzoeken kent de derde pijler de volgende kernvraag:

In hoeverre waarborgen huidige kaders de generieke kwaliteit, toegankelijkheid en veiligheid van overheidsinformatie gedurende de gehele levenscyclus van informatie?

Om deze kernvraag adequaat te kunnen behandelen, komen in het onderzoeksrapport de volgende criteria aan bod:

- Generieke zorgplicht: bestaat er een overheidsbrede, juridisch afdwingbare zorgplicht voor informatiekwiteit of zijn deze verplichtingen sectoraal (te) verdeeld?
- Informatiebeveiliging, privacy en governance: worden informatiebeveiliging, privacy en governance juridisch afdwingbaar integraal meegenomen in het ontwerp en beheer van de informatiehuishouding?
- Monitoring en kwaliteit: bestaan er juridische verplichtingen voor periodieke kwaliteitsmetingen, audits en het definiëren en vaststellen van volwassenheidsniveaus?

3.1. Antwoord op de kernvraag

Huidige kaders voor het borgen van overheidsinformatie gedurende de gehele levenscyclus hebben tot dusver helaas nog altijd niet geleid tot het niveau van kwaliteit, toegankelijkheid en veiligheid van overheidsinformatie dat burgers mogen verwachten. Zoals verderop en ook in andere pijlers van dit onderzoek op diverse plaatsen is aangegeven, hebben zich onder de huidige kaders diverse gevallen voorgedaan waarbij de kwaliteit, toegankelijkheid, veiligheid en privacybescherming van overheidsinformatie op diverse punten van de levenscyclus ernstig tekort hebben geschoten. Daardoor heeft de overheid aanzienlijke schade berokkend aan burgers. De frequentie en ernst van dergelijke incidenten ondersteunen de conclusie van de initiatiefnemers voor de Aiw dat er sprake is van een structureel probleem dat ook een structurele aanpak verdient.

3.1.1. De behoefte aan eenduidige kaders en invulling

Om de kwaliteit, toegankelijkheid en beveiliging van overheidsinformatie te borgen gedurende de hele levenscyclus van de informatie en daarbij tegelijkertijd privacy en persoonsgegevens te beschermen, is het nodig dat het toepassen van wettelijke

regels en toetsingskaders leidt tot heldere, eenduidige en goed onderbouwde antwoorden op praktische vragen als de volgende:

- a. Wie mag of moet welke rechten hebben om de betreffende gegevens te verwerken?
- b. Welke personen moeten op basis van hun functie en taken gegevens kunnen aanmaken, lezen, aanpassen, doorgeven en/of verwijderen?
- c. In welke informatiesystemen, van welke overheidsorganen, mag of moet de informatie worden verwerkt?
- d. Hoe lang moeten de gegevens worden bewaard en wanneer vernietigd? Kan het gebruikte systeem dat automatisch helpen borgen?
- e. Wat zou er bij het verwerken van de gegevens fout kunnen gaan; wie lijdt er hoeveel schade of ander (ernstig) nadeel als:
 - i. de gegevens worden ingezien door onbevoegden (of de vertrouwelijkheid is aangetast),
 - ii. de inhoud van de gegevens onjuist of aangetast is (of de integriteit is aangetast), of
 - iii. de gegevens helemaal niet meer beschikbaar zijn (of de beschikbaarheid is aangetast)?
- f. Wat moeten we redelijkerwijs doen of laten (ter invulling van onze zorgplicht) om de kans en impact daarvan tot een acceptabel niveau terug te dringen?
- g. Op welke manier kunnen of moeten we vaststellen welk niveau van risico op schade 'acceptabel' is en voor wie:
 - i. voor de burger (of 'betrokkene' in de zin van de AVG),
 - ii. voor de overheidsorganisatie en ambtenaren zelf, of
 - iii. voor anderen (derden)?
- h. Hoe stellen we nu echt op zinnige wijze vast welk niveau van bescherming en beveiliging passend is en brengen we de juiste prioritering aan?
- i. Hoe zien we erop toe dat de maatregelen die we hebben geselecteerd ook goed zijn geïmplementeerd en hoe evalueren we periodiek of onze inschatting van de risico's en de reductie daarvan door onze maatregelen (nog steeds) juist is?

Huidige wet- en regelgeving en toetsingskaders bevatten verschillende zorgplichten die gedeeltelijk kunnen overlappen of juist tegenstrijdig kunnen zijn.⁹⁸ Dit maakt het geven van concrete antwoorden op praktische vragen als hiervoor omschreven complex en tijdrovend. In de praktijk leidt dit ertoe dat overheidsorganisaties terughoudend worden om überhaupt gegevens te delen, hoewel dat in sommige situaties een enorm belang heeft voor de burger. Dit probleem wordt erkend, onder meer door de Vereniging van Nederlandse Gemeenten (VNG). Omdat het landschap te complex is, wordt er uit onvrijwillige onkunde 'nee' geantwoord op de vraag of gegevens gedeeld kunnen worden. Dat dit een lastig gegeven is, wordt meermaals beaamd door de overheid zelf. De Belastingdienst publiceerde openbaar ter ondersteuning van de praktijk een Handleiding Wetsanalyse in de praktijk. Dit document en de bijbehorende website

⁹⁸ In de bijlage bij dit hoofdstuk is een niet-uitputtend overzicht opgenomen van diverse algemene en domeinspecifieke zorgplichten. Eerder in dit rapport is al gewezen op de Woo, de Archiefwet, de AVG en cyberbeveiligingswetgeving, die vanuit verschillende belangen verschillende richtingen kunnen uitwijzen ten aanzien van verwerking van informatie.

dienen als handleiding bij de aanpak voor wetsanalyse om wetten gemakkelijker te kunnen toepassen in de praktijk.⁹⁹

Een significant probleem voor de feitelijke uitvoerbaarheid, toepasbaarheid en onderlinge consistentie en interoperabiliteit van de huidige kaders en zorgplichten is bovendien dat diverse wetten en regels aan de ene kant een risicogebaseerde benadering voorschrijven, maar aan de andere kant specifieke bepalingen bevatten die juist afbreuk kunnen doen aan de mogelijkheid om risico's optimaal in samenhang of integraal in te schatten en te beperken. Dit vergroot de kans dat dezelfde vragen op sterk verschillende wijze worden beantwoord in verschillende overheidsorganisaties of vanuit verschillende invalshoeken of disciplines. Zoals in Pijler 1 en 2 hiervoor omschreven, is voor de gewenste informatiehuishouding juist eerder uniforme toepassing of interpretatie wenselijk, zodat praktisch kan worden gefaciliteerd dat steeds de juiste gegevens tussen de juiste (ICT- of AI-)systemen van de juiste overheidsorganen kunnen worden uitgewisseld.

Monitoring en audits vinden op diverse niveaus en momenten plaats door verschillende interne auditfuncties en externe toezichthouders zoals de AP en de RDI, maar de toetsingskaders die daarbij worden gehanteerd, sluiten niet integraal op elkaar aan. Wanneer het risicobeheer ten aanzien van de verwerking van informatie vanuit het perspectief van privacy, informatiebeveiliging en AI niet integraal plaatsvindt en ook de monitoring en toetsing niet, belemmert dit het juridisch afdwingbaar *integraal* meenemen van informatiebeveiliging, privacy en (AI-)governance in het ontwerp en beheer van de informatiehuishouding.

3.1.2. Afstemming en begeleiding

Wenselijk is dat zowel de Nederlandse als de EU-wetgever werken aan het verbeteren van de samenhang en structuur in wetten die voorzien in risicogebaseerde zorgplichten voor het borgen van de juistheid, beveiliging, privacy en goed beheer van informatie. Het staatsrechtelijke of constitutionele niveau van de wet- en regelgeving moet steeds goed passen bij het technische detailniveau van de inhoud. Technisch gedetailleerde regels moeten vooral in lagere uitvoeringsregels worden vervat en snel en gemakkelijk gewijzigd kunnen worden. In hogere regels moeten juist de principes en kaders worden gevat die meer techniekonafhankelijk zijn geformuleerd en langer toepasbaar blijven. Waar verschillende zorgplichten elkaar raken, moeten de wet- en regelgeving en de gehanteerde toetsingskaders voor het controleren van de naleving daarvan duidelijk maken (a) welke verplichting voorgaat, of (b) hoe een redelijke balans of redelijk midden kan worden gevonden. Een uitwerking van de toepasselijke wetgeving door begeleiding en informatievoorziening kan hierbij ook eenduidigheid creëren. Let wel: het orgaan dat de begeleiding faciliteert moet zo te werk gaan dat elk orgaan dat te maken heeft met de regelgeving bereikt wordt.

Het instellen van een adviescollege zou daarbij kunnen helpen. Het is dan wel belangrijk dat wordt voorzien in een ruime, multidisciplinaire expertise en ervaring. Denk aan juristen, ICT-technici, risicomangers, projectmanagers en data- en AI-wetenschappers. Daarbij is ook van belang om goed vast te stellen hoe een dergelijk adviescollege zich zou (moeten) verhouden tot verschillende bestaande

⁹⁹ Handleiding Wetsanalyse in de praktijk, Expertisecentrum Business Rule Management, Belastingdienst, 9 februari 2023 en <https://wendbarewetsuitvoering.pleio.nl/>.

adviescolleges die onder het programma Realisatie IBDS al zijn ingesteld, zoals de Adviesfunctie Verantwoord Datagebruik en de CCG.

Als een ultiem (eind)doel voor een optimale borging van informatiekwaliteit zou wellicht kunnen worden gezien dat iets als een FDS ervoor zorgt dat de juiste informatie steeds (uitsluitend) bij de juiste overheidsorganen en personen beschikbaar is. Technische koppelpunten of kruispunten (bijvoorbeeld API's) tussen informatiesystemen die in gebruik zijn bij verschillende overheidsorganen borgen steeds dat gegevens wel (proactief) worden gedeeld en uitgewisseld waar dat nodig is voor een goede dienstverlening aan de burger en voor democratische verantwoording, maar juist niet waar dat onacceptabele risico's voor burgers zou veroorzaken. Dit impliceert een vermogen om in iets als een FDS een integraal kader voor risicobeheer te verwerken en toe te passen om steeds de juiste verwerking (waaronder eventueel het delen) van ieder informatieobject te borgen. Daaronder valt ook het praktisch borgen van de juiste bewaartermijnen, zoveel mogelijk geautomatiseerd waar de juiste bewaartermijn al specifiek vastligt en waar dat niet het geval is automatische herinneringen worden gegeven voor het toetsen of de gegevens nog wel juist zijn en nog wel nodig zijn om te bewaren.

3.1.3. Concluderend

Er is veel sectorale wetgeving die specifiek invulling geeft aan zorgplichten. Hoewel dit logisch lijkt bij de opzet van een sectorale wet, is er hierdoor ook een gebrek aan integrale samenhang van dergelijke plichten. Dit leidt tot tegenstrijdigheden en onduidelijkheden en beperkt interoperabiliteit als bedoeld in de vorige pijler. De samenhang en consistentie hiervan moeten verbeterd worden.

Aan te raden is om een begrijpelijke maar paradoxale reflex te bedwingen om het probleem dat er (te) veel wetgeving naast elkaar van toepassing is op dezelfde gegevens, gegevensverwerkingen en ambtenaren, die moeilijk met elkaar te verenigen en integraal toe te passen zijn, aan te pakken met nóg weer een nieuwe wet. In dit verband kan verbetering eerder worden gezocht in het gericht schrappen van wetgeving die inconsistent, onnodig of onvoldoende duidelijk is en het verbeteren van de coherentie en consistentie van lagere wet- en regelgeving met hogere.

Daarnaast is van belang om de (complexe) wetgeving die er al wel is om de kwaliteit, beveiliging, privacy en beheer van informatie te borgen, wel steeds beter in de praktijk te brengen. Overheidsorganen moeten zorgen dat zij professionele managementsystemen, beleid en processen inrichten voor goed beheer van informatie, waarbij risicobeheer ten aanzien van privacy, informatiebeveiliging en AI zoveel mogelijk wordt geïntegreerd.

3.2. Generieke zorgplicht

In deze paragraaf en de bijbehorende subparagrafen staat de vraag *“bestaat er een overheidsbrede, juridisch afdwingbare zorgplicht voor informatiekwaliteit of zijn deze verplichtingen sectoraal (te) verdeeld?”* centraal.

Een zorgplicht kan algemeen worden omschreven als een plicht om zorgvuldig te handelen en de belangen van anderen te beschermen, of om schade aan mens en milieu te voorkomen. In de context van het aansprakelijkheidsrecht worden zorgplichten in brede zin beschouwd als de verplichting de ‘in het maatschappelijk verkeer vereiste zorgvuldigheid’ in acht te nemen, een norm die de Hoge Raad in

het arrest *Lindenbaum/Cohen* (1919) zijn constitutionele basis gaf.¹⁰⁰ Over de jaren is een algemene ontwikkeling (of progressie) waar te nemen in de richting dat niet alleen van private partijen maar in het bijzonder van overheidsorganisaties steeds meer wordt verwacht om proactief rekening te houden met anderen en om (risico's op) schade bij anderen door eigen handelen of nalaten te voorkomen of te beperken. Het Urgenda-arrest van 2019, waarin de Hoge Raad op basis van fundamentele rechten zoals het recht op (privé-)leven¹⁰¹ de Nederlandse Staat ertoe heeft gehouden om de uitstoot van broeikasgassen te reduceren, is hiervan een scherp voorbeeld.¹⁰² Naar aanleiding van dit arrest wordt wel gesproken van een 'nieuw constitutionalisme', waarbij de rechter een uitdrukkelijke, constitutionele taak heeft om de staat waar nodig en op uitdrukkelijk verzoek van burgers op te dragen om fundamentele rechten daadwerkelijk in de praktijk te brengen en te beschermen.¹⁰³ Deze ontwikkeling vergroot de (juridische) afdwingbaarheid van zorgplichten die de overheid draagt. Voor een goed begrip van de zorgplichten in de huidige wettelijke kaders ten aanzien van de informatiehuishouding van de overheid is het van belang om dergelijke historische ontwikkelingen in verband met de betekenis en inhoud van het begrip zorgplicht in het achterhoofd te houden.

Op dit moment bestaat een uitgebreide en flink groeiende verzameling van wetten en regels die verplichtingen bevatten voor het borgen van de juistheid, vindbaarheid, duurzame toegankelijkheid, veiligheid (of beveiliging) en privacy van informatie en voor het beheer (of de governance) daarvan. Een niet-uitputtend overzicht hiervan is vervat in bijlage 2.

De meest generieke verplichtingen zijn vervat in of komen voort uit nationale en internationale regelingen ter bescherming van fundamentele rechten of grondrechten. Denk hierbij aan het fundamentele recht op privacy, dat ook een zorgplicht omvat om de juistheid van persoonsgegevens te borgen.¹⁰⁴ Dergelijke verplichtingen gelden in beginsel voor de hele overheid en alle overheidsorganen over alle bestuurslagen.

De Woo bevat de plicht om er zoveel mogelijk voor te zorgen dat informatie die onder deze wet wordt verstrekt actueel, nauwkeurig en vergelijkbaar is.¹⁰⁵ De Woo bepaalt ook dat als een bestuursorgaan weet dat verstrekte informatie onjuist is, hiervan melding moet worden gedaan.¹⁰⁶ Volgens de Woo is een bestuursorgaan echter niet verantwoordelijk voor onjuistheid of onvolledigheid van door derden opgestelde informatie.¹⁰⁷ Informatiekwaliteit in het kader van de Woo omvat ook een verplichting tot het borgen van de vindbaarheid van informatie die onder de Woo openbaar moet worden gemaakt.

¹⁰⁰ HR 31 januari 1919, ECLI:NL:HR:1919:AG1776 (*Lindenbaum/Cohen*).

¹⁰¹ Zoals beschermd in o.a. art. 2 en art. 8 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

¹⁰² HR 20 december 2019, ECLI:HR:2019:2006 (*Klimaatzaak Urgenda*).

¹⁰³ Zie bijvoorbeeld <https://www.nederlandrechtsstaat.nl/urgenda-arrest-is-voorbeeld-van-nieuw-constitutionalisme/>.

¹⁰⁴ De AVG en de plicht voor het borgen van de juistheid van persoonsgegevens in art. 5 lid 1 sub d en het recht op rectificatie volgens art. 16 AVG gelden voor de hele overheid. Ook Verdrag 108 van de Raad van Europa bevat in art. 5 uitdrukkelijk de plicht om te zorgen dat persoonsgegevens juist zijn en om deze waar nodig te updaten.

¹⁰⁵ Zie art. 2.4 lid 2 Wet open overheid.

¹⁰⁶ Zie art. 2.4 lid 5 Wet open overheid.

¹⁰⁷ Zie art. 2.4 lid 4 Wet open overheid.

Uit het zorgvuldigheidsbeginsel in de Awb vloeit voort dat bestuursorganen besluiten nemen op basis van feiten waarvan de juistheid voldoende is vastgesteld.¹⁰⁸ Dat moet in beginsel meer worden gezien als een sterke inspanningsplicht dan een absolute resultaatsverplichting of garantie. Bij materiële onjuistheden kan een besluit wel worden vernietigd in bezwaar of beroep.

In dit verband is het belangrijk om bewust te zijn van een nuance of verschil waar het gaat om het borgen van de integriteit van informatie in de context van informatiebeveiliging, dat wil zeggen dat de informatie niet onbevoegd of per ongeluk is aangepast, tegenover de juistheid van informatie, wat gaat over de vraag of de informatie zelf überhaupt juist is of was. Voor het borgen van een goede informatiehuishouding en het vermijden van schade voor burgers door fouten of tekortkomingen daarin, is zowel het borgen van de juistheid van informatie van belang als ook de integriteit in de context van de beveiliging van informatie. Van belang is hier in elk geval dat wettelijke zorgplichten voor het beveiligen van informatie vooral gedeeltelijk betrekking hebben op de kwaliteit van de informatie in de zin dat de informatie beschermd moet worden tegen aantasting en onbevoegde aanpassing. Dergelijke plichten zijn beperkter dan het integraal borgen van de kwaliteit of juistheid van informatie.

Uit het voorgaande, en uit het overzicht in de bijlage, blijkt dat er niet één algemene zorgplicht geldt voor alle vormen van overheidsinformatie om de kwaliteit of juistheid daarvan in brede zin te borgen.¹⁰⁹ Daar komt bij dat de kaders en zorgplichten voor privacy, informatiebeveiliging en verantwoord gebruik van AI, die mede betrekking hebben op de kwaliteit of juistheid van informatie, deels kunnen overlappen, zoals in de beantwoording van de kernvraag onder deze pijler ook is aangegeven. Om concrete en heldere antwoorden te kunnen geven op praktische vragen over wat er met bepaalde informatie moet gebeuren en in welke systemen, is het nodig dat steeds de juiste balans wordt gevonden tussen zorgplichten die deels ook strijdig kunnen zijn. Een integraal, praktisch toepasbaar kader om die balans in ieder praktijkgeval optimaal te vinden, uit te voeren en waar passend vast te leggen ontbreekt op dit moment echter nog.

Een zorgplicht voor informatiekwaliteit impliceert het gebruik van informatiesystemen die passend zijn beveiligd tegen aantasting, verlies en onbevoegde inzage van informatie. Verder impliceert een zorgplicht voor informatiekwaliteit dat de gebruikte systemen geschikt zijn voor het verkeer van de informatieobjecten die binnen, tussen en met overheidsorganen die deze systemen gebruiken voor het verwerken van informatie. Dergelijke zorgplichten omvatten ook verplichtingen om persoonsgegevens en ICT-diensten passend te beveiligen. Wanneer een informatiesysteem onvoldoende beveiligd zou zijn of anderszins niet geschikt zou zijn, zou dit immers afbreuk doen aan de juistheid, vindbaarheid en duurzame toegankelijkheid van informatie.

¹⁰⁸ Zie art. 3:2 Algemene wet bestuursrecht.

¹⁰⁹ Ook in het voorstel voor de Algemene informatiewet overheid wordt dit niet geïntroduceerd. De zorgplicht in art. 7 Algemene informatiewet overheid houdt in dat overheidsorganen geschikte informatiesystemen gebruiken voor het verwerken en uitwisselen van informatie. Dit kan weliswaar wellicht impliceren dat een geschikt systeem ook de informatiekwaliteit in brede zin borgt, maar in de praktijk zal een 'geschikt systeem' moeten voldoen aan alle (gestapelde) zorgplichten die daar tegelijkertijd op van toepassing zijn.

In dit verband is ook van belang om op te merken dat niet alleen het borgen van de kwaliteit van de informatie zelf belangrijk is voor overheden om te vermijden dat burgers schade lijden door fouten in informatieverwerking, maar ook de kwaliteit van de informatiesystemen die beschikbaar worden gesteld aan burgers om informatie mee te verwerken. Vanzelfsprekend geldt dat des te meer waar een verplichting geldt voor burgers om een bepaald systeem (zoals een website of een app) te gebruiken en zij dus niet de vrijheid hebben om te kiezen voor een ander systeem dat beter werkt.

Hoe belangrijker en tijdkritischer de overheidsdienst waar de burger digitaal gebruik van wil maken, hoe belangrijker het is dat zowel de inhoudelijke digitale dienst zelf als de dienst voor betrouwbare identificatie en authenticatie (zoals DigiD) zeer betrouwbaar en gebruiksvriendelijk werkt. Van belang is daarbij ook dat steeds een deskundige helpdesk goed bereikbaar is om problemen te melden en hulp te ontvangen bij het oplossen daarvan.

Waar burgers zelf de verplichting of verantwoordelijkheid hebben om belangrijke informatie door te geven en daarbij bijvoorbeeld ook eisen worden gesteld aan de identificatie door de burger, kan ook een zorgplicht voor de overheid worden gezien om de goede werking te borgen van de informatiesystemen die daarvoor beschikbaar worden gesteld. Als een burger een verandering in persoonsgegevens niet kan doorgeven in het daarvoor beoogde systeem doordat het systeem waarin dat moet gebeuren daar niet de mogelijkheid toe biedt of de vereiste identificatiemethode niet werkt, kan dat schade veroorzaken voor de burger. Een zorgplicht voor de overheid houdt in dit verband in dat zij ervoor zorgt dat informatiesystemen en bijbehorende identificatiemethoden naar behoren functioneren. Daarmee wordt indirect ook de informatiekwiteit geborgd door te faciliteren dat burgers informatie eenvoudig zelf kunnen corrigeren waar dat passend is.

3.2.1. Juridische afdwingbaarheid

Formeel gezien zijn de hierboven bedoelde verplichtingen voor het borgen van informatiekwiteit juridisch afdwingbaar, bijvoorbeeld door burgers die naar de rechter kunnen stappen of een klacht kunnen indienen bij een bevoegde toezichthouder.¹¹⁰ Dergelijke toezichthouders hebben niet alleen de plicht om klachten in ontvangst te nemen en af te handelen maar vaak ook om zelf proactief toezicht uit te oefenen. Dat een toezichthouder als de AP boetes kan uitdelen, ook aan overheidsorganen, blijkt bijvoorbeeld uit de recordboetes die de AP heeft uitgedeeld aan de Belastingdienst van 3,7 en 2,75 miljoen euro.¹¹¹

Dergelijke boetes volgden echter pas na jarenlange overtredingen, terwijl meer proactief toezicht wellicht meer schade had kunnen voorkomen. Dat kost toezichtcapaciteit, terwijl de AP al jaren klaagt over een groot tekort aan budget. Bijvoorbeeld in 2024 gaf de AP nog aan dat het budget voor dat jaar (49 miljoen euro) niet genoeg zou zijn om zelfs aan de meest basale eisen te voldoen. Voor 2026 bedraagt het budget ongeveer 53,5 miljoen euro, terwijl de AP op basis van onafhankelijk onderzoek in 2023 had aangegeven dat een budget van minimaal

¹¹⁰ Denk bij toezichthouders aan de AP, de RDI, de Inspectie Gezondheidszorg en Jeugd, Inspectie Overheidsinformatie en Erfgoed en het College voor de Rechten van de Mens.

¹¹¹ Zie <https://autoriteitpersoonsgegevens.nl/actueel/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze> en <https://autoriteitpersoonsgegevens.nl/documenten/boete-belastingdienst-zwarte-lijst-fsv>.

100 miljoen euro nodig zou zijn om al haar taken goed uit te kunnen voeren.¹¹² Handhaving van de beveiligingsplichten onder de Cyberbeveiligingswet, die op 7 april 2026 is aangenomen in de Tweede Kamer, is grotendeels ondergebracht bij de RDI en voor specifieke sectoren bij andere toezichthouders, zoals de Inspectie Gezondheidszorg en Jeugd (IGJ) voor de zorg.

Uiteraard moeten de toezichthouders ook zelf hun informatiehuishouding goed op orde hebben en de kwaliteit en veiligheid borgen van de informatie die zij daarbij verwerken en de systemen waarmee zij dat doen. Recent maakte het NCSC nog bekend dat de AP en de Raad voor de rechtspraak slachtoffer zijn geworden van kwetsbaarheden in een oplossing voor het beheer en de beveiliging van mobiele apparaten.¹¹³ In 2025 waren de systemen van het Openbaar Ministerie voor langere tijd geheel offline vanwege een ernstige kwetsbaarheid in gebruikte systemen, waarbij wel is vastgesteld dat er inderdaad gebruik is gemaakt van de kwetsbaarheden in het systeem, maar voor zover bekend geen data (strafvorderlijk of anderszins) zijn gemanipuleerd of weggehaald.¹¹⁴

Dergelijke incidenten illustreren dat de kans dat een (beveiligings)incident of inbreuk zich voordoet in de praktijk nooit volledig weg te nemen is.¹¹⁵ Daarom richten veel nieuwe verplichtingen onder de Digital Decade in verband met informatiebeveiliging zich ook vooral op het vergroten van de weerbaarheid en het (operationele) vermogen om systemen, diensten en informatie snel te herstellen en de verdere nadelige gevolgen van incidenten te beperken.

De Woo wordt regelmatig gebruikt om de toegankelijkheid van overheidsinformatie af te dwingen. Ook wordt inmiddels via de Woo-Index op gestructureerde wijze inzage gegeven in de aantallen verzoeken die onder de Woo zijn gedaan en de afhandeling daarvan.¹¹⁶ Enerzijds kan het bestaan van een dergelijk overzicht worden beschouwd als een sterk staaltje informatiehuishouding, maar anderzijds blijkt uit het overzicht wel dat slechts 35% van de Woo-verzoeken op tijd zijn afgerond en de gemiddelde afhandeltijd maar liefst 147 dagen bedraagt.

3.2.2. Concluderend

Op basis van het voorgaande en bijlage 2 kan worden geconcludeerd dat de verplichtingen voor het borgen van informatiekwiteit op dit moment sectoraal te sterk verdeeld zijn.

Hoewel het aan de ene kant passend is dat sectorale wetgeving specifieke invulling geeft aan zorgplichten in relatie tot het betreffende domein, leidt een gebrek aan samenhang tussen dergelijke verplichtingen al snel tot overlap, tegenstrijdigheden

¹¹² Zie bijvoorbeeld de memo van de AP van 27 november 2023 genaamd 'Een toekomstbestendige Autoriteit Persoonsgegevens (AP)', bekend gemaakt op

<https://autoriteitpersoonsgegevens.nl/documenten/een-toekomstbestendige-ap>.

¹¹³ Zie <https://www.binnenlandsbestuur.nl/digitaal/datalek-bij-autoriteit-persoonsgegevens> en <https://www.ncsc.nl/alerts/ncsc-roept-organisaties-op-zich-te-melden-bij-gebruik-van-ivanti-endpoint-manager>.

¹¹⁴ Zie <https://www.om.nl/actueel/nieuws/2025/07/24/veelgestelde-vragen-inbreuk-op-ict>.

¹¹⁵ In veel gevallen waar daadwerkelijk sprake is geweest van een inbreuk is echter ook wel een oorzaak te vinden waar de beveiliging toch tekort heeft geschoten. De conclusie dat alles echt helemaal op orde was zoals het moest zijn maar er toch een inbreuk plaats kon vinden, is in de praktijk niet zo makkelijk te verdedigen.

¹¹⁶ Zie <https://wooincijfers.open-overheid.nl/woo-verzoek> en <https://www.overheid.nl/help/woo-index>.

en onduidelijkheden. In de uitgebreide verzameling van sectorale wet- en regelgeving zoals genoemd in de bijlage, is het ook niet eenvoudig om een heldere samenhang te vinden tussen (a) de wettelijke verplichtingen die bepalen wat een overheidsorganisatie of overheidsfunctionaris in concrete gevallen mag of moet doen met informatie en (b) de normen of toetsingskaders die bij audits worden gehanteerd om te verifiëren in hoeverre de betreffende overheidsorganisaties voldoen aan hun verplichtingen in verband met het verwerken van informatie.

Uit het voorgaande blijkt dat het concrete probleem voor burgers vooral zit in de feitelijke nakoming door de overheid van haar verplichtingen. Van belang is dat de nakoming van de geldende zorgplichten wordt verbeterd. Dat kan bijvoorbeeld door meer toezicht uit te voeren op de naleving en waar passend sterkere nalevingsprikkels (in de eerste plaats positief, waar mogelijk) te implementeren binnen overheidsorganisaties. Eventueel zou ook getest kunnen worden in hoeverre zorgvuldige inzet van AI de efficiëntie en snelheid kan verhogen, maar daarbij is het direct van groot belang om te borgen dat daarmee niet juist problemen ontstaan met de juistheid, privacy en beveiliging van (gevoelige) informatie.

3.3. Informatiebeveiliging, privacy en governance

In deze paragraaf en de bijbehorende subparagrafen staat de vraag “worden informatiebeveiliging, *privacy en governance juridisch afdwingbaar integraal meegenomen in het ontwerp en beheer van de informatiehuishouding?*” centraal.

Zorgplichten voor privacy by design en by default¹¹⁷ en voor information security by design en by default¹¹⁸ maken deel uit van de huidige wet- en regelgeving. Zoals in de vorige pijler besproken, zijn de verplichtingen juridisch afdwingbaar en zijn toezichthouders aangewezen.¹¹⁹

Over governance van informatiebeveiliging stelt de BIO 2 dat de bestuurder van de entiteit verantwoordelijk is voor het beheersen van informatiebeveiligingsrisico's. Het is aan de entiteit om deze structuur aan te brengen volgens NEN-EN-ISO/IEC 27001. Dat wil zeggen dat er een information security management system (ISMS) moet worden ingericht. Verder bepaalt het Cyberbeveiligingsbesluit dat diverse beleidsstukken moeten worden opgesteld en geïmplementeerd over een aantal specifieke onderwerpen (in lijn met ISO 27001). De bestuurder laat zich adviseren door functionarissen als de Chief Information Security Officer (CISO), Chief Information Officer (CIO) en functionaris gegevensbescherming (FG). De samenhang van wet- en regelgeving ter implementatie van de NIS2-richtlijn is vrij complex. In het volgende schema is deze weergegeven.

¹¹⁷ Zie art. 25 Algemene verordening gegevensbescherming.

¹¹⁸ Zie paragraaf 14 van de BIO 2 en overheidsmaatregelnummer 8.27.01.

¹¹⁹ Voor de Cyberbeveiligingswet zal het toezicht pas effectief worden als de wet definitief is aangenomen. Op moment van schrijven is de wet al wel aangenomen door de Tweede Kamer maar nog niet door de Eerste Kamer.



Afbeelding 4: Hiërarchie Cyberbeveiligingsregelgeving.

Voor beheer van privacyrisico's is sterk aan te raden, maar niet met zoveel woorden verplicht om ook een managementsysteem in te richten. Wel verplicht is om naleving van de AVG, waaronder de beveiligingsplicht, aan te kunnen tonen. Om aan die verplichting te voldoen is het implementeren van een managementsysteem in de praktijk noodzakelijk. Certificering van overheden voor het aantonen van naleving van privacygerelateerde verplichtingen is echter nog altijd niet voorzien onder het mechanisme dat de AVG daarvoor biedt.¹²⁰ Voor specifieke soorten overheidsorganisaties, zoals onderwijs- en onderzoeksinstituten, zijn wel toetsingskaders en volwassenheidsmodellen ontwikkeld, zoals het SURF Toetsingskader Privacy en het SURF Toetsingskader Informatiebeveiliging.¹²¹

Zowel de AVG als de Cyberbeveiligingswet bevatten verplichtingen om in beveiliging te voorzien die passend is voor de risico's. Er bestaan wel enkele subtiele verschillen tussen de AVG en de Cbw in de formulering van de beveiligingsplicht. Waar de AVG bijvoorbeeld spreekt van 'passende technische en organisatorische maatregelen', voegt de Cbw het woord 'operationele' daaraan toe. Daarmee zal vermoedelijk bedoeld worden dat de maatregelen in verband met het borgen van weerbaarheid en het veerkrachtig optreden bij inbreuken in het algemeen operationeel van aard zijn.

Een probleem voor het integraal meenemen van privacy en informatiebeveiliging bij het ontwerp van de informatiehuishouding is dat wetten en regels aan de ene kant een 'risicogebaseerde' benadering voorschrijven, maar aan de andere kant specifieke bepalingen bevatten die juist afbreuk kunnen doen aan de mogelijkheid om risico's optimaal in samenhang of integraal in te schatten en te beperken. De grote hoeveelheid (zorg)plichten die tegelijkertijd op dezelfde gegevens en (ICT- en AI-)systemen van toepassing kunnen zijn, maakt het toepassen van de

¹²⁰ Zie art. 42 Algemene verordening gegevensbescherming.

¹²¹ Zie <https://pec.surf.nl/toetsingskader-privacy/> en <https://sec.surf.nl/surfaudit-toetsingskader-informatiebeveiliging/>.

huidige kaders om concrete antwoorden te geven op concrete vragen als hierboven omschreven, complex en tijdrovend.

Zowel de wetgeving voor privacy¹²² als die voor informatiebeveiliging¹²³ als die specifiek betrekking heeft op ontwikkeling en gebruik van AI-systemen¹²⁴ bevatten specifieke categorieën gegevens, verwerkingen en (ICT- of AI-)systemen die in de regels zelf als 'hoog risico' of 'bijzonder' of 'belangrijk' worden aangemerkt. Hoewel dat aan de ene kant als behulpzaam kan worden gezien voor het specifiek toepassen van de betreffende wetgeving, kan een gebrek aan samenhang het *integraal* toepassen van deze kaders juist moeilijker maken. Bovendien kan al snel de vraag ontstaan of de specifieke wettelijke classificaties niet (te) arbitrair zijn en juist eerder in de weg staan aan het uitvoeren van zinnige, *integrale* risicobeheersing. Ook kunnen technische ontwikkelingen ervoor zorgen dat specifieke wettelijke verplichtingen die in de context van het gebruik van bepaalde specifieke technieken zijn opgeschreven, snel verouderd kunnen raken, terwijl de staatsrechtelijke processen om wetgeving aan te passen of zelfs in te trekken te tijdrovend en arbeidsintensief kunnen zijn om tijdig in de benodigde aanpassingen te voorzien.¹²⁵

Bijvoorbeeld het feit dat gegevens over gezondheid wel als 'bijzonder' zijn aangemerkt in de AVG¹²⁶ maar financiële gegevens niet, kan ertoe leiden dat mensen die de wet moeten toepassen zich genoodzaakt voelen om te concluderen dat het gegeven of iemand lenzen draagt of op enig moment griep heeft, gevoeliger zou zijn en meer beschermd moet worden dan iemands salaris, vermogen of juist schulden. Dit terwijl betoogd kan worden dat een meer algemene of integrale risico-inschatting waarschijnlijk tot een ander resultaat of tot een andere conclusie zou (moeten) leiden. Ook kan het wat omslachtig worden genoemd dat de AVG eerst voorschrijft om vast te stellen of verwerkingen van persoonsgegevens 'waarschijnlijk een hoog risico'¹²⁷ opleveren voor betrokkenen en pas als dat is vastgesteld de verplichting geldt om een data protection impact assessment (DPIA) uit te voeren. Dit terwijl de AVG in het algemeen ook al vereist om aantoonbaar te maken dat verwerking van persoonsgegevens aan de AVG voldoet. Logischer kan het zijn om risicobeheer voor te schrijven waarbij risico's van verwerkingen voor betrokkenen integraal worden ingeschat op basis van het geheel van diverse (indicatieve) factoren en als het risiconiveau een acceptabel niveau zou overschrijden, maatregelen vast te stellen waarmee het risico tot een acceptabel niveau kan worden beperkt.

De Cyberweerbaarheidsverordening geeft op haar beurt een zeer brede definitie van 'producten met digitale elementen', maar sluit op moeilijk navolgbare wijze

¹²² Zoals de Algemene verordening gegevensbescherming en Uitvoeringswet algemene verordening gegevensbescherming.

¹²³ Zoals de NIS2-richtlijn, de voorgestelde Cyberbeveiligingswet, Cyberweerbaarheidsverordening, Cyberbeveiligingsverordening.

¹²⁴ Zoals de AI-verordening.

¹²⁵ Dit is ook te zien in de 'Omnibus'-pakketten van Europese regels die op vereenvoudiging gericht zijn maar die vooral diverse details veranderen in plaats van een eenvoudig kader voor integraal risicobeheer te verschaffen.

¹²⁶ Zie art. 9 Algemene verordening gegevensbescherming.

¹²⁷ Dit kan als dubbelop worden beschouwd omdat risico normaliter wordt beschouwd als kans maal impact en waarschijnlijk ook ziet op kans.

clouddiensten uit onder verwijzing naar de NIS2-richtlijn.¹²⁸ Dit terwijl het toepassingsgebied van die richtlijn weer is vervat in een omvangrijk schema van categorieën *entiteiten* op basis van hun aard, grootte en soorten activiteiten en de NIS2-richtlijn (of de nationale implementatiewetgeving) juist niet in het algemeen, specifiek of per definitie toepasselijk is op clouddienstverlening. Daar komt bij dat de term en definitie van 'product met digitale elementen' lezers al snel op het verkeerde been kan zetten, omdat ook zuiver digitale producten, zoals software, er uitdrukkelijk onder vallen. Verder bestempelt de Cyberweerbaarheidsverordening een aantal producten met digitale elementen als 'belangrijk' (in een bijlage) en stelt daar specifieke eisen voor vast in verband met informatiebeveiliging. Op basis van het complexe geheel is het nog niet zo eenvoudig om concreet, snel en met zekerheid vast te stellen of bijvoorbeeld DigiD ook kwalificeert als een dergelijk product en welke verplichtingen dan specifiek gelden voor de overheidsorganisatie die DigiD aanbiedt (Logius, dat onder het ministerie van BZK valt) en voor overheidsorganisaties die DigiD gebruiken.¹²⁹

Verder stellen de Wet weerbaarheid kritieke entiteiten (Wwke) en het bijbehorende Besluit weerbaarheid kritieke entiteiten eisen aan entiteiten die onder de wet als kritiek zijn aangewezen.¹³⁰ Daarnaast stellen de Cyberbeveiligingswet en het bijbehorende Cyberbeveiligingsbesluit eisen aan essentiële en belangrijke entiteiten die onder de betreffende definities van die wet vallen. Het is mogelijk dat overheidsorganisaties onder beide sets wetten en besluiten vallen. Het goed regelen van de mogelijke samenloop tussen Cbw en Wwke en het vermijden van dubbeling van toezicht, registratieplichten en meldplichten vormt nog een punt van aandacht.¹³¹

Het ministerie van BZK valt zelf in elk geval onder het toepassingsgebied van de Cbw en voor Logius als onderdeel van het ministerie zal dat logischerwijs ook het geval zijn. Vooralsnog lijkt het erop dat het aanbieden van DigiD door (Logius als onderdeel van) het ministerie van BZK zowel onder de Cbw zal vallen als onder de Cyberweerbaarheidsverordening, en onder de specifieke regels die op nationaal niveau al zijn vastgesteld in verband met het gebruik van DigiD, zoals de Wdo. En daarbij is voor DigiD ook de eIDAS-verordening specifiek van belang.

Nog complexer wordt het wanneer ICT-producten of -diensten die door de overheid worden gebruikt of aangeboden AI-functionaliteiten of AI-elementen bevatten of

¹²⁸ Zie overweging 12 Cyberweerbaarheidsverordening. Dit laat zien dat een onduidelijke samenhang, of zelfs schijnbare tegenstrijdigheid, tussen overwegingen bij EU-verordeningen en de inhoud van de verordening zelf ook nog wel eens kan opspelen. De algemene stelregel is dan dat de tekst van de verordening zelf voorgaat op de overwegingen.

¹²⁹ DigiD lijkt vrij duidelijk te voldoen aan de brede definitie van 'product met digitale elementen' en geen van de uitzonderingen in art. 2 lijkt direct van toepassing. Eventueel zou lid 5 toegepast kunnen worden, voor zover specifieke voorschriften voor DigiD zouden voorzien in een hoger beschermingsniveau dan de Cyberweerbaarheidsverordening. Om tot een concrete conclusie te komen over de toepasselijkheid van deze verordening op DigiD moet dan wel eerst een vergelijking worden gemaakt tussen het beschermingsniveau dat (a) de Cyberweerbaarheidsverordening voorschrijft (voor zover van toepassing) en (b) de nationale voorschriften, in dit geval vermoedelijk vooral het Normenkader (3.0) voor ICT-beveiligingsassessments DigiD.

¹³⁰ Zie <https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/organisaties-aangewezen-onder-de-wwke>.

¹³¹ Zie bijvoorbeeld het wetgevingsoverleg van 23 maart 2026 en de bijbehorende moties die zijn gepubliceerd op <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?qry=wetsvoorstel%3A36764&cf=wetsvoorsteldetails>.

toepassen waardoor sprake is of zou kunnen zijn van een AI-systeem als bedoeld in de AI-verordening. Juist voor de beveiliging van ICT-systemen wordt in toenemende mate gebruikgemaakt van AI-oplossingen die risicoprofielen definiëren en afwijkingen ten opzichte van bepaalde als 'normaal' beschouwde (gebruiks- of verwerkings)patronen signaleren op basis van dergelijke risicoprofielen. Bijvoorbeeld *intrusion prevention and detection systems*, *firewalls*, *endpoint protection systems* en andere cybersecurity-producten en -diensten maken in toenemende mate gebruik van AI. Om DigiD weer als voorbeeld te nemen, ligt het voor de hand dat AI-systemen niet alleen een belangrijke rol spelen bij de beveiliging van de infrastructuur waar DigiD op draait, maar in toenemende mate ook deel uitmaken of zullen uitmaken van de maatregelen in DigiD zelf om misbruik tegen te gaan. Om vast te stellen in hoeverre de AI-verordening van toepassing is op DigiD of de beveiliging van de infrastructuur waar dit op draait en om vast te stellen welke concrete verplichtingen er op basis daarvan gelden, naast of in aanvulling op alle andere verplichtingen onder andere wet- en regelgeving, zal een complexe analyse moeten worden uitgevoerd. Hierbij moeten de specifieke stappen van de AI-verordening worden gevolgd. Daarmee kan vastgesteld worden of er sprake is van een 'hoog risico' zoals specifiek in de AI-verordening is vastgelegd.¹³² In het geval van DigiD kan worden afgevraagd in hoeverre er sprake is van een veiligheidscomponent bij het beheer of de exploitatie van kritieke digitale infrastructuur¹³³ en of biometrische authenticatie via de DigiD-app op een smartphone ook onder de AI-verordening is gereguleerd of daar juist (specifiek) van is uitgesloten.¹³⁴ In verband met het borgen van de duurzame beschikbaarheid van DigiD vindt ook veel discussie plaats over soevereiniteit en de mogelijkheden om het risico op buitenlandse invloeden die verstoring kunnen werken, terug te dringen. Het nieuwe Cyberbeveiligingsbesluit kan een rol spelen bij het borgen van soevereiniteit door de minister van Justitie en Veiligheid de mogelijkheid te geven dat bepaalde producten en diensten van leveranciers kunnen worden geweigerd als daar zwaarwegende redenen voor zijn.

Een algemene wettelijke zorgplicht om integraal risicobeheer toe te passen voor zowel privacy als informatiebeveiliging als AI kan in dit verband als wenselijk worden beschouwd. De staats- en bestuursrechtelijke complexiteit in Europees en nationaal verband maakt dat wel een moeilijke opgave. Een Nederlandse wet in formele zin, zoals de nieuw voorgestelde Aiw, kan immers niets veranderen aan verordeningen die op EU-niveau zijn vastgesteld, behalve voor zover de verordening daar uitdrukkelijk ruimte toe heeft gelaten. Ook de achtergrond dat wettelijke verplichtingen en toetsingskaders voor (a) bescherming van persoonsgegevens, (b) informatiebeveiliging in brede zin en (c) verantwoord gebruik van AI en algoritmen tot stand lijken te zijn gekomen en worden toegepast vanuit verschillende opleidingsachtergronden en expertises, maakt het moeilijk om praktisch te borgen dat informatiebeveiliging, privacy en (AI-)governance juridisch afdwingbaar *integraal* worden verwerkt in het ontwerp en beheer van de informatiehuishouding en de (ICT- en AI-)systemen waarin (persoons)gegevens worden verwerkt. Het is aan te raden om managementsystemen voor risicobeheer en bijbehorende beleidsstukken en procedures, zoals leveranciersbeheer, zoveel

¹³² Zie art. 6 AI-verordening.

¹³³ Zie Bijlage III lid 2 AI-verordening.

¹³⁴ Op basis van Annex III lid 1 sub a lijkt een authenticatiedienst als DigiD zelf in elk geval niet als 'hoog risico AI-systeem' te kwalificeren, ook of zelfs al wordt AI ingezet voor biometrische verificatie.

mogelijk te integreren. Nauwe samenwerking tussen CISO, Chief Privacy Officer (CPO), CIO en AI-compliance officer(s) is daarvoor wenselijk.

3.3.1. UAVG

De Aiw beoogt de UAVG te wijzigen.¹³⁵ Deze wijziging creëert een juridische opening om persoonsgegevens in lijn met de AVG en UAVG te delen tussen verwerkingsverantwoordelijken. Wanneer persoonsgegevens worden verwerkt op basis van artikel 6 lid 1 onder e AVG, stelt de Aiw dat het delen van deze persoonsgegevens per definitie verenigbaar is met het doel waar de persoonsgegevens in eerste instantie voor zijn verkregen als er sprake is van 'het verlenen van passende ondersteuning aan de betrokkene'¹³⁶ en de verwerking van persoonsgegevens daarbij noodzakelijk is¹³⁷. Hiermee expliciteert de Aiw het vraagstuk van doelbinding.¹³⁸ De vraag is echter in hoeverre deze explicitering noodzakelijk is of een (wezenlijke) verandering aanbrengt in het geldend recht. Overweging 45 van de AVG stelt immers al dat niet iedere overheidsverwerking expliciet in de wet vastgelegd hoeft te worden:

"Indien de verwerking wordt verricht omdat de verwerkingsverantwoordelijke hiertoe wettelijk is verplicht of indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag, dient de verwerking een grondslag te hebben in het Unierecht of het lidstatelijke recht. Deze verordening schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen op grond van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust, of voor verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag."

De Aiw¹³⁹ lijkt juist wél een specifieke basis te creëren. Een specifieke basis die gelet op de AVG mogelijk niet noodzakelijk is. Juist ook omdat de Aiw spreekt over 'passende ondersteuning van de betrokkene' kan onder de huidige AVG en UAVG in beginsel ook al worden gesteld dat een dergelijk doel al valt onder de wettelijke taak van het overheidsorgaan. Met andere woorden: als een overheidsorgaan al tot taak heeft om persoonsgegevens van een burger te verwerken, bijvoorbeeld een gemeente die aanvragen voor rijbewijzen afhandelt, dan mag in beginsel worden aangenomen dat het bieden van een 'passende ondersteuning van de betrokkene' daar al een doelstelling bij vormt of in elk geval niet strijdig is met het primaire doel.

Een punt van zorg in dit verband kan wel zijn dat het gaat om gegevensdeling tussen verschillende overheidsorganen en er verschil van inzicht kan bestaan over welke overheidsorganen welke persoonsgegevens nodig hebben om te kunnen voorzien in 'passende ondersteuning van de betrokkene'. Het zonder toestemming delen van zeer gevoelige gegevens over de gezondheid van burgers waarbij de overheidsorganisaties zelf een 'passende ondersteuning' vaststellen die de

¹³⁵ Zie art. 17 Algemene informatiewet overheid.

¹³⁶ Zie art. 17 lid 1 Algemene informatiewet overheid.

¹³⁷ Zie art. 17 lid 2 Algemene informatiewet overheid.

¹³⁸ Zoals vastgelegd in art. 6 lid 3 en lid 4 Algemene verordening gegevensbescherming.

¹³⁹ Zie art. 17 Algemene informatiewet overheid.

belangen van de betrokkene juist zou kunnen schaden, zal in principe juist niet goed verenigbaar zijn met de AVG en fundamentele rechten ter bescherming van privacy en persoonsgegevens. Of anders gezegd: doorgifte van persoonsgegevens door de ene overheidsorganisatie naar de andere moet wel daadwerkelijk tot doel hebben om de betrokkene te ondersteunen en daar ook noodzakelijk voor zijn. Van groot belang om te vermijden is dat gevoelige persoonsgegevens worden uitgewisseld tussen verschillende overheidsorganisaties onder het mom of zelfs voorwendsel van het bieden van een passende ondersteuning, terwijl in werkelijkheid niet de belangen van de betrokkene centraal staan maar andere belangen.

Bij het voorzien van wijzigingen in de UAVG is van belang dat niet wordt getreden buiten de ruimte die de AVG zelf laat voor lidstaten om de AVG nader in te vullen. De AVG is immers een verordening, en geen richtlijn, en streeft als zodanig in beginsel volledige harmonisatie na, met uitzondering van specifieke aspecten waar de AVG uitdrukkelijk ruimte laat aan lidstaten voor nadere invulling of afwijking.

3.3.2. Namen, termen en definities die de lading dekken

De complexiteit en moeizame of zelfs gebrekkige samenhang van Europese en Nederlandse informatiewetten begint overigens bij de naamgeving. De naam 'Algemene verordening gegevensbescherming' leidt leken al snel op het verkeerde been: de verordening heeft uitsluitend betrekking op bescherming van persoonsgegevens, niet op gegevens in het algemeen.¹⁴⁰ De naam van de oude richtlijn bescherming persoonsgegevens en bijbehorende Wet bescherming persoonsgegevens dekte de lading wat dit betreft beter en hoefde niet tot nodeloze verwarring te leiden van niet-ingewijden. Verwarrend is bijvoorbeeld ook dat de voorgestelde Cyberbeveiligingswet géén uitvoeringswet vormt bij de Cyberbeveiligingsverordening, zoals op basis van de naamgeving logisch zou lijken, maar de implementatiewet van de NIS2-richtlijn. Daarnaast is er ook nog een Uitvoeringswet Cyberbeveiligingsverordening. De huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) volgt qua naamgeving wel de EU-richtlijn waar deze op is gebaseerd. In plaats van een integraal, eenduidig toepassingsgebied te definiëren, zoals netwerk- en informatiesystemen of aanbieders van digitale diensten die gebruikmaken van netwerk- en informatiesystemen, bevatten de NIS2-richtlijn en (concept) Cbw een complex stelsel van categorieën entiteiten die eronder vallen of juist specifiek zijn uitgezonderd van het toepassingsbereik. Deze complexiteit maakt het tijdrovend en kostbaar om vast te stellen welke organisaties nu precies onder welke verplichtingen en bijbehorend toezicht vallen.

Het is wenselijk dat namen en toepassingsgebieden van wet- en regelgeving goed worden doordacht en dat titels zorgvuldig worden gekozen, zodat zij de inhoud zo nauwkeurig mogelijk weergeven en de kans op verwarring minimaliseren. Door het verminderen van onnodige cognitieve belasting kan ook de snelheid en efficiëntie van de toepassing worden vergroot.

3.3.3. Terug naar de kern

¹⁴⁰ Ook al zal de term 'gegevensbescherming' of 'data protection' ingewijden direct een associatie geven met 'privacy' omdat die woorden heel vaak samen worden gebruikt, kan dat zuiver taalkundig al snel verwarrend zijn voor niet-ingewijden. Dit maakt het moeilijker voor juristen om de inhoud en bedoeling van wettelijke verplichtingen uit te leggen aan de personen die de verplichtingen feitelijk moeten (helpen) uitvoeren of implementeren.

Een gevaar in verband met het daadwerkelijk in de praktijk brengen van zorgplichten en het realiseren van een mensgerichte, duurzame en inclusieve digitale transformatie, is dat de wet- en regelgeving die deel uitmaakt van de informatiehuishouding dermate complex wordt dat het door de bomen moeilijk wordt om het bos te zien. In de praktijk kan dit zorgen voor een handelingsterughoudendheid als het gaat om het delen van gegevens. Het feit dat onduidelijk is wat wel of niet mag, kan ervoor zorgen dat ambtenaren hun handen er liever vanaf trekken. In dit verband is het belangrijk om te blijven beseffen dat de fundamentele rechten als geborgd in het EVRM en het EU-Handvest in hiërarchie boven alle lagere wet- en regelgeving staan.

Dit kan helpen bij het integraal toepassen van risicobeheer dat in lijn is met de hoogste doelen voor de overheid, waarbij als meest fundamentele kern kan worden beschouwd het borgen van het duurzaam welzijn van de democratie en van de burgers die daar deel van uitmaken. Waar technologische en maatschappelijke omstandigheden snel veranderen, bijvoorbeeld ten gevolge van de opkomst van AI, is het ook van belang dat de wettelijke kaders flexibel genoeg blijven om mee te bewegen maar juist rotsvast zijn in het bewaren en beschermen van de kern. In dit opzicht is het van fundamenteel belang dat digitalisering en AI in lijn blijven met democratische kernbeginselen uit grondwetten en mensenrechtenverdragen en dat het realiseren van de verklaring van digitale rechten scherp gemonitord blijft.¹⁴¹ Wenselijk in verband met de samenwerkingscyclus met de EU is om te voorzien in duidelijke, constructieve feedback om te zorgen dat EU-wetgevingsinstrumenten eenvoudiger worden om toe te passen voor integraal risicobeheer en voor het optimaal tot uitdrukking brengen van zorgplichten naar burgers.

3.3.4. Concluderend

Hoewel er specifieke juridisch afdwingbare verplichtingen zijn voor informatiebeveiliging, privacy en governance, faciliteren deze nog te weinig dat zij integraal aan de basis worden gezet voor het ontwerp en beheer van de informatiehuishouding. Wenselijk is om handvatten te ontwikkelen waarmee integraal risicobeheer beter kan worden ingebed in managementsystemen, beleid en procedures om optimaal invulling te geven aan zorgplichten.

3.4. Monitoring en kwaliteit

In deze paragraaf wordt de volgende deelvraag van Pijler 3 behandeld: *bestaan er juridische verplichtingen voor periodieke kwaliteitsmetingen, audits en het definiëren en vaststellen van volwassenheidsniveaus?*

Naast de mogelijkheden van audits door toezichthouders zoals de AP en de RDI, zijn er in beperkte mate verplichtingen tot het uitvoeren van periodieke kwaliteitsmetingen, audits en het definiëren en vaststellen van volwassenheidsniveaus.

De AVG verplicht tot het uitvoeren van risicobeoordelingen om vast te stellen of er sprake is van een hoog risico¹⁴² en om DPIA's uit te voeren waar dat het geval is

¹⁴¹ Zie <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-declaration-digital-rights-and-principles-monitoring-report-2025>.

¹⁴² Dergelijke beoordelingen worden ook wel pré-DPIA of DPIA-voortoets genoemd. Daarvoor heeft de Autoriteit Persoonsgegevens een lijst gepubliceerd op <https://wetten.overheid.nl/BWBR0042812/2019-11-27>.

en het risico te reduceren tot een aanvaardbaar niveau. Daarbij moet worden voorzien in toezicht door de FG op de uitvoering van de maatregelen.¹⁴³ In verband met leveranciers die persoonsgegevens verwerken verplicht de AVG om in een (verwerkers)overeenkomst mogelijkheden op te nemen voor het uitvoeren van audits en verplichtingen voor de verwerker om daaraan mee te werken. De AVG bevat echter geen verplichting tot het uitvoeren van dergelijke audits.

De BIO 2 bevat diverse verplichtingen tot het uitvoeren van risicobeheer, monitoring en continue verbetering en voor incidentprocedures waarbij geëvalueerd wordt of er passende maatregelen kunnen worden getroffen om de kans op soortgelijke incidenten in de toekomst te verkleinen. Monitoring maakt als vaste component deel uit van het ISMS dat de BIO 2 vereist en dat in overeenstemming met ISO 27001 moet worden ingericht. Op rijksniveau is de Auditdienst Rijk ingesteld, die diverse audits uitvoert in verband met privacy¹⁴⁴ en daarnaast ook IT-audits zoals DigiD-assessments en cybersecuritychecks, zoals red teaming en pentesten. Ook gaat deze dienst na of rijksonderdelen AI verantwoord inzetten.¹⁴⁵

Het definiëren en bepalen van volwassenheidsniveaus is een veelgebruikte manier om te toetsen in welke mate de organisatie structureel en duurzaam in staat is om aan die verplichtingen te voldoen. Het Centrum voor Informatiebeveiliging en Privacybescherming heeft in 2025 een Privacy Volwassenheidsmodel geïmplementeerd in een Privacy Self-Assessment¹⁴⁶, waarmee een organisatie op basis van een vragenlijst het volwassenheidsniveau kan bepalen op een schaal van 1 tot en met 5. Voor informatiebeveiliging binnen de overheid is er de BIO 2 Self-Assessment.¹⁴⁷ Voor onderwijs- en onderzoeksinstituten heeft SURF het Toetsingskader Privacy en het Toetsingskader Informatiebeveiliging geïntroduceerd, waarbij ook een volwassenheidsniveau wordt bepaald met een score van 1 tot en met 5.

3.4.1. Concluderend

Naast formeel toezicht door toezichthouders zoals de AP en de RDI en de verplichtingen voor risicobeheer die periodieke monitoring en evaluatie impliceren, onder andere op basis van inbreuken op de beveiliging en in verband met persoonsgegevens, zijn er weinig juridische verplichtingen tot het uitvoeren van kwaliteitsmetingen en het definiëren en toetsen van volwassenheidsniveaus. Het zorgvuldig inrichten van risicobeheer door managementsystemen met passend beleid en procedures voor informatiebeveiliging, privacybescherming en verantwoord gebruik van AI impliceert wel dat er periodieke interne en eventueel ook externe audits worden gehouden. Ook volwassenheidsmodellen zijn nuttige hulpmiddelen, maar in het algemeen niet juridisch verplicht.

4. Pijler 4: Maatschappelijke functionaliteit

De huidige inrichting van de overheid ondersteunt de transformatie naar een proactieve en responsieve overheid onvoldoende. Om dit te realiseren moet het streven zijn om de informatiehuishouding fundamenteel in te richten ten dienste

¹⁴³ Zie art. 39 lid 1 sub c Algemene verordening gegevensbescherming.

¹⁴⁴ Zie bijvoorbeeld de audit ten aanzien van de naleving van de Wpg door de Nederlandse Arbeidsinspectie.

¹⁴⁵ Zie <https://www.auditdienstrijk.nl/onze-vakgebieden/it-audit>.

¹⁴⁶ Zie <https://www.cip-overheid.nl/producten-en-diensten/privacyselfassessmenttool>.

¹⁴⁷ Zie <https://www.bio-overheid.nl/category/producten/bio-sa>.

van de burger en maatschappelijke opgaven, gericht op passende ondersteuning en het versterken van participatie.

Deze pijler gaat over de bijdrage van de informatiehuishouding aan burgerrechten in een democratische rechtsstaat, proactieve dienstverlening, transparantie en een responsieve overheid. Met de Aiw wordt beoogd de informatiehuishouding te richten op maatschappelijk functioneren, niet alleen op interne processen.

Om te onderzoeken in hoeverre er passende juridische waarborgen zijn die bijdragen aan deze vierde pijler, wordt de volgende kernvraag in het onderzoeksrapport behandeld:

In welke mate ondersteunen bestaande juridische kaders de informatieverhouding overheid-burger en dragen zij bij aan transparante, proactieve en toegankelijke publieke dienstverlening?

Om deze kernvraag adequaat te kunnen behandelen, komen in het onderzoeksrapport de volgende criteria aan bod:

- Burgerrechten in de informatiesamenleving: worden rechten op toegang, correctie, inzicht, navolgbaarheid en openbaarheid juridisch afdoende geborgd?
- Proactieve en passende dienstverlening: ondersteunen bestaande juridische kaders de mogelijkheid tot proactieve dienstverlening en bieden zij voldoende houvast om de grenzen van deze zorgplicht te markeren?
- Transparantie over informatiegebruik en besluitvorming: zijn juridische eisen voor uitlegbaarheid, verantwoording, logging en algoritmische transparantie aanwezig en toepasbaar?

4.1. Antwoord op de kernvraag

Centraal in deze pijler staan de bestaande juridische kaders die de informatieverhouding tussen de overheid en de burger ondersteunen en bijdragen aan transparante, proactieve en toegankelijke publieke dienstverlening. De kernvraag is in welke mate deze kaders aanwezig zijn en enige bijdrage leveren. Om die kernvraag te beantwoorden, is er gekeken naar wettelijke kaders over transparantie, proactiviteit en toegankelijkheid van de publieke dienstverlening.

"De overheid betracht bij de uitvoering van haar taak openbaarheid volgens regels bij de wet te stellen", zo stelt de Grondwet.¹⁴⁸ Er zijn vervolgens tal van wetten die deze openbaarheid in meer of mindere mate verder reguleren. De Woo reguleert de proactieve en reactieve openbaarmaking van documenten, de Awb verplicht overheidsinstanties om besluiten te motiveren en de Archiefwet reguleert toegankelijkheid van informatieobjecten over een langere periode. Deze kaders hangen alle met elkaar samen. De informatieverhouding tussen de overheid en de burger wordt enerzijds gereguleerd door de burger rechten toe te kennen, daarover later meer, en anderzijds door de overheid verplichtingen op te leggen. Waar de verplichtingen zien op openbaarmaking, transparantie en in mindere mate proactiviteit, is het zaak voor de overheid om haar informatiehuishouding daarop in te richten. Waar dat binnen de huidige wettelijke kaders niet altijd expliciet is gemaakt, volgt het wel impliciet uit de verschillende verplichtingen die de Woo, Awb en Archiefwet met zich meebrengen. Maar ook meer privacygerelateerde

¹⁴⁸ Zie art. 110 Grondwet.

wetgeving zoals de AVG of de Wpg stimuleert en verplicht transparantie en biedt burgers daartoe rechten.

Proactiviteit in de publieke dienstverlening daarentegen is een ander verhaal. Dat is minder stevig verankerd in juridische kaders. Er zijn momenteel verschillende wetsvoorstellen in de maak die hier op specifieke domeinen verandering in pogen te brengen. Daaruit is op te maken dat de huidige juridische kaders onvoldoende worden geacht. Deels omdat de kaders te algemeen zijn, deels omdat zij in het privacydomein als te beperkend worden ervaren. Deze wetsvoorstellen laten zien dat proactiviteit via wetgeving sectorspecifiek wordt aangepakt. Hoewel dat voor een sector een passende oplossing kan zijn, bestaat hiermee tegelijkertijd het risico op een lappendeken aan sectorspecifieke wetgeving om een proactieve dienstverlening te reguleren. Wetgeving die overheidsbreed inzet op deze vorm van dienstverlening is wellicht een duurzamere oplossing.

Dezelfde privacywetgeving die burgers rechten, en overheden verplichtingen, geeft, is bij het niet juist scheppen van wettelijke kaders een blokkerende factor voor proactievare dienstverlening. Taken en daarbij horende gegevensverwerkingen zonder wettelijke grondslag zijn strijdig met de AVG. Door bovengenoemde sectorspecifieke wetgevingsvoorstellen wordt deze blokkerende factor weggenomen. Een sectoroverstijgende juridische basis moet tevens tegen de meetlat van de AVG en de Wpg gelegd worden om te beoordelen in hoeverre het grondrecht op privacy voor burgers wordt gerespecteerd.

Kort gezegd bevatten bestaande juridische kaders een fundament, maar dient dit fundament nog verder en consistentier uitgebouwd te worden om een volwaardige transparante, proactieve en toegankelijke publieke dienstverlening voor burgers te kunnen realiseren. Via de deelvragen hieronder wordt nader ingegaan op de kernvraag.

4.2. Burgerrechten

4.2.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“worden rechten op toegang, correctie, inzicht, navolgbaarheid en openbaarheid juridisch afdoende geborgd?”* centraal.

Toegankelijke publieke dienstverlening is uitsluitend mogelijk als er transparantie bestaat over dezelfde publieke dienstverlening. Hoe en wanneer men toegang kan krijgen tot welke informatie is kenmerkend voor toegankelijkheid. Transparantie wordt als actieve verplichting in wet- en regelgeving neergelegd, maar ook als reactieve verplichting. Bij een actieve verplichting dient een verantwoordelijke partij proactief, op voorhand, informatie te verstrekken. Reactieve verplichtingen dienen op verzoek nagekomen te worden en zijn bijvoorbeeld verplichtingen om burgers recht op toegang of inzage in gegevens te geven. Deze verplichtingen worden hieronder beknopt behandeld. De actieve verplichtingen worden nader in paragraaf 4.3 behandeld.

Zodra informatie is te definiëren als een persoonsgegeven¹⁴⁹ en onder de reikwijdte van de AVG valt, zijn er strikte voorwaarden op het gebied van burgerrechten. Onder de AVG hebben betrokkenen recht op onder andere inzage, correctie, toegang of uitleg. Het bestaan van dergelijke rechten impliceert

¹⁴⁹ Zie art. 4 lid 1 Algemene verordening gegevensbescherming.

overigens niet dat verzoeken ter uitvoering van deze rechten altijd gehonoreerd dienen te worden. De AVG, maar ook de Wpg, stellen voorwaarden aan de uitvoering van deze rechten.

Iedere verwerking van persoonsgegevens, ook door overheidsorganen, dient rechtmatig, behoorlijk en transparant te zijn.¹⁵⁰ De AVG vult dit principe op verschillende vlakken verder in, waarbij transparantie in de vorm van een privacyverklaring¹⁵¹ op een website een bekende vorm is. Wanneer persoonsgegevens politiegegevens worden, omdat ze worden verwerkt in het kader van de uitvoering van de politietaak¹⁵², kent de Wpg haar eigen regime als het gaat om burgerrechten. Daarover later meer. Vastgesteld is dat privacywetgeving op het gebied van toegang, correctie en inzicht stevige juridische waarborgen kent.

4.2.2. Openbaarheid

Het recht op reactieve openbaarheid is stevig verankerd als het gaat om overheidsinformatie. Ongeacht het soort informatieobject, persoonsgegeven of niet, reguleert de Woo openbaarheid van overheidsinformatie. Behoudens uitzonderingen heeft iedereen recht op toegang tot publieke informatie verwerkt door overheidsorganen of instanties.¹⁵³ Om aan dit recht gehoor te kunnen geven, dienen overheidsorganen ervoor te zorgen dat alle documenten die zij ontvangen, maken of tot hun beschikking hebben, op een adequate manier worden verwerkt om gehoor te kunnen geven aan dit recht.¹⁵⁴ Hier dient de informatiehuishouding op ingericht te zijn. Daarbij dient opgemerkt te worden dat dit geen absolute rechten zijn. Openbaarheid van overheidsinformatie is een belangrijke pijler als het gaat om democratische controle van de overheid. Tegelijkertijd zijn er juridische nuanceringen om in bepaalde situaties andere belangen dan openbaarheid te laten prevaleren.¹⁵⁵ Veiligheid van de staat, privacybelangen of het goed functioneren van bestuursorganen zijn voorbeelden van dergelijke situaties. Openbaarheid als onderdeel van burgerrechten is in juridische zin met de Woo stevig verankerd. In praktische zin blijkt het vertalen van deze juridische verankering naar praktijk niet altijd even goed werkbaar. Zie daarover ook paragraaf 4.3.2 hieronder.

4.2.3. Toegang, correctie en inzicht

Toegang krijgen tot informatieobjecten is mogelijk zowel via de Woo als via privacywetgeving. De Woo reguleert allerhande gegevens, waarbij privacywetgeving uitsluitend de gegevens beheerst die zijn te classificeren als persoons- of politiegegevens. Dit onderscheid is grofweg te vertalen naar publieke informatie en eigen persoons- of politiegegevens. 'Eigen', omdat privacywetgeving uitsluitend ziet op eigen gegevens van een verzoeker. Publieke informatie is toegankelijk via de Woo en gegevens in de privacy sfeer via de AVG dan wel Wpg. De Woo en privacywetgeving kennen beide hun eigen reikwijdte en kennen, afhankelijk van die reikwijdte, juridische definities toe aan de term informatieobject. Daarmee kan gesteld worden dat het recht op toegang tot die informatieobjecten afdoende juridisch wordt geborgd.

¹⁵⁰ Zie art. 5 lid 1 Algemene verordening gegevensbescherming.

¹⁵¹ Zie art. 12, 13 en 14 Algemene verordening gegevensbescherming.

¹⁵² Zie art. 1 onder a Wet politiegegevens.

¹⁵³ Zie art. 1.1 en art. 2.2 Wet open overheid.

¹⁵⁴ Zie art. 2.4 Wet open overheid.

¹⁵⁵ Zie art. 5.1 en verder Wet open overheid.

Het recht op correctie of rectificatie is voor persoonsgegevens juridisch geborgd in de AVG¹⁵⁶ en voor politiegegevens in de Wpg¹⁵⁷. Feitelijk onjuiste gegevens kunnen met een beroep op de AVG of Wpg gecorrigeerd worden. Het is geen onbeperkt recht en in sommige gevallen met redenen beperkt. Een van die beperkingen geldt voor openbare registers. Als de openbare registers een bijzondere eigen wettelijke procedure kennen om persoonsgegevens te laten corrigeren, dient die procedure gevolgd te worden.¹⁵⁸

Er dient bijzondere aandacht te zijn voor de complexiteit en praktische uitvoerbaarheid van het correctierecht. Zeker als persoonsgegevens verspreid binnen een overheidsorgaan aanwezig zijn of wanneer persoonsgegevens worden gebruikt in complexe technische processen zoals risicobeoordelingen.¹⁵⁹ Naast de privacyrechtelijke constructie om persoonsgegevens te laten corrigeren, is er geen algemeen juridisch verankerd correctierecht op alle gegevens binnen de overheid. Hoewel betoogd kan worden dat het correctierecht praktisch en technisch soms moeilijk realiseerbaar is, is de juridische borging wel aanwezig voor gegevens in het privacydomein.

Naast toegang en correctie bestaat er een solide juridische borging van het inzagerecht. Privacywetgeving in de vorm van de AVG¹⁶⁰ en Wpg¹⁶¹ biedt de randvoorwaarden voor een inzagerecht. Dit inzagerecht strekt tot informatieobjecten die als persoons- of politiegegevens aangemerkt worden. De juridische borging van deze rechten is verder, naast de wettelijke verankering, verstevigd door aan de AP een boetebevoegdheid toe te kennen jegens organisaties die niet in lijn met dit inzagerecht handelen.

Met het bestaan van dit inzagerecht dient rekening gehouden te worden bij het herinrichten en structureren van de informatiehuishouding. Dit wordt terecht benoemd als een van de aandachtspunten in de memorie van toelichting van de Aiw.¹⁶²

4.2.4. Navolgbaarheid

In aanvulling op bovenstaande rechten is navolgbaarheid ook een onmisbare schakel als het gaat om burgerrechten. Het is, in tegenstelling tot bovenstaande burgerrechten, minder expliciet verankerd in de wet. In een democratische samenleving is begrijpelijke besluitvorming een onmisbaar instrument. Besluitvorming moet gemotiveerd én gevolgd kunnen worden. Toch is deze navolgbaarheid niet als zodanig expliciet gemaakt in de wet. Het volgt uit principes van motivering en transparantie die samen zorgen voor navolgbaarheid.

Zo stelt de Awb diverse voorwaarden aan het nemen van besluiten. Op basis van de Woo kunnen burgers, tot op zekere hoogte, vervolgens inzicht krijgen in de

¹⁵⁶ Zie art. 16 Algemene verordening gegevensbescherming.

¹⁵⁷ Zie art. 28 Wet politiegegevens.

¹⁵⁸ Zie art. 47 lid 1 Uitvoeringswet Algemene verordening gegevensbescherming.

¹⁵⁹ Zie o.a. boetebesluit Belastingdienst zwarte lijst FSV, AP, 12 april 2022 en Onderzoeksrapport Gebruik van geautomatiseerde risicoclassificering op basis van een risicoprofiel bij Controleproces Uitwonende Beurs (CUB), AP, 11 november 2024.

¹⁶⁰ Zie art. 15 Algemene verordening gegevensbescherming.

¹⁶¹ Zie art. 25 Wet politiegegevens.

¹⁶² Zie MvT Algemene informatiewet overheid, p. 21.

motivering van het betreffende besluit. Daarnaast draagt het openbaar maken van beslisnota's bij aan transparantie.¹⁶³ De voorwaarden voor het nemen van een besluit, het bieden van inzicht en het openbaren daarvan bieden in juridische zin een gevoel van navolgbaarheid.

De komst van AI heeft navolgbaarheid uitdagender gemaakt. AI staat bekend als complexe technische, en daarmee moeilijk te begrijpen, technologie. Naarmate AI meer ingezet gaat worden om besluiten te nemen, zal daarbij de navolgbaarheid voor burgers onder druk kunnen komen te staan. De AI-verordening introduceert daarom een nieuwe reactieve informatieplicht voor specifieke situaties waarin gegevens worden verwerkt door middel van kunstmatige intelligentie. Meer specifiek bestaat de informatieverplichting vanuit de AI-verordening alleen als er sprake is van een AI-systeem met een hoog risico, met rechtsgevolgen of andere aanzienlijke nadelige gevolgen voor personen.¹⁶⁴ In de praktijk zullen hier vaak persoonsgegevens bij verwerkt worden, maar de verplichting tot transparantie en daarmee in zekere mate ook de navolgbaarheid, geldt ongeacht het soort gegeven.

Het is niet alleen het begrip 'navolgbaarheid' zelf en de techniek die zorgen voor een complex geheel. De fragmentatie van informatieobjecten binnen de overheid, de verschillende lagen en soorten organisaties binnen dezelfde overheid, de verschillende informatiesystemen die gebruikt worden én de uiteenlopende juridische kaders die van toepassing zijn op de informatieobjecten zorgen voor een lappendeken aan invalshoeken ten aanzien van dit begrip.

Vanuit dat perspectief bezien is het verdedigbaar en begrijpelijk dat er met de Aiw wordt beoogd om kwaliteit en betrouwbaarheid van informatie de nodige aandacht te schenken.¹⁶⁵ Zonder die termen is navolgbaarheid moeilijk te realiseren.

4.2.5. Concluderend

Gelet op de bovenstaande stevige waarborgen vanuit zowel Europees als nationaal recht is er sprake van juridische borging van burgerrechten. Sommige rechten zijn expliciet geborgd, terwijl andere rechten meer impliciet volgen uit wet- en regelgeving. Waar rechten juridisch zijn geborgd, weerspiegelt dit echter niet per definitie de praktisch uitvoerbare werkelijkheid.

4.3. Proactieve en passende dienstverlening

4.3.1. Toelichting deelvraag

In deze paragraaf staat de vraag *"ondersteunen bestaande juridische kaders de mogelijkheid tot proactieve dienstverlening en bieden zij voldoende houvast om de grenzen van deze zorgplicht te markeren?"* centraal.

Zoals in Pijler 3 toegelicht, kan een zorgplicht algemeen worden omschreven als een plicht om zorgvuldig te handelen en de belangen van anderen te beschermen, of om schade aan mens en milieu te voorkomen. Proactieve dienstverlening is in de praktijk een integraal onderdeel van het handelen van de Nederlandse overheid en komt terug in verschillende wetten zoals de Awb, de Woo en de Archiefwet.

Met de komst van de Woo is een proactievere plicht tot openbaarmaking van informatie geïntroduceerd voor de overheid (in de vorm van een

¹⁶³ Zie ook actieplan Open Overheid, p. 10.

¹⁶⁴ Zie art. 86 lid 1 AI-verordening.

¹⁶⁵ Zie MvT Algemene informatiewet overheid, p. 31.

inspanningsverplichting). In de Woo zijn informatieobjecten aangewezen die de overheid, zonder daarom gevraagd te worden, zelf openbaar moet maken. De voorloper van de Woo, de Wet openbaarheid van bestuur (Wob), kende deze verplichting niet. Bovendien rust er sinds de komst van de Woo een zwaardere plicht op de overheid om uit te leggen waarom bepaalde informatieobjecten niet openbaar worden gemaakt. Deze verplichtingen zien uitsluitend op openbaarmaking en de proactieve houding die daarbij wordt verwacht. Later wordt ingegaan op de mogelijkheid of onmogelijkheid die huidige juridische kaders bieden ten aanzien van andere proactieve dienstverlening.

4.3.2. Proactief

Met de Woo is er een juridisch kader ontstaan voor proactieve openbaarmaking van bepaalde informatieobjecten. De digitale infrastructuur die deze proactieve openbaarmaking moet borgen, de generieke Woo-voorziening, komt echter moeilijk van de grond. De openbaarmaking wordt in fases, tranches, uitgevoerd. Half februari is duidelijk geworden dat het verder uitrollen van de digitale infrastructuur naar schatting minimaal negen maanden vertraging oploopt. Als oorzaak daarvoor worden *"de complexiteit van de bouwopgave en de architectuur, de afhankelijkheden tussen verschillende functionaliteiten, de hoeveelheid betrokken partijen, de beschikbare capaciteit en knelpunten rondom het continueren van een attenderingsfunctie"* genoemd.¹⁶⁶ Dit voorbeeld laat zien dat wetgeving slechts één stap is naar een betere informatiehuishouding waarin informatieobjecten gedeeld kunnen worden. Na wetgeving dient de huishouding ook technisch ingericht te worden om uitvoering aan deze wetgeving te kunnen geven.

Proactieve openbaarmaking van de overheid gaat echter verder dan uitsluitend het bieden van transparantie over informatieobjecten. Zo is het actief informeren van burgers over bijvoorbeeld het recht op enige toeslag of andere voorzieningen waar zij mogelijk recht op hebben, een andere vorm van proactieve dienstverlening.¹⁶⁷ Deze proactieve zorgplicht kan echter bemoeilijkt worden door wet- en regelgeving die het delen van persoonsgegevens ter uitvoering van de zorgplicht complexer maakt.

Deze constatering heeft er onder andere voor gezorgd dat het wetsvoorstel voor de Wet proactieve dienstverlening SZW tot stand is gekomen. Het UWV, de SVB en gemeenten krijgen door deze wet meer ruimte om persoonsgegevens van mensen uit te wisselen en burgers op deze manier actiever te wijzen op hun recht op uitkering of ondersteuning. Niet alleen biedt dit wetsvoorstel de instanties een bevoegdheid om proactieve dienstverlening toe te passen¹⁶⁸, maar het wetsvoorstel voorziet daarnaast ook in een legitimering om de gegevensverwerking horend bij de bevoegdheid vorm te geven¹⁶⁹. Daarnaast is er de Verzamelwet Gegevensbescherming (de Verzamelwet) die op 1 september 2026 in werking is getreden. De Verzamelwet verheldert het een en ander ten aanzien van de uitvoering van de UAVG en de AVG en creëert een aantal uitzonderingen op het verbod om gezondheidsgegevens te gebruiken en

¹⁶⁶ Zie Kamerbrief 16 februari 2026 betreffende de vertraging ontwikkeling generieke Woo-voorziening, 2026-0000058565, p. 1.

¹⁶⁷ Zie MvT Algemene informatiewet overheid, p. 11.

¹⁶⁸ Zie art. 10b lid 1 wetsvoorstel Wet proactieve dienstverlening SZW.

¹⁶⁹ Zie art. 73b wetsvoorstel Wet proactieve dienstverlening SZW.

grondslagen in onder meer de uitvoering van de Vreemdelingenwet.¹⁷⁰ Op die manier poogt ook deze wet de gegevensuitwisseling voor de interne organisatie van de overheid te vergemakkelijken om proactieve dienstverlening aan de burger te verbeteren.

Ook op andere terreinen zijn wetsvoorstellen gedaan om gegevensdeling binnen de overheid te legitimeren en daarmee te vergemakkelijken. Zo wordt geprobeerd om via de Wet aanpak meervoudige problematiek sociaal domein, die al sinds 2023 is aangeboden aan de Tweede Kamer maar nog niet verder dan een wetsvoorstel is gekomen, een wettelijk kader te bieden om gegevens in het sociaal domein gemakkelijker te kunnen uitwisselen. Een ander voorbeeld is de Wgs, waarin een opening wordt gemaakt zodat via ministeriële regelingen signalen van schuldeisers over betalingsachterstanden met een college van B&W gedeeld kunnen worden, zodat een college proactief een gesprek met een burger aan kan gaan over deze achterstanden.¹⁷¹ Daarnaast wordt door verschillende stakeholders gepleit voor een algemene grondslag voor gegevensuitwisseling voor proactieve dienstverlening voor de overheid, zoals onder meer door de VNG.¹⁷²

Dit zijn allemaal, via bestaande wetgeving of wetsvoorstellen, constructies om proactievere dienstverlening aan de burgers door overheden te rechtvaardigen. Waar deze proactiviteit mogelijk stuit op remmingen vanuit andere wetgeving, zoals de AVG, wordt gezocht naar passende oplossingen. Tegelijkertijd laat het bestaan van de wetsvoorstellen op dit gebied zien dat de huidige juridische kaders onvoldoende ruimte bieden om proactief handelen te legitimeren. Hetzij omdat het niet als taak in de wet is opgenomen, hetzij omdat er andere wetgeving is die het delen van aanwezige gegevens mogelijk belemmert.

4.3.3. Grenzen van proactieve dienstverlening

Op sectorniveau zijn, en komen er mogelijk meer, juridische kaders die bijdragen aan proactieve dienstverlening richting burgers. Het tweede deel van de deelvraag gaat daarbij in op de vraag of die kaders voldoende houvast bieden om de grenzen van een mogelijke zorgplicht tot openbare dienstverlening van de overheid te markeren. De vraag is of dit voldoende expliciet is opgenomen in de wet om eraan te kunnen refereren als zorgplicht, of dat dit uitgangspunt alleen terugkomt in verschillende kernwetten en het handelen van de overheid.

De grenzen worden hoofdzakelijk gemarkeerd door de AVG of Wpg zodra het gaat om persoonsgegevens of politiegegevens. Zodra informatieobjecten niet zijn te definiëren als persoons- of politiegegevens, geldt er vanuit informatieobjecten bezien een minder strikt regime ten aanzien van het gebruiken van informatieobjecten om te voldoen aan enige zorgplicht. De informatieobjecten zelf zijn in die gevallen minder strikt gereguleerd.

In dat geval zit de mogelijkheid of onmogelijkheid tot het delen van informatieobjecten vooral in de wettelijke kaders die de bevoegdheden tot delen voor het betreffende overheidsorgaan legitimeren. En die kaders zijn niet altijd

¹⁷⁰ Wet van 10 juni 2026 tot wijziging van de Uitvoeringswet Algemene verordening gegevensbescherming en enkele andere wetten in verband met het stroomlijnen en actualiseren van het gegevensbeschermingsrecht (Verzamelwet gegevensbescherming).

¹⁷¹ Zie art. 10 lid 1 Wet gemeentelijke schuldhulpverlening.

¹⁷² Rondetafelgesprek Verzamelwet Gegevensbescherming, Vereniging Nederlandse Gemeenten, 4 december 2024.

even expliciet. Zo wordt in de Awb gesteld dat er passende ondersteuning vanuit het bestuursorgaan moet zijn bij het verkeer met dat bestuursorgaan.¹⁷³ Een diepere blik op die bepaling uit de Awb leert dat de bepaling een voorbeeld is van het invullen van de zorgplicht van de overheid en daarmee een wettelijk kader is.¹⁷⁴

Nergens in de wet is tot nu toe echter een algemene specifieke zorgplicht tot proactieve dienstverlening opgenomen, hoewel proactieve dienstverlening regelmatig binnen verschillende wetten en regelgeving als uitgangspunt dient. Daardoor is het moeilijk te definiëren wanneer de overheid mag wachten tot de burger initiatief neemt, of wanneer de overheid zelf proactief actie dient te ondernemen.

4.3.4. Concluderend

Op verschillende plaatsen in de wet wordt ruimte geboden voor proactieve dienstverlening naar burgers toe. Bovenstaande, niet-limitatieve, voorbeelden illustreren dit. De bovenstaande voorbeelden laten echter ook zien dat een proactievere aanpak vooral per sector of per probleem via de wetgevende route wordt aangepakt. Door het ontbreken van een overkoepelende algemene wettelijke verankering van proactieve dienstverlening blijft er onduidelijkheid bestaan over de daarbij horende zorgplicht. Gelet op alle toepasselijke wettelijke kaders kan het gevoel ontstaan dat er meer duidelijkheid is over de grenzen die vanuit privacywetgeving bepalen hoe ver de overheid niet mag gaan, dan dat er duidelijkheid is over de juridische en praktische mate waarin de overheid proactief moet zijn. Voor zover deze proactiviteit is geborgd, betreft het hoofdzakelijk open normen die voor interpretatie vatbaar zijn en daarmee onduidelijkheid scheppen.

4.4. Transparantie

4.4.1. Toelichting deelvraag

In deze paragraaf staat de vraag *"zijn juridische eisen voor uitlegbaarheid, verantwoording, logging en algoritmische transparantie aanwezig en toepasbaar?"* centraal.

Uitlegbaarheid, verantwoording, logging en algoritmische transparantie zijn alle termen die in meer of mindere mate zijn bedoeld om mensen inzicht te geven in de manier waarop er met hun gegevens om wordt gegaan. Door middel van dit inzicht kunnen risico's bloot worden gelegd die betrekking hebben op schending van fundamentele rechten zoals discriminatie of uitsluiting¹⁷⁵, worden betrokkenen in staat gesteld om bezwaar te maken¹⁷⁶ en krijgen betrokkenen meer controle over de verwerking¹⁷⁷. Zo is althans de gedachte van de wetgever. Het geven van deze inzichten vereist een adequate informatiehuishouding en bij gebrek daaraan komen bovengenoemde burgerrechten onder druk te staan.¹⁷⁸

¹⁷³ Zie art. 2:1 lid 1 Algemene wet bestuursrecht.

¹⁷⁴ Zie *Kamerstukken II* 2018/19, 35261, nr. 3, p. 7.

¹⁷⁵ HvJ EU 7 december 2023, C-634/21, ECLI:EU:C:2023:957 (*SCHUFA*).

¹⁷⁶ Zie art. 22 lid 3 Algemene verordening gegevensbescherming.

¹⁷⁷ Zie Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 p. 23.

¹⁷⁸ Zie ook Maatschappij zoekt informatie, Reflectie op wetsvoorstel 'Algemene informatiewet overheid' in opdracht van de Regeringscommissaris Informatiehuishouding, Waag Futurelab, 2023, p. 3.

Juridische eisen voor deze termen zijn grofweg te verdelen in twee categorieën. Informatie die valt binnen het begrip persoonsgegevens en informatie die daarbuiten valt.

Transparantie dient op basis van de AVG onder andere aanwezig te zijn op het gebied van geautomatiseerde besluitvorming. Indien enige vorm van geautomatiseerde besluitvorming plaatsvindt, mag dit uitsluitend indien wordt voldaan aan strikte voorwaarden¹⁷⁹ én inzicht gegeven kan worden in de manier waarop de besluitvorming tot stand is gekomen.¹⁸⁰ Dat deze regels niet alleen in de wet zijn opgenomen, maar ook toepasbaar en handhaafbaar zijn, blijkt onder andere uit het onderzoeksrapport van de AP naar fraudeaanpak bij DUO.¹⁸¹ Specifiekere transparantieverplichtingen ten aanzien van persoonsgegevens zijn ook verwerkt in andere wet- en regelgeving, aanvullend op de AVG.¹⁸²

Net als de AVG kent ook de Wpg aan personen informatierechten toe op het gebied van transparantie en verantwoording.¹⁸³ In vergelijking met de AVG zijn de gegevensverwerkingen binnen het domein van de Wpg bewust minder transparant voor betrokkenen gemaakt. Dit alles om een goede balans te zoeken tussen opsporing en handhaving enerzijds en het recht op eerbiediging van de persoonlijke levenssfeer anderzijds. Omdat volledige openheid politietaken kan bemoeilijken, is het informatierecht in de Wpg strikter uitgelegd dan in de AVG het geval is. Het verschil tussen deze twee privacygerelateerde rechten is een voorbeeld van de vele nuanceringen die gemaakt moeten worden ten aanzien van de informatieobjecten en de context waarbinnen informatieobjecten verwerkt worden.

Het is tegelijk een voorbeeld van de moeilijkheid om informatieobjecten qua juridische terminologie gelijk te moeten, willen of kunnen trekken. Het huidige juridische onderscheid in de termen 'persoonsgegeven' en 'politiegegeven' is bewust aangebracht. Daarmee worden de domeinen waarbinnen deze gegevens verwerkt kunnen en mogen worden geduïd.

Zelfs dezelfde soort informatieobjecten in de vorm van persoonsgegevens kunnen afhankelijk van hun gebruikscontext aan verschillende vormen van transparantie onderworpen worden. Dat wordt geïllustreerd aan de hand van transparantie over algoritmes, geautomatiseerde besluitvorming en de toepasbaarheid daarvan onder de AVG en de AI-verordening. Beide verordeningen schrijven verplicht enige mate van transparantie voor om betrokkenen inzage te geven in de manier waarop hun gegevens worden verwerkt, om hen in de gelegenheid te stellen de gegevensverwerking te controleren en hen te beschermen tegen fouten en

¹⁷⁹ Zie art. 22 Algemene verordening gegevensbescherming.

¹⁸⁰ Zie onder andere art. 15 Algemene verordening gegevensbescherming.

¹⁸¹ Zie Onderzoeksrapport fraudeaanpak DUO, AP, 11 november 2024, waarbij dient opgemerkt te worden dat uit één voorbeeld van handhaving niet afgeleid mag worden dat de wetgeving goed werkt en altijd en overal goed wordt toegepast en handhaafbaar is.

¹⁸² Zie bijvoorbeeld art. 20 Datagovernanceverordening.

¹⁸³ Zie art. 24 en verder en art. 32a Wet politiegegevens.

onzorgvuldige verwerking¹⁸⁴, om bezwaar te maken¹⁸⁵ en om risico's op schending van fundamentele rechten bloot te leggen.¹⁸⁶

Deze principes worden in de AVG vertaald naar de verplichting om inzage te bieden in verwerking van persoonsgegevens¹⁸⁷ en in de AI-verordening naar de verplichting om uitleg te geven over bepaalde vormen van AI-besluitvorming¹⁸⁸. De mate waarin de inzage en uitleg gegeven dient te worden verschilt echter per verordening. Waar de AI-verordening spreekt over duidelijke inhoudelijke uitleg over de rol van AI bij de besluitvorming en de voornaamste elementen daarvan, inclusief het loggen van handelingen bij bepaalde AI-systemen¹⁸⁹, spreekt de AVG over nuttige informatie over de onderliggende logica van geautomatiseerde besluitvorming. Het Hof van Justitie van de Europese Unie heeft dit recht op uitleg nader gespecificeerd door te stellen dat het inhoudt welke procedure en beginselen er concreet zijn toegepast bij de geautomatiseerde besluitvorming.¹⁹⁰

Het betreft twee verordeningen die met verschillende bewoordingen een gewenst niveau van transparantie beschrijven. Dit voorbeeld laat zien dat juridische eisen voor transparantie aanwezig zijn, toepasbaar zijn, maar jurisprudentie nodig hebben om deze toepasbaarheid nader te duiden.

4.4.2. Concluderend

De AVG, Wpg, AI-verordening, de Woo en andere wet- en regelgeving brengen allemaal verplichtingen met zich mee die bijdragen aan een transparante manier van gegevensverwerking rondom informatiegebruik en besluitvorming. Afhankelijk van het soort gegeven en de omgeving waarin, en de manier waarop, de gegevens worden verwerkt, stellen deze wetten verplichtingen. Verplichtingen die niet alleen aanwezig, maar ook toepasbaar zijn vanwege het detailniveau waarin ze in wet- en regelgeving zijn omschreven.

¹⁸⁴ Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, 6 februari 2018 p. 23.

¹⁸⁵ Zie art. 22 lid 2 Algemene verordening gegevensbescherming en overweging 171 AI-verordening.

¹⁸⁶ HvJ EU 7 december 2023, C-634/21, ECLI:EU:C:2023:957 (*SCHUFA*).

¹⁸⁷ Zie art. 15 lid 1 sub h Algemene verordening gegevensbescherming.

¹⁸⁸ Zie art. 86 AI-verordening.

¹⁸⁹ Zie art. 12 AI-verordening.

¹⁹⁰ HvJ EU 27 februari 2025, C-203/22, ECLI:EU:C:2025:117 (*Dun & Bradstreet*).

5. Pijler 5: Oplossend en lerend vermogen

Er bestaan gepercipieerde belemmeringen tussen bestaande en toekomstige wettelijke kaders. Bijvoorbeeld als het gaat om principes van geheimhouding tegenover principes van openbaarheid.

Deze pijler gaat over de structurele capaciteit van het huidige en toekomstige juridische en beleidsmatige kader om knelpunten van een vrij en consistent verkeer van informatieobjecten binnen de overheid tijdig te signaleren, op te lossen en continu te verbeteren.

Ten behoeve van het onderzoeksrapport staat daarbij de volgende kernvraag centraal:

In hoeverre maken bestaande juridische instrumenten het mogelijk om structurele knelpunten in gegevensdeling, kwaliteit en standaardisatie tijdig te signaleren en duurzaam op te lossen?

Om deze kernvraag adequaat te kunnen behandelen, komen in het onderzoeksrapport de volgende criteria aan bod:

- Knelpuntenmechanismen en escalatie: zijn er organen, processen of bevoegdheden om actief dataknelpunten te ontdekken en op te lossen?
- Lerend vermogen: wordt monitoring juridisch verplicht gesteld en zijn feedbackloops verankerd?
- Innovatie en experiment: is er binnen huidige en toekomstige juridische kaders ruimte voor innovatie, pilots en experimenten?
- Professionalisering en vakmanschap: zijn er juridisch bindende maatregelen voor permanente ontwikkeling van informatieprofessionals?

5.1. Antwoord op de kernvraag

Knelpunten in gegevensdeling, kwaliteit en standaardisatie zijn in de voorgaande pijlers uitvoerig besproken. Het soort gegevens, de context waarbinnen het wordt verwerkt, door wie en voor wie het wordt verwerkt en welke wet- en regelgeving daarop van toepassing is, bepalen de knelpunten. Naast de knelpunten bepalen de genoemde factoren de reikwijdte waarbinnen gezocht moet worden naar passende juridische instrumenten om deze knelpunten te signaleren en duurzaam op te lossen. Gelijk aan de voorgaande pijlers doemt ook hier het probleem van juridische fragmentatie op. Door de lappendeken aan toepasselijke wet- en regelgeving, met daarin overlappende verplichtingen maar ook discrepanties ten aanzien van dezelfde gegevens, is het uitdagend om knelpunten tijdig te signaleren en duurzaam op te lossen.

Het daarbij te gebruiken juridisch instrumentarium kan oplossingen expliciteren, impliceren of aan de andere kant verbieden. In paragraaf 4.3.2 is geïllustreerd hoe privacywetgeving als blokkerend wordt ervaren, waardoor initiatieven ontstaan om nieuwe wetgeving te creëren. Deze nieuwe wetgeving bevat vervolgens een expliciet instrument om geconstateerde knelpunten op te lossen. Tegelijkertijd is het maken van nieuwe wetgeving een van de oorzaken dat er een complexe lappendeken van regels is ontstaan. Een lappendeken die het juridisch mogelijk maakt om knelpunten in gegevensdeling, datakwaliteit en standaardisatie te signaleren en aan te pakken, maar tegelijkertijd ook geen samenhangend, afdwingbaar en duurzaam karakter heeft. Verordeningen, richtlijnen, wetten in

formele zin, lagere wetgeving, standaarden en beleidsprogramma's reguleren allemaal in meer of mindere mate signalerende en oplossende mogelijkheden. Wat dat betekent voor achtereenvolgens gegevensdeling, datakwaliteit en standaardisatie is hieronder nader toegelicht.

5.1.1. Gegevensdeling

Het juridische gegevensdelingskader is bijzonder gefragmenteerd. De VIE, Wdo, Wgds, AVG en Wpg zijn voorbeelden van wetgeving met kaders waarbinnen gegevensdeling plaats moet vinden. Daarnaast zijn er, zoals omschreven in Pijler 2 en 3, nog tal van sectorale wetten met elk hun eigen structuur en eigen bepalingen over welke gegevens op welke manier en onder welke voorwaarden gedeeld mogen worden. Niet alleen zorgt dit voor praktische onduidelijkheid over de mogelijkheid van gegevensdeling, maar schept het ook een haast onmogelijke situatie om centraal gegevensdeling te monitoren op knelpunten. De knelpunten kunnen immers, naast uit de praktische uitvoering, uit tal van verschillende juridische hoeken komen. Naast deze problematiek rondom de versplinterde regels over gegevensdeling bemoeilijkt het juridisch kader omtrent datakwaliteit de goede aanpak van knelpunten nog verder. Ook vanuit de VNG wordt deze problematiek benadrukt. De VNG stelt zelfs een centraal mechanisme voor om gegevensknelpunten te melden en waar het mandaat ligt om knelpunten op te lossen door uitwisseling toe te staan.¹⁹¹

5.1.2. Datakwaliteit

Datakwaliteit is divers. Zoals meerdere malen in dit rapport omschreven, is de belangrijkste knip in gegevens en wetgeving daarover te maken in gegevens die bestaan uit persoonsgegevens en gegevens zonder persoonsgegevens. Voor persoonsgegevens is de AVG de meest omvattende wet die, naast vele andere zaken, datakwaliteit vereist. Zowel vanuit actief perspectief, waarbij een overheidsorgaan verplicht wordt om de juistheid van persoonsgegevens te borgen¹⁹², als reactief wanneer betrokkenen verzoeken om rectificatie van onjuiste gegevens¹⁹³, dient men op te treden om datakwaliteit te realiseren. Laatstgenoemde illustreert een expliciet juridisch instrument. De AVG schrijft duidelijk voor dat, hoe en binnen welke periode gehoor gegeven dient te worden aan een verzoek. Eerstgenoemde is een voorbeeld van het impliciete juridische instrument en bevat veel minder juridische kaders.

Een ander expliciet juridisch instrument is terug te vinden in de Wet BRP. Op verschillende plaatsen in die wet is expliciet opgenomen dat gegevens niet gebruikt mogen worden¹⁹⁴, of van een aantekening voorzien moeten worden¹⁹⁵, indien het aannemelijk is dat deze onjuist zijn. Ook de Kadasterwet kent expliciete bepalingen om onjuistheden te herkennen en te corrigeren.¹⁹⁶ Beide voorbeelden richten zich echter expliciet op het corrigeren of herkennen van individuele fouten. Het zijn geen instrumenten om op systematische basis de algehele kwaliteit van data te monitoren en te verbeteren.

¹⁹¹ Rondetafelgesprek Verzamelwet Gegevensbescherming, Vereniging van Nederlandse Gemeenten, 4 december 2024.

¹⁹² Zie art. 5 lid 1 sub d Algemene verordening gegevensbescherming.

¹⁹³ Zie art. 16 Algemene verordening gegevensbescherming.

¹⁹⁴ Zie bijvoorbeeld art. 2.75 en 2.75a Wet basisregistratie personen.

¹⁹⁵ Zie art. 2.76 Wet basisregistratie personen.

¹⁹⁶ Zie bijvoorbeeld art. 42 Kadasterwet.

Ook het toezicht hierop is niet structureel. De AP onderzoekt niet doorlopend de datakwaliteit van persoonsgegevens binnen de overheid en de Algemene Rekenkamer onderzoekt incidenteel IT-systemen en informatiebeheer¹⁹⁷, maar doet dit niet stelselmatig en doorlopend.

5.1.3. Standaardisatie

In tegenstelling tot de gegevensdelingskaders en juridische kaders rondom datakwaliteit is er op het vlak van standaardisatie meer vooruitgang geboekt. De Wdo is hierin een van de voornaamste oorzaken. De Wdo biedt een juridisch kader om standaarden op het gebied van onder andere veiligheid, betrouwbaarheid of toegankelijkheid te ontwikkelen.¹⁹⁸ De reikwijdte en toepassing van deze standaarden is tot nu toe echter nog beperkt. Ook de VIE is nog relatief nieuw, waarbij bezien moet worden in hoeverre daaruit kaders kunnen vloeien die preventieve monitoring mogelijk maken.

5.1.4. Concluderend

Het huidige juridische instrumentarium is ten aanzien van het tijdig signaleren en oplossen van knelpunten in gegevensdeling, kwaliteit en standaardisatie onvoldoende. Hoewel er binnen de huidige juridische kaders bepalingen te vinden zijn die omgang met knelpunten reguleren, is deze omgang hoofdzakelijk gericht op reactief handelen, in plaats van stelselmatige preventieve monitoring. De lappendeken van wetgeving, maar ook de diversiteit van gegevens, gegevensverwerkingen en overheidsorganen en -lagen bemoeilijken een overheidsbreed systeem van preventieve monitoring. Een breed gedragen, uitvoerbaar en wettelijk verplicht informatieplan zoals genoemd in de Aiw¹⁹⁹ kan hiervoor in ieder geval in juridische zin een passende oplossing bieden.

5.2. Knelpuntenmechanismen en escalatie

5.2.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“zijn er organen, processen of bevoegdheden om actief dataknelpunten te ontdekken en op te lossen?”* centraal. Deze paragraaf biedt inzicht in wat een dataknelpunt is en of er op dit moment aandacht is voor knelpunten binnen de informatiehuishouding van de overheid.

Dataknelpunten zijn belemmeringen die overheidsorganisaties ervaren bij de wens om informatie te delen met andere overheidsorganisaties. Een voorbeeld is een situatie waarbij de overheid door een Woo-verzoek gegevens moet delen, maar de gegevensbeschermingswetgeving regels stelt voor het delen van gevoelige gegevens van medewerkers. In de praktijk lakt de overheidsorganisatie in zo’n geval de gevoelige gegevens zwart. Het kan voorkomen dat de ontvanger of een andere partij het daar niet mee eens is op grond van bescherming van de persoonlijke levenssfeer.²⁰⁰ Dat is een voorbeeld van een knelpunt.

¹⁹⁷ Zie bijvoorbeeld het onderzoek van de Algemene Rekenkamer naar de cyberveiligheid van grenstoezicht op Schiphol, <https://www.rekenkamer.nl/actueel/nieuws/2020/04/20/cyberveiligheid-grenstoezicht-op-schiphol-onvoldoende>.

¹⁹⁸ Zie art. 3 Wet digitale overheid.

¹⁹⁹ Zie art. 11 Algemene informatiewet overheid.

²⁰⁰ Zie bijvoorbeeld Rb. Oost-Brabant 8 mei 2025, ECLI:NL:RBOBR:2025:2687, Rb. Midden-Nederland 16 december 2025, ECLI:NL:RBMNE:2025:6662 en Rb. Oost-Brabant 17 december 2025, ECLI:NL:RBOBR:2025:8214.

Specifiek de CCG is opgericht om doorbraken te faciliteren bij knelpunten op het gebied van gegevensgebruik.²⁰¹ Zij agendeert knelpunten op hoog ambtelijk niveau. Daarnaast is er de Adviesfunctie Verantwoord Datagebruik die als doel heeft dataprojecten te ondersteunen met gezaghebbend advies en praktische handvatten.²⁰²

Er zijn, gelijk aan de wetgeving, verder gefragmenteerde organen die vanuit hun doelstelling (bijvoorbeeld toezicht houden op persoonsgegevensbescherming) wel te maken krijgen met dataknelpunten en waar dit in sommige gevallen kan leiden tot een melding. Zie hiervoor het onderstaande schema.

Toezicht en inspectie	Adviesorganen	Politiek/bestuurlijk
Inspectie Overheidsinformatie en Erfgoed	Adviescollege Openbaarheid en Informatiehuishouding	Nationale ombudsman
Toezicht op informatiehuishouding en archivering.	Onafhankelijk adviesorgaan ter bevordering van de toepassing van de Woo.	Klachten over overheidshandelen inclusief informatievoorziening.
Autoriteit Persoonsgegevens	Adviescollege ICT-toetsing	Tweede Kamer
Toezicht op verwerking van persoonsgegevens.	Onafhankelijk adviescollege bijdragend aan een betere beheersing van ICT-projecten en informatiesystemen.	Via moties, debatten, voorstellen enzovoort
Autoriteit Consument en Markt		Ministerie van BZK/CIO Rijk
Toezicht op eerlijke concurrentie, consumentenrecht en specifieke sectoren.		Verantwoordelijk voor informatiehuishouding.
Auditdienst Rijk		Algemene Rekenkamer
Onafhankelijke interne auditor van de rijksoverheid.		Onderzoekt uitgaven van de overheid, waaronder informatiehuishouding.
Inspectie Gezondheidszorg en Jeugd		Afdeling advisering Raad van State
Toezicht op zorg en jeugdhulp.		Onafhankelijk adviseur van de overheid.
		Centrale Commissie gegevensgebruik
		Faciliteert doorbraken bij knelpunten ten

²⁰¹ Zie <https://realisatieibds.nl/groups/view/56d3fbd7-fd82-4869-93e1-7530114c037c/centrale-commissie-gegevensgebruik-ccg/wiki/view/577ad0f4-2ba5-4cd1-9225-3622b1acd852/centrale-commissie-gegevensgebruik-ccg>.

²⁰² Zie <https://realisatieibds.nl/page/view/f896fe3b-f93f-450e-a107-e280cbe8ecf6/adviesfunctie>.

		aanzien van gegevensgebruik.
		Adviesfunctie Verantwoord Datagebruik
		Ondersteunt maatschappelijke dataprojecten.

Programma's/fora	Juridische routes	Interbestuurlijk
Programma Open Overheid	Rechtbank	Vereniging van Nederlandse Gemeenten
Ondersteunt rijksprofessionals die werken aan open overheid.	Escalatie bij informatiegeschillen.	Behartigt belangen van gemeenten en kennisplatform voor alle gemeenten.
Rijksprogramma voor Duurzaam Digitale Informatiehuishouding	Bezwaar- en beroepsprocedures	Interprovinciaal Overleg
Ondersteunt rijksorganisaties bij het organiseren, vindbaar en duurzaam toegankelijk maken van digitale informatie.	Bij concrete besluiten over informatiedelen.	Behartigt belangen van provincies.
Forum Standaardisatie		Unie van Waterschappen
Platform voor het delen van ervaring met open standaarden in de publieke sector.		Koepel van waterschappen.

De CCG is het centrale punt voor dataknelpunten van overheidsorganisaties. Dit betekent echter niet dat zij overzicht heeft over dataknelpunten betreffende de gehele informatiehuishouding.

Niet ieder individu heeft toegang tot bovenstaande kanalen. Voor burgers is het doorgaans lastig om contact op te nemen met het Programma Open Overheid. Ook sommige overheidsorganen zijn mogelijk niet op de hoogte van beschikbare escalatieroutes, terwijl zij wel degelijk met dataknelpunten te maken hebben. Een burger die ontevreden is over de terugkoppeling van zijn Woo-verzoek kan naar het ACOI stappen, maar die weg ligt voor de gemiddelde burger niet voor de hand. De autoriteiten ontvangen klachten als het misgaat vanuit de overheid, maar dit ziet altijd op specifieke situaties zoals het gebruik van persoonsgegevens. Overheidsorganisaties die dataknelpunten ervaren, kunnen dit melden bij de CCG, die dit bestuurlijk en politiek agendeert. Dit is wel onder de voorwaarde dat alle overheidsorganisaties op de hoogte zijn van het bestaan van de CCG.

Dit betekent dat er signalen worden opgevangen door verschillende instituten, binnen en buiten de overheid.

5.2.2. CIO Rijk

Aparte aandacht is er voor de CIO Rijk. Sinds 1 januari 2026 heeft de CIO Rijk de expliciete bevoegdheid gekregen om bindende regels vast te stellen en te controleren voor informatiesystemen van ministeries.²⁰³ Hoewel de reikwijdte hiervan is beperkt tot ministeries, is dit een duidelijk voorbeeld van een orgaan dat mede tot taak heeft om actief dataknelpunten te ontdekken en op te lossen. Indien daarvoor innovatie nodig is, hebben CIO's de bevoegdheid om deze innovatie te stimuleren.²⁰⁴

Voor decentrale overheden is er momenteel geen equivalent van de CIO Rijk. De VNG en op provinciaal niveau het Interprovinciaal Overleg (IPO) zijn wel voorbeelden van kennisplatformen voor decentrale overheden, maar treden niet op om actief dataknelpunten te signaleren en op te lossen. Als gevolg hiervan zullen dataknelpunten die zich manifesteren op het niveau van decentrale overheden momenteel moeilijker gesignaleerd, gecoördineerd en aangepakt kunnen worden.

Naast de centrale en decentrale overheden kennen de grote publieke uitvoeringsorganisaties een samenwerkingsvorm via de Manifestgroep. Gelijk aan de VNG en het IPO focust deze groep zich echter niet op dataknelpunten, maar hoofdzakelijk op het verbeteren van de dienstverlening in algemene zin. Onderdeel van het verbeteren van die dienstverlening is het beoordelen van de vraag of gegevens onderling gedeeld kunnen worden, maar dat wordt slechts als voorbeeld van het grotere geheel genoemd.²⁰⁵ Bovendien is de Manifestgroep een informeel netwerk dat daarmee een legitieme basis om daadkrachtig op te treden rondom dataknelpunten lijkt te missen.

5.2.3. Concluderend

De CCG geldt als centraal meldpunt voor dataknelpunten. Er is geen centraal toegankelijk punt dat zelf dataknelpunten actief onderzoekt en escaleert. Buiten de CCG is signalering mogelijk via meerdere routes, maar er is geen plek waar alle dataknelpunten ten aanzien van de informatiehuishouding worden overzien, besproken en erop wordt gehandeld.

5.3. Lerend vermogen

5.3.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“wordt monitoring juridisch verplicht gesteld en zijn feedbackloops verankerd?”* centraal. Deze vraag zoekt naar een essentiële voorwaarde voor een effectieve informatiehuishouding. Het eerste onderdeel van de vraag ziet op de juridische legitimering, terwijl het tweede onderdeel ingaat op monitoring en kwaliteit.

In de voorgaande paragraaf is gesteld dat het ontbreekt aan een centraal gecoördineerde aanpak van dataknelpunten. Die lijn kan doorgetrokken worden als het gaat om feedbackloops. Een centraal gecoördineerde aanpak en juridische verplichting tot monitoring ontbreken. Dat neemt echter niet weg dat er vanuit verschillende juridische invalshoeken wel degelijk directe en indirecte

²⁰³ Zie onder andere art. 19 lid 2 Besluit CIO-stelsel Rijksdienst 2026.

²⁰⁴ Zie art. 4 onder d Besluit CIO-stelsel Rijksdienst 2026 en paragraaf 5.5.

²⁰⁵ Zie <https://manifestgroep.nl/page/view/e68c842e-93ac-498e-adc7-e3405f13874f>.

verplichtingen bestaan die feedbackloops impliceren of verankeren. Achtereenvolgens worden basisregistraties, de AVG, de Archiefwet en de BIO hieronder nader uitgewerkt. Deze dienen als voorbeelden om vast te stellen in hoeverre er een juridische verplichting tot monitoring van de informatiehuishouding bestaat, inclusief feedbackloops.

5.3.2. Basisregistraties

Het juridisch meest uitgebreide kader op dat gebied is terug te vinden in de basisregistraties, zoals hierboven eerder aangehaald.²⁰⁶ Gelet op het belang van de basisregistraties zijn er juridische verplichtingen voor de bronhouders die hen verplichten om de registraties bij te houden en actueel te houden. Hierin kan een verplichting tot feedbackloops gelezen worden. Het impliceert immers een zekere mate van monitoring en feedback. Gegevens kunnen niet actueel gehouden worden zonder enige vorm van monitoring en verwerking van feedback in te richten. Details over de verdere inrichting ontbreken echter in de wettelijke basis en worden daarmee overgelaten aan de uitvoeringspraktijk. Die uitvoeringspraktijk bestaat voor de BRP uit de colleges van burgemeester en wethouders voor ingezetenen²⁰⁷ en de minister van BZK voor niet-ingezetenen²⁰⁸. De uitvoeringspraktijk van de Kadasterwet is neergelegd bij het Kadaster²⁰⁹.

De basisregistraties kennen daarnaast een terugmeldplicht voor alle afnemers. Ieder bestuursorgaan dat gebruikmaakt van gegevens uit een basisregistratie dient zich tot de bronhouder te wenden als er enige twijfel bestaat over de juistheid van de verkregen gegevens.²¹⁰ De betreffende bronhouder is vervolgens gehouden hier actie op te ondernemen. Dit is een juridische verankering van een feedbackloop die uitsluitend ziet op gegevens uit de basisregistratie. De terugmeldplicht is bovendien beperkt tot gegevens waar twijfel bestaat over de juistheid daarvan. Dit dient niet gezien te worden als een volledige feedbackloop om systematisch de juistheid van de basisregistraties te kunnen borgen.

5.3.3. AVG

Zodra informatie bestaat uit persoonsgegevens en de verwerking van die gegevens onder de AVG valt, bestaat er een verantwoordingsplicht voor organisaties die de persoonsgegevens verwerken. Deze verantwoordingsplicht kent verschillende vertakkingen in de AVG. De basisprincipes die zien op de verplichting om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken, in lijn met een duidelijk vooraf bepaald doel én de verplichting om te zorgen dat de gegevens juist zijn, zijn hier voorbeelden van.²¹¹ Een equivalent hiervan is terug te vinden in de Wpg voor politiegegevens.²¹²

Aan deze verplichtingen kan niet voldaan worden zonder actief te monitoren op het gebruik van persoons- of politiegegevens. De AVG en Wpg expliciteren de monitoringsverplichting zelfs nog verder door bepaalde organisaties te verplichten een onafhankelijke toezichthouder aan te stellen in de vorm van een functionaris

²⁰⁶ Zie paragraaf 5.2.

²⁰⁷ Zie art. 1.4 lid 1 Wet basisregistratie personen.

²⁰⁸ Zie art. 1.4 lid 2 Wet basisregistratie personen.

²⁰⁹ Zie art. 2a en art. 3 Kadasterwet.

²¹⁰ Zie art. 2.34 lid 1 Wet basisregistratie personen en art. 7m lid 1 Kadasterwet.

²¹¹ Zie art. 5 Algemene verordening gegevensbescherming.

²¹² Zie art. 3 en 4 Wet politiegegevens.

gegevensbescherming²¹³, en een privacyfunctionaris.²¹⁴ De monitoringsverplichting onder de Wpg wordt verder geëxpliciteerd doordat de functionaris gegevensbescherming verplicht is om jaarlijks een verslag van zijn bevindingen op te stellen.²¹⁵

Daarnaast dienen bepaalde vormen van gevoelige verwerkingen van persoons- en politiegegevens uitsluitend plaats te vinden nadat er een voorafgaande risicoanalyse is gedaan, ook wel bekend als DPIA.²¹⁶ Dit zijn enkele voorbeelden van monitoringsverplichtingen uit privacywetgeving die niet alleen juridisch stevig zijn verankerd, inclusief toezicht daarop door de AP, maar ook sectoroverstijgend zijn en voor alle overheidsorganen gelden.

5.3.4. Archiefwet

De al eerder aangehaalde Archiefwet, die ziet op een deel van de informatiehuishouding, kent een algemene verplichting om archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren.²¹⁷ Dit impliceert een bepaalde vorm van monitoring. Zonder monitoring is het immers niet mogelijk om te voldoen aan deze verplichting. De praktische uitvoerbaarheid hiervan wordt echter niet uitgewerkt in de Archiefwet.

5.3.5. BIO

De BIO ziet als informatiebeveiligingsnorm op de gehele overheid. Ook hierin wordt monitoring niet expliciet genoemd, maar volgt het wel impliciet uit de verplichting tot zelfevaluaties. Aan de hand van deze evaluaties dient men te beoordelen in hoeverre er is voldaan aan toepasselijke verplichtingen en dient er een rapportage opgesteld te worden.²¹⁸ De verplichting onder de BIO ziet echter hoofdzakelijk op informatiebeveiliging en daarmee niet primair op een goede inrichting van de informatiehuishouding.

5.3.6. Concluderend

Gelet op deze vier voorbeelden van wet- en regelgeving valt op dat een integraal juridisch kader met daarin een juridische grond voor monitoring en feedbackloops ontbreekt. Hoewel er wel kaders zijn, zijn die kaders ofwel gericht op een specifiek soort gegeven zoals een persoonsgegeven of een politiegegeven, ofwel zijn de kaders gericht op segmenten binnen de overheid, maar strekken deze zich niet uit over de gehele overheid.

5.4. Innovatie en experiment

5.4.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“is er binnen huidige en toekomstige juridische kaders ruimte voor innovatie, pilots en experimenten?”* centraal. Deze paragraaf biedt inzicht in de balans tussen rechtszekerheid en het ontwikkelen van nieuwe technologieën.

Vanuit de rechtsstaatgedachte komt het principe dat al het overheidshandelen berust op duidelijke, transparante en vooraf vastgestelde regels. Het maken van

²¹³ Zie art. 37 Algemene verordening gegevensbescherming en art. 36 Wet politiegegevens.

²¹⁴ Zie art. 34 Wet politiegegevens.

²¹⁵ Zie art. 36 lid 4 Wet politiegegevens.

²¹⁶ Zie art. 35 AVG en art. 4c Wet politiegegevens.

²¹⁷ Zie art. 3 Archiefwet.

²¹⁸ Zie Baseline Informatiebeveiliging Overheid 2 (BIO2), v.1.3, paragraaf 6 en 8.

deze regels kost tijd. Daar staat een razendsnelle ontwikkeling van techniek tegenover. De kunst is het vinden van een balans tussen deze twee vaststaande feiten. Gelet op de juridische kaders is er ruimte om te experimenteren. De ruimte is echter begrensd en niet systematisch en specifiek ingericht om te kunnen functioneren op het gebied van informatiehuishouding. Hieronder worden enkele voorbeelden behandeld van juridische kaders die pogen om experimenten juridisch mogelijk te maken. De voorbeelden zijn gekozen om juridische ruimte tot experimenten, innovatie en pilots ten aanzien van data te bespreken. Er zijn daarnaast nog meer voorbeelden van wet- en regelgeving die dezelfde soort ruimte bieden. Bijvoorbeeld de Wet structuur uitvoeringsorganisaties werk en inkomen²¹⁹, de Wet maatschappelijke ondersteuning²²⁰ en de Jeugdwet²²¹ voor het sociale domein. Of de Omgevingswet voor het omgevingsrecht.²²²

5.4.2. Wdo

De Wdo kent een experimenteerbepaling.²²³ De bepaling maakt het mogelijk om, binnen de kaders van de Wdo, regels te stellen die het experimenteren mogelijk maken. De betreffende experimenten zijn echter wel beperkt tot de reikwijdte van de Wdo en zijn bovendien gebonden aan beperkende voorwaarden die alles te maken hebben met de hierboven genoemde balans tussen rechtszekerheid en innovatie. Experimenten moeten tijdelijk van aard zijn en mogen geen afbreuk doen aan andere rechten van betrokken personen.

5.4.3. Participatiewet

Ook in het sociale zekerheidsdomein bestaat wetgeving die het mogelijk maakt om te experimenteren. De Participatiewet stelt, gelijk aan de Wdo, dat er nadere regels gemaakt kunnen worden om delen van de Participatiewet doeltreffender uit te voeren.²²⁴ Deze juridische ruimte voor innovatie ziet niet primair op de informatiehuishouding, maar impliceert wel dat de ruimte er is. Efficiënter en effectiever omgaan met data kan een doeltreffendere werking van delen van de Participatiewet mogelijk maken.

5.4.4. Wgds

De Wgds is een ander voorbeeld van wetgeving met ruimte voor experimenten. Het experimenteren wordt niet als zodanig in de Wgds genoemd, maar de wet biedt ruimte om nieuwe samenwerkingsverbanden aan te wijzen waarbinnen het delen van gegevens tussen overheidsorganisaties mogelijk wordt gemaakt.²²⁵ Ook hier is de ruimte zeer beperkt om de fragiele balans tussen innovatie en rechtszekerheid niet te verstoren.

²¹⁹ Zie art. 82a Wet structuur uitvoeringsorganisaties werk en inkomen.

²²⁰ Zie art. 5.4.1 Wet maatschappelijke ondersteuning 2015.

²²¹ Zie art. 12.1 Jeugdwet.

²²² Zie art. 23.3 Omgevingswet.

²²³ Zie art. 26 Wet digitale overheid.

²²⁴ Zie art. 83 Participatiewet.

²²⁵ Zie art. 3.1 Wet gegevensverwerking door samenwerkingsverbanden.

5.4.5. Europees niveau

Op Europees niveau is er onder andere in de AI-verordening, de VIE, de DV en de DGV ruimte voor experimentele toepassingen die alle direct of indirect raken aan data en de informatiehuishouding.

De AI-verordening, bij uitstek op dit moment de wetgeving die een zeer delicate balans kent tussen innovatie en rechtszekerheid, kent het principe van een testomgeving voor regelgeving.²²⁶ Een testomgeving waarin, onder streng toezicht, geëxperimenteerd kan worden met innovatieve AI-systemen. Het doel van deze testomgeving bestaat onder andere uit het bieden van rechtszekerheid met betrekking tot AI-systemen, het bevorderen van innovatie en het leren op het gebied van regelgeving.²²⁷ Ook voor dit voorbeeld geldt dat deze juridische experimenteerruimte beperkt is tot de scope van de AI-verordening, te weten de ontwikkeling van AI-systemen en de data die daarbij hoort.

De VIE²²⁸, DV²²⁹ en DGV²³⁰ scheppen alle drie kaders voor experimentele toepassingen. Hetzij op het vlak van technische standaarden, hetzij op het gebied van juridische uitlegbaarheid in de vorm van het Europees Comité voor gegevensinnovatie. Alle drie op hun beurt ook binnen de kaders van de specifieke verordeningen en daarmee niet uniform toepasbaar op de gehele informatiehuishouding van de overheid.

5.4.6. Concluderend

Er is juridische ruimte voor innovatie, pilots en experimenten. Die ruimte is echter wel, zoals op andere vlakken in dit rapport ook geconstateerd, zeer gefragmenteerd en niet systematisch inzetbaar voor de gehele informatiehuishouding van de overheid. Op verschillende vlakken is het mogelijk om strikt gecontroleerd en gereguleerd te experimenteren. Bij alle mogelijkheden geldt echter de balans tussen fundamentele grondrechten die bij een democratische rechtsstaat horen, waaronder transparantie over overheidshandelen, en de mogelijkheid tot innovatie.

Feedbackloops, of evaluaties, ten aanzien van de innovaties en experimenten zijn in veel mindere mate aanwezig. Er kan gesteld worden dat Europese wetgeving wel steeds meer kaders schept, maar dat die kaders ook op het gebied van feedbackloops nog zeer minimaal zijn en zeker niet van dusdanig niveau dat ze systematisch en uniform van toepassing zijn op de informatiehuishouding van de overheid.

Een stevigere juridische verankering is wenselijk. Een efficiënte en effectieve overheidsbrede informatiehuishouding die ook gegevensdeling tussen verschillende overheden mogelijk moet maken, is juridisch complex. Om daarmee te kunnen experimenteren zijn juridische waarborgen nodig die niet alleen gefragmenteerd controle bieden, maar juist overheidsbreed controle bieden. De rapportageverplichting, de zorgplicht en de bronregistraties uit de Aiw kunnen hier mogelijk aan bijdragen.²³¹

²²⁶ Zie art. 57 AI-verordening.

²²⁷ Zie art. 57 lid 9 AI-verordening.

²²⁸ Zie art. 10 Verordening Interoperabel Europa.

²²⁹ Zie art. 42 Dataverordening.

²³⁰ Zie art. 29 Datagovernanceverordening.

²³¹ Zie art. 6, 7 en 14 Algemene informatiewet overheid.

5.5. Professionalisering en vakmanschap

5.5.1. Toelichting deelvraag

In deze paragraaf staat de vraag *“zijn er juridisch bindende maatregelen voor permanente ontwikkeling van informatieprofessionals?”* centraal. Deze paragraaf biedt inzicht in een ander belangrijk aspect van een consistente en goed uitvoerbare informatiehuishouding, te weten de permanente ontwikkeling van personen die met, in of voor de informatiehuishouding werkzaam zijn.

Ook hier is de conclusie dat er geen systematische en overheidsbrede bindende maatregelen bestaan die informatieprofessionals verplichten tot permanente ontwikkeling. Toch zijn er wel aanwijzingen in de wet te vinden die voor specifieke functies en sectoren educatieverplichtingen in zich hebben. Zowel expliciet als meer impliciet.

Gelet op de personen die werken aan de informatiehuishouding van de overheid kan gesteld worden dat velen van hen ambtenaren zijn en als zodanig ook gereguleerd worden door de Ambtenarenwet 2017. Die wet regelt de arbeidsverhouding tussen personeel en overheidswerkgevers in algemene zin, maar bevat geen expliciete bepalingen over permanente ontwikkeling of scholing. Laat staan permanente ontwikkeling specifiek voor informatieprofessionals. Naast de Ambtenarenwet is ook de Cao Rijk van toepassing. De cao biedt ruimte voor ambtenaren om zichzelf te ontwikkelen en geeft hen recht op studie en opleiding.²³² Dit recht is echter van dusdanige algemene aard dat er niet gesteld kan worden dat dit een juridisch bindende maatregel tot permanente educatie is. Decentrale overheden kennen soortgelijke cao-bepalingen waarin scholing en ontwikkeling als recht wordt aangeboden en wordt gestimuleerd, maar permanente educatie niet verplicht wordt gesteld.²³³

Informatieprofessionals binnen de overheid vallen niet onder een verplichte beroepsregistratie waaruit de verplichting tot permanente educatie volgt, zoals die bijvoorbeeld bij advocaten of artsen wel het geval is. Toch zijn er wel enkele specifieke functies die raken aan de informatiehuishouding en meer wettelijke kaders kennen.

5.5.2. Functionaris gegevensbescherming

Zodra gegevens kwalificeren als persoons- of politiegegevens, vallen deze binnen het overheidsdomein onder toezicht van een functionaris gegevensbescherming. De rol en taken van de functionaris gegevensbescherming zijn wettelijk verankerd, maar expliciteren geen permanente educatie.²³⁴ De AVG impliceert wel dat deze functie kennis van wetgeving en het toezichtsdomein vereist, maar gaat daarbij niet nadrukkelijk in op specifieke kennis of permanente educatie ten aanzien van de informatiehuishouding. Qua permanente educatie is er inmiddels wel, met steun van het ministerie van Justitie en Veiligheid, een initiatief gestart om dit te professionaliseren.²³⁵

²³² Zie CAO Rijk 2024-2025, paragraaf 12.3.

²³³ Zie bijvoorbeeld artikel 8.4 Cao Gemeenten 2025-2027 en hoofdstuk 9 Cao provinciale sector.

²³⁴ Zie artikel 37 en verder Algemene verordening gegevensbescherming.

²³⁵ In de vorm van het Nederlands Register voor Functionarissen voor Gegevensbescherming, zie ook www.nrfg.nl.

5.5.3. Archiefprofessionals

Naast de functionaris gegevensbescherming zijn er ook professionals in het archiefdomein. De rol van deze archiefprofessionals is minder strak omlijnd dan die van de functionaris gegevensbescherming. Hoewel de Archiefwet overheden verplicht om overheidsinformatie adequaat te beheren, bevat de wet zelf geen bepalingen over de kwalificaties of scholing van de professionals die dit beheer uitvoeren. Gelijk aan het initiatief voor functionarissen gegevensbescherming is er op het vlak van archiefprofessionals beweging vanuit een beroepsvereniging om permanente educatie te ontwikkelen. Deze beweging is niet juridisch geborgd.²³⁶

5.5.4. Chief Information Officer

Met de toenemende hoeveelheid data en toepassingen daarvan neemt de rol van de CIO ook toe in waarde. De kennisborging en permanente educatie van CIO's is niet juridisch geborgd. Er bestaat geen wettelijk kader waarbinnen de scholing en ontwikkeling van CIO's is geborgd ten aanzien van de overheidsbrede informatiehuishouding.

5.5.5. Chief Information Security Officer

De CISO kent een kader als het gaat om taken en bevoegdheden. Deze zijn terug te vinden in de BIO.²³⁷ Wat dit kader echter niet doet, is eisen stellen aan de kwalificaties of permanente educatie van de CISO. Deze kaders worden ook in andere toepasselijke wet- en regelgeving op het domein van cybersecurity niet gesteld.

5.5.6. AI-verordening

Los van de functie die informatieprofessionals vervullen, zoals hierboven omschreven, verdient de AI-verordening op deze plek nog kort de aandacht. Deze verordening bevat een verplichting tot AI-geletterdheid.²³⁸ Deze verplichting is qua scope echter beperkt tot het gebruik van AI-systemen. Zodra deze systemen onderdeel uitmaken van de informatiehuishouding, dienen informatieprofessionals adequaat geschoold te zijn. De verplichting rust echter niet direct op de informatieprofessionals, maar op de werkgever van de professionals. De verplichting tot AI-geletterdheid bevat geen expliciete verplichting tot permanente educatie. Impliciet kan deze verplichting er wel uit afgeleid worden, aangezien er wordt gesteld dat rekening gehouden dient te worden met de context waarbinnen de AI-systemen gebruikt worden en de razendsnelle ontwikkeling van AI heeft aangetoond dat deze context zeer aan verandering onderhevig is.

5.5.7. Concluderend

Samenvattend ontbreekt het momenteel aan een stelsel van juridisch bindende maatregelen die informatieprofessionals binnen de overheid dwingen tot permanente educatie ten aanzien van de informatiehuishouding. Gelet op de toenemende mate van gegevensverwerkingen, het complexe juridische speelveld waarbinnen dit plaatsvindt en de maatschappelijke impact die het delen van gegevens binnen een adequate informatiehuishouding kan hebben, is het aan te raden om de wenselijkheid en uitvoerbaarheid van juridisch bindende maatregelen nader te onderzoeken.

²³⁶ Zie <https://www.kvan.nl/themas/permanente-educatie/> van de Koninklijke Vereniging van Archivarissen.

²³⁷ Zie Baseline Informatiebeveiliging Overheid 2 (BIO2), v.1.3, paragraaf 12.3.

²³⁸ Zie artikel 4 AI-verordening.

Concluderend

Het ministerie van BZK verzocht ICTRecht om een onderzoek en rapportage om inzicht te bieden in het huidige landschap aan (data)wet- en regelgeving in relatie tot de eigenschappen die een verbeterde informatiehuishouding van de overheid nodig heeft.

De kernvraag luidt: in hoeverre bestaande wet- en regelgeving ten aanzien van informatieobjecten de verbetering van de informatiehuishouding (belegd in de vijf pijlers) al realiseert of kan realiseren, ten opzichte van de conceptversie van de Aiw en de bedoelingen hierachter?

De doelen van de Aiw worden breed gedragen vanuit wet- en regelgeving, zowel vanuit de EU als binnen Nederland, als het gaat om het vrije verkeer van informatieobjecten en het opheffen van blokkades om gegevens te delen. De uitwerking van deze doelen is in het huidige juridische landschap te breed, complex en te gefragmenteerd. Dit zorgt ervoor dat het voor overheidsorganisaties in de praktijk niet mogelijk is om consequent helder antwoord te kunnen geven op de vraag of informatieobjecten of gegevens gedeeld moeten of mogen worden. Er zijn aanvullende inspanningen nodig om binnen het huidige landschap van beleid en wet- en regelgeving de informatiehuishouding van de overheid structureel te kunnen verbeteren. Elke alternatieve oplossing in het huidige landschap die informatiehuishouding kan verbeteren, is afhankelijk van het bestaande landschap van wetgeving. Daarom is (sectoraal) inzicht in de huidige stand van zaken onmisbaar en aanvullend een analyse of alle facetten gewenst zijn en bijdragen aan de doelen uit de nationale en Europese programma's. Op basis daarvan moeten volgende stappen worden bepaald, zoals het opstellen en handhaven van coherente sturingsmechanismen, uniforme begrippen en standaarden. Zonder inzicht blijft de simpele kernvraag uit de praktijk, "mag ik dit delen?", continu verschuiven.

De beredenering voor deze conclusie is hieronder samengevat op basis van de analyses in Pijler 1 tot en met 5.

Wil een overheidsorganisatie gegevens delen in de praktijk, zijn er twee vragen te beantwoorden. Vraag 1) *hoe* mag die overheidsorganisatie de informatie delen (op welke manier, over welke applicatie, met welke beveiliging) en vraag 2) *wat* mag of moet die overheidsorganisatie delen. Op die ene situatie is zowel op de vorm (vraag 1) als op de inhoud (vraag 2) veel verschillend beleid en wet- en regelgeving van toepassing.

Zowel de EU als Nederland verankeren in verschillende initiatieven de behoefte aan een vrij verkeer van gegevens (EU) en informatieobjecten (Nederland). Gezien de maatschappelijke, commerciële en persoonlijke waarde van gegevens, en om grondrechten te waarborgen, zijn er regels over wanneer gegevens wel of niet gedeeld mogen worden. Deze regels vormen, logischerwijs, een soort blokkade of in ieder geval een uitdaging ten aanzien van het realiseren van het eerdergenoemde vrije verkeer.

Hoewel er samenhang is tussen deze regels, is de dichtheid van regels zodanig hoog, zodanig sectorspecifiek en worden termen zodanig veel door elkaar gebruikt,

dat het zeer complex is om het gehele landschap van regelgeving over gegevensdeling helder te krijgen.

De complexiteit van dit landschap is niet recht te zetten met een wet in formele zin. Dit komt onder meer door het feit dat onderliggende wetten dezelfde termen ('informatie', 'document') afwijkende invulling toekennen. 'Informatieobject' als overkoepelende term lijkt geschikt. Het is echter niet helemaal duidelijk wat en welke juridische termen hier dan onder zullen vallen. In de praktijk is het dan lastig te zien hoe het kader van de Aiw samenvalt met bestaande regels en een passend overkoepelend kader neer kan zetten. Bovendien is de hiërarchie tussen wetten onduidelijk, waardoor er nog meer termen naast elkaar bestaan.

Een nieuwe Nederlandse wet in formele zin om de informatiehuishouding van de overheid te verbeteren is bovendien beperkt door hogere EU-wetgeving. De EU kent in haar regelgeving een structuur van gelaagdheid van eigen definities en kruisreferenties. Bovendien kan de Nederlandse overheid geen regels opstellen die in strijd zijn met de hogere Europese regels.

De moeilijkheid van het realiseren van het vrije verkeer van gegevens zit zowel in de complexiteit van regelgeving als in de striktheid van de regels zelf. Om te kunnen weten of de regels te strikt zijn, is inzicht nodig in de van toepassing zijnde wet- en regelgeving. Zo zou bijvoorbeeld verzocht kunnen worden om een specifieke wettelijke grondslag om persoonsgegevens voor doel A te gebruiken, wat inmiddels ook al gebeurt. Een dergelijk verzoek kent echter geen waarde zonder helderheid of en hoe de bestaande wetgeving van toepassing is.

Het toevoegen van meer regelgeving creëert eerder verwarring dan helderheid. Zonder dat de andere regels verhelderd worden, wordt het probleem verschoven dat de vragen (1) hoe gegevens gedeeld kunnen worden en (2) welke gegevens gedeeld mogen worden, geen antwoord hebben.

Buiten specifieke regels die aangeven wat een overheidsorganisatie wel of niet mag delen, zijn er verschillende initiatieven ter bevordering van een vrij verkeer van informatieobjecten. Het is niet duidelijk hoe deze met elkaar samenhangen en of alle organisaties achter de initiatieven op de hoogte zijn van elkaar.

Er is geen duidelijkheid over welke informatiestructuur (vraag 1) toegestaan is binnen en tussen overheidsorganisaties om informatieobjecten te delen. Het is daarom ook niet duidelijk of bestaande structuren hieraan (volledig) voldoen.

Er gelden verschillende standaarden van technische vereisten per situatie en de samenhang daartussen is onduidelijk. Het is onduidelijk wanneer welke beveiligingsverplichtingen van toepassing zijn en wat toekomstige (nog niet definitieve) wetgeving verder oplegt qua beveiligingsnormen. Een infrastructuur opbouwen die aan toekomstige eisen voldoet is niet mogelijk. Het risico is dan dat er een infrastructuur wordt opgesteld die snel niet meer voldoet aan de eisen. Bovendien verplichten Europese regels 'passende maatregelen' ten aanzien van beveiliging. De invulling daarvan is niet eenduidig en organisatie- en sectorafhankelijk.

Zorgelijk is dat in de uitvoering van al deze regels over het delen van gegevens, of het mogelijk maken om gegevens te delen, het hogere doel vergeten lijkt te

zijn. In de regel gaat het om het beschermen van grondrechten, veiligheid voor de burger, bescherming van persoonsgegevens en het ontzorgen van de burger. De verwezenlijking van dergelijke ambities is geblokkeerd door de complexiteit van regelgeving. Die complexiteit veroorzaakt een verlamming: zelfs in situaties waarin het de burger, maatschappij en overheid ten goede kan komen, wordt er geen informatie meer gedeeld. Dit schaadt de hogere doelen van dit beleid en deze wet- en regelgeving.

Al deze bevindingen roepen om inzicht in de juridische brei aan wet- en regelgeving.

Inzicht door overzicht: technologische basis en juridische analyse per sector

Uiteindelijk is het relevant dat de overheid zoveel mogelijk ten dienste van de burger staat. Voor burgers telt het resultaat: eenvoudige, veilige en laagdrempelige communicatie met de overheid en een overheid die haar gegevens, wanneer nodig, veilig deelt ten behoeve van haar rechten en vrijheden. Dit realiseren begint bij het creëren van inzicht in de huidige stand van zaken, eerder dan het aanvullen van nieuwe regelgeving.

Toepasselijkheid van beleid en wet- en regelgeving is echter ook bij de overheid afhankelijk van de sector of het werkveld waarbinnen de behoefte is om gegevens te delen. De zorg, de opsporing en de financiële sector kennen specifieke regels voor gegevensdeling. Een algemeen overzicht van wetten en regelgeving is niet praktisch uitvoerbaar of in ieder geval te uitgebreid om in de praktijk toe te passen. Een gedetailleerde analyse van de van toepassing zijnde wetgeving per sector (zorg, openbaarheid bestuur, enzovoort) kan eerder inzicht bieden in wanneer in welke situatie voor welke soort overheidsorganisatie gegevens gedeeld mogen of moeten worden.

Dat inzicht moet zien op de vorm en de inhoud van de vraag welke gegevens hoe gedeeld mogen en/of moeten worden. Dat betekent dat allereerst duidelijk moet zijn onder welke technische standaarden (inclusief beveiligingsnormen) overheidsorganen informatieobjecten mogen delen. Op basis daarvan is een technische infrastructuur nodig die de uitwisseling van informatieobjecten faciliteert.

Een nieuwe wet in formele zin biedt meer verwarring tussen welke regels wanneer van toepassing zijn, de verhouding en gelaagdheid daartussen. Nieuwe regels gaan immers altijd gepaard met de al bestaande 'erfenis' aan regels over gegevensdeling. Nieuwe regels bieden alleen helderheid als het huidige gegevensdelingskader aan wet- en regelgeving buiten werking wordt gesteld of verhelderd is. Aangezien deze verweven is met veel andere bestaande regels en uitvoering daarvan, is dat geen optie. Als deze 'erfenis' blijft bestaan, wordt de vraag of, wat en hoe gedeeld mag worden alleen vooruitgeschoven, niet opgelost. Een overkoepelend systeem kan nieuwe initiatieven verder verankeren, maar omdat de onderliggende regelgeving hetzelfde blijft, blijft de erfenis onopgelost.

Daarom is het essentieel om inzicht te krijgen in welke regels van toepassing zijn op de vraag welke gegevens gedeeld moeten worden. Dit rapport verkent (zie Pijler 2 en 3) de huidige overlap en discrepantie in het regelgevingslandschap.

In de praktijk staan overheidsorganisaties voor de vraag “moet ik deze gegevens delen, en mag ik deze gegevens delen?”. Het inzicht en vertrouwen in het wet- en regelgevingskader moet zodanig zijn dat overheidsorganisaties op basis daarvan een analyse kunnen uitvoeren of zij gegevens in die situatie mogen of moeten delen en weten hoe ze dat (vorm) mogen doen. Op basis van praktijkvoorbeeldvragen moet de overheidsorganisatie (per sector) inzicht kunnen krijgen in haar opties. De technische infrastructuur hiervoor moet voldoen aan de overheidsbrede regels voor beveiliging en interoperabiliteit. Ervaring leert dat een decentrale aanpak hierbij wenselijker is.

Afkortingenlijst

Afkorting	Term
ACM	Autoriteit Consument en Markt
ACOI	Adviescollege Openbaarheid en Informatiehuishouding
ADR	Auditdienst Rijk
AI	Kunstmatige intelligentie
Aiw	Algemene informatiewet overheid
AMvB	Algemene maatregel van bestuur
AP	Autoriteit Persoonsgegevens
API	Application Programming Interface
AVG	Algemene verordening gegevensbescherming
Awb	Algemene wet bestuursrecht
Awgb	Algemene wet gelijke behandeling
B2B	Business-to-business
BIO 2	Baseline Informatiebeveiliging Overheid 2
BRP	Basisregistratie personen
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Cbw	Cyberbeveiligingswet
CCG	Centrale Commissie Gegevensgebruik
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
DGV	Datagovernanceverordening
DPIA	Data protection impact assessment
DSA	Digitaledienstenverordening
DUO	Dienst Uitvoering Onderwijs
DV	Dataverordening
EC	Europese Commissie
EDPB	European Data Protection Board
EHDS	European Health Data Space
eIDAS	electronic IDentification, Authentication and trust Services
EIF	European Interoperability Framework
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FDS	Federatief Datastelsel
FG	Functionaris gegevensbescherming
GGD	Gemeentelijke gezondheidsdienst
IBDS	Interbestuurlijke Datastrategie
ICO	Inkoopeisen Cybersecurity Overheid
IGJ	Inspectie Gezondheidszorg en Jeugd
IOE	Inspectie Overheidsinformatie en Erfgoed
IPO	Interprovinciaal Overleg
ISMS	Information security management system
MvT	Memorie van toelichting
NCSC	Nationaal Cyber Security Centrum
NDS	Nederlandse Digitaliseringsstrategie
NORA	Nederlandse Overheid Referentie Architectuur
ODR	Open Data-richtlijn
RDI	Rijksinspectie Digitale Infrastructuur
SVB	Sociale Verzekeringsbank
SZW	Sociale Zaken en Werkgelegenheid
Tw	Telecommunicatiewet
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
UWV	Uitvoeringsinstituut werknemersverzekeringen
VIE	Verordening Interoperabel Europa
VNG	Vereniging van Nederlandse Gemeenten
Wbni	Wet beveiliging netwerk- en informatiesystemen
Wdo	Wet digitale overheid
Wgds	Wet gegevensverwerking door samenwerkingsverbanden

Wgs	Wet gemeentelijke schuldhelpverlening
Who	Wet hergebruik van overheidsinformatie
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wob	Wet openbaarheid van bestuur
Woo	Wet open overheid
Wpg	Wet politiegegevens
Wwke	Wet weerbaarheid kritieke entiteiten
ZBO	Zelfstandig bestuursorgaan

Bijlagen

Bijlage 1: Overzicht begrippen 'informatieobject'

Regeling	Object	Begrippen	Wettelijke omschrijving
Algemene verordening gegevensbescherming	Bescherming van persoonsgegevens	Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
		Bestand	Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.
		Genetische gegevens	Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.
		Biometrische gegevens	Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.
		Gegevens over gezondheid	Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
AI-verordening	Regels voor AI-systemen	AI-systeem	Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.
		Trainingsdata	Data die worden gebruikt voor het trainen van een AI-systeem door de leerbare parameters hiervan aan te passen.
		Validatiedata	Data die worden gebruikt voor het verrichten van een evaluatie van het getrainde AI-systeem en voor het afstemmen van onder andere de niet-leerbare parameters en het leerproces ervan, om underfitting of overfitting te voorkomen.
		Validatiedataset	Een afzonderlijke dataset of deel van de trainingsdataset, als vaste of variabele opdeling.
		Testdata	Data die worden gebruikt voor het verrichten van een onafhankelijke evaluatie van het AI-systeem om de verwachte prestaties van dat systeem te bevestigen voordat het in de handel wordt gebracht of in gebruik wordt gesteld.

		Inputdata	Data die in een AI-systeem worden ingevoerd of direct door een AI-systeem worden verworven en op basis waarvan het systeem een output genereert.
		Biometrische gegevens	Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk persoon, zoals gezichtsafbeeldingen of vingerafdrukgegevens.
		Gevoelige operationele gegevens	Operationele gegevens met betrekking tot activiteiten op het gebied van preventie, opsporing, onderzoek of vervolging van strafbare feiten waarvan de openbaarmaking de integriteit van strafprocedures in het gedrang zou kunnen brengen.
		Niet-persoonsgebonden gegevens	Andere gegevens dan persoonsgegevens zoals gedefinieerd in art. 4, punt 1, van Verordening (EU) 2016/679.
		Deepfake	Door AI gegenereerd of gemanipuleerd beeld-, audio- of videomateriaal dat een gelijkenis vertoont met bestaande personen, voorwerpen, plaatsen, entiteiten of gebeurtenissen, en door een persoon ten onrechte voor authentiek of waarheidsgetrouw zou worden aangezien.
Dataverordening	Toegang tot en delen van data	Gegevens	Elke digitale weergave van handelingen, feiten of informatie en elke compilatie van dergelijke handelingen, feiten of informatie, ook in de vorm van geluids-, visuele of audiovisuele opnames.
		Metagegevens	Een gestructureerde beschrijving van de inhoud of het gebruik van gegevens die het vinden en gebruiken van die gegevens vergemakkelijkt.
		Niet-persoonsgebonden gegevens	<i>Gelijk aan definitie AI-verordening.</i>
Datagovernanceverordening	Hergebruik van bepaalde categorieën beschermde gegevens	Gegevens	<i>Gelijk aan definitie Dataverordening</i>
		Niet-persoonsgebonden gegevens	<i>Gelijk aan definitie AI-verordening.</i>
Wet hergebruik van overheidsinformatie	Hergebruik van overheidsinformatie	Document	a. door een met een publieke taak belaste instelling opgemaakt of ontvangen schriftelijk stuk of ander geheel of deel van vastgelegde gegevens, dat naar zijn aard verband houdt met de publieke taak van die instelling; b. door een overheidsonderneming opgemaakt of ontvangen schriftelijk stuk of ander geheel of deel van vastgelegde gegevens, dat naar zijn aard verband houdt met de dienstverlening in het algemeen belang van die overheidsonderneming; of c. door een publiek gefinancierde onderzoeksorganisatie opgemaakt of ontvangen schriftelijk stuk of ander geheel of deel van vastgelegde gegevens, dat naar zijn aard verband houdt met de geheel of gedeeltelijk publiek gefinancierde activiteiten van die onderzoeksorganisatie.
		Dynamische gegevens	Digitale documenten die frequent of in real time worden geactualiseerd, hoofdzakelijk

			vanwege hun volatiliteit of omdat ze snel verouderd zijn.
		Onderzoeksgegevens	Documenten in digitale vorm, anders dan wetenschappelijke publicaties, die: a. worden verzameld of geproduceerd tijdens wetenschappelijke onderzoeksactiviteiten; en b. als bewijs in het onderzoeksproces worden gebruikt, of waarvan binnen de onderzoeksgemeenschap algemeen wordt erkend dat ze noodzakelijk zijn om onderzoeksresultaten te valideren;
		Specifieke hoogwaardige dataset.	Document dat in een HVD-uitvoeringsverordening is aangemerkt als specifieke hoogwaardige dataset waarop die HVD-uitvoeringsverordening en hoofdstuk V van de richtlijn van toepassing zijn;
Wet overheid open	Openbaarmaking van overheidsinformatie	Document	Een door een orgaan, persoon of college als bedoeld in art. 2.2, eerste lid, opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college.
		Milieu-informatie	In dit hoofdstuk en de daarop berustende bepalingen wordt verstaan onder milieu-informatie: alle informatie, neergelegd in documenten, over: (verschillende toestanden, factoren, maatregelen, economische analyses en toestand van gezondheid ten aanzien van het milieu).
		Publieke informatie	Informatie neergelegd in documenten die berusten bij een orgaan, persoon of college als bedoeld in art. 2.2, eerste lid (bestuursorganen, Kamers en verenigde vergadering der Staten-Generaal, de Raad voor de rechtspraak en College van afgevaardigden, Raad van State, Algemene Rekenkamer, Nationale ombudsman).
Archiefwet 1995	Zorg voor archiefbescheiden	Archiefbescheiden	1°.bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten; 2°.bescheiden, ongeacht hun vorm, met overeenkomstige bestemming, ontvangen of opgemaakt door instellingen of personen, wier rechten of functies op enig overheidsorgaan zijn overgegaan; 3°.bescheiden, ongeacht hun vorm, welke ingevolge overeenkomsten met of beschikkingen van instellingen of personen dan wel uit anderen hoofde in een archiefbewaarplaats zijn opgenomen om daar te berusten; 4°.reproducties, ongeacht hun vorm, welke bij of krachtens de wet in de plaats zijn gesteld van de onder 1°, 2° of 3° bedoelde archiefbescheiden of welke op grond van het bepaalde in art. 7 zijn vervaardigd;
Wet gegevensverwerking door samenwerkingsverbanden	Gegevensverwerking binnen samenwerkingsverbanden	Gegevens	Persoonsgegevens en andere gegevens.
		Sturingsinformatie	Gegevens betreffende natuurlijke personen, rechtspersonen of fenomenen, inhoudende een eerste vermoeden dat sprake is van onrechtmatige activiteiten, of voornemens daartoe, op de bestrijding waarvan het

			samenwerkingsverband is gericht, met inbegrip van de onderliggende gegevens uit een risicoanalyse, ten behoeve van de uitvoering van publiekrechtelijke taken of uitoefening van publiekrechtelijke bevoegdheden.
Wet digitale overheid	Betrouwbare toegang tot elektronische dienstverlening	Identificatiemiddel	Middel waarmee een natuurlijke persoon zich elektronisch kan identificeren; middel dat persoonsidentificatiegegevens bevat en gebruikt wordt voor de authenticatie van een natuurlijke persoon, rechtspersoon of onderneming die toegang wenst tot elektronische dienstverlening.
Databankenwet	Bescherming van databanken	Databank	Een verzameling van werken, gegevens of andere zelfstandige elementen die systematisch of methodisch geordend en afzonderlijk met elektronische middelen of anderszins toegankelijk zijn en waarvan de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering.
		Informatie betreffende het beheer van rechten	Alle door de producent van een databank en zijn rechtverkrijgenden verstrekte informatie welke verbonden is met een exemplaar van een databank of bij het hergebruiken van een databank bekend wordt gemaakt, die dient ter identificatie van de databank, of informatie betreffende de voorwaarden voor het gebruik van de databank, alsmede de cijfers of codes waarin die informatie is vervat.
Wet bescherming bedrijfsgeheimen	Bescherming van bedrijfsgeheimen	Bedrijfsgeheim	Informatie die aan de volgende voorwaarden voldoet: a. zij is geheim in die zin dat zij, in haar geheel dan wel in de juiste samenstelling en ordening van haar bestanddelen, niet algemeen bekend is bij of gemakkelijk toegankelijk is voor degenen binnen de kringen die zich gewoonlijk bezighouden met dergelijke informatie; b. zij bezit handelswaarde omdat zij geheim is, en c. zij is door degene die daar rechtmatig over beschikt, onderworpen aan redelijke maatregelen, gezien de omstandigheden, om deze geheim te houden;
Wet politiegegevens	Verwerking van politiegegevens	Politiegegevens	Elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaken, bedoeld in de art. 3 en 4 van de Politiewet 2012 , met uitzondering van: de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften; de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in art. 1, eerste lid, onderdeel i, onder 1° en art. 4, eerste lid, onderdeel f, van de Politiewet 2012 ;
Wet justitiële en strafvorderlijke gegevens	Verwerking van justitiële gegevens	Justitiële gegevens	Bij algemene maatregel van bestuur te omschrijven persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafvordering, die in een gegevensbestand zijn of worden verwerkt.
		Strafvorderlijke gegevens	Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of

			langs geautomatiseerde weg in een gegevensbestand verwerkt.
		Persoonsdossier	Een gestructureerd dossier waarin zijn opgenomen de aan rechterlijke autoriteiten uitgebrachte rapporten over onderzoeken naar het gedrag of de levensomstandigheden van een natuurlijk persoon in verband met tegen hem aanhangige strafzaken, de tenuitvoerlegging van aan hem opgelegde straffen of maatregelen of zijn reclassering.
		Gerechtelijke strafgegevens	Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van het behandelen en beslissen van zaken waarop het Nederlandse strafrecht van toepassing is en die in een gegevensbestand zijn of worden verwerkt.
		Justitiële documentatie	Een samenhangende verzameling van op verschillende personen betrekking hebbende justitiële gegevens die langs geautomatiseerde weg wordt gevoerd.
		Documentatie persoonsdossiers	Een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsdossiers die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd.
		Gegevensbestand	<i>Gelijk aan AVG, aanpassing voor justitie.</i> Justitiële documentatie, persoonsdossiers, documentatie persoonsdossiers en elk ander gestructureerd geheel van justitiële of strafvorderlijke gegevens, gerechtelijke strafgegevens of tenuitvoerleggingsgegevens dat volgens bepaalde criteria toegankelijk is, ongeacht of dit geheel van gegevens gecentraliseerd of gedecentraliseerd is, dan wel verspreid op een functioneel of geografisch bepaalde wijze.
		Genetische gegevens	<i>Vrijwel gelijk aan definitie AVG.</i>
		Biometrische gegevens	<i>Vrijwel gelijk aan definitie AVG. Verandert voorbeeld van vingerafdrukgegevens (in AVG) naar "dactyloscopische gegevens".</i>
		Gegevens over gezondheid	<i>Gelijk aan definitie AVG.</i>
Wet basisregistratie personen	Basisregistratie persoonsgegevens	Basisregistratie	Gegeven over een ingeschrevene in de basisregistratie
		Persoonslijst	Het geheel van gegevens, bedoeld in art. 2.7, eerste lid , 2.69, eerste lid , en 2.84, eerste lid , over één persoon in de basisregistratie.
		Contactgegevens	Telefoonnummer en e-mailadres van de niet-ingezetene.
Verordening (EU) nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten	Juridische geldigheid van elektronische transacties	Elektronisch document	Elke inhoud die is opgeslagen in elektronische vorm, in het bijzonder tekst of geluid, beeld of audiovisuele opname.
Telecommunicatiewet	Regulering elektronische communicatie	Verkeersgegevens	Gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.
		Locatiegegevens	Gegevens die worden verwerkt in een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven.

		Elektronisch bericht	Tekst-, spraak-, geluids- of beeldbericht dat over een openbaar elektronisch communicatienetwerk wordt verzonden en in het netwerk of in de randapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald.
Wet algemene bepalingen burgerservicenummer	Omgang met BSN	Nummerregister	Het nummer dat deel uitmaakt van de beheervoorziening.
Verordening betreffende de Europese Ruimte voor gezondheidsgegevens (EHDS)	Delen van gezondheidsgegevens binnen de EU	Persoonsgegevens	<i>Gelijk aan definitie AVG</i>
		Gegevens over gezondheid	<i>Gelijk aan definitie AVG</i>
		Genetische gegevens	<i>Gelijk aan definitie AVG</i>
		Gegevens over gezondheid	<i>Gelijk aan definitie AVG</i>
		Gegevens	<i>Gelijk aan definitie Dataverordening</i>
		Persoonlijke elektronische gezondheidsgegevens	Gegevens over gezondheid en genetische gegevens die in elektronische vorm worden verwerkt.
		Niet-persoonsgebonden elektronische gezondheidsgegevens	Andere elektronische gezondheidsgegevens dan persoonlijke elektronische gezondheidsgegevens, met inbegrip van zowel gegevens die geanonimiseerd zijn zodat zij niet langer betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene") als gegevens die nooit betrekking hebben gehad op een betrokkene.
		Elektronische gezondheidsgegevens	Persoonlijke of niet-persoonsgebonden elektronische gezondheidsgegevens.
		Dataset	Een gestructureerde verzameling van elektronische gezondheidsgegevens.
		Dataset met een grote impact bestemd voor secundair gebruik	Een dataset waarvan het hergebruik aanzienlijke voordelen met zich meebrengt vanwege de relevantie ervan voor gezondheidsonderzoek.
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg	Beschermt zorggegevens bij elektronische uitwisseling	Dossier	De schriftelijk of elektronisch vastgelegde gegevens met betrekking tot de verlening van zorg aan een cliënt.
Wet op de inlichtingen- en veiligheidsdienst 2017	Regelt bevoegdheden van de AIVD en MIVD ter bescherming van nationale veiligheid.	Gegevens	Persoonsgegevens en andere gegevens
		Persoonsgegevens	<i>Gelijk aan definitie AVG.</i>
Algemene wet bestuursrecht		Besluit	Een schriftelijke beslissing van een bestuursorgaan, inhoudende een publiekrechtelijke rechtshandeling.

Bijlage 2: Overzicht van zorgplichten bij Pijler 3

Hieronder volgt een overzicht met wet- en regelgeving waarin zorgplichten zijn opgenomen die van toepassing (kunnen) zijn voor de overheid in verband met het borgen van juistheid, privacy, beveiliging en goed beheer (governance) van informatie. Dit overzicht geeft een indicatie van de hoeveelheid en de globale strekking van algemene en sectorale wet- en regelgeving waarin zorgplichten zijn vervat die van belang zijn voor het borgen van een goede informatiehuishouding. Het overzicht is indicatief en niet uitputtend.

Internationale verdragen

Naam	Omschrijving zorgplicht(en)	Artikel(en)
Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)	Bescherming van privéleven, woning en correspondentie (privacy).	8
	Vrijheid van meningsuiting en informatiegaring.	10
	Verbod op ongerechtvaardigde discriminatie op basis van geslacht, ras, huidskleur, taal, religie, politieke of andere opvatting, nationale of sociale afkomst, het behoren tot een minderheid, eigendom, geboorte of andere status.	14
	Algemene systematiek EVRM: geen beperking of inmenging van overheidswege tenzij noodzakelijk en proportioneel voor specifieke doelen die in het EVRM zelf zijn genoemd.	
Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR)	Geen arbitraire of onnodige inmenging in privacy, familie, woning of correspondentie en geen onrechtmatige aanvallen op eer en reputatie.	17
	Vrijheid van meningsuiting, inclusief vrijheid om informatie en ideeën te zoeken, ontvangen en verschaffen, via ieder medium naar keuze.	19
	Verbod op ongerechtvaardigde discriminatie op basis van ras, huidskleur, geslacht, taal, religie of sociale afkomst.	4
Handvest van de grondrechten van de Europese Unie (Handvest EU of EU-grondrechtenhandvest).	Recht op bescherming van persoonsgegevens en toezicht door een onafhankelijke autoriteit.	8
	Vrijheid van meningsuiting en van informatiegaring.	11
	Verbod op ongerechtvaardigde discriminatie op basis van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of overtuigingen, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele geaardheid.	21
Verdrag 108 van de Raad van Europa	Persoonsgegevens moeten juist zijn en waar nodig up-to-date gehouden worden.	5

	De vereisten in dit verdrag vormen een belangrijke basis voor de AVG en de beginselen en vereisten voor verwerking van persoonsgegevens daarin.	
--	---	--

Europese verordeningen

Naam	Omschrijving zorgplicht(en)	Artikel(en)
Algemene verordening gegevensbescherming (AVG)	Algemene beginselen voor verwerking van persoonsgegevens, waaronder juistheid, doelbinding, opslagbeperking, integriteit en vertrouwelijkheid, verantwoordingsplicht. Verplichting om verwerking van persoonsgegevens te baseren op (ten minste) een van de zes wettelijke grondslagen, zoals toestemming, uitvoering van een overeenkomst met de betrokkene of noodzaak voor legitiem belang. Verplichtingen om transparante informatie te verschaffen over verwerking van persoonsgegevens. Verplichting om te kunnen aantonen dat verwerking van persoonsgegevens voldoet aan de AVG. Verplichting om privacy by design & by default toe te passen. Verplichting om persoonsgegevens passend te beveiligen in verhouding tot risico's. Verplichting om inbreuken in verband met persoonsgegevens te melden bij toezichthouder en/of betrokkenen. Vaststellen of verwerking van persoonsgegevens leidt tot hoge risico's voor betrokkenen en maatregelen treffen om risico's te beperken en om aan te tonen dat de verwerkingen aan de AVG voldoen.	5 6 12 t/m 15 24 25 32 33 en 34 35
AI-verordening	Geen verboden AI-praktijken toepassen. Maatregelen treffen om vast te stellen of AI-systemen een hoog risico hebben en vereiste maatregelen nemen om risico's te verminderen tot een acceptabel niveau, waaronder het risico op bias of vooringenomenheid en discriminatie die daaruit voort kan vloeien. Transparantie en informatieverstrekking.	5 6 t/m 27 Bijlage I Bijlage III 13, 50
eIDAS-verordening (Versie 2.0 sinds 2024)	Aanbieders van elektronische identificatie-, authenticatie- en vertrouwensdiensten zijn verplicht om cyberbeveiligingsvoorschriften na te leven. Aanbieders van vertrouwensdiensten en van EUDI-wallets zijn verplicht om significante incidenten te melden aan de toezichthouder en lidstaten moeten	1 13, 46 bis en

Europese richtlijnen

Naam	Omschrijving zorgplicht(en)	Artikel(en)
NIS2-richtlijn (of tweede richtlijn beveiliging netwerk- en informatiesystemen)	Essentiële en belangrijke entiteiten zijn verplicht om passende en evenredige, technische, operationele en organisatorische maatregelen te treffen om beveiligingsrisico's voor netwerk- en informatiesystemen te beheren en incidenten te voorkomen of de gevolgen daarvan te beperken.	21
Richtlijn weerbaarheid kritieke entiteiten	Kritieke entiteiten moeten risicobeoordelingen uitvoeren om risico's te identificeren die het leveren van essentiële diensten kunnen verstoren, technische en organisatorische beveiligingsmaatregelen nemen om hun weerbaarheid te vergroten en aanzienlijke versturende incidenten rapporteren aan nationale entiteiten.	12, 13, 15

Nederlandse (uitvoerings)wetten

Naam	Omschrijving zorgplicht(en)	Artikel(en)
Grondwet	Vrijheid van meningsuiting	7
	Bescherming persoonlijke levenssfeer en persoonsgegevens	10
	Verbod op discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, handicap, seksuele gerichtheid	1
Algemene wet gelijke behandeling	Verbod op het maken van onderscheid tussen mensen op basis van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat.	5, 6, 7
Uitvoeringswet AVG (UAVG)	Uitzondering van verbod om biometrische gegevens te verwerken voor unieke identificatie, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.	29
Wet politiegegevens (Wpg)	Verwerkingsverantwoordelijke en verwerker treffen passende technische en organisatorische maatregelen om te waarborgen en aan te kunnen tonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met de Wet politiegegevens. Dit is een brede zorgplicht die zowel bescherming van privacy als informatiebeveiliging bevat, inclusief het aantonen daarvan.	4a
Uitvoeringswet Cyberbeveiligingsverordening (nog definitief vast te stellen)	De minister van Economische Zaken en Klimaat is aangewezen als nationale certificeringsautoriteit voor cyberbeveiliging. De Woo is uitgesloten van toepassing op cyberbeveiligingscertificaten voor zekerheidsniveau hoog.	2
Uitvoeringswet Verordening cyberweerbaarheid (nog definitief vast te stellen)	De minister van Economische Zaken is aangewezen als aanmeldende autoriteit (als bedoeld in art. 36, eerste lid	2

	Verordening cyberweerbaarheid) en als markttoezichtautoriteit (als bedoeld in art. 52, tweede lid Verordening cyberweerbaarheid).	
	De Raad voor Accreditatie beoordeelt en monitort certificeringsinstanties.	
Wet maatschappelijke ondersteuning (Wmo)	De minister van VWS kan beveiligingseisen vaststellen in lagere regelgeving waar verwerking van persoonsgegevens in verband met de uitvoering van de Wmo aan moet voldoen. Er lijkt momenteel geen lagere regelgeving te zijn aangenomen.	5.2.7
	De Wmo bevat verder diverse bepalingen over verplichten tot geheimhouding en uitzonderingen daarop.	3.4, 3a.2.1, 4.3.1, 5.2.6
Wet langdurige zorg (Wlz)	De wet geeft aan dat bij ministeriële regeling beveiligingseisen vastgesteld kunnen worden voor het gebruik van het burgerservicenummer door de Wlz-uitvoerder en aan de administratie daarvan. Dat is gebeurd in de Regeling gebruik burgerservicenummer in de zorg (zie verderop).	9.1.1
Wet elektronische gegevensuitwisseling in de zorg (Wegiz)	Gegevensuitwisseling wordt alleen aangewezen als de gegevens op het volledige traject tussen zender en ontvanger zijn beveiligd.	1.4
	Geheimhoudingsplichten zijn uitgezonderd van toepassing ten opzichte van ambtenaren die toezicht houden. Toezichthoudende ambtenaren hebben ook een geheimhoudingsplicht.	4.1
Wet op de geneeskundige behandelingsovereenkomst (Wgbo, BW 7, Afdeling 5)	Hulpverleners zijn verplicht te zorgen dat anderen dan de patiënt en degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelovereenkomst geen inzage hebben in gegevens uit het dossier, behalve met toestemming van de patiënt en behalve waar verstrekking wettelijk verplicht is. Deze zorgplicht impliceert ook een passende beveiligingsplicht, mede in verband met de AVG (art. 32).	7:457
	De Wgbo stelt een bewaartermijn verplicht van in principe 20 jaar voor het dossier met gezondheidsgegevens.	7:454
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)	Beveiligingseisen voor verwerking door zorgaanbieders van burgerservicenummer en dossier kunnen bij ministeriële regeling worden bepaald. Dat is gebeurd in de Regeling gebruik burgerservicenummer in de zorg (zie verderop).	10
	In deze wet is ook gedefinieerd wat een elektronisch uitwisselingssysteem is. Naar die definitie wordt in andere	1

	Het opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker is enkel toegestaan op grond van geïnformeerde toestemming als bedoeld in de AVG, behalve in specifieke uitzonderingsgevallen. Deze verplichting is in principe bedoeld voor websites en aanbieders van cookies en vergelijkbare technieken waarmee online gedrag kan worden gevolgd en geprofileerd, maar is techniekneutraal opgeschreven en breed toepasselijk op het opslaan en uitlezen van gegevens op randapparatuur van gebruikers. In het algemeen leidt dit tot een zorgplicht voor aanbieders van allerlei ICT-producten en -diensten om geïnformeerde toestemming te krijgen van gebruikers voor het opslaan of uitlezen van gegevens op apparatuur van eindgebruikers. Aanbieders van openbare telecommunicatienetwerken en -diensten zijn verplicht om hun diensten aftapbaar te maken en om verkeers- en locatiegegevens te bewaren voor een periode van twaalf maanden voor telefonie en zes maanden voor internettoegang. Daarbij zijn deze aanbieders ook verplicht om deze gegevens geheim te houden en te beveiligen tegen kennisname door onbevoegden.	11.7a Hoofdstuk 13
Wet bescherming bedrijfsgeheimen	Deze wet bepaalt dat het onrechtmatig is om bedrijfsgeheimen te verkrijgen of openbaar te maken zonder toestemming van de houder. Dit impliceert een zorgplicht om bedrijfsgeheimen geheim te houden en passend te beveiligen. Er zijn uitzonderingen opgenomen in verband met het onthullen van wangedrag, fouten of illegale activiteiten door klokkenluiders en het uitoefenen van de vrijheid van meningsuiting en vrijheid en pluralisme van de media. Hierbij wordt verwezen naar de Wet bescherming klokkenluiders (zie hieronder).	2 4
Wet bescherming klokkenluiders	Een werkgever waar ten minste vijftig werknemers werkzaam zijn, is verplicht een procedure vast te stellen voor het melden van een vermoeden van een misstand binnen zijn organisatie. Voor het instellen van de procedure moet ook de ondernemingsraad of andere personeelsvertegenwoordiging worden betrokken, of anders de instemming hebben van meer dan de helft van de werknemers. Meldingen moeten worden geregistreerd in een daarvoor ingericht register en gegevens in het register	2

	moeten worden vernietigd als deze niet meer noodzakelijk zijn om te voldoen aan de wet.	
Wet justitiële en strafvorderlijke gegevens (Wjsg)	De minister van Justitie en Veiligheid is verplicht om de nodige maatregelen te treffen om te borgen dat justitiële gegevens juist en nauwkeurig zijn en om passende technische en organisatorische maatregelen te treffen om te kunnen waarborgen en aantonen dat de verwerking van justitiële gegevens wordt verricht in overeenstemming met de toepasselijke wet- of regelgeving. Er zijn specifieke bewaartermijnen opgenomen voor justitiële gegevens.	3, 7 4
Burgerlijk Wetboek 7	Bij koop van een zaak met digitale elementen is de verkoper verplicht te zorgen dat beveiligingsupdates worden geleverd waar nodig om te zorgen dat de zaak aan de overeenkomst voldoet.	18

Lagere nationale uitvoeringsregels

Naam	Omschrijving zorgplicht(en)	Artikel(en)
Besluit beveiliging netwerk- en informatiesystemen (te vervangen door Cyberbeveiligingsbesluit en Besluit weerbaarheid kritieke entiteiten)	In dit besluit zijn vooral diverse aanbieders van essentiële diensten en andere vitale aanbieders in diverse relevante sectoren specifiek aangewezen, die onder de zorgplicht van de Wbni vallen.	2, 3
	De minister van BZK is bijvoorbeeld aangewezen als 'andere vitale aanbieder' wat betreft de centrale voorzieningen die in de Wet basisregistratie personen zijn aangewezen en voor uitgifte of activatie van elektronische authenticatiemiddelen en elektronische authenticatie via DigiD (bereikbaar via www.digid.nl).	
	In het voorgestelde Cyberbeveiligingsbesluit is de minister van Veiligheid en Justitie aangewezen als Cyber Security Incident Response Team (CSIRT) voor essentiële en belangrijke entiteiten.	2
	Verder is een aantal specifieke entiteiten uitgezonderd van diverse verplichtingen in de Uitvoeringsverordening NIS2 (2024/2690), waarin specifieke criteria zijn opgenomen om te bepalen wanneer er sprake is van een 'significant incident' waarop de meldplicht van toepassing is.	4
	Ter uitvoering van de zorgplicht in art. 21 van de Cbw is het vaststellen van een aantal specifieke beleidsstukken verplicht gesteld.	6 t/m 16
	Ook kan de minister in bepaalde specifieke omstandigheden bepaalde producten en diensten van leveranciers weren.	18
Besluit weerbaarheid kritieke entiteiten (Bwke)	In dit besluit is op een aantal punten specifieke invulling gegeven aan	3 t/m 14

	verplichtingen in de Wet weerbaarheid kritieke entiteiten, waaronder de uitvoering van risicoboordelingen en de maatregelen ter uitvoering van de zorgplicht in art. 15 van de Wwke, zoals identificatie van kritieke infrastructuur, verwerving, ontwikkeling, onderhoud, herstel en beëindiging van kritieke infrastructuur, rechtstreekse leveranciers, fysieke bescherming van gebouwen en kritieke infrastructuur, crisismanagement, toegang tot en rubricering van gevoelige informatie, het weren van producten en diensten van leveranciers en evaluatie van de maatregelen. Daarnaast zijn nog enkele aanvullende details opgenomen over de meldplicht voor aanzienlijke verstoringen. Tot slot zijn bewaartermijnen voor persoonsgegevens vastgesteld ter uitvoering van taken onder de Wwke. Dat is niet langer dan noodzakelijk en in elk geval binnen 60 maanden na eerste verwerking en 120 maanden voor de gegevens die de bevoegde autoriteit verwerkt.	16 en 17 19
Cyberbeveiligingsregeling sector overheid (voorstel)	De Cyberbeveiligingsregeling sector overheid werkt regels van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit verder uit voor de overheidssector. Als Computer Security Incident Response Team (CSIRT) is de informatiebeveiligingsdienst (Ibd), onderdeel van VNG Realisatie B.V. voor gemeenten en gemeenschappelijke openbare lichamen onder de Wet gemeenschappelijke regelingen aangewezen. Voor invulling van de zorgplicht voor informatiebeveiliging zijn de BIO 2 en ISO 27001 (2023-versie) en 27002 (2022-versie) aangewezen. Ter invulling van de meldplicht en het begrip 'significant incident' zijn specifieke criteria vastgesteld voor enerzijds centrale overheden en anderzijds decentrale overheden.	3 6 9 en 10
Besluit aanwijzing CSIRT voor digitale diensten en vaststelling tijdstip inwerkingtreding Wet en Besluit beveiliging netwerk- en informatiesystemen	In dit besluit is de minister van EZK aangewezen als het CSIRT voor digitale diensten als bedoeld in art. 4, tweede lid onderdeel b van de Wbni.	1
Besluit beveiligde verbinding met overheidswebsites en -webapplicaties	In dit besluit is een standaard opgenomen als bedoeld in art. 3 Wdo voor de beveiligde verbinding van overheidswebsites en webapplicaties. Hierin is HTTPS als vastgelegd in IETF RFC 9110	1 en 2

	voorgeschreven en Transport Layer Security (TLS), versie 2.1.1.	
Regeling voorzieningen Wdo	In deze regeling is vastgelegd hoe een rechthebbende als gebruiker een DigiD kan aanvragen, voor de verschillende betrouwbaarheidsniveaus. Verder is omschreven hoe DigiD Machtigen kan worden aangevraagd en gebruikt en hoe MijnOverheid kan worden gebruikt.	3 4 en 5
Regeling gebruik burgerservicenummer in de zorg	In deze regeling is bepaald dat NEN 7510 en de uitwerking daarvan in de NEN 7511 en 7512 moet worden toegepast voor beveiliging van diverse gegevensverwerkingen in de zorg.	2
Besluit elektronische gegevensverwerking door zorgaanbieders	Dit besluit verplicht toepassing van NEN 7510 en 7512 voor (1) de verantwoordelijke voor een elektronisch uitwisselingssysteem en (2) de zorgaanbieder bij gebruik van een zorginformatiesysteem. Bij het vastleggen van beleid, procedures en verantwoordelijkheden zijn de verantwoordelijke voor een elektronisch uitwisselingssysteem en de zorgaanbieder verplicht om de termen en definities te gebruiken als genoemd in NEN 7510, NEN 7512 of NEN 7513. Logging van een elektronisch uitwisselingssysteem moet voldoen aan NEN 7513. De termen 'elektronisch uitwisselingssysteem' en 'zorginformatiesysteem' zijn beide gedefinieerd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.	3 4 5