Bijlagen

Inventarisatie standaardisatie

30 augustus 2019

Versie | **1.0**

Projectnummer | **20196050**

VERDONCK KLOOSTER & ASSOCIATES

Berenschot

Inventarisatie standaardisatie

Bijlagen

30 augustus 2019

Versie | **1.0**
Projectnummer | **20196050**

Inhoudsopgave bijlagen

A. Nadere uitwerking analysemodel 6

A.1 Standaardisatie om een doelstelling te bereiken: een proces in vijf stappen 6
A.2 Proces 7
A.3 Inhoud 8
A.4 Eén analysekader voor standaardisatie 9
A.5 Interventiestrategieën 10

B. Onderzoeksopzet en bronnen 12

B.1 Samenstelling begeleidingscommissie 13
B.2 Lijst geïnterviewden 13
B.3 Documentatie 14

C. Casuïstiek 15

C.1 Schuldhulpverlening 16
C.2 Phishing 18
C.3 Omgevingswet 20
C.4 Standard Business Reporting (SBR) 23
C.5 Regie op eigen gegevens 27

D. Observaties over adoptie 30

D.1 Observaties over speelvelden 31
D.2 Observaties over coalities 31
D.3 Observaties over spelregels en werkwijzen 31
D.4 Observaties over kennis 32
D.5 Observaties over gedragen richtingen 33
D.6 Observaties over besluiten en resultaten 33

E. Analyse wetgeving en standaardisatie 34

E.1 Huidige praktijk standaardisatie: 'Pas Toe of Leg Uit' 35
E.2 Ontwikkeling richting een gedeeltelijke de jure standaardisatie 35
E.3 EU-praktijk op het gebied van standaardisatie 37
E.4 Sectoraal reeds verplichte standaardisatie (buiten het werkveld van BZK) 38
E.5 Toezicht 38
E.6 Analyse: De rol van wet- en regelgeving bij adoptie van standaarden 40

F. Wetgeving die beleidsdoelen uit NL DIGIbeter raakt 42

F.1 E-overheid in Europa (Tallinnverklaring) 43
F.2 Wetsvoorstel modernisering elektronisch bestuurlijk verkeer 43
F.3 Algemene verordening Gegevensbescherming (AVG) 44
F.4 Verordening: Single digital Gateway (EU 2018/1724) 44
F.5 Wet basisregistratie personen (Wet BRP) 46
F.6 ePrivacy Verordening 46

Nadere uitwerking analysemodel

Bijlage A

A.1 Standaardisatie om een doelstelling te bereiken: een proces in vijf stappen

Standaardisatie staat altijd ten dienste van een (beleids) doelstelling en de standaard zelf is dus een middel waaraan partijen zich committeren om een gezamenlijk doel te bereiken. Om een uitspraak te kunnen doen over het type interventie dat nodig is om een doelstelling van NL DIGIbeter te bereiken met behulp van standaardisatie, is het noodzakelijk om een beschouwingsmodel te hanteren voor de standaardisatietrajecten die met die doelstelling samenhangen.

Het model wat wij hiervoor gebruiken kent twee invalshoeken: het standaardisatieproces en de standaard zelf. Door de combinatie van deze invalshoeken toe te passen op de vraagstukken van NL DIGIbeter kan per doelstelling worden aangegeven welke interventies aangewezen zijn gezien de fase van het standaardisatieproces. Ook kan per laag van de standaard in kwestie de aanpak om tot afspraken te komen verschillend zijn. Dit hangt samen met het vraagstuk dat moet worden opgelost. Zo kan het zijn dat op men het snel eens kan worden over de technische invulling van een standaard maar veel discussie hebben over de organisatielaag, beleid en semantiek.

A.2 Proces

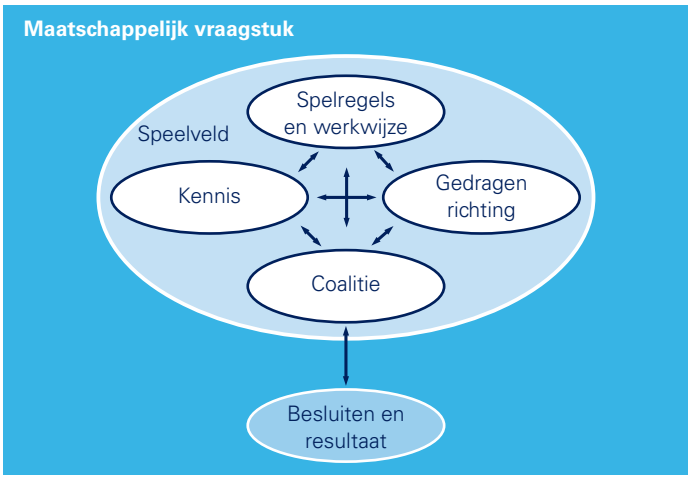
De eerste invalshoek is het proces om een doelstelling of maatschappelijk vraagstuk door middel van standaardisatie te helpen oplossen en de standaard te onderhouden (life cycle van standaardisatie). We noemen dit het standaardisatieproces maar het is meer dan alleen het opstellen van de inhoudelijke standaard zelf.

De life cycle kent op hoofdlijnen de volgende fasen die soms kort-cyclisch worden doorlopen (omdat de inhoud van de standaard interacteert met de oplossingsrichting en de randvoorwaarden):

1. Identificatie van het op te lossen (maatschappelijk) vraagstuk en overeenstemming over het probleem dat moet worden opgelost bij alle betrokken partijen.
2. Verkenning van de mogelijke oplossingsrichtingen en onderkennen van de rol van standaardisatie daarbij (overeenstemming over de oplossing) en de randvoorwaarden (waaronder die voor adoptie).
3. Het vormen van een coalitie met de betrokken belanghebbenden om tot standaarden te komen (waarbij alle vijf lagen aandacht krijgen), deze vast te stellen en te publiceren.
4. In gebruik nemen en toepassen van de standaarden (adoptiefase en netwerkeffect).
5. Onderhouden van de standaard en evalueren van gebruik en waarde.

Het standaardisatieproces speelt zich af rond een maatschappelijk vraagstuk waarbij op vijf aspecten antwoorden van belang zijn:

- **Speelveld:** Zijn de juiste partijen betrokken bij het vraagstuk, welke inbreng en kennis hebben ze en wat dragen zijn bij?
- **Coalitie:** Wat is de leidende coalitie die verantwoordelijkheid neemt en komt tot besluiten?
- **Kennis:** Welke kennis is er over het vraagstuk en de oplossingsrichtingen en is daar overeenstemming over?
- In hoeverre is er een **gelijke gerichtheid** van de betrokken vanuit belangen en emoties op het vraagstuk?
- Hoe zijn door de coalitie **spelregels** en een **werkwijze** afgesproken om met elkaar samen te werken in het speelveld en tot gedragen besluiten te komen?



Figuur 1. **Arena-model van Berenschot.**

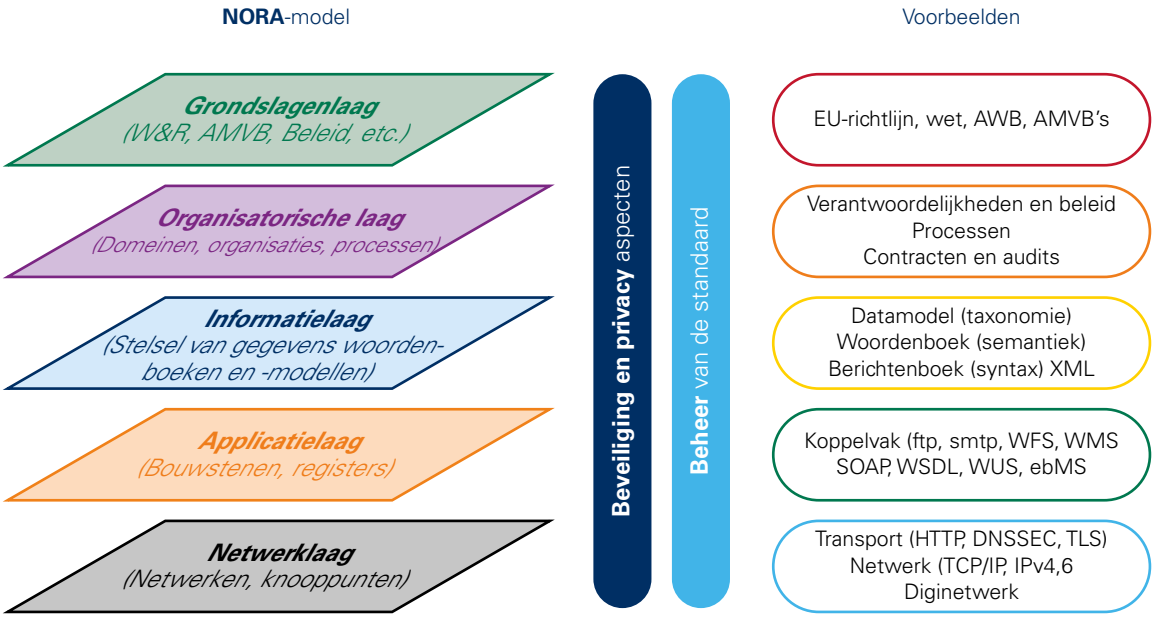
In de praktijk kunnen zich op al deze aspecten knelpunten voordoen waardoor standaardisatie niet van de grond komt:

- Het speelveld kan niet adequaat zijn ingericht: bij standaardisatie kan dat zich bijvoorbeeld uiten in onvoldoende aanhaking van het bestuurlijke niveau. Professionals die vanuit hun vakdiscipline uitstekende standaarden ontwikkelen, maar waarbij het risico bestaat dat zij andere belangen van de betrokken organisaties uit het oog verliezen. Of leveranciers die binnen een bepaalde standaardisatie community een te dominante rol spelen of juist niet zijn betrokken.
- Er is geen overtuigende coalitie te vormen die doorslaggevend is in een keten. Of de trekkers van de coalitie hebben te weinig mandaat en krijgen hun eigen organisaties niet mee in de voorgestelde oplossingsrichtingen.
- Gebrek aan een gedragen richting. De belangen van de betrokken spelers kunnen te veel uiteenlopen waardoor er bijvoorbeeld geen goede coalitie is te vormen om het probleem op te lossen of er geen besluiten kunnen worden genomen die tot resultaat leiden.
- Ook kennis is vaak het probleem. Het is in sommige gevallen onvoldoende duidelijk waar de schoen wringt en wat dan passende oplossingsrichtingen zijn. Of het is nog niet bekend wat in een bepaalde, op zichzelf duidelijke situatie zou helpen.
- Vaak ontbreekt het aan adequate spelregels en werkwijze. Er is geen goede agenda voorbereiding, besluiten worden niet vastgelegd of opgevolgd of er zijn te weinig middelen beschikbaar om de benodigde activiteiten uit te voeren.

De mate waarin deze aspecten bekend/onbekend, divergent/convergent zijn, bepalen de aard van het type standaardisatievraagstuk en dus wat daarbij passende interventiestrategieën zijn. We werken dit uit in de paragraaf interventiestrategieën.

A.3 Inhoud

Anderzijds kan de standaard zelf inhoudelijk worden beschouwd op vijf lagen van interoperabiliteit waarop die standaard zich richt. We hanteren in dit onderzoek het vijflaagsmodel van de NORA.



Figuur 2. **Vijflaagsmodel van de NORA.**

- De onderste **Netwerklaag** is die van de connectiviteit; de standaarden om knooppunten in het netwerk veilig met elkaar te verbinden (bijvoorbeeld het internetprotocol). Ook de netwerkbeveiliging zit in deze laag.
- De tweede **Applicatielaag** gaat over het koppelvlak voor interoperabiliteit op systeemniveau; ze bevat de registers, bouwstenen en voorzieningen en hun koppelvlakken en service afspraken (incl. beveiliging).
- De derde **Informatielaag** gaat over de woordenboeken, informatiemodellen of taxonomieën waarin de betekenis is beschreven in een bepaald format. Op de informatielaag is onderscheid te maken tussen semantische afspraken (betekenis van data) en de technische datamodellen of berichtenboeken voor gegevensuitwisseling waarin de syntax afspraken (structuur van de data) ook zijn opgenomen.
- De vierde **Organisatorische laag** gaat over de afspraken (beleid), besturing en processen van de uitwisseling; verantwoordelijkheden, wijzigingsprocessen, producten en diensten, aansluitvoorwaarden en dergelijke (bijvoorbeeld zoals in het stelsel van basisregistraties).
- De vijfde **Grondslagenlaag** tenslotte gaat over de wetgeving op basis waarvan de standaard wordt toegepast; de juridische basis voor het gebruik van de uit te wisselen gegevens (bijvoorbeeld de wet basisregistratie personen of een opsporingsbevoegdheid).

Over al deze lagen heen spelen de aspecten Beveiliging en Privacy binnen de standaard en Beheer van de standaarden of afsprakenstelsels (versies, onderhoud, backward compatibility, etc.).

Met dit vijflaagsmodel kunnen we per standaard of een toepassingsprofiel van standaarden voor een concreet maatschappelijk vraagstuk aangeven op welke lagen de standaarden hun werking hebben en kunnen we standaarden vergelijken op deze aspecten. In principe kent iedere nieuwe standaard voor gegevensuitwisseling een invulling op alle vijf de lagen maar vaak worden bepaalde lagen ingevuld met bestaande standaarden en voegt de nieuwe standaard slechts op een bepaalde laag iets nieuws toe. Dit bepaalt dan de echte toegevoegde waarde van de standaard.

Als het om een samengestelde set standaarden gaat met een specifieke doelstelling en organisatorische maatregelen dan spreekt men ook wel van een afsprakenstelsel.

A.4 Eén analysekader voor standaardisatie

Op grond van deze modellen en aangetroffen best practices om tot standaarden te komen, kan geen vast recept worden voorgeschreven voor standaardisatie. Ieder vraagstuk kent zijn eigen unieke omstandigheden en context, maar er zijn wel controlevragen af te leiden die helpen bij het identificeren van de activiteiten die moeten worden gestart om een volgende stap te zetten.

Deze controlevragen zijn de volgende:

1. Is duidelijk bij alle betrokkenen voor welk doel of gemeenschappelijk (strategisch) vraagstuk de standaardisatie tot stand moet komen? Is dit doel helder geformuleerd en is duidelijk welke bijdrage de standaardisatie moet gaan leveren?
2. Is het speelveld in kaart gebracht, wie zijn betrokken in de coalitie en in welke (initiatief nemende, faciliterende of volgende) rol? Welke belangen spelen er (stakeholderanalyse)? Gaat het om een keten of een sector overstijgend of internationaal vraagstuk? Ligt het initiatief bij de overheid of niet?
3. Zijn de partijen gecommitteerd aan het bereiken van het doel? Is duidelijk waar kosten en baten liggen? Wie heeft de pijn als er niks gebeurt en wie heeft de pijn als er juist wel iets gebeurt?
4. Welke governance (spelregels en werkwijze) is afgesproken om tot samenwerking en vertrouwen te komen?
5. Is er voldoende eenduidigheid over de oplossingsrichting (het soort standaard) in de coalitie?
6. Is er voldoende kennis over de oplossingsrichting (het soort standaard) in de coalitie?
7. Is sprake van nieuwe (experimentele) oplossingen of moet er rekening gehouden worden met bestaande (legacy) oplossingen of technische standaarden?
8. Op welke lagen richten de vraagstukken rond de inhoud van de standaard zelf zich? Is een analyse gemaakt van de uitdagingen per laag (ervaring leert dat iedere laag andere uitdagingen kent)? Zijn afspraken over juridisch kader, operationele toepassing, processen, connectiviteit en semantische interoperabiliteit (metadata) voldoende ingevuld?
9. Hoe is de vaststelling en het beheer van de standaarden open en transparant ingericht? Hoe wordt dynamiek in het speelveld en wijzigingsbehoefte of transitie naar de standaard ondersteund?
10. Is wetgeving nodig voor de adoptie en of juridische grondslag van de standaard?
11. Hoe wordt het al dan niet verplicht voldoen aan de standaard gecontroleerd (toelating tot het stelsel, audits, etc.)?
12. Hoe helpen stimuleringsmaatregelen of incentives bij gebruik en adoptie? (financieel, voorlichting en communicatie, verplichting/dwang, etc.)
13. Is sprake van een netwerkeffect en wat is dan de kritische massa?
14. Wat is de exit strategie als blijkt dat de standaard niet voldoende bijdraagt?

A.5 Interventiestrategieën

Gerichte interventiestrategieën om met behulp van standaardisatie beleidsdoelstellingen te realiseren, zijn te definiëren vanuit het soort probleem wat aan de orde is en vanuit de analyse hoe het speelveld rond een specifiek maatschappelijk vraagstuk is georganiseerd. Op hoofdlijnen bepaalt het aangrijpingspunt de meest passende interventiestrategie. Onderstaande hoofdstrategieën zijn vanuit deze gedachte te identificeren.

Een wezenlijk element bij vraagstukken rondom standaardisatie en oplossingsrichtingen is de mate waarin de handelende actor over handelingsruimte beschikt. Deze handelingsruimte kan beperkt zijn door bijvoorbeeld internationale afspraken en standaarden of historisch gegroeide situaties en investeringen. Dit laat onverlet dat het soms ook mogelijk is om in te grijpen op de vijf aspecten beschreven in onderstaande hoofdstrategieën door meer handelingsruimte te creëren of te pakken.

Interventies op gedragen richting: Als het knelpunt vooral veroorzaakt wordt door een gebrek aan gezamenlijk besef van de meest passende richting, zijn interventies gericht op gezamenlijke perspectiefontwikkeling het meest passend. Te denken valt aan interventies als visievormingstrajecten, marktverkenningen, maatschappelijke kosten- en batenanalyses waarmee met de betrokken stakeholders tot een gedeeld begrip van de probleemstelling en de oplossingsrichtingen wordt gekomen.

Bijvoorbeeld bij het thema ‘regie op gegevens’ is de aard groot en omvangrijk en verbonden aan een betrekkelijk urgent maatschappelijk probleem in de informatiesamenleving. De exacte oplossingen zijn nog niet helder. Een meer experimenterende en doelzoekende houding die gericht is op visie- en perspectiefvorming is dan passend.

Andersom kan het ook gaan om een betrekkelijk uitgekristalliseerd onderwerp zoals toegankelijke websites: iedereen ziet dat het nodig is, maar kosten en baten zijn voor sommigen nog niet voldoende in balans. Dan zou je aan een financieringsarrangement kunnen denken om die specifieke belangen dichter bij elkaar te brengen.

Interventies op kennis: Op het moment dat er eigenlijk onvoldoende kennis over het probleem en de oplossingsrichting is, past een innovatie- en leerstrategie het beste. Daarbij valt te denken aan interventies die gericht zijn op het uitvoeren van experimenten, het doen van onderzoek naar de problemen en mogelijke oplossingsrichtingen.

Bijvoorbeeld bij het thema Linked Open Data. In potentie is dit de basis voor veelbelovende technologische innovaties, maar voor veel bestuurders en managers is nog moeilijk te doorgronden wat dit kan brengen. Een passende strategie zou zich kunnen richten op voorbeeldtoepassingen creëren, protoytpes ontwikkelen, dan kan helder en tastbaar gemaakt worden wat zoiets kan brengen en daaromheen kennis – en awareness-sessies organiseren.

Interventies op speelveld: Als niet de juiste actoren zijn betrokken bij het standaardisatietraject, bijvoorbeeld als bepaalde belangen gaan overheersen, dan kan het verstandig zijn in te grijpen in de vormgeving van het speelveld. De vorming van adequate en goed functionerende (open) communities zijn vaak van wezenlijk belang bij standaardisatie vraagstukken.

Eén aspect van bijvoorbeeld de Common Ground-beweging bij gemeenten is dat gemeenten weer zelf aan het roer van hun informatievoorziening willen komen en zelf meer sturend kunnen optreden rond het gebruik van data, het inzetten van innovatieve oplossingen voor (nieuwe) maatschappelijke vraagstukken en het reduceren van de afhankelijkheid van leveranciers. Daarbij is nadrukkelijk gekozen om de meer traditionele gegevensuitwisseling en het repliceren van basisgegevens, op basis van StUF, los te laten en over te gaan op een open API-benadering binnen een overheidsbreed gegevenslandschap. Daarmee zijn ook de gremia waarin besloten wordt over koers en richting wezenlijk veranderd. Gemeenten nemen nadrukkelijk de regie, waarbij Samen Organiseren het vertrekpunt is en de VNG faciliteert.

Interventies op coalities: Uiteindelijk zijn er partijen nodig die voor de troepen uitlopen en als eerste bereid zijn te investeren in kennisontwikkeling maar ook toepassing van een bepaalde standaard. Terugkerend probleem bij standaardisatietrajecten is dat de baten pas verzilverd kunnen worden als een heel domein of sector er gebuik van maakt. Echter de pionier heeft de nadelen van een 'early adopter' (kinderziektes, lange tijd voordat ketenpartners overstappen, etc.).

Een goed voorbeeld is Standard Business Reporting (SBR). Door intensief de samenwerking te zoeken tussen accountants, intermediairs, softwareleveranciers en verschillende overheidsinstanties is op een organische wijze een brede 'community' met een veelheid aan instanties en personen binnen uiteenlopende sectoren van markt en overheid ontstaan. Als een vernieuwingsprogramma gestart en inmiddels als een 'onder architectuur' functionerend permanent samenwerkingsverband operationeel. De casus rond SBR is uitgewerkt in bijlage C.

Interventies op spelregels en werkwijze: Soms zijn de problemen meer technisch van aard en is er geen adequate procesvoering op het speelveld, de coalities, de beschikbare kennis en de gedragen richting waarheen het moet ontwikkelen. Ogenschijnlijk eenvoudige problemen waarvan ook helder is wat passende oplossingsrichtingen zijn komen dan niet van de grond. Interventies gericht op een goede procesvoering (adequate agendavorming, afstemming met betrokkenen, verslaglegging, opvolging van besluiten, etc.) kunnen dan wonderen doen, in het realiseren van voortgang. Bij vraagstukken waar deze interventies voor ingezet kunnen worden, is zowel het probleem als de oplossingsrichting helder en is men het eens dat er wat moet gebeuren. Het probleem is dat dit niet gebeurt, bijvoorbeeld omdat er geen geld is voor een programma of omdat er geen regie-organisatie is aangewezen.

Een best practice op het gebied van een interventie op werkwijze en spelregels is bijvoorbeeld Integrated Health Enterprise (IHE) in de zorg, een internationale strak geregisseerde en gefaciliteerde aanpak om tot standaarden in de zorg te komen.

Interventies op de besluiten en resultaten: Belangrijke succesfactor bij standaardisatie is de wijze waarop adequaat wordt gestuurd op de opvolging van de genomen besluiten zodat bredere resultaten worden bereikt. Als alle bovenstaande stappen zijn genomen, ligt er vaak nog een brede agenda om tot uiteindelijke adoptie te komen. Daarbij geldt dat standaardisatie vaak ingrijpt op de 'infrastructuur' van de bedrijfsvoering van organisaties. Adoptie van standaarden kan iets van de lange adem zijn, interventies die hierbij passen zijn bijvoorbeeld gericht op de planning en control cycli van organisaties en het opnemen van standaarden in investerings- en vernieuwingsagenda's door leveranciers. Het wettelijk verplicht stellen van standaarden kan in deze strategie ook passend zijn (als voldaan is aan een adequate invulling van de overige beschreven elementen), maar veelal als sluitstuk als de probleemstelling en de oplossingsrichting voor alle betrokkenen klip en klaar is.

Als het probleem en de oplossingsrichting helder is, is het ook van belang om vol te houden en tot implementatie te komen. Hierbij speelt soms dat leveranciers moeten investeren, maar ook willen terugverdienen. Sommige standaarden staan al jaren op de Pas toe of leg uit (PTOLU)-lijst van het Forum Standaardisatie, maar zijn onvoldoende opgenomen in inkoopvoorwaarden bij aanbestedingen

Onderzoeksopzet en bronnen

Bijlage B

De onderzoeksaanpak bestond uit drie fasen om tot een complete beantwoording van de vraag van de opdrachtgever te komen. Gedurende het onderzoek zijn de onderzoeksvragen verder afgepeld om tot een concreet en toepasbaar resultaat te komen.

Er is in dit onderzoeksrapport gekozen om de resultaten eerst te presenteren en de onderbouwing als bijlagen op te nemen als grondslag voor de resultaten.

Fase	Activiteit	Resultaat
1.Voorbereiding	Kick-Off	Afgestemde onderzoekopzet
		Samengestelde begeleidingcommissie met duidelijke rol
		Overeen gekomen interviewleidraad voor interviews
		Afgestemde lijst te interviewen personen
		Object van onderzoek vastgesteld
	Voorbereiding onderzoek	Documentstudie en oriëntatie op de vraag
		Ingeplannen van de interviews
2.Uitvoering	Interviews afnemen	30 interviews
	Aanvullende documentstudie	Aanvullende documenten (n.a.v. interviews) verzameld en opgenomen in documentstudie
	Uitwerken rapportage	Conceptrapportage opgesteld en tussentijdse afstemming met begeleidings-commissie
3. Afronding	Afstemmen concept rapportage	Conceptrapportage afgestemd, inclusief verbetervoorstellen begeleidingscommissie
	Definitieve rapportage	Definitieve rapportage opgeleverd

In dit onderzoek is nauw samengewerkt met de begeleidingscommissie en in meerdere iteraties is dit rapport tot stand gekomen. In de eerste fase is er afstemming geweest met de begeleidingscommissie voor het definitief maken van het plan van aanpak, de documenten die erbij hoorden en is de interviewlijst definitief gemaakt. In de tweede fase is er een afstemmingsoverleg geweest over de methodiek en modellen die door het onderzoeksteam zijn ontwikkeld en gebruikt. Ten slotte zijn er drie afstemmingsmomenten geweest om het eindrapport definitief te maken.

Het onderzoek is gestart in februari 2019 en de concept eindrapportage is opgeleverd op 26 juni 2019. Het definitieve rapport is op 22 augustus 2019 opgeleverd.

B.1 Samenstelling begeleidingscommissie

Naam	Functie
Rob Kuipers	Voorzitter begeleidingscommissie, Adviseur Rijksdienst
	Adviseur Nationaal Cyber Security Centrum
Michiel Steltman	Managing Director, DINL
Ludwig Oberendorff	Hoofd Bureau Forum Standaardisatie
Theo Peters	Unitmanager, VNG Realisatie

Katinka Petronia (BZK/DIO) nam deel aan de begeleidingscommissie als gedelegeerd opdrachtgever.

B.2 Lijst geïnterviewden

Nr.	Geïnterviewde	Organisatie
1		NCSC
2	Gertjan van den Akker	NEN
3	Douwe Leguit, Eric Brouwer	ICTU, Regie op Gegevens
4	Michiel Steltman	DINL
5	Ludwig Oberendorff	BFS
6	Theo Peters	VNG Realisatie
7	Ad Reuijl	CIP
8	Dennis de Wit	Drechtsteden
9	Rob van de Velde, Yvonne Verdonk	Geonovum
10	Peter van Dueren, Edwin Platier	Douane
11	Rob Verweij, Hans Sinnige	Stichting RINIS
12	Tie Tjee, Onno Gabel	IHE
13	Frans Hietbrink	Belastingdienst
14	Geert Nederhorst, Anna Wamelink	Logius
15	Jelle Attema, René Montenarie	ECP
16	Sander Middendorp	SBR Nexus
17	David de Nood	VNO-NCW
18	Maarten van Haasteren	Gemeente Amsterdam
19	Erwin Folmer	Kadaster
20	Wim van Nunspeet	CBS
21	Dirk Jan van Blijderveen	NOAB
22	Nicole Zwart, Katinka Petronia	BZK, dir DIO
23	Zohra Bouguillara, Munish Ramlal	Autoriteit Persoons-gegevens
24	Steven Gort	ICTU
25	Geerten van de Kaa	TU Delft
26	Maarten Hillenaar	Centric
27	Theo Hooghiemstra	MedMij
28	Frank Ossewaarde	Provincie Noord-Holland
29	Jan Middendorp	2e Kamer
30	Joost Sitskoorn	Evofenedex

B.3 Documentatie

In de tekst van het rapport wordt verwezen naar gebruikte documentatie. Onderstaand een kort overzicht van de belangrijkste bronnen die in dit onderzoek gebruikt zijn.

Nr.	Document	Context
1	NL DIGIbeter 2018	De Agenda Digitale Overheid, NL DIGIbeter, richt zich op de overheid en het contact met burgers en ondernemers. Deze Agenda Digitale Overheid is een agenda van alle overheden gezamenlijk en legt de verbinding met belangrijke publieke en private partners. Op basis van vijf thema's worden initiatieven genomen, kansen ontdekt en plannen gemaakt om de strategie concreet te maken. Parallel aan het afronden van dit rapport zijn in juli 2019 de geactualiseerde NL DIGIbeter en een brief aan de Tweede Kamer over regie op gegevens verschenen. Deze zijn in dit rapport niet verwerkt, de peildatum is 1 juli 2019.
2	Pas Toe Of Leg Uit Lijst (PTOLU)	De overheid stimuleert het gebruik van open ICT-standaarden, waarin afspraken zijn gemaakt over de manier om gegevens uit te wisselen. Binnen de publieke sector wordt gewerkt met aanbevolen (gangbare) open standaarden en verplichte open standaarden. Dat laatste gebeurt door middel van het 'pas toe of leg uit'-principe (PTOLU). Een overheidsorganisatie mag afwijken van de 'pas toe of leg uit'-lijst op het moment dat een open standaard tot problemen leidt. De organisatie moet dit wel uitleggen in het jaarverslag.
3	Generiek afsprakenstelsel voor data-deelinitiatieven als basis van de digitale economie	Onderzoek naar het bevorderen van datadelen in het MKB, in opdracht van het Ministerie van Economische Zaken en Klimaat. Dit onderzoek bevestigt dat de huidige 'infrastructuur' voor het op schaal en gestructureerd delen van data nog niet op orde is. Belemmeringen voor datadelen zijn vooral bewustwording en er zijn diverse technische-, juridische- en operationele belemmeringen. In het onderzoek wordt geadviseerd om een datadeelcoalitie op te zetten die kennis gaat delen en het voorstel gedaan om een generiek afsprakenstelsel voor data-deelinitiatieven op te zetten vanuit de markt waarmee de belemmeringen voor met name het MKB kunnen worden opgelost.
4	Wijzigingswet Open Overheid	Het voorstel verankert de toegang tot publieke informatie als recht van burgers. Daarnaast wordt de actieve openbaarheid versterkt door het verplicht stellen van openbaarmaking uit eigen beweging van bepaalde categorieën informatie. In de gewijzigde Woo worden specifieke informatiecategorieën benoemd, zoals besluitvorming, subsidies en informatieverzoeken, die elke overheid actief openbaar moet maken.
5	Wetsvoorstel Digitale Overheid	In het wetsvoorstel Digitale Overheid wordt de wettelijke basis gelegd voor de gehele generieke digitale infrastructuur (GDI). Onderdeel hiervan zijn regels over informatieveiligheid en privacy. Het wetsvoorstel biedt daarmee de grondslag om overheidsinstanties te verplichten open standaarden te gebruiken. Ook toezicht en handhaving krijgt hiermee een wettelijke basis. Hiermee wordt invulling gegeven aan de invulling van de één-overheids-gedachte, in het belang van de burger en ondernemer.
6	Algemene Leidraad voor maatschappelijke kosten-batenanalyse	In het beleid moeten keuzes worden gemaakt. Beleidsmaatregelen hebben veelal verschillende effecten. Om over een beleidsmaatregel te kunnen besluiten moeten ongelijksoortige voor- en nadelen tegen elkaar worden afgewogen. De maatschappelijke kosten-batenanalyse (MKBA) is een instrument dat een overzicht kan bieden van de voor- en nadelen van maatregelen, zo mogelijk gekwantificeerd en in euro's uitgedrukt en gepresenteerd als een saldo van baten minus kosten. In deze algemene MKBA-leidraad beschrijven we hoe een MKBA moet worden opgesteld en presenteren we de theoretische uitgangspunten van een MKBA.
7	Kader voor Regie op Gegevens v0.1	Het doel van het kader voor regie op gegevens, is het zorgdragen dat mensen (en organisaties) met RoG-stelsels en toepassingen kunnen gaan (samen) werken, omdat het voor iedereen navolgbaar is – dankzij de gezamenlijke normen en eisen – dat er veilig en betrouwbaar met gegevens wordt omgegaan.
8	Nederland Digitaal: De Nederlandse visie op datadeling tussen bedrijven	De visie is aangekondigd in de Nederlandse Digitaliseringsstrategie en komt tegemoet aan de breed gevoelde wens om duidelijkheid over de rol van de Nederlandse overheid op de korte en lange termijn bij de (verantwoorde) bevordering van datadeling tussen bedrijven.
9	Monitor Open standaarden: Rapportage 2018	Onderzoek naar het gebruik van open standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie door overheidsorganisaties. Onderzoek of, en zo ja in welke mate, overheden de verplichte open standaarden (pas toe of leg uit) van het Forum Standaardisatie daadwerkelijk gebruiken wanneer ze van toepassing zijn, zoals onder meer wordt voorgeschreven in de Instructie rijksdienst voor de aanschaf van ICT-diensten en ICT-producten.
10	Rolling plan for ICT stand-ardisation 2018 (Europese Commissie)	The Rolling Plan for ICT Standardisation provides a uniquebridge between EU policies and standardisation activities in the field of information and communication technologies (ICT), allowing for increased convergence of standardisation makers' eff orts towards European policy goals. This document is the result of a yearly dialogue involving a wide-ranging representation of the major standardisation's interested parties as represented in the multi-stakeholder platform on ICT standardisation. The Rolling Plan focuses on those actions that can support the EU policies and does not seek comprehensiveness as regards to the work programmes of the various standardisation bodies.
11	De Nederlandse Digitaliseringsstrategie, Nederland Digitaal	De Nederlandse Digitaliseringsstrategie, Nederland Digitaal, is een kabinetsbrede strategie over álles wat met digitalisering te maken heeft.

Casuïstiek

Bijlage C

In dit rapport is een analyse uitgevoerd op het standaardisatie vraagstuk van NL DIGIbeter. Door de veelheid van opgehaalde opvattingen en beleidsvisies blijft de analyse daarom soms beperkt tot meer algemene termen. Om het onderzoeksresultaat meer tastbaar te maken is aan de hand van het analysemodel een vijftal casussen uitgewerkt van een actueel maatschappelijk vraagstuk. In de hoofdtekst wordt op deze casussen teruggegrepen.

C.1 Schuldhulpverlening

Maatschappelijk vraagstuk

In Nederland hebben naar schatting bijna 1,4 miljoen huishoudens problematische schulden of een risico daarop. Daarnaast weten veel mensen niet hoe ze er financieel voorstaan. Dit gebrek aan inzicht in de eigen financiële situatie maakt het lastig om uit de schulden te komen. Deze schulden zijn niet alleen een maatschappelijk probleem voor individuele burgers zelf, maar leiden ook tot bredere maatschappelijke problemen, zoals financiële gevolgen voor bedrijven, gezondheidsproblemen en hogere zorgkosten. De overheid biedt mogelijkheden om burgers hierbij te helpen: schuldhulpverlening. Schuldhulpverlening ondersteunt mensen bij het vinden van een oplossing voor hun schulden. Op 1 juli 2012 is daarvoor ook de Wet gemeentelijke schuldhulpverlening (Wgs) in werking getreden. Deze wet legt de zorgplicht van gemeenten t.b.v. schuldhulpverlening expliciet vast. Hierdoor kunnen burgers aanspraak maken op schuldhulpverlening als zij voldoen aan de gestelde eisen.[1]

Indien een burger in aanmerking wil komen voor schuldhulpverlening krijgt hij de opdracht om zijn administratie op orde te brengen en noodzakelijke documenten te verzamelen. Op basis daarvan beslist de gemeente of iemand het recht heeft op gemeentelijke schuldhulpverlening. Deze fase wordt als cruciaal gezien en daarbij wordt ook aangegeven dat dit de fase is waarin het vaak fout gaat *'Veel mensen hebben grote stress en kunnen eigenlijk niet zelfstandig alle gevraagde stukken verzamelen. Aanleiding voor de gemeente de aanvraag voor schuldhulpverlening (al dan niet met een formele beslissing) af te wijzen, voor schuldenaren reden om voortijdig af te haken.'*[2]

Om in deze fase burgers te helpen zijn er initiatieven vanuit uitvoeringsorganisaties en gemeenten om mensen met schulden meer inzicht en regie over hun financiële gegevens geven. Daar waar de 'bewijslast' bij de burger ligt, wordt naar gegevens gevraagd die verschillende overheden vaak al hebben. Met andere woorden op dat moment vraag je als overheid om gegevens van de klant, die je als overheid vaak al grotendeels hebt. Gezocht wordt naar mogelijkheden om financiële informatie op een gestandaardiseerde manier beschikbaar te stellen en daarbij ook te ondersteunen in de zoektocht naar meer regie voor burgers op de eigen gegevens.

De doelstellingen uit NL DIGIbeter en schuldhulpverlening

In zijn algemeenheid wordt in NL DIGIbeter onder kansen en uitdagingen in de digitale samenleving aangegeven dat de overheid toewerkt naar breed gebruik van standaarden, zodat burgers en ondernemers hun gegevens maar eenmalig hoeven vast te leggen en deze vervolgens eenvoudig hergebruikt kunnen worden.

In het eerste thema (Investeren in Innovatie) wordt benoemd dat het mogelijk maken van experimenten in innovatieve projecten en het uitvoeren van pilots daar een belangrijk onderdeel van is. Het programma Regie op Gegevens gaf ICTU de opdracht voor een voorstudie naar een kader voor regie op gegevens en publiceerde dit in maart 2019.

In het derde thema van NL DIGIbeter (Toegankelijk, begrijpelijk en voor iedereen) liggen de meeste aanknopingspunten voor het voorbeeld van schuldhulpverlening. Gegevensverzamelingen van de overheid zullen vaker en beter ontsloten worden. Verdere standaardisatie van de vorm waarin de data beschikbaar komen zal de toepasbaarheid ten goede komen, specifiek voor burgers die met moeite hun eigen gegevens over schulden beschikbaar kunnen krijgen.

In het vierde thema van NL DIGIbeter (Onze dienstverlening maken we persoonlijker) wordt aangegeven dat de dienstverlening vanuit de leefwereld van burgers en ondernemers gebruiksvriendelijker, persoonlijker en proactief gemaakt worden. Er wordt gestreefd naar uniformering en standaardisatie voor een overheidsbrede samenwerking waar het kan en moet. Specifiek voor dit thema wordt genoemd dat levensgebeurtenissen centraal moeten komen te staan in de integrale dienstverlening. Een situatie waarin een burger of ondernemer schuldhulpverlening nodig heeft is een dergelijke levensgebeurtenis. Daarnaast is de doelstelling dat overheidsportalen worden gemoderniseerd ten behoeve van een beter inzicht in (en betrouwbaarheid van) de gegevens van de burger.

1 Wet gemeentelijke schuldhulpverlening, https://wetten.overheid.nl/BWBR0031331/2017-04-01
2 Burgerperspectief op schuldhulpverlening (rapportnummer: 2016/050), De Nationale Ombudsman, 2016

Standaarden voor gegevensuitwisseling

Op de juridische grondslagenlaag bestaat er een spanning als het gaat om de verdere standaardisatie van gegevensuitwisseling rondom schulden en wet- en regelgeving voor de bescherming van privacy van burgers (voornamelijk vanuit de AVG). Vanuit de AVG is het recht op 'wissen van je eigen geschiedenis' een belangrijk speerpunt om de autonomie van mensen en hun gegevens te garanderen. Maar indien er hulp nodig is, zoals schuldhulpverlening, kan deze wetgeving ook tegenwerken. Voornamelijk schuldeisers weten in het kader van AVG vaak niet wat ze kunnen en mogen doen. Ondanks het feit dat er een wettelijke grondslag is voor het uitwisselen van gegeven (de Wgs) en dus de opgevraagde gegevens bij schuldeisers noodzakelijk zijn om hun (publieke) taak uit te voeren[3] is het in de praktijk onduidelijk waar de grens precies ligt met betrekking tot het handelen op basis van die grondslag.

De basis voor de gegevensuitwisseling (informatie en applicatielaag) tussen overheden en met de burger is gebaseerd op het op een juiste manier semantisch labelen van gegevens. Zolang er goed gedocumenteerd wordt hoe per organisatie gegevens worden gedefinieerd kunnen deze gegevens worden uitgewisseld en eventueel verrijkt. De uitdaging bij schuldhulpverlening ligt dus bij de semantische interoperabiliteit. Hierdoor kunnen linked data ontstaan door gegevens uit verschillende bronnen te combineren, waarbij de diversiteit van bronnen, beheerders en uiteenlopende bestandsindelingen goed gekoppeld kunnen worden. Het gebruik van open standaarden is daarbij essentieel. De Linked Data-standaarden RDF, OWL, SKOS en SHACL staan op de lijst open standaarden die het Forum Standaardisatie aanbeveelt.

Coalities in Nederland

Binnen het programma Regie op Gegevens worden initiatieven in de praktijk ondersteund via onder andere pilots om verder te komen met regie op gegevens. Om zo te leren van de mogelijkheden en direct ook te beproeven in de praktijk. Binnen de pilot Regie op gegevens onderzoekt een aantal gemeenten hoe bijvoorbeeld apps zoals het Financieel Paspoort en de fiKks ingezet kunnen worden bij schuldhulpverleningstrajecten. Daarnaast wordt vanuit dit programma gewerkt aan een pilot rond 'de Blauwe Knop'. Dit programma tracht om, in plaats van het downloaden van bepaalde persoonlijke gegevens op een verschillende manier bij verschillende organisaties, op een complete en vergelijkbare manier te standaardiseren.

Daarom werken een aantal gemeenten en uitvoeringsorganisaties nu aan één herkenbare oplossing ('de Blauwe Knop'). Een oplossing waarmee mensen (deelsets van) persoonlijke data kunnen downloaden in een gewaarmerkt document, zodat ze deze gegevens vervolgens kunnen gebruiken, om zelf inzage te krijgen of bijvoorbeeld bij het aanvragen van schuldhulpverlening.[4]

Ten behoeve van de vernieuwing van het systeem waarmee overheidsinstanties (gemeenten, het UWV en de SVB) binnen het domein Werk en Inkomen gegevens met elkaar uitwisselen is het programma 'Toekomst Gegevensuitwisseling Werk en Inkomen (TWI): Op weg naar inzage, inzicht en hergebruik voor de burger' gestart door de VNG. Doel van dit programma is binnen het domein Werk en Inkomen stapsgewijs toe te werken naar een toekomstbestendig stelsel voor gegevensuitwisseling, waarbij de burger regie en zeggenschap over zijn eigen gegevens krijgt.[5] Als onderdeel van het programma hebben UWV, SVB, de Vereniging van Nederlandse Gemeenten (VNG), Inlichtingenbureau (IB), Bureau Keteninformatisering Werk en Inkomen (BKWI) en het ministerie van SZW in 2018 een demo 'Persoonlijke inkomensomgeving' (PIO) ontwikkeld. Onderstaand een weergave van een eerste demo rondom deze dienstverlening.

Figuur 3. **Demo PIO.**[6]

3 https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gemeente/sociaal-domein

4 https://www.vngrealisatie.nl/producten/blauweknop

5 https://www.vngrealisatie.nl/index.php/producten/toekomst-gegevensuitwisseling-werk-en-inkomen-twi-op-weg-naar-inzage-inzicht-en

6 Samenvoordeklant.nl, demo PIO, 2018, https://www.samenvoordeklant.nl/sites/default/files/bestandsbijlage/sessie_17_demo_persoonlijke_inkomensomgeving_voor_burgers.pdf

Spelregels, werkwijze en gedragen richting

Vanuit de interviews komt een beeld naar voren dat, ondanks het feit dat dit een helder maatschappelijk probleem is, waarbij de dienstverlening naar de burger toe verbeterd moet worden, een goede governance op het vraagstuk en het speelveld ontbreekt (de spelregels en werkwijze). In de huidige pilots en onderzoeken komt naar voren dat het probleem dat de betrokken organisaties moeten oplossen de burger de mogelijkheid te geven zijn eigen gegevens overzichtelijk in te zien en te combineren, maar dat die organisaties vooral kijken naar het verrijken van de eigen data. De samenwerking benaderen ze daarbij vooral vanuit hun eigen perspectief en belang. Een interventie van sturing op dit proces lijkt nodig om het maatschappelijke vraagstuk te kunnen oplossen.

Vanuit VNG Realisatie wordt aangegeven, op basis van een proeftuin rondom Regie op Gegevens, dat een overheid die zich positief uitspreekt over een afsprakenstelsel, ook actief gaat participeren in dit afsprakenstelsel (in de rollen van toezichthouder, gegevenshouder en gegevensvrager).[7] Hier kunnen nog stappen gezet worden.

Kennis

Op dit moment zijn er pilots gaande die gegevensuitwisseling rondom schuldhulpverlening mogelijk maken op basis van een gegevensrotonde. Dit is een netwerkmodel waarin partijen gegevens beschikbaar stellen en de burger ook partij is op die rotonde.

Besluiten en resultaten

Steeds meer gemeenten bieden actief schuldhulpverlening aan. Toch valt nog steeds een grote groep af omdat zij niet aan de voorwaarden voldoen. Wijkteams helpen mensen vóór deze in een schuldhulpverleningstraject belanden. Door de voorspoedige economie neemt het aantal mensen bij schuldhulpverlening af, maar het aantal mensen met schulden neemt niet af. Tien procent minder mensen heeft het afgelopen jaar een beroep gedaan op schuldhulpverlening, blijkt uit cijfers van schuldhulpverleners van de NVVK. De vereniging vermoedt echter dat het werkelijke aantal mensen met schulden 'aanzienlijk hoger' ligt.

Er is een sterke wens om het systeem eenvoudiger te maken, waardoor, vaak laag geletterde, mensen niet in een wirwar van loketten en regeltje terecht komt, maar geholpen worden dit op een rij te zetten. Hier lijkt een interventie op onderlinge afstemming, coördinatie en vereenvoudiging van de processen van de deelnemende overheidsorganisatie noodzakelijk.

C.2 Phishing

Maatschappelijk vraagstuk

Phishing is een vorm van online fraude waarbij getracht wordt persoonlijke gegevens te verkrijgen van iemand om vervolgens misbruik van die gegevens te maken. De gebruikelijke manier is dat iemand via een e-mail naar een valse, maar echt lijkende, website wordt gebracht. Hierop worden dan de persoonsgegevens achtergelaten. De verzender van de e-mail doet alsof dit van een vertrouwde instantie komt, zoals een bank of een overheidsorganisatie. Als mensen niet doorhebben dat het niet daadwerkelijk de vertrouwde instantie betreft, zijn ze genegen om hun gegevens ook daadwerkelijk achter te laten. Een veel gebruikte techniek voor phishing is spoofing. Zo kan worden gedaan alsof de e-mail van de vertrouwde instantie is, maar in werkelijkheid is dit niet het geval. Het tegengaan van phishing is dan ook een combinatie van de juiste informatiebeveiliging en bewustwording van alle burgers en normen voor legitieme communicatie.

Veel van de gebruikte communicatie rondom overheids-evenementen (uitnodigingen, tickets), onderzoeken (enquêtes) en systemen (gemailde scans, notificaties) maken gebruik van dezelfde omwegen die ook worden gebruikt door oplichters. En juist dit maakt het onderscheid ondanks bewustwording lastig.

Al jaren zijn de kosten als gevolg van phishing acties enorm. En de gevolgen van deze vorm van internetcriminaliteit blijven toenemen. Zo heeft de getroffen burger te maken met financiële schade van bijvoorbeeld enkele honderden euro's tot majeure gevolgen van identiteitsfraude. Ook stijgen al jaren de kosten van banken als gevolg van phishing. In 2018 kostte het de banken 3,8 miljoen euro, 3,5 maal zoveel als in 2017 (bron: Betaalvereniging Nederland en Nederlandse Vereniging van Banken). Daarnaast hebben banken, net als getroffen overheidsorganisaties, last van imagoschade als gevolg van phishing-acties. Over het algemeen kan dan ook gesteld worden dat breed gedragen wordt dat phishing een maatschappelijk vraagstuk is.

7 https://www.vngrealisatie.nl/sites/default/files/2018-08/Verkenning%20Impact%20Regie%20op%20Gegevens%20-%20Proeftuin%20Boxtel.pdf

Beleidsdoelstellingen uit NL DIGIbeter

Phishing als onderwerp staat niet expliciet genoemd in NL DIGIbeter. Er zijn echter voldoende aanknopingspunten die een relatie hebben met phishing in de agenda. Thema drie en vier dragen beide veiligheidsaspecten met zich mee. Zo spreekt thema drie – Toegankelijk, begrijpelijk en voor iedereen - over fraudebestendige identificatiemiddelen en over de digitale weerbaarheid van burgers. En in thema vier – Onze dienstverlening maken we persoonlijker – wordt gesproken over het zorgen voor veilige informatie en dienstverlening.

Tot slot wordt in NL DIGIbeter verwezen naar de Nederlandse Cyber Security Agenda. Maatregelen tegen cybercriminaliteit daarin liggen op de vernieuwing van wetgeving tegen computercriminaliteit, burgers en bedrijven meer digitaal vaardig maken en het stimuleren van veilige hard- en software.

Standaarden voor gegevensuitwisseling

Er zijn diverse standaarden beschikbaar die helpen om spoofing van legitieme domeinnamen onmogelijk te maken. Deze liggen met name op de technische laag. Advies van het NCSC om phishing tegen te gaan betreft het implementeren van deze technische standaarden (DKIM, DMARC, SPF). Zo lijkt de phishing-mail in elk geval niet van een betrouwbare partij te komen en kunnen burgers phishing gemakkelijker herkennen. Voor organisaties verkleint het de kans dat zij imagoschade lijden als gevolg van spoofing van hun domeinnaam. Maar op gebied van eenheid van communicatie en domeinnaamgebruik zijn nog wel afspraken nodig zodat de herkenbaarheid van onechte sites nog groter wordt.
Alle drie de technische standaarden zijn door de EU aangewezen als standaarden die bij overheidsopdrachten als referentie dienen.

Op de grondslagenlaag bestaat er tevens wetgeving om phishing te bestrijden. Waar het toepassen van technische beveiligingsstandaarden en de burgers meer weerbaarder maken toezien op voorkomen, gaat de wetgeving om vervolging. Hoewel hier ook een preventieve werking van uit kan gaan, betreft het feitelijk repressieve handhaving. Vervolging is echter ingewikkeld.

Niet alleen vanwege het feit dat er met regelmaat phishing acties worden uitgevoerd vanuit andere landen, maar ook omdat wetgeving lang niet altijd voldoende mee gaat in de digitale wereld. De vernieuwing van de wet Computercriminaliteit per 1 maart 2019 is dan ook van groot belang voor de bestrijding van phishing.

Standaardisatiespeelvelden en coalities in Nederland

De Nederlandse wetgever speelt op juridisch vlak een grote rol. Het is niet duidelijk of er met partijen buiten de overheid wordt samengewerkt voor de totstandkoming van dergelijke wetgeving, maar in elk geval zullen verschillende overheidsorganisaties betrokken zijn geweest bij de totstandkoming. Het is een lang traject geweest. Eind 2015 is het voorstel voor het eerst naar de Tweede Kamer gegaan. De hackbevoegdheid voor politie en Justitie voor de opsporing van ernstige delicten heeft tot de nodige discussie geleid.
Voor de technische standaarden geldt dat het wereldwijde standaarden zijn die beheerd worden door de organisatie IETF.

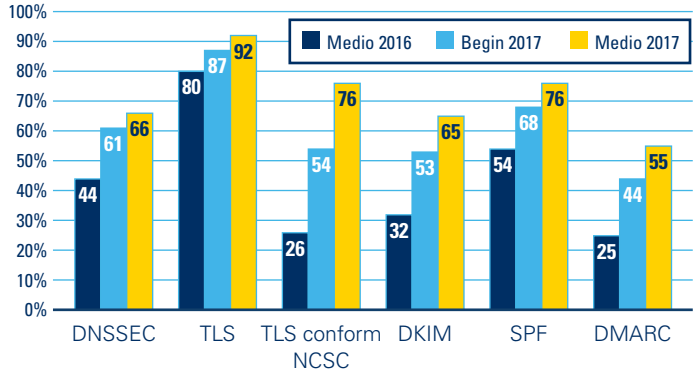
In Nederland houden verbanden als de Veilige Email Coalitie, Betrouwbare Overheids Mail samen met het NCSC zich bezig met e-mailveiligheid. Zij werken hiervoor samen met bij de Veilige E-mail Coalitie aangesloten brancheorganisaties, bedrijven en overheidsorganisaties[8]. Dit is voor het onderwerp emailveiligheid dan ook de belangrijkste coalitie. Deze coalitie is tot stand gekomen onder regie van het ministerie van EZK en verbindt zich aan het doorvoeren van maatregelen die e-mailveiligheid verbeteren en gezamenlijk vastgestelde standaarden.

NCSC beheert ook factsheets, waarvan één zich specifiek richt op de bescherming tegen phishing door e-mailveiligheid. Verder volgen zij ook het internationale speelveld op dit onderwerp, onder meer door intensieve samenwerking binnen de EU.

8 PostNL, KPN, Betaalvereniging Nederland, DDMA, Thuiswinkel.org, VNO-NCW, MKB-Nederland, Stichting Zeker-OnLine, Dutch Datacenter Association, Stichting DINL, XS4ALL, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Rijks-CIO), Fraudehelpdesk, Nederland ICT en de Belastingdienst.

Kennis

Zoals eerder gemeld zijn de technische standaarden internationale standaarden. Hoewel implementatie ervan enige inspanning vraagt van een organisatie, zijn het niet de meest ingewikkelde standaarden voor adoptie. Desalniettemin is de adoptiegraad nog zeker niet op het gewenste niveau. Hoewel de standaarden verplicht zijn voor overheden, laat onderstaand figuur zien dat de adoptie binnen de overheid niet op 100% zit, al is er wel een stijging te zien over de jaren heen.



Figuur 4. Adoptiegraad van de individuele standaarden over alle getoetste domeinen. (Figuur van https://www.forumstandaardisatie.nl/nieuws/mail-spoofing-voorkomen)

Een groot issue is de bewustwording van burgers. Uit onderzoeken de afgelopen jaren, waaronder van Alert Online, blijkt dat burgers de kans dat zij slachtoffer worden van internetcriminaliteit structureel onderschatten. Internetcriminelen worden tegelijkertijd steeds slimmer en zijn meer en meer in staat om e-mails zo op te zetten dat ze moeilijk van echt te onderscheiden zijn. Alleen het doorvoeren van technische standaarden is dus zeker niet voldoende om phishing tegen te gaan. Acties op het gebied van de weerbaarheid van de burger om het kennisniveau te vergroten kunnen niet achterblijven.

Gedragen richting

Hoewel de maatschappelijke opgave helder lijkt te zijn en de bewustwording over de problematiek sterk lijkt te groeien, is het de vraag of organisaties de urgentie voelen. Immers, wanneer men urgentie zou voelen, zou je ook verwachten dat de technische standaarden doorgevoerd waren. Kortom, phishing lijkt een typisch vraagstuk waar iedereen het eens is over het probleem, er in elk geval voor een deel een goede oplossing is (technische standaarden), maar de vrijblijvendheid niet leidt tot de gewenste adoptiegraad.

Besluiten en resultaten

Het doorvoeren van maatregelen en standaarden kan helpen bij de adoptie van de standaarden door andere organisaties. Het besluit van de Veilige E-mail Coalitie kan in theorie dus helpen bij het vergroten van de adoptiegraad. Tegelijkertijd is het maar de vraag of hiervandaan daadwerkelijk doorwerking gaat plaatsvinden. Hiervoor moeten andere organisaties de indruk hebben dat er daadwerkelijk een voordeel is voor hun wanneer ze dit doorvoeren. De kans bestaat daarom dat organisaties pas maatregelen treffen wanneer ze daadwerkelijk met gevolgen van spoofing te maken krijgen. Op dit moment is het in elk geval zo dat de adoptiegraad van de standaarden te laag ligt.

Gezien het feit dat het technische vraagstuk relatief eenvoudig is en de technische oplossing ook, is het hier zeer voor de hand liggend om de technische standaarden wettelijk te verplichten en hierop te handhaven. Wanneer dit gecombineerd wordt met een norm voor legitieme communicatie voor overheden en domeinnaamgebruik en bewustwordingsacties voor burgers, is het zeer waarschijnlijk dat de maatschappelijke kosten niet meer (dermate) toenemen.

Omdat in dit geval de baten van het tegengaan van phising vooral bij de maatschappij liggen en de kosten bij de dienstverlener ligt het voor de hand om als overheid hier de maatregelen te verplichten of te vergoeden.

C.3 Omgevingswet

Maatschappelijk vraagstuk

Er is zeer veel verschillende wet- en regelgeving op het gebied van de fysieke leefomgeving. In de loop der jaren is een ingewikkeld stelsel van wet- en regelgeving ontstaan waarin de burger of ondernemer nauwelijks meer de weg kan vinden. Ook zijn de oude regels niet meer geschikt voor maatschappelijke opgaven van nu. Denk bijvoorbeeld aan de energietransitie en gebiedstransformaties. De Omgevingswet bundelt en moderniseert alle wetten voor de leefomgeving in één wet. De wetgever heeft daarbij een viertal doelstellingen:

- Het omgevingsrecht is inzichtelijk, voorspelbaar en gemakkelijk in het gebruik.
- De leefomgeving staat op een samenhangende manier centraal in beleid, besluitvorming en regelgeving.
- Een actieve en flexibele aanpak biedt overheden meer afwegingsruimte om doelen voor de leefomgeving te bereiken.
- Besluitvorming over projecten in de leefomgeving gaat sneller en beter.

Uiteindelijk moet de burger of ondernemer via één geïntegreerd Omgevingsloket worden bediend. Dit is de centrale plek waar alle digitale informatie over de fysieke leefomgeving straks samenkomt. Zo kan iedereen informatie over de leefomgeving straks op één plek bekijken en direct gebruiken.

Doelstellingen uit NL DIGIbeter en relatie met standaardisatie

De Omgevingswet is zelfstandig beleid en staat dan ook in beginsel los van NL DIGIbeter. Maar tegelijkertijd sluit (een deel) van de beleidstheorie nauw aan bij de doelstellingen van NL DIGIbeter. Immers één van de grote opgave in de Omgevingswet is overheidsinformatie uit de fysieke leefomgeving veel begrijpelijker en inzichtelijker voor inwoners en ondernemers te maken. Zij weten dan beter wat wel en niet mag en belanghebbenden kunnen dan veel beter hun afwegingen maken over plannen in de leefomgeving. Daarnaast staat in de Omgevingswet de open data benadering centraal.

Standaarden voor gegevensuitwisseling

De Omgevingswet betreft een brede stelselherziening die vrijwel alle lagen van het lagenmodel voor standaarden raakt. Vertrekpunt voor de Omgevingswet vormt de herziening van de complexe regelgeving in de fysieke leefomgeving.

Grondslagenlaag

Het idee achter de Omgevingswet is simpel: Eén wet die alle wetten voor de leefomgeving bundelt en moderniseert. De Omgevingswet heeft als doel om alle onderdelen van de fysieke leefomgeving met elkaar in samenhang te brengen. Met ruimte om lokale initiatieven mogelijk te maken en oplossingen op maat te creëren.
Het stelsel van de Omgevingswet gaat uit van minder regels en meer vertrouwen in de mensen die ermee werken. De Omgevingswet biedt hiervoor een palet aan instrumenten die voor alle bestuurslagen vergelijkbaar zijn. Er zijn 6 kerninstrumenten waarmee de fysieke leefomgeving wordt beheerd en benut (omgevingsvisie, programma, decentrale regelgeving (omgevingsplan, omgevingsverordening, waterschapverordening), algemene rijksregels (besluit activiteiten en bouwwerken), omgevingsvergunning, projectbesluit).
Op het gebied van gegevensuitwisseling sluit de Omgevingswet aan bij de richtlijn hergebruik overheidsinformatie en bepaalt artikel 20.8 dat gegevens zoveel mogelijk beschikbaar worden gesteld langs elektronische weg, in een open een machinaal leesbaar formaat, samen met de metadata. Het formaat en de metadata voldoen voor zover mogelijk aan formele open standaarden, overeenkomstig artikel 5, eerste lid, van de richtlijn hergebruik van overheidsinformatie.

Organisatorische laag

In het kader van de Omgevingswet is het Digitaal Stelsel Omgevingswet (DSO) in ontwikkeling. De invoering van de Omgevingswet stelt andere eisen aan de interactie tussen initiatiefnemers (zoals burgers en bedrijven), belanghebbenden en bevoegde overheidsorganen. De Omgevingswet vereist dan ook een geheel andere manier van (samen)werken bij vergunningverlening, toezicht en handhaving.
Om deze nieuwe manier van samenwerken vorm te geven zijn er veel standaarden ontwikkeld/in ontwikkeling, zoals voor Omgevingswetbesluiten publiceren (STOP/TPOD), voor toepasbare regels voor vragenbomen (STTR) en voor vergunningaanvragen en meldingen ontvangen (STAM).
In het digitaal stelsel Omgevingswet (DSO) komt alle digitale informatie over de fysieke leefomgeving samen. Het digitaal stelsel ondersteunt 3 ketens. Samen beslaan ze alle functionaliteiten van het digitaal stelsel.

1. Van plan tot publicatie.
2. Van idee tot afhandeling
3. Van vraag naar informatie

Informatielaag

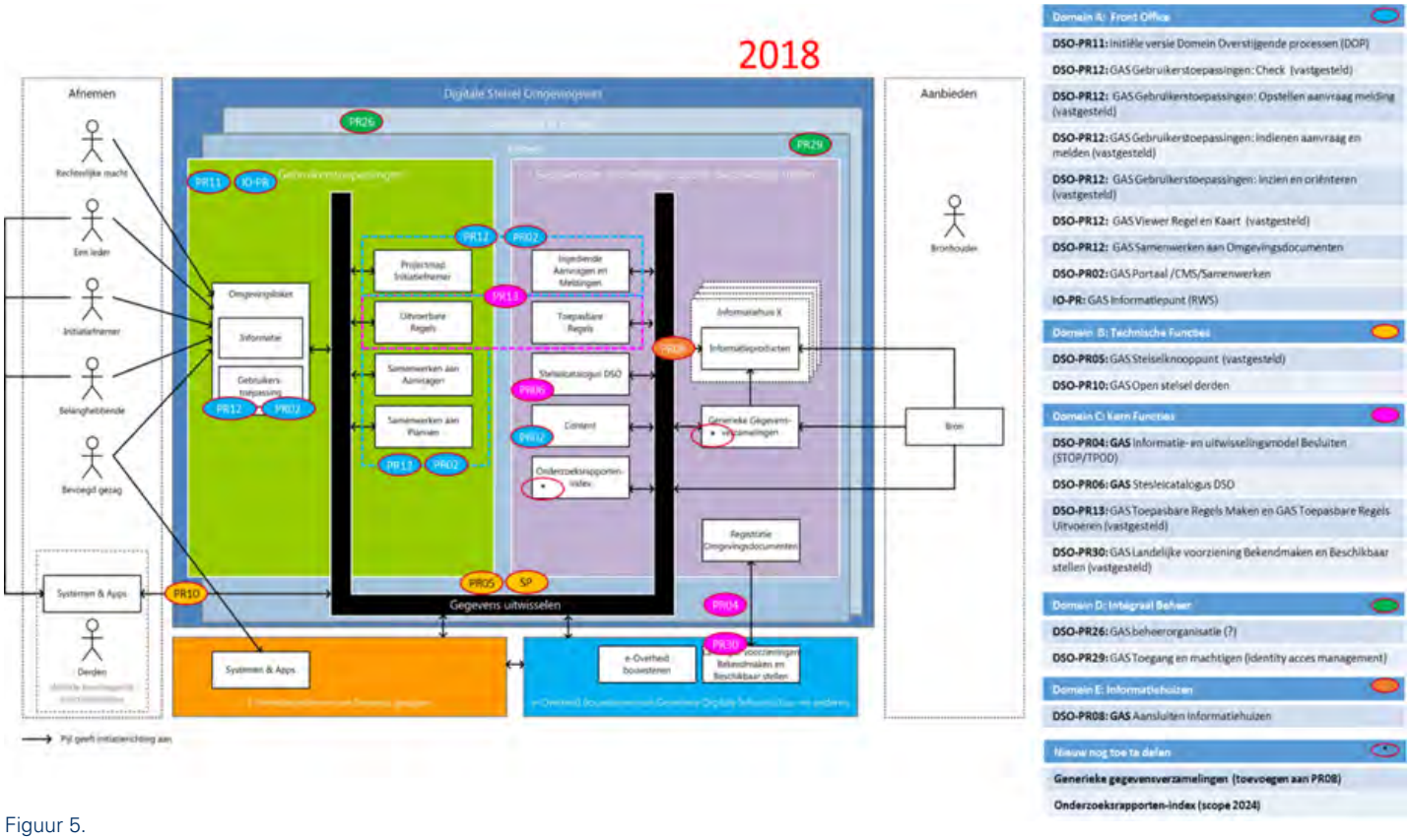
In de fysieke leefomgeving worden vele verschillende termen en definities gehanteerd. Al deze definities komen terug in de stelselcatalogus Omgevingswet. De stelselcatalogus bevat informatie over welke gegevens er in het Digitaal Stelsel Omgevingswet (DSO) beschikbaar zijn en wat deze gegevens betekenen. Daarmee zorgt de stelselcatalogus ervoor dat iedereen dezelfde taal spreekt en dat vereenvoudigt interbestuurlijk (samen)werken.
Tevens is het conceptueel informatiemodel Omgevingswet en het informatiemodel Omgevingswet van plan tot publicatie gereali-seerd. Een belangrijke bron voor het digitaal stelsel zijn de informatieproducten. Dit zijn verrijkte gegevens over bijvoor-beeld geluid, bodem en water. Via de landelijke voorziening DSO ontsluit het Omgevingsloket straks deze brongegevens.
Binnen het DSO wordt een zogeheten API en URI-strategie gehanteerd. API- en URI-strategieën zijn eigenlijk geen standaardenvoor een gegevensstructuur, maar eerder een set van voorschriften om gegevens te ontsluiten en op te vragen. Een API-strategie beschrijft hoe de gegevens ontsloten worden en hoe je ze kan bevragen. De URI-strategie beschrijft hoe en waar je gegevens kan vinden. Uitgangspunten voor de DSO is dan ook het bevragen van gegevens bij de bron via een API. De gegevensstructuur van de bron wordt daarmee leidend.
Er is dan ook geen sprake van berichtenspecificaties waar aanleverende en gebruikende applicaties gegevens naar moeten vertalen. Dat maakt het implementeren gegevensuitwisseling met behulp van API's veel eenvoudiger dan via meer traditioneel berichtenverkeer.

Applicatielaag

Het beoogde DSO functioneert als een open stelsel van informatievoorzieningen dat gebruik maakt van een stelselknooppunt. Dit is onderdeel van de landelijke voorziening DSO. Via het stelselknooppunt kunnen alle gegevens over de fysieke leefomgeving worden ontsloten. Daarbij wordt gebruik gemaakt van bestaande standaard koppelvlakken.

Het DSO fungeert middels de genoemde API's als het middel voor gegevensuitwisseling tussen deze voorzieningen en de voorzieningen van (decentrale) overheden.

Het volgende schema geeft een overzicht van de standaarden die in 2018 binnen het DSO zijn onderkend.



Figuur 5.

Speelvelden

De API-specificatie van het DSO voldoet aan de aanpak van het wereldwijde OpenAPI Initiatief. In Nederland staat de OpenAPI specificatie op PTOLU-lijst van het Forum Standaardisatie.

Daarnaast bouwt het DSO verder op de Generieke Digitale Infrastructuur en maakt dus gebruik van bijvoorbeeld Digikoppeling. Ook de sector specifieke geo-standaarden zijn van cruciaal belang.

Overigens geldt dat veel van de standaarden binnen de DSO nog in ontwikkeling zijn en als zodanig niet in de beheer en adoptiefase verkeren.

Coalities in Nederland

De Omgevingswet is feitelijk een brede bestuurlijke transitie van de overheidsdienstverlening wat betreft vergunningverlening, handhaving en toezicht in de fysieke leefomgeving. Alle decentrale overheden en een flink aantal landelijke overheden hebben directe raakvlakken met de Omgevingswet en zullen met elkaar afspraken moeten maken. Ook de leveranciers van deze overheden worden geraakt door de Omgevingswet. Uiteraard speelt standaardisatie binnen deze coalities een belangrijke rol. Belangrijke spil binnen de standaardisatieagenda van de DSO is Geonovum. De samenwerking is met name vormgegeven binnen het programma 'Aan de slag met de Omgevingswet.'

Spelregels en werkwijze (governance)

De Omgevingswet is breed en kent een complexe governance. Het voert te ver om in dit verband de gehele governance te beschrijven. In het kader van standaardisatie is het volgende van belang: het programma 'Aan de slag met de Omgevingswet' wordt aangestuurd vanuit een interbestuurlijk opdrachtgevend beraad. Dit beraad stuurt de programmaraad implementatie aan. Er is een afzonderlijke werkgroep standaardisatie ingesteld die zowel het opdrachtgevend beraad als de implementatieraad adviseert over zaken met betrekking tot standaardisatie. Daarnaast is binnen het deelprogramma DSO specifiek een aantal projectmatige activiteiten rond standaardisatie gepositioneerd.

Kennis

De Omgevingswet is nieuw en innovatief. En als zodanig is er nog veel kennis op het gebied van standaardisatie in ontwikkeling. Vele partijen zijn actief in het ontwikkelen van die kennis. Natuurlijk het programma 'Aan de slag met de Omgevingswet' maar ook Geonovum, vele Onderzoeks- en architectenbureaus, VNG realisatie, het Waterschapshuis, IPO en de Unie van Waterschapen.

Gedragen richting

De Omgevingswet is een breed gedragen transitie die veel momentum heeft. Er heeft al veel perspectief- en visieontwikkeling plaats gevonden. Gesteld kan worden dat er over het algemeen consensus is over het feit dat het eenvoudiger en beter moet met besluitvorming over de fysieke leefomgeving. Ook over de hoofdlijnen van de oplossingsrichtingen bestaat consensus. Er is echter vanuit diverse bronnen ook veel kritiek (geweest) op de omvang, kosten, haalbaarheid, breedte en ambitie van de Omgevingswet. Dit heeft diverse malen tot bijstellingen geleid. Zo zijn de bijvoorbeeld de voorziene Informatiehuizen en het register van Omgevingsdocumenten geschrapt.

Besluiten en resultaten

De Omgevingswet is een stevig wettelijke verankerde transitie waar ook vanuit bestuur en een stevige programma organisatie regie op wordt gevoerd. In alle overheidslagen zijn programma's ingericht om verder te komen met de Omgevingswet. Er is nu sprake van een gefaseerde invoering.

C.4 Standard Business Reporting (SBR)

Maatschappelijk vraagstuk

Bedrijven en organisaties ervaren administratieve lasten bij het voldoen aan de informatie verplichtingen over financiële en fiscale aangelegenheden. Door SBR worden de administratieve lasten verlaagd en neemt de transparantie en de kwaliteit van de data toe, zowel binnen de organisatie als bij de rapportage aan de overheid. Met SBR worden de gegevens in de financiële administratie eenmalig op een standaard manier vastgelegd. De gegevens zijn her te gebruiken voor verschillende rapportages aan overheidsinstellingen en een aantal banken. Door SBR kan ook de digitale dienstverlening vanuit de overheid richting ondernemend Nederland verbeteren.

Naast SBR voor de overheid bestaat ook een SBR-toepassing voor banken. Ondernemingen kunnen via SBR Nexus met behulp van hun accountant, boekhouder of taxateur data aanleveren bij banken. SBR Nexus ontwikkelt zich tot een netwerk waar ondernemers hun bedrijfsinformatie delen met tal van bedrijven en organisaties. Met de accountants werkt SBR Nexus aan een vereenvoudiging van de aanleverprocessen. Samen met tientallen financieringsverstrekkers heeft SBR Nexus een taxonomie ontwikkeld, waarin alle informatie zit wat een onderneming nodig heeft om een kredietaanvraag te doen.

In deze casusbeschrijving ligt de focus op SBR voor de overheid, maar een vergelijkbare casus is ook voor SBR-banken te maken

Doelstellingen uit NL DIGIbeter en SBR

In NL DIGIbeter wordt onder kansen en uitdagingen in de digitale samenleving aangegeven dat de Overheid toewerkt naar breed gebruik van standaarden, zoals Standard Business Reporting (SBR), zodat ondernemers hun gegevens maar eenmalig hoeven vast te leggen en deze vervolgens eenvoudig hergebruikt kunnen worden. Tevens geeft NL DIGIbeter aan dat programma's gebaseerd op standaarden als Standard Business Reporting bijdragen aan vermindering van administratieve lasten voor ondernemers en dat ze het zakendoen met de overheid makkelijker maken. Daarmee krijgt SBR een prominente rol in NL DIGIbeter.

Standaarden voor gegevensuitwisseling

SBR hanteert standaarden op alle vijf de lagen voor standaardisatie van gegevensuitwisseling.

Grondslagenlaag

De bestaande fiscale wetgeving bood de Belastingdienst reeds de mogelijkheid om belastingaangiften langs digitale weg verplicht te stellen.

Door de toevoeging van artikel 19a in het Handelsregisterwet 2007 is het vanaf 1 januari 2017 (boekjaar 2016) niet meer toegestaan dat publicatiestukken van ondernemingen behorende tot de bedrijfsklassen micro en klein op papier worden gedeponeerd bij de Kamer van Koophandel. Enkele uitzonderingen daar gelaten moeten de publicatiestukken voortaan elektronisch worden gedeponeerd in het handelsregister. Naast de system-to-system aanlevering is het voor ondernemers ook mogelijk om het online serviceportaal Zelf deponeren jaarrekening van de Kamer van Koophandel te gebruiken.

Voor beursgenoteerde ondernemingen dient het besluit van de European Securities and Markets Authority (ESMA) te worden gevolgd. Dit besluit schrijft voor dat een Europese beursgenoteerde onderneming minimaal de geconsolideerde jaarrekening op basis van Inline XBRL moet opstellen (Inline XBRL is een variant van XBRL, waarbij in een HTML-pagina XBRL-code wordt geplaatst. Bij de presentatie van de HTML-pagina in een standaard webbrowser wordt de XBRL-code niet getoond, waardoor er voor de mens een leesbare rapportage ontstaat). Dit besluit impliceert dat grote ondernemingen (niet beursgenoteerd) en middelgrote ondernemingen met als holdingorganisatie een grote of beursgenoteerde onderneming ook op basis van Inline XBRL hun deponeringsstuk moeten opstellen. De exacte details worden in een latere stadium bekendgemaakt, zoals op welke wijze de enkelvoudige jaarrekening op Dutch GAAP moet worden opgesteld. Bekend is wel dat de verplichting ingaat op 1 januari 2021 en daardoor betrekking heeft op de jaarrekening over boekjaar 2020. De exacte invulling van de ‘verplichtstelling’ is nader bepaald door een algemene maatregel van bestuur (AMvB), die op 25 april 2016 is gepubliceerd in het Staatsblad.

Organisatorische laag

De Nederlandse Proces Architectuur (NPA) ziet toe op de interactie met de SBR- infrastructuur. De verschillende interacties tussen gebruiker en verwerkende infrastructuur zijn gebundeld in een SBR-proces. Ieder proces stelt functionele eisen aan de standaard ‘bouwblokken’ waaruit het proces bestaat. Het beheer van de processen is belegd bij de beheerorganisatie Logius.

De gebruiker (aanleverende partij) communiceert met de SBR-infrastructuur door interacties met een SBR-proces. Ieder proces (aanleveren, eMededelen en statusinformatie) maakt gebruik van een aantal bouwblokken.

Ook voor SBR-Nexus zijn dergelijke procesafspraken gemaakt.

Informatielaag

De Nederlandse Taxonomie (NT) is het gemeenschappelijk gegevenswoordenboek van SBR. Het is een woordenboek met definities van gegevens die nodig zijn voor het samenstellen van diverse soorten verplichte rapportages. De Nederlandse Taxonomie (NT) is één van de bouwstenen van SBR die door softwareleveranciers wordt gebruikt. Softwareleveranciers zorgen ervoor dat de Nederlandse Taxonomie wordt ingelezen in de software. Vervolgens wordt er een koppeling gemaakt (ook wel mapping genoemd) tussen de NT-begrippen en de gegevens zoals deze in de financiële administratie, fiscale software en/of rapportgenerator zijn opgenomen. De Nederlandse Taxonomie (NT) maakt gebruik van XBRL. Naast de NT is er ook een aparte Bankentaxonomie. Deze bevat de gegevens die specifiek nodig zijn voor kredietrapportages.

SBR hanteert XBRL of eXtensible Business Reporting Language voor het structureren van de gegevens. XBRL is een internationale standaard voor digitaal rapporteren en wordt beheerd door een wereldwijd non-profit consortium, XBRL International. In EU verband is de Europese Commissie (EC) onder voorbehoud akkoord gegaan met de Regulatory Technical Standards (RTS) voor een European Single Electronic Format (ESEF). Dit voorstel schrijft voor dat ondernemingen vanaf boekjaar 2020 hun jaarrekening in Inline XBRL moeten insturen naar de lokale toezichthouder (in Nederland de Autoriteit Financiële Markten). De verwachting is dat ca. 5.000 Europese ondernemingen, waaronder ongeveer 200 Nederlandse, te maken zullen krijgen met deze verplichting.

In Nederland staat XBRL op PTOLU-lijst van het Forum Standaardisatie. XBRL is een open standaard waarin rapportages in het kader van SBR gestructureerd worden. De standaard maakt het mogelijk om online gegevens van overheidsinstellingen en het bedrijfsleven te verzamelen en uit te wisselen. XBRL is een open standaard voor het delen van informatie via internet. XBRL staat op de Pas-toe-of-leg-uit lijst van het Forum Standaardisatie. De standaard beschrijft de 'grammatica' voor op te stellen rapportages. In Nederland wordt XBRL gebruikt voor onder andere belastingaangiften, jaarverantwoording en kredietrapportages. SBR houdt ook zicht op de ontwikkelingen in de XBRL-standaard, zoals Inline en daarnaast JSON en CSV-syntax alternatieven voor de XML-syntax. Als XBRL bijvoorbeeld uiteindelijk wordt gebruikt voor het indienen van loonheffingen, is de CSV-syntaxis mogelijk een betere oplossing dan de XML-syntaxis vanwege de betreffende volumes. Om SBR-rapportages te kunnen uitwisselen worden technische koppelvlakken gebruikt. Voor de overheid is dat Digipoort.

Applicatielaag

Voor het uitwisselen van SBR-rapportages zijn de volgende technische koppelvlakken nodig: FTP, SMTP-MTA en SMTP-MSA/POP3, WUS voor bedrijven, WUS voor overheden en ebMS voor overheden.

Digipoort gebruikt deze koppelvlakken en zorgt naast een veilige verbinding met de overheid vooral voor de ontvangst, verwerking en aflevering van elektronische berichten die organisaties zoals bedrijven of hun vertegenwoordigers zoals intermediairs uitwisselen met verschillende overheidsorganisaties. Digipoort wordt door Logius beheerd. De Bancaire Infrastructurele Voorziening (BIV) is eenzelfde soort voorziening als Digipoort, maar dan bestemd voor aanlevering van rapportages aan banken.

Speelvelden en Coalities in Nederland

SBR is begonnen als een initiatief van organisaties uit de markt, zoals accountants, fiscale intermediairs, software-leveranciers, banken en de Nederlandse overheid. De volgende partijen zijn inmiddels aangesloten: Belastingdienst, KVK, OCW/DUO, woningcorporaties (SBR Wonen), banken (Rabobank, ING, ABN-AMRO en Volksbank via SBR Nexus) en CBS. Daarbij wordt onderscheid gemaakt tussen SBR-partners: die voldoen aan alle eisen/verplichtingen vanuit het SBR-stelsel en SBR-toetreders: zij die een route hebben uitgezet om SBR-partner te worden.

Na een lange aanloop-periode is er nu veel support van accountants, fiscale intermediairs, softwareleveranciers voor SBR. De overheid geeft prioriteit aan het stroomlijnen van de SBR-ontwikkelingen met lopende initiatieven als eID Stelsel, e-Factureren, Auditfiles, Basisregistraties, Open Data, de Berichtenbox, Fink (voorheen: SBR+), MijnOverheid voor Ondernemers, etcetera. Het slagen van deze ontwikkelingen, ook in hun onderlinge samenhang, hangt nauw samen met het (actief) aangehaakt zijn van private partijen, in casu ondernemers, veelal via hun intermediairs en hun softwareleveranciers.

Om al deze redenen hebben de partijen die nu betrokken zijn bij de SBR-ontwikkelingen zich gecommitteerd aan het consequent hanteren van een gezamenlijke 'SBR-Roadmap'.

Uitgebreide papieren rapporten gaan verdwijnen en worden vervangen door standaard rapporten in SBR-formaat. De accountant zal zich meer op de kwaliteit van de data moeten richten. Zijn toegevoegde waarde zit niet zozeer in het maken van het dashboard, maar in de interpretatie van de gegevens. Hij kan ook een bepaalde mate van zekerheid aan de cijfers geven, zodat een partij daar waarde aan kan ontlenen. Als de accountant daarmee aan de slag gaat, dan wordt hij een datamakelaar of -regisseur. Voor veel kantoren voor het MKB is dit nog een hele ontwikkeling en vraagt dat een vergaande omschakeling. Binnen de sector wordt dit gezien als een transitie.

Governance en gedragen richting

De overkoepelende governance van SBR wordt gevormd door een publiek-private samenwerking van partijen. Het SBR-team en de Rijksregisseur SBR, die als onafhankelijke partij het geheel aanstuurt, zoekt continu afstemming met de verschillende koepels, branche- en beroepsorganisaties, zoals onder meer NBA, SRA dat 370 accountants- en advieskantoren verenigt en NOAB waarbij ongeveer 1.000 kantoren zijn aangesloten.

Er is een SBR Roadmap 2020 opgesteld met als doel de partijen die betrokken zijn bij SBR een gezamenlijk draagvlak te creëren en inzichtelijk te maken welke activiteiten cruciaal zijn om dit publiek-private samenwerkingsverband tot een succes te maken: de stip aan de horizon waar we gezamenlijk naar toe werken. Alle partijen hebben zich hieraan gecommitteerd, waardoor een gemeenschappelijke agenda en basis voor vertrouwen voor de komende jaren ontstaat.

Het SBR Beraad is het besluitvormende orgaan. Het Beraad is er om strategisch richting te geven aan SBR. Het SBR Beraad bestaat uit vertegenwoordigers van onder andere: Belastingdienst, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Big 5 accountantsorganisaties, NBA, NOAB, XBRL Nederland, NOB, VNO-NCW/MKB Nederland, Nederland ICT, Ministerie van Economische Zaken en Klimaat, Raad voor de Jaarverslaggeving, SBR Nexus (SBR Banken). Het Beraad doet voorstellen rond maatregelen die door één of meer betrokken partijen aangepakt moeten worden om de realisatie van de strategische koers binnen bereik te krijgen en te houden.

Strategische beslissingen worden via het SBR Platform voorgelegd aan het Beraad.
Het platform wordt geadviseerd door Expertgroepen over de inrichting, het beheer en het onderhoud van SBR.

Kennis

Voor SBR is een architectuur opgesteld. De SBR Nederlandse Taxonomie Architectuur (NTA). De NTA zijn bouwvoorschriften voor de Nederlandse Taxonomie (NT) en NT-extensies. Het doel van de NTA is het realiseren van consistentie en voorspelbaarheid van de NT, controleerbaarheid van de NT, modulariteit en daarmee de uitbreidbaarheid en onderhoudbaarheid van de NT. Daarnaast hanteert SBR Internationale ‘best practice’ om software aanbieders een stabiel platform te geven.
Er zijn diverse cursussen en trainingen en SBR maakt bij een aantal hogescholen deel uit van het vaste onderwijscurriculum.

Een aandachtspunt is de schaarse kennis die er nu veelal is rond SBR. Initiatieven worden genomen om dit uit te breiden en borging, door het verder ontwikkelen van kennis en het verspreiden daarvan naar verschillende doelgroepen. Diverse partijen werken samen met de HvA die SBR in haar opleiding heeft verankerd. Het boek ‘De Keten Uitgedaagd’, biedt een uitgebreide onderbouwing van SBR. Diverse deskundigen op het gebied van SBR/XBRL leveren bijdragen in seminars en workshops.

Besluiten en resultaten

SBR is de enige methode om met aangifte- of administratiesoftware de aangiften inkomstenbelasting, vennootschapsbelasting, omzetbelasting (btw) en de opgaaf intracommunautaire prestaties (ICP) aan de Belastingdienst aan te leveren.

CBS-uitvragen voor de economische Maand- en Kwartaalstatistieken (omzetstatistiek) kunnen direct vanuit het boekhoudsysteem ingezonden worden. Als stimulans voor het inzenden kan het CBS-informatie terug leveren. Informatie waar de ondernemer en zijn/haar intermediair iets aan hebben.

De Autoriteit woningcorporaties, het Waarborgfonds Sociale Woningbouw, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Aedes hebben in december 2017 afgesproken de informatieketen binnen de corporatiesector te verbeteren. In vijf jaar wordt toegewerkt naar geautomatiseerd uitwisselen van informatie binnen de keten.

Om corporaties niet met verschillende aanlevermethoden te confronteren is gekozen om aan te sluiten op het gebruik van SBR voor het aanleveren van verantwoordings- en sturingsinformatie. Door eenduidige definities te bepalen en in de administratie gegevens te standaardiseren is geautomatiseerde uitwisseling van informatie mogelijk, met vermindering van administratieve lasten als gevolg. Daarnaast leidt dit tot betere informatie voor sturing, vergelijking en verantwoording.

SBR wordt in het onderwijsveld gebruikt voor de financiële verantwoordingsketen. OCW streeft daarmee naar betere kwaliteit van de informatie, een snellere en robuuste verantwoordingsketen en administratieve lastenverlichting.

Vanaf 2017 is het aanleveren van kredietrapportages via SBR Banken de standaard. De ABN- AMRO Bank, de ING Bank en de Rabobank zijn de initiatiefnemers van SBR Banken. Het proces van een kredietaanvraag kan door middel van SBR Banken worden verkort tot 1 dag. Een SBR Kredietrapportage genereert meer informatie dan in eerste instantie uit een standaard jaarrekening blijkt. Dit verkleint de kans dat banken om aanvullende informatie vragen, vermindert fouten en bespaart tijd.
Er zijn nog legio rapportageverplichtingen die ondersteund kunnen worden door SBR.

De volgende domeinen worden onderkend:
- departementale financiële verantwoording;
- interbestuurlijk informatieverkeer;
- zorgdomein;
- duurzaamheid (waaronder agrarische sector).

Deze domeinen kenmerken zich veelal door uitwisseling van rapportages over publieke gelden, waarbij SBR met haar aanpak een belangrijke bijdrage kan leveren aan de verantwoording van deze publieke middelen. Door de standaardisatie van gegevens kan daadwerkelijk betekenis worden gegeven aan de uit te wisselen financiële data. Transparantie en vergelijkbaarheid van deze data worden sterk vergroot.

C.5 Regie op eigen gegevens

Maatschappelijk vraagstuk

Door commerciële partijen en overheden worden veel persoonsgegevens in (online) databronnen verzameld en aan elkaar verbonden om nieuwe inzichten en opsporingsmogelijkheden te krijgen. Tegelijkertijd kan dit de rechten van burgers inperken, bijvoorbeeld op het gebied van privacy.

Een probleem is dat in de (online) digitalisering van de afgelopen decennia de hoeveelheid (digitale) identiteiten per persoon is gegroeid naar honderden: van het Nederlandse paspoort tot een Facebook of Bol.com account. Daardoor bestaan er honderden kopieën naast elkaar van hetzelfde persoonsgegeven. Het is nu zeer moeilijk voor een persoon om dat persoonsgegeven overal (tegelijkertijd) aangepast te krijgen of fouten gecorrigeerd te krijgen: kortom de regie op zijn eigen gegevens te krijgen.

Een ander probleem is dat het voor burgers niet duidelijk is of de overheid (en bedrijven) hun recht op privacy respecteert[9]. NL DIGIbeter schrijft: ‘Om het vertrouwen in systemen te vergroten, hebben mensen het recht op inzicht wie, op welk moment en voor welk doel, hun gegevens inziet, gebruikt of aan anderen geeft. Dit recht is vastgelegd in de Algemene Verordening Gegevensbescherming. Dit vraagt veel van alle overheidsorganisaties en mogelijk leidt dit tot gezamenlijke acties.’

Beleidsdoelstellingen in NL DIGIbeter

NL DIGIbeter schrijft vanuit het perspectief van de overheid: ‘Autonomie van burgers en ondernemers is ons uitgangspunt. Dat betekent dat we ervoor gaan zorgen dat mensen op één plek dingen kunnen regelen die aan hun persoon gekoppeld zijn. Denk daarbij aan het kunnen aanpassen van je persoonlijke gegevens, inzicht hebben in geregistreerde gegevens over jezelf, het toestemming kunnen geven voor gebruik van je persoonlijke gegevens, en het beheer van je digitale identiteit en je digitale inlogmiddelen.’

De AVG geldt echter voor alle organisaties, ook voor bedrijven. Daar is ook behoefte bij bedrijven en klanten aan gestandaardiseerde manieren van ‘regie op eigen gegevens’. De pensioensector is een mooi voorbeeld waar op een gestandaardiseerde manier informatie wordt gebundeld en waar burgers hun gegevens of situatie kunnen aanpassen op de website MijnPensioenOverzicht. Dit wordt beheerd door Stichting Pensioenregister: een publiek-privaat initiatief van de gezamenlijke Nederlandse pensioenfondsen, de pensioenverzekeraars en de Sociale Verzekeringsbank (SVB).

De Nederlandse overheid zou standaardisatie rondom ‘regie op eigen gegevens’ ook in andere sectoren kunnen stimuleren en faciliteren.

9 https://www.nationaleombudsman.nl/system/files/onderzoek/WEB_117668_Privacy-in-ketenoverleggen.pdf

Standaarden in vijf lagen

Grondslagenlaag

Vanuit wetgeving is in de Europese GDPR (en Nederlandse uitwerking in de AVG) specifiek aandacht voor privacyrechten van burgers. Zo is er inzagerecht, recht op vergetelheid, recht op rectificatie (en portabiliteit). Om deze rechten uit te oefenen moeten burgers in staat zijn om toegankelijk inzage te krijgen en data aan te laten passen of te verwijderen of over te brengen naar andere systemen.

NL DIGIbeter kijkt onder andere naar de ontwikkelingen rondom de Europese Payment Service Directive (PSD2) en Algemene Verordening Gegevensbescherming (AVG), waarmee mensen meer regie krijgen over data die hen betreft en het mogelijk wordt om deze in te zetten voor andere doeleinden.

Organisatorische, Informatie en applicatie laag

Er bestaan inmiddels verschillende open standaarden en enkele afsprakenstelsels (QIY trusted framework, Medmij) en er zijn veel initiatieven (IRMA, iShare, Schluss etc) die ondersteunen bij het invoeren van regie op eigen gegevens. Dit convergeert echter nog niet naar één oplossing.

NL DIGIbeter geeft aan dat nog een aantal basisafspraken moet worden gemaakt voor veilige en betrouwbare uitwisseling van gegevens en de regie daarover van de desbetreffende burger of ondernemer en dat er actieve sturing nodig is voor de juistheid van gegevens (in basisregistraties). NL DIGIbeter geeft aan dat aanpassingen noodzakelijk zijn in de gegevenshuishouding van de overheid, in het bijzonder in de basisregistraties.

Het speelveld: programma 'Burgers en bedrijven in regie op hun gegevens' (RoG)

Het programma 'Burgers en bedrijven in regie op hun gegevens' (RoG) is geïnitieerd door het ministerie van BZK om het speelveld en de reikwijdte van dit thema in kaart te brengen. De afgelopen periode is er informatie verzameld in het veld, bijvoorbeeld door middel van pilots op het gebied van het gebruik van afsprakenstelsels. Maar ook is er nagedacht over passende afspraken om systemen te kunnen koppelen en gegevens te kunnen delen op een verantwoorde wijze, in juridische, technische en morele zin[10].

Samen met spelers in de coalitie wordt in werkgroepen gewerkt aan 1) functioneel/technische aspecten, 2) juridische aspecten en 3) governance aspecten.

Coalitie

In de coalitie (van het programma RoG) werken publieke en private partijen samen. Daarin zitten onder andere het ministerie van BZK, ministerie van OCW, VNG, ICTU, DUO, Logius, Belastingdienst, CZW, SZW, Pels Rijcken en TU Delft. De vraag is of deze coalitie groot genoeg is om gedragen besluiten te nemen die effect hebben op honderden overheidsorganisaties en marktpartijen.

Kennis

Op verschillende vlakken wordt kennis ontwikkeld rondom het vraagstuk en de mogelijke oplossingen voor regie op eigen gegevens. Het programma RoG gaf ICTU opdracht voor een voorstudie naar een kader voor regie op gegevens en publiceerde dit in maart 2019 [11]. Daarnaast stimuleert het programma RoG ook initiatieven in de praktijk via simulaties, hackathons en pilots om verder te komen met regie op gegevens. Om zo te leren van de mogelijkheden en direct ook te beproeven in de praktijk[12]. In NL DIGIbeter staat dit omschreven als 'Living Labs'.

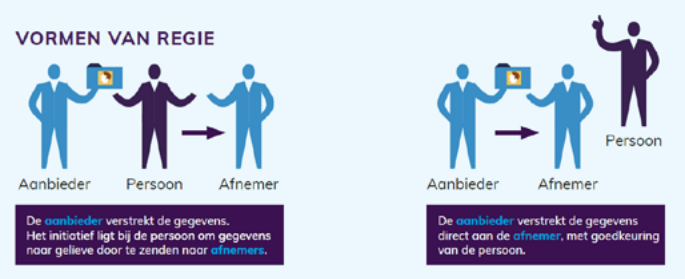
10 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens/vraag-en-antwoord/wat-doet-het-programma-regie-op-gegevens/
11 https://rog.pleio.nl/file/download/57899614/ICTU%20ROG%20Rapport%20Kader%20voor%20RoG.pdf
12 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens/vraag-en-antwoord/wat-doet-het-programma-regie-op-gegevens/

Gedragen richting

Het programma RoG richt zich op drie doelen:

1. **Inclusiviteit.** Mensen met persoonlijke verschillen in mogelijkheden, omstandigheden en culturen nemen vrijelijk deel aan het (digitale) maatschappelijke leven.
2. **Mens centraal.** Personen krijgen meer grip op het leven door regie op eigen persoonlijke gegevens.
3. **Digitale autonomie.** Personen verstevigen hun positie door vergroten van inzicht in en invloed op persoonlijk gegevensverkeer.

Daar horen op hoofdlijnen twee typen oplossingen bij zoals in Figuur 6 is weergegeven.



Figuur 6. **Vormen van regie (uit infographic Kader Regie op Gegevens).**

De kennis en ervaring om deze typen oplossingen grootschalig door overheid en bedrijfsleven in de praktijk in te voeren staat nog in de kinderschoenen.

NL DIGIbeter stelt twee concrete oplossingen voor in de interactie tussen overheid aan de ene kant en burgers/ ondernemers aan de andere kant:

1. Het huidige ***MijnOverheid*** omvormen naar een plek waar de burger de regie op zijn (persoons-)gegevens kan voeren.
2. Op of via ***MijnOverheid*** en ***MijnOverheid voor Ondernemers*** kunnen burgers en ondernemers een onjuist gegeven (laten) corrigeren.

Hiervoor moet volgens NL DIGIbeter aan een aantal randvoorwaarden worden voldaan:

1. Een **aantal basisafspraken** moet worden gemaakt voor veilige en betrouwbare uitwisseling van gegevens en de regie daarover van de desbetreffende burger of ondernemer.
2. Aanpassingen zijn noodzakelijk in de **gegevenshuishouding** van de overheid, in het bijzonder in de **basisregistraties**.
3. De juistheid van gegevens is van groot belang en vraagt om **actieve sturing**.

Wat opvalt is dat hier niet concreet is gemaakt met wie deze afspraken moeten worden gemaakt en welke partij(en) hier actief op gaan sturen.

De consequenties van 'regie op eigen gegevens' zijn ook groot voor veel overheden. In NL DIGIbeter wordt dat bijvoorbeeld aangekaart als: 'De gevolgen van het gebruik van een onjuist gegeven gaan we snel herstellen.' De omvang, urgentie en oplossing voor dit vraagstuk komen niet aan de orde.

Besluiten en Resultaat

De coalitie is gevormd, er is een visie voor de oplossingsrichtingen en kennis wordt actief ontwikkeld met publieke en private partijen. Niet alleen theoretisch, maar ook in de praktijk met behulp van hackathons en pilots.

Privacybescherming is met de invoering van de AVG bij veel organisaties goed op de kaart gekomen, zowel bestuurlijk als in de operatie (mei 2018). Hoewel de meeste eisen in de AVG al verplicht waren in de voorgaande wet (Wbp), is er in 2018 overeenstemming gekomen op verschillende niveaus in veel organisaties over het maatschappelijke vraagstuk en de urgentie ervan. Dat is terug te zien in een deel van de implementatie. Organisaties hebben Functionarissen Persoonsgegevens en de verantwoordelijke voor het melden van datalekken aangesteld. Daarnaast hebben veel organisaties onderlinge juridische afspraken gemaakt over gegevensuitwisseling: de verwerkersovereenkomsten. Ook is er meer aandacht gekomen voor doelbinding en privacy-by-design.

Het grootste probleem na invoering van de AVG is dat weinig organisaties bereid of geslaagd zijn om nieuwe technische functionaliteit te introduceren voor het voeren van regie op eigen gegevens. Zo'n functionaliteit is bijvoorbeeld het eenduidig en toegankelijk inzichtelijk maken voor een burger van zijn opgeslagen persoonsgegevens. Sommige organisaties gebruiken daar een 'MijnOmgeving' voor, maar deze zijn nauwelijks gestandaardiseerd.

Hier ligt dus nog een grote uitdaging om deze rechten beter in organisaties en de techniek te borgen. Standaardisatie kan helpen om de kosten en inspanningen bij het invoeren van deze functionaliteit te verlagen. Dit vraagt om interventies die het bij bestuurders, directies en management in allerlei (overheids-) organisaties stevig op de agenda zet en waar middelen en capaciteit wordt vrijgemaakt om de rechten van burgers beter te borgen.

Observaties over adoptie

Bijlage D

In deze bijlage hebben wij langs de onderwerpen uit het analysemodel de observaties over adoptie van standaarden uit de interviews verzameld. Uit veel interviews kwam naar voren dat adoptie van standaarden door de betrokken partijen vaak een lastige opgave is, maar er ook kansen zijn. Een veelheid aan opvattingen en stellingen is genoteerd, waarbij partijen vaak een grote passie voor dit vraagstuk aan de dag legden.

Er zijn altijd innovatoren (innovators) en pioniers (early adopters), maar hoe krijg je de achterlopers (late majority[13]) en achterblijvers (laggards) mee? In grote lijnen komen daar vier benaderingen bij in beeld:

1. Financiële prikkels
2. Organisatorische ondersteuning en begeleiding
3. Verplichtstelling
4. 'Onder de radar'

D.1 Observaties over speelvelden

Het uitgangspunt op het speelveld moet zijn: We willen iets, welke standaard kunnen we daarbij gebruiken. Niet andersom. Daarbij zien geïnterviewden een getraptheid: als er een internationale standaard is, gebruiken we die (bijvoorbeeld een ISO standaard). Dit kan zowel verplicht als niet verplicht zijn. De volgende stap is op Europees niveau. Dan op nationaal niveau. Dan hou je wat over en dat ga je zelf definiëren met de sector. Je krijgt vanzelf een hogere adoptiesnelheid als je een internationale standaard gebruikt. Als je niet op technisch niveau hoeft te innoveren kun je gemakkelijker op procesniveau innoveren. Early adopters krijg je sneller mee als je op internationale standaarden kunt aansluiten. In dat licht is het goed om te kijken hoe de W3C domeinen standaarden ontwikkelen. Deze zijn veel opener. Een open proces, ondersteund door goede tools. Daardoor is maar ¾ jaar nodig om tot overeenstemming te komen.

Daar staat tegenover dat adoptie ook 'onder de radar' kan plaatsvinden. Klankbordgroepen uit de zogenaamde 'vitale sectoren' geven aan geen behoefte te hebben aan nog meer regels om elkaar te vinden.

D.2 Observaties over coalities

Door vroegtijdig het bedrijfsleven te betrekken bij standaardisatie kan een vliegwiel ontstaan. Goede voorbeelden zijn SBR en eHerkenning en sommige geo-standaarden. Een standaard die in de markt niet gebruikt wordt werkt niet. De overheid moet meer van buiten naar binnen kijken. Niet alleen vanuit jezelf denken, maar waar de markt behoefte aan heeft.

Vanuit de overheid moet je delen wat je weet, ook met het bedrijfsleven. Samenwerken met bedrijfsleven op specifieke thema's. De Dutch Blockchain Coalition is daar een goed voorbeeld van.
Het NCSC werkt nauwelijks met wetgeving voor de adoptie van standaarden. Het belangrijkste middel is inspelen op marktwerking, het creëren van vraag. Ook het bundelen van vraag vanuit diverse partijen werkt goed richting een leverancier.

D.3 Observaties over spelregels en werkwijzen

Een belangrijke factor voor adoptie is de afweging tussen betalen en genieten. Aansluiten bij een standaard/platform kost geld. Vaak draaien de innovators en de pioniers op voor de kosten en profiteren de volgers. Daarom helpt het om voorafgaand aan de standaardisatie een stakeholder analyse uit te voeren: kijk wie er pijn lijdt, wie draagt kosten, op wie heeft het impact, wat is de toegevoegde waarde. Een maatschappelijke kosten-baten analyse (MKBA) kan dan heel erg belangrijk zijn. Daarbij moet het ook gaan over de verbetering van de informatiekwaliteit in de keten, daar kun je niet alleen aan beginnen. Zeker bij een concept als 'halen bij de bron' gaat het dan om informatie te geven en te delen in de keten en afhankelijkheid van de bron. De waarde van een standaard is nooit de standaard alleen, omdat de standaard slechts een onderdeel is van een informatieketen of netwerk.

Bij het gebruik van standaarden is de vraag welk verdienmodel je hebt als het alleen open standaarden mogen zijn. Zullen ICT-leveranciers nog investeren in toepassingen? Protectionisme is dan een bekende defensieve strategie, maar als je alles opengooit dan is de totale taart groter en kun je daar een grotere punt van krijgen en er meer aan verdienen. Je kunt je bijvoorbeeld op de domein specifieke zaken specialiseren. Het verdienmodel zit dan in prijs/kwaliteit/ aanvullende dienstverlening, etc. Denk aan de generic strategies van Porter. Je bent de beste, de goedkoopste of je specialiseert je heel erg. In een open markt kies je ervoor jezelf te onderscheiden met inachtneming van standaarden. Alle drie de strategieën kunnen werken.

Een centrale subsidiepot kan werken als katalysator: dan staat men in de rij 'want anders is de pot op'. Hierbij moeten wel prioriteiten gesteld worden, zodat gestuurd kan worden aan wat echt belangrijk is voor het beleidsterrein en niet op basis van wie het eerst komt, wie het eerst maalt. Een voorbeeld hiervan is het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional (VIPP) van VWS.

Bij publiek-private samenwerking is de uitdaging de maatschappelijke en commerciële belangen in balans te houden en liefst te combineren. Een overheid kan best stimuleren, maar de commerciële partijen moeten het initiatief overnemen.
Als de maatschappelijke baten positief zijn, dan moet je gewoon als overheid overwegen om verplichtstelling te gebruiken.

13 Everett Rogers: Diffusion of Innovations

Bij de PTOLU-lijst komt zowel 'pas-toe', als 'leg uit' niet voldoende uit de verf.In de publieke sector wordt maar in 15% van de aanbestedingen om alle cruciale standaarden van deze lijst gevraagd (pas-toe), hoewel dat verplicht is door de Rijksinstructie, waarvan bestuurlijk is afgesproken dat die overheidsbreed zal worden toegepast. De verplichting om in het jaarverslag uit te leggen welke zwaarwegende redenen je hebt gehad om een standaard niet uit te vragen en toe te passen, wordt door geen enkele partij gevolgd.
Wetgeving met een verplichting om toe te passen kan – wanneer de urgentie groot genoeg is - helpen, want ambtenaren houden zich aan de wet. In het wetsvoorstel Digitale Overheid (WDO) is daarom een grondslag opgenomen om per AMvB het gebruik van – nader te bepalen – standaarden te verplichten. Overwogen kan worden om – naast verplichting van het gebruik van bepaalde standaarden op grond van de WDO – ook de 'leg-uit' van de pas-toe-of-leg-uit te verplichten, maar over wetgeving moet niet te makkelijk gedacht worden.
Elke verplichting zal immers gehandhaafd moeten kunnen worden. En verdere verplichtstellingen kunnen administratieve lasten en weerstand opwekken. Een middel als naming & faming (of 'naming & shaming') werkt ook zonder wetgeving.

In sommige gevallen is het voor de adoptie van standaarden noodzakelijk om de specificaties van de standaarden vrij beschikbaar te maken. Voor veel standaarden in beheer bij een privaat nationaal of internationaal instituut moet nu voor het raadplegen van de specificaties een bedrag betaald worden. Dat is de manier waarop normalisatie-organisaties (zoals NEN, CEN en ISO) worden gefinancierd (het gebruik van de standaard zelf is wel vrij). Er is een ontwikkeling om de specificaties van meer NEN-standaarden vrij beschikbaar te maken. Ook op Europees niveau gebeurt dit. Op dit moment bijvoorbeeld op het gebied van elektronisch factureren.
Het onderhouden en publiceren van een standaard, ook van een open standaard, kost nu eenmaal geld. Het gaat er hier dus om hoe de kosten worden gedragen; door doorbelasting aan gebruikers van de standaard of door gezamenlijke publiek-private financiering of lump-sum financiering door de overheid. Per beleidsdomein kunnen de spelregels verschillend zijn hoe 'verplicht' je iets wil gaan stellen. Op een schaal van verleiden (aantonen toegevoegde waarde) tot verplichtstellen: dat hele spectrum moet er zijn. Bij veel partijen en veel (bestaande) standaarden kan zeker gedacht worden aan verplichtstelling.

Certificering is ook een belangrijk adoptie middel.
Onafhankelijke certificeringsorganisaties voeren dat uit. Maar de certificering is vaak niet beschermd en in de praktijk wordt het nog te weinig toegepast.
Door in het inkoopproces eisen te stellen aan leveranciers kan adoptie van standaarden door deze partijen bevorderd worden.

D.4 Observaties over kennis

Het publiceren van best practices vanuit de overheid helpt partijen om zelf na te denken over standaardisatie. Dit moet wel georganiseerd worden in een kennisnetwerk. Voordelen van standaarden zijn nog niet zo zichtbaar. Dit zou beter kunnen. Aantonen van voordelen in de praktijk, waarom werken standaarden, wie hebben er voordeel van.

Ook kunnen experts zelf enigszins sturend zijn in wat zij oppakken binnen de dossiers waar zij verantwoordelijk voor zijn. Zij houden zelf in de gaten wat er speelt, ook via internet, social media, informeel netwerk...onder de radar.

Kennis moet ook geborgd worden door inrichten van beheer. Maar alleen beheer voeren kan leiden tot stilstand. Dus ook de (door)ontwikkeling moet georganiseerd worden. Een goed model hiervoor is het Beheer- en Ontwikkel Model voor Open Standaarden (BOMOS) versie 2, vooral voor semantische standaarden.

Alleen centraal opleggen van de standaarden is niet voldoende. Er is een nieuwe set van standaarden nodig, generieke agnostische en veiligheidsstandaarden werken anders qua adoptie. Daar ontstaat bijvoorbeeld via internet.nl een soort van zelftesten en geven statistieken feedback aan degenen die ermee moeten werken. Zo ontstaat een niet hiërarchische manier van kijken naar toepassing van standaarden.

Het inzetten van tooling is heel belangrijk om te toetsen of je organisatie voldoet aan een standaard, zoals internet.nl. Ook self-assessments en hulpmiddelen (checklist, tooling) zijn effectief, liever dan alleen een rapportageverplichting.

D.5 Observaties over gedragen richtingen

Door partijen vroegtijdig bij nieuwe ontwikkelingen te betrekken ontstaat er draagvlak voor het toepassen van een standaard door belanghebbenden. In het begintraject moet er al aandacht voor elkaar zijn. Hoe kunnen we elkaar helpen in plaats van: wat heb ik van jou nodig. Adoptie wordt niet vanzelf door de markt opgepakt. Je krijgt niet iedereen zomaar aan tafel. Iedereen die belang heeft moet aan tafel kunnen zitten. Daarbij moet er voldoende ruimte zijn om input te geven op een concept, bijvoorbeeld in een publieke commentaarronde. Zo wordt er consensus gezocht. De mening van een minderheid wordt zo meegenomen. Het ontwikkelproces wordt nadrukkelijk open georganiseerd. Dit vereist een professionele communicatie-strategie.

Trusted frameworks en vertrouwen in de beoordeling door een gekwalificeerde derde partij is enorm belangrijk (waardoor betrokken organisaties niet ‘steeds weer door een hoepel moeten springen, maar dat je de centraal afgesproken hoepel erkent en vertrouwt en kunt hergebruiken als je daaraan al voldoet’). Als er geen ‘trusted party’ is voor samenwerkende partijen dan ligt het gevaar van een Wild West op de loer. Initiatieven gaan dan alle kanten op. De rol van een neutrale facilitator in de keten of het netwerk is belangrijk om de samenwerking op gang te krijgen. Vertrouwen komt nu eenmaal te voet en moet verdiend worden.

D.6 Observaties over besluiten en resultaten

Politieke sturing en besluitvorming is vaak gericht op directe resultaten en verantwoording. De focus bij standaardisatie ligt juist op continuous improvement. Google is nooit af bijvoorbeeld. De term ‘permanent bèta’ is hierop van toepassing. Dat is een andere manier van technologisch ontwikkelen. Kijk hierbij naar startups. Een standaardisatieproces vergt veel tijd, want je moet het grondig doen. Neem bijvoorbeeld de introductie van API’s, een kwestie van lange adem. De politiek verwacht directe resultaten en dat staat haaks op digitale ontwikkelingen en daarmee een innovatieve digitale overheid.

Voorkomen moet worden dat het realiseren van het instrument (de standaard) het doel wordt, in plaats van de (maatschappelijke) waarde van een oplossing. Waarvoor deden we dit ook alweer? Het belangrijkste is om een gezamenlijk doel te formuleren en daar omheen de samenwerking en besturing te regelen.

Analyse wetgeving en standaardisatie

BIJLAGE E

In deze bijlage belichten we standaardisatie vanuit een wetgevingsperspectief. We beschrijven de huidige praktijk en ontwikkelingen ten aanzien van (wettelijk verplichte) standaardisatie en geven weer op welke wijze het wetsontwerp Digitale Overheid vormen van toezicht onderkent. Vervolgens volgt een conclusie van de huidige praktijk en de ontwikkelingen en geven we aan welke adviezen, vanuit het juridische perspectief, onzes inziens mogelijk zijn.

E.1 Huidige praktijk standaardisatie: 'Pas Toe of Leg Uit'

Op dit moment worden open standaarden voorgeschreven op basis van een pas-toe-of-leg-uit-lijst (PTOLU-lijst). De adoptieverplichting van open standaarden op de PTOLU-lijst vloeit voort uit artikel 3, eerste lid van de bijlage bij Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten (hierna: Instructie Rijksdienst). Dit betekent dat overheden en organisaties uit de publieke sector een open standaard op de PTOLU-lijst moeten toepassen óf moeten uitleggen waarom de organisatie de standaard niet toepast. Dit zogenaamde *comply or explain* regime zien we ook veelal terugkomen in de Europese wet en regelgeving zoals bijvoorbeeld in de Algemene Verordening Gegevensbescherming (AVG).

Van een standaard op de PTOLU-lijst mag een overheidsorgaan alleen afwijken als dit leidt tot onoverkomelijke problemen. Artikel 3, tweede lid uit de bijlage van de Instructie Rijksdienst geeft aan dat hiervan sprake is als:
'(...) een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht.'

De verantwoordingsverplichting *(explain)* bij het niet toepassen van een PTOLU open standaard vloeit voort uit de Rijksbegrotingsvoorschriften.[14] Dit betekent dat overheden en organisaties uit de publieke sector het afwijken van de PTOLU standaard dienen te verantwoorden in het jaarverslag.

Het PTOLU-principe staat onder druk. Zo blijkt uit de ' Monitor open standaarden 2018' dat maar in 15 procent van de onderzochte aanbestedingen naar alle cruciale relevante standaarden is gevraagd. Er wordt dus nog te weinig toegepast. Verder neemt het Forum in de duiding en maatregelen op de 'Monitor open standaarden 2018' waar dat:
'Na ruim tien jaar verplichten tot leg-uit komt het nog steeds zelden of nooit voor dat een overheidsorganisatie zich in het jaarverslag verantwoordt over het niet-toepassen van de relevante standaard(en).'[15]

Ondanks de zogenaamde pas-toe-of-leg-uit verplichting voor overheden en organisaties uit de publieke sector betekent het dus niet dat de open standaarden op de PTOLU-lijst wettelijk verplicht zijn (de jure) om toe te passen. Van een (de jure) wettelijke verplichting is pas sprake als niet mag worden afgeweken van een voorgeschreven standaard. Met het oog daarop is een grondslag voor een dergelijke verplichting opgenomen in het wetsvoorstel Digitale Overheid (WDO).

Als een organisatie toch besluit af te wijken dan overtreedt het daarmee de wet of het besluit waarin de norm verplicht is. Bij het niet nakomen of toepassen van een de jure opgelegde standaard zou er ook nog voor gekozen kunnen worden om een aangewezen toezichthouder sanctionerend of herstellend te laten optreden.

E.2 Ontwikkeling richting een gedeeltelijke de jure standaardisatie

Het is nu nog niet wettelijk (de jure) verplicht om de open standaarden op de PTOLU-lijst toe te passen. Overheidsorganen hebben de mogelijkheid om af te wijken van de voorgeschreven standaard.
Voor sommige standaarden van de PTOLU-lijst is dat ongewenst. Bijvoorbeeld voor een aantal informatieveiligheidstandaarden, waarmee phishing kan worden bestreden, of standaarden voor de Digitoegankelijkheid van (ondermeer) overheidsinformatie.
De aanleiding om open standaarden wettelijk te kunnen voorschrijven komt voort uit onder andere internationale regelgeving over d
Digitoegankelijkheid, en de motie Oosenbrug 2016.16 Deze internationale regelgeving en motie zijn mede aanleiding voor onderdelen in het Wetsvoorstel Digitale Overheid (WDO), waar de Minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) de mogelijkheid krijgt om bij Algemene Maatregel van Bestuur bepaalde open standaarden te verplichten. In artikel 3, tweede lid van het Wetsvoorstel vinden we de grondslag:

- ***'(...) Bij algemene maatregel van bestuur kan een standaard worden aangewezen, indien:***
  a. ***a. aanwijzing van die standaard 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;***
  b. ***b. de standaard tot stand is gekomen volgens een voor eenieder toegankelijke procedure, en***
  c. ***c. de standaard openbaar toegankelijk en kosteloos bruikbaar is en over de specificaties ervan blijvend vrijelijk kan worden beschikt of waarvan de specificaties blijvend kunnen worden verkregen tegen een redelijke vergoeding.'***

14 Rijksbegrotingsvoorschriften 2019, 3 april 2019, Toelichting paragraaf 2 - Rijksbrede bedrijfsvoering onderwerpen, p.297.
15 Forum Standaardisatie, Duiding en maatregelen Monitor Open standaarden 2018, 12 december 2018, FS 181212.4A1, p.2.

Deze grondslag geeft de Minister van BZK in de toekomst het ultimum remedium om implementatie van bepaalde open standaarden bij overheden[16] te bewerkstelligen, zonder daarbij afhankelijk te zijn van de pas toe of leg uit lijst en de bereidwilligheid van het betreffende overheidsorgaan. Naast de grondslag is in artikel 17 van de WDO een paragraaf opgenomen die toezicht en naleving mogelijk maakt. Dit betekent dat handhavend kan worden opgetreden als (bestuurs) organen niet voldoen aan de standaarden die op grond van artikel 3 Wetsvoorstel Digitale Overheid zijn verplicht. Ondanks dat de WDO nog in behandeling is, zijn reeds een aantal (aankomende) wettelijk verplichte standaarden in wetgeving verankerd. Voorbeelden daarvan zijn:

1. **Publicaties** in het Staatsblad en de Staatscourant, provinciaal blad, het gemeenteblad of waterschapblad moeten worden uitgeven en beschikbaar worden gehouden conform de open standaarden PDF/A-1a (ISO 19005-1:2005) of PDF/A-2a (ISO 19005-2:2011)
   Achtergrond: Deze verplichting bestaat sinds 14 januari 2009 en is opgenomen in artikel 2 van de Bekendmakingregeling die de verplichting opgelegd aan de Minister van Justitie en Veiligheid en de Minister van BZK om publicaties in het Staatsblad en de Staatscourant uit te geven en beschikbaar te houden conform de open standaarden PDF/A-1a (ISO 19005-1:2005) of PDF/A-2a (ISO 19005-2:2011). Dezelfde verplichting zien we ook terugkomen voor de decentrale overheden.

2. Bij het inkopen, bouwen en beheren van websites en apps door overheidsinstanties moet de standaard EN 301 549 worden gebruikt. De standaard EN 301 549 is een verzameling van technische eisen, *die content* toegankelijk maken voor **mensen met een functiebeperking**.
   Achtergrond: De Minister van BZK heeft op 1 juli 2018 een tijdelijke Algemene Maatregel van Bestuur van kracht laten gaan die overheidsinstanties wettelijk verplicht om een open standaard toe te passen. De AMvB betreft een tijdelijke besluit en is een implementatie van de Europese richtlijn inzake de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties. Omdat het Wetsvoorstel Digitale Overheid nog niet is afgerond, is de grondslag voor deze verplichting (tijdelijk) gebaseerd op artikel 89 van de Grondwet omdat anders de Europese implementatietermijnen niet zouden worden gehaald. Met deze tijdelijke AMvB wordt dan ook reeds aangesloten bij één van de NL DIGIbeter beleidsdoelen: informatie en dienstverlening worden begrijpelijk en toegankelijk

3. Overheden zijn verplicht om **e-facturen** te kunnen ontvangen en verwerken conform de Europese norm NEN EN 16931-1:2017 en CEN/TS 16931-2:2017.
   Achtergrond: De Europese Commissie heeft op 16 april 2014 de richtlijn inzake elektronische facturering bij overheidsopdrachten gepubliceerd.[17] In deze richtlijn worden twee open standaarden verplicht opgelegd aan lidstaten. De Europese Commissie heeft onderzocht dat jaarlijks € 40 miljard kan worden bespaard in Europa als iedereen elektronisch factureert en geen papieren facturen meer stuurt. Om de overheden het goede voorbeeld te laten geven heeft de Europese Commissie een richtlijn gepubliceerd waarin alle aanbestedende diensten verplicht worden elektronische facturen van toeleveranciers volgens een Europese norm EN 16931-1 te kunnen ontvangen en verwerken. Vanaf 18 april 2019 zijn overheden verplicht om e-facturen te kunnen ontvangen en verwerken conform de voorgeschreven standaarden. In Nederland is de richtlijn geïmplementeerd in artikel 4.12 Aanbestedingswet 2012 en de Aanbestedingswet op defensie- en veiligheidsgebied en de daaronder liggende besluiten.[18]

4. Het verplicht stellen van de **HTTPS standaard** zodat gegevensuitwisseling tussen bezoekers en de overheidswebsite zijn versleuteld. In 2017 heeft de voormalige Minister van Binnenlandse Zaken en Koninkrijkrelaties het belang van de standaard HTTPS voor overheid websites benadrukt.
   Achtergrond: In 2018 heeft de Minister van BZK een toezegging gedaan ten aanzien van het verplicht stellen van de HTTPS standaard. In zijn Kamerbrief stelt de minister het volgende over veilige overheidswebsites:
   Om de beveiliging van overheidswebsites verder te bevorderen, wordt de open informatieveiligheidsstandaard HTTPS verplicht, zoals eerder aan uw Kamer toegezegd in 2017. (...) De Wet Digitale Overheid, die naar verwachting in 2019 van kracht zal worden, biedt de mogelijkheid open standaarden aan te wijzen voor een verplichting bij AmvB. De AMvB voor HTTPS is naar verwachting per medio 2019 van kracht.[19]
   De AMvB die de standaard HTTPS zou moeten gaan verplichten is echter nog niet beschikbaar omdat het Wetsvoorstel Digitale Overheid nog in behandeling is bij de Tweede Kamer. Dit betekent dat er voorlopig nog geen wettelijke verplichting komt ten aanzien van de HTTPS standaard. Wanneer de nog te vormen AMvB in werking kan treden is afhankelijk van het parlementaire traject van het Wetsvoorstel Digitale Overheid.

16 Het betref hier de in het wetsvoorstel onder artikel 3 opgenomen organen: a. bestuursorganen; b. organen, personen en colleges als bedoeld in artikel 1:1, tweede lid van de Algemene wet bestuursrecht; c. rechtspersonen met een wettelijke taak als bedoeld in artikel 1.1 van de Comptabiliteitswet 2016.

17 EU 2014/55.

18 https://zoek.officielebekendmakingen.nl/stb-2018-321.html

19 Tweede Kamer, Kamerbrief 16 oktober 2018, Verhogen informatieveiligheid bij de overheid

5. (Verplichte) standaardisatie opgenomen in de **Gemeentelijke inkoopvoorwaarden bij IT (GIBIT)**
   Achtergrond: In de GIBIT zijn de Gemeentelijke ICT-kwaliteitsnormen beschreven die normen en standaarden verplicht stellen. De reikwijdte van de GIBIT omvat primair alle producten en/of diensten die gemeenten en gemeentelijke samenwerkingsverbanden op het gebied van ICT verwerven. De opgenomen ICT-kwaliteitsnormen en standaarden in de GIBIT zijn verplicht en worden gezien als de minimumeisen waaraan leveranciers moeten voldoen. De opgenomen standaarden of normen in de GIBIT komen voort uit:
   a. Een wettelijk kader; en/of
   b. Standaarden op de lijst van open standaarden (pas-toe-of-leg-uit); en/of
   c. Standaarden die als landelijke gemeentelijke standaard of norm door VNG/VNG Realisatie zijn vastgesteld.

   De GIBIT vormt een goede stap in de richting van de uitrol van standaardisatie bij aanbestedingen van Gemeenten. Ondanks dat er geen wettelijke verplichting is om als Gemeente de GIBIT voorwaarden te gebruiken laten de laatste cijfers van VNG realisatie zien dat inmiddels 80% van de gemeenten de GIBIT van toepassing heeft verklaard.[20]

E.3 EU-praktijk op het gebied van standaardisatie

Op EU-niveau is op twee manieren aandacht voor standaardisatie, namelijk enerzijds door het (financieel) stimuleren en aanmoedigen van standaardisatie en anderzijds het verplichten van standaardisatie via wet- en regelgeving. De Europese Commissie brengt standaardisatieverzoeken uit en ondersteunt financieel het werk van verschillende Europese normalisatieorganisaties. Ook kan de EU in regelgeving (verordeningen of richtlijnen) bepaalde standaarden verplichten.

Een van deze gebieden waar de Europese Unie kan optreden is in standaardisatie. Deze bevoegdheid is opgenomen in Verordening 1025/2012 van het Europees Parlement en de Raad betreffende Europese normalisatie. De doelstelling en bevoegdheid om als Europese Unie maatregelen te kunnen treffen ten aanzien van normalisatie zien we terug in considerans 52 van de Verordening.

'Daar de doelstellingen van deze verordening, namelijk de doeltreffendheid en doelmatigheid van normen en normalisatie als beleidsinstrumenten voor de Unie te garanderen via samenwerking tussen de Europese normalisatieorganisaties, de nationale normalisatie-instellingen, de lidstaten en de Commissie, de opstelling van Europese normen en Europese normalisatieproducten voor producten en voor diensten ter ondersteuning van wetgeving en beleid van de Unie, de identificatie van technische ICT-specificaties die in aanmerking komen om te dienen als referentie, de financiering van Europese normalisatie en de deelname van de belanghebbenden aan Europese normalisatie, niet voldoende door de lidstaten kunnen worden verwezenlijkt en derhalve vanwege de omvang en de gevolgen ervan beter op het niveau van de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 TEU (red. Verdrag van Lissabon) neergelegde subsidiariteitsbeginsel, maatregelen vaststellen. (...).'

Ten aanzien van verplichtingen tot ICT-normalisatie/standaardisatie is in de Verordening opgenomen dat relevante normen kunnen worden voorgeschreven. Considerans 34 van Verordening zet dit als volgt uiteen:
'Er kunnen zich situaties op het gebied van ICT voordoen waarin het wenselijk is de toepassing van de relevante normen op niveau van de Unie aan te moedigen of voor te schrijven om voor interoperabiliteit op de eengemaakte markt te zorgen en gebruikers meer keuzevrijheid te geven. In andere omstandigheden kunnen bepaalde Europese normen eventueel niet meer aan de behoeften van consumenten voldoen of de technologische ontwikkeling schaden. (...)'

Deze verordening geeft de wettelijke basis om Europese standaarden voor producten en diensten te gebruiken, ICT-technische specificaties te identificeren en het Europese normalisatieproces te financieren. Het legt ook een verplichting op aan Europese normalisatie-instellingen en nationale normalisatie-instellingen voor transparantie en participatie.

De EU hanteert het beleidsuitgangspunt dat standaarden/normen op zichzelf altijd vrijwillig moeten zijn. Maar dat in de regelgeving kan worden verwezen naar normen ter ondersteuning van de implementatie van deze regelgeving, waarbij de toepassing van standaardisatie meestal vrijwillig is en dus slechts in uitzonderlijke gevallen verplicht wordt via onder andere Europese Richtlijnen of Verordeningen. Veelal zien we in regelgeving een minimumeis neergelegd die verwijst naar een gestandaardiseerde norm. Het is aan een lidstaat om hier uitvoering aan te geven en minimaal te voldoen aan de voorschreven en verplichte standaard.

20 Cijfers eind 2018 via https://www.vngrealisatie.nl/gibit

E.4 Sectoraal reeds verplichte standaardisatie (buiten het werkveld van BZK)

De Staatssecretaris van BZK heeft als taak het goed laten functioneren van het openbaar bestuur. Hieronder vallen ook de beleidsdoelstellingen uit NL DIGIbeter en de nakoming en opvolging van de standaarden op de PTOLU-lijst. Ook op andere, specifieke beleidsterreinen, die onder de verantwoordelijkheid van andere ministers vallen, zien we standaarden reeds verplicht worden in wetgeving.

Een eerste voorbeeld is standaardisatie binnen de *zorg*. Er is veel aandacht voor informatieveiligheid en het zorgvuldig omgaan met persoonsgegevens. Het opleggen van verplichte standaarden binnen de zorg is in bepaalde gevallen wettelijk geregeld. Zo zijn bepaalde zorgorganisaties die Burgerservicenummers (BSN) verwerken, verplicht om te voldoen aan de informatiebeveiligingsstandaard NEN7510.[21]

In de *financiële sector* zien we ook verschillende (wettelijk verplichte) standaarden die wel veelal vanuit de EU worden opgelegd en in bepaalde gevallen rechtstreekse werking hebben, zoals de International Financial Reporting Standards (IFRS) [22] en de EU-MiFID II-richtlijn en de MiFIR-verordening.[23]

Ook rondom *geografische informatie* (geodata), bestaan standaarden die wettelijk verplicht zijn, zoals de INSPIRE standaarden[24], de standaarden voor Basisregistraties (BAG, BGT, BRO)[25] en de standaarden voor de Ruimtelijke ordening (RO Standaarden)[26].

In dit kader kan ook de Omgevingswet niet ongenoemd blijven. Voor de uitvoering van de Omgevingswet is een Digitaal Stelsel Omgevingswet (DSO) in het leven geroepen. Samen met het kennis- en exploitatiecentrum voor Officiële Overheidspublicaties (KOOP) ontwikkelt Geonovum de standaarden die ervoor zorgen dat omgevingsdocumenten digitaal uitwisselbaar en raadpleegbaar zijn. Voorbeelden zijn het Toepassingsprofiel omgevingsdocumenten (TPOD's) en de Toepasbare Regels (STTR) en Aanvragen en Meldingen (STAM).

De Rijksoverheid wil dat de uitwisselingsstandaard voor overheidspublicaties, zoals omgevingsdocumenten, breder toepasbaar is dan alleen het domein van de Omgevingswet. Daarom wordt samen met KOOP een generieke standaard ontwikkeld die voor alle officiële overheidspublicaties gaat gelden: de Standaard voor Overheidspublicaties (STOP).

E.5 Toezicht

Met het Wetsvoorstel digitale overheid (WDO) krijgt toezicht op het toepassen van standaarden een juridische grondslag. Het uitgangspunt van de WDO en de uitleg die daarover aan de Tweede Kamer is gegeven is die van preventief toezicht door zelfevaluatie van betrokken organisaties. Die moeten zich afvragen: Voldoe ik aan wettelijke vereisten en aan afspraken die ik met ketenpartijen heb gemaakt? Pas ik de standaarden uit de Pas-toe-of-leg-uit (PTOLU- lijst) toe of heb ik uitgelegd om welke reden de standaard niet toegepast wordt?

De Memorie van Toelichting op de WDO geeft het volgende beeld van naleving en toezicht op standaarden.[27]
'De digitale dienstverlening van bestuursorganen en aangewezen organisaties is allereerst een aangelegenheid van de desbetreffende organen en organisaties zelf. Een goede taakuitvoering door hen vergt ook naleving van de aan hen gestelde normen, zoals de acceptatieplicht en het voldoen aan de eisen met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de elektronische dienstverlening. Voorts geldt voor bestuursorganen (en eventueel rechtspersonen met een wettelijke taak) het verplicht gebruik van bij algemene maatregel van bestuur voorgeschreven standaarden.'

21 Artikel 2 van de 'Regeling gebruik Burgerservicenummer in de zorg'.
22 Verordening (EG) nr. 1606/2002 van het Europees Parlement en de Raad van 19 juli 2002 betreffende de toepassing van internationale standaarden voor jaarrekeningen.
23 De richtlijn is geïmplementeerd in de Wet op het financieel toezicht (Wft) en de lagere regelgeving en de verordening is rechtstreek werkend.
24 Implementatiewet EG-richtlijn infrastructuur ruimtelijke informatie en het onderliggende Besluit Inspire.
25 Onder andere in de Wet basisregistratie adressen en gebouwen en het onderliggende Besluit basisregistratie adressen en gebouwen.
26 Wet Ruimtelijke Ordening en bijvoorbeeld in het onderliggende Besluit algemene regels ruimtelijke ordening

27 Tweede Kamer, vergaderjaar 2017–2018, 34 972, nr. 3.

Voor wat betreft de naleving van deze wet door bestuursorganen, aangewezen organisaties (en rechtspersonen met een wettelijke taak waar het de open standaarden betreft) geldt het reguliere toezicht en de reguliere ministeriële verantwoordelijkheid. Voor de overheidsorganen op niveau van het rijk en de aangewezen organisaties is ook voorzien in het aanwijzen van toezichthouders. Waar de ministeries zelf als dienstverlener uitvoering geven aan het wetsvoorstel, is het aan de betrokken Ministers er voor zorg te dragen dat de eigen uitvoeringsorganisaties, zoals de Belastingdienst, dit wetsvoorstel naleven. Voor de zelfstandige bestuursorganen op het niveau van de centrale overheid, zoals het UWV en de SVB, geldt dat de naleving van het wetsvoorstel (eveneens) in eerste instantie een eigen verantwoordelijkheid van deze bestuursorganen zelf betreft. Het wetsvoorstel creëert geen nieuwe, formele toezichtsbevoegdheden ten aanzien van deze zelfstandige bestuursorganen. Dit betekent dat de Minister, ook al is deze overheidstaak op afstand gezet, vanuit zijn algemene ministeriële verantwoordelijkheid de betrokken zelfstandige bestuursorganen zo nodig tot naleving dient te bewegen.

Het streven is om het toezicht op de aangewezen organisaties en overheidsorganen op het niveau van het rijk ook zo veel als mogelijk binnen de bestaande toezichtstructuren en met gebruik van bestaande instrumenten te laten plaatsvinden. Om dit te kunnen realiseren, is de vakminister op grond van dit wetsvoorstel gehouden om personen aan te wijzen die belast zijn met het toezicht op de naleving van dit wetsvoorstel door deze aangewezen organisaties. De vakminister kan hier reeds bestaande toezichthouders dan wel nieuwe toezichthouders aanwijzen.

Bij decentrale overheden is sprake van interbestuurlijk toezicht (IBT), in lijn met de Wet revitalisering generiek toezicht. Het primaat voor het toezicht op de naleving ligt bij de horizontale verantwoording binnen een bestuurslaag. Het gaat dan om het toezicht op een juiste en toereikende naleving. In de tweede plaats komt het interbestuurlijk toezicht op de decentrale overheden. Uitgangspunt daarbij is dat slechts één bestuurslaag – de naast hoger gelegen bestuurslaag – toezicht houdt.

Het interbestuurlijk toezicht biedt de naast hoger gelegen bestuurslaag (uitsluitend) de mogelijkheden tot repressief ingrijpen: schorsing en vernietiging bij handelen in strijd met het recht of het algemeen belang (door de Kroon) en in uiterste gevallen indeplaatsstelling (bij taakverwaarlozing).

Provincies gaan toezicht houden op de gemeenten en waterschappen, de ministeries op de eigen uitvoeringsorganisaties en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) daarnaast ook op de provincies. De provincies en ministeries delen hun bevindingen met het ministerie van BZK over de (mate van) naleving door de gemeenten, waterschappen en instanties bij de rijksoverheid. Over de uitkomsten van het toezicht rapporteert het ministerie van BZK aan de Tweede Kamer en elke drie jaar aan de Europese Commissie.

Het wetsvoorstel biedt ook de mogelijkheid om in aanvulling op het generiek toezicht het bestuursorgaan of de aangewezen organisatie te verplichten regulier een verklaring van een auditor aan de Minister te laten overleggen. Deze auditor toetst daarbij of de dienstverlener aan de eisen voldoet. De verklaring van de auditor sluit aan bij de systematiek die thans gehanteerd wordt bij de aansluiting op DigiD. Op deze wijze kan, daar waar dat noodzakelijk wordt geacht, door toezicht het gebruik van standaarden worden gestimuleerd, zonder dat direct sprake is van afdwingen.

De WDO biedt als ultimum remedium het verplicht stellen van standaarden bij overheden, zonder daarbij afhankelijk te zijn van de PTOLU-lijst en de bereidwilligheid van het betreffende overheidsorgaan. De Minister van BZK kan via een Algemene Maatregel van Bestuur standaarden gaan verplichten indien dit noodzakelijk en proportioneel is voor de werking, de veiligheid, de betrouwbaarheid of de doelmatigheid van het elektronische verkeer of indien dit voortvloeit uit internationale verplichtingen (waaronder mede begrepen EU-regelgeving). Van noodzakelijkheid is bijvoorbeeld sprake, wanneer er aantoonbaar een veiligheidsprobleem is in de informatie-uitwisseling met natuurlijke personen of rechtspersonen, tussen bestuursorganen of wanneer individuele bestuursorganen niet profiteren van standaardisatie maar de netwerkvoordelen neerslaan bij anderen of bij de samenleving als geheel (maatschappelijke baten).

E.6 Analyse: De rol van wet- en regelgeving bij adoptie van standaarden

De overheid heeft een klassieke verantwoordelijkheid ten aanzien van het creëren van gunstige randvoorwaarden voor innovatie. Dit speelt ook bij standaardisatie. De overheid heeft een voorbeeldfunctie en dient richting de markt een stimulerend effect te hebben. We zien dit ook terug in het onderzoek vanuit het Ministerie van EZK naar datadelen binnen het MKB waar aangegeven wordt dat adoptie van standaarden worden versneld door aansluiting van grote marktpartijen en/of stimulering vanuit de overheid. Een kritische massa is de voorwaarde van succes.

In de markt zien we successen ten aanzien van adoptie van standaarden als iDEAL en iSHARE. Daar waar in de markt sprake is van marktfalen treedt de overheid soms stimulerend op, zoals bij Simplerinvoicing en iSHARE. Tegelijkertijd zien we dat binnen de overheid het veel inspanning kost om tot implementatie en naleving van standaarden, bijvoorbeeld zoals opgenomen in de PTOLU-lijst, te komen. Het Forum voor standaardisatie zegt over deze adoptieverplichting en over de verantwoording vanuit overheden in haar 'Monitor open standaarden 2018' het volgende:
'Na ruim tien jaar verplichten tot leg-uit komt het nog steeds zelden of nooit voor dat een overheidsorganisatie zich in het jaarverslag verantwoordt over het niet-toepassen van de relevante standaard(en).' [28]
(Hoewel dit wel verplicht is volgens de Rijksbegrotingsvoorschriften; VKA/Berenschot.)

Daar waar in de markt gesproken wordt over marktfalen bij toepassen van standaarden, kent ook de overheid vormen van ontwijkend gedrag en niet-naleving. Hier kunnen verschillende oorzaken aan ten grondslag liggen. Bijvoorbeeld door het simpelweg vasthouden aan eigen methoden en technieken, daar waar de standaarden uit de PTOLU-lijst voor de hand liggen en daar tevens geen verantwoording over afleggen conform de Rijksbegrotingsvoorschriften.[29]

De overheid dient het goede voorbeeld te geven, maar het komt nog steeds voor dat verplichte standaarden niet geïmplementeerd worden, zonder dat daar een goede reden voor gegeven wordt. Het wettelijk verplichten van standaarden via het Wetsvoorstel Digitale Overheid is een ingreep die mogelijk kan leiden tot een bredere naleving van de standaarden van de PTOLU-lijst, maar is wel een ultimum remedium en verplichtstelling is alleen effectief als daarbij ook handhaving en toezicht op de naleving van deze verplichtingen wordt ingevuld. Hierdoor kan de Minister van BZK tijdig ingrijpen en voorkomen dat standaarden niet worden geadopteerd zoals dit nu waargenomen wordt bij de PTOLU-lijst. Naast wettelijke verplichting is het zeer wenselijk dat ook andere methoden van adoptie worden nagestreefd.

De richting die de WDO gekozen heeft voor toezicht gaat echter sterk uit van de bestaande (inter-)bestuurlijke verhoudingen en bestaande toezichtmechanismen. Vaak zijn de toetsingen te laat en bestaat alleen een verantwoording achteraf, waardoor bijsturen onmogelijk of zeer kostbaar is. In het uiterste geval leidt dit tot afblazen van het initiatief.

28 Forum Standaardisatie, Duiding en maatregelen Monitor Open standaarden 2018, 12 december 2018, FS 181212.4A1, p.2.
29 Rijksbegrotingsvoorschriften 2019, 3 april 2019, Toelichting paragraaf 2 - Rijksbrede bedrijfsvoering onderwerpen, p.297.

Bij veel innovatieve projecten waar standaardisatie een rol speelt is vaak sprake van kleine stapjes en kort cyclische ontwikkeling, ook wel Agile en Scrum genoemd. Alleen een formele business case en projectplan als legitimatie voldoet daar niet. Ook meer formele projectaudits dragen niet bij aan de innovatie. Juist bij deze innovatieve trajecten is een andere aanpak nodig: meer van onderaf en met meer kennisdeling op de werkvloer. Niet vrijblijvend en met een sterk appel op de eigen verantwoordelijkheid van de betrokken organisatie. De overheid kan daarbij een voorbeeld nemen aan ICT gedreven lean startup initiatieven. Veel overheidsinitiatieven zijn sterk innovatief en vergelijkbaar met lean startups. Deze voeren voorafgaand aan het bouwtraject een gebruikerstoets uit. Wil en kan de gebruiker dit product afnemen? Is gebruik gemaakt van de laatste ICT-standaarden? Volgen we markt best practices? Veel impactanalyses bij de overheid zijn juridisch en/of technologisch gedreven, terwijl de wenselijkheid voor de burger of de ondernemer meer centraal moet staan. Programma's als Gebruiker Centraal benadrukken dit stellig.

Goede voorbeelden van een dergelijke benadering treffen we aan in het Verenigd Koningrijk (VK) en de Verenigde Staten (VS). In het VK is een Service Standard opgesteld, waarbij overheidsorganisaties verplicht worden om aan de hand van veertien checkpunten na te gaan of de digitale dienst die men ontwikkelt goed genoeg is voor publiek gebruik van de dienst. In de VS is met het bureau 18F een instituut opgericht dat organisaties actief helpt om publieke diensten zoals websites of toepassingen te verbeteren, om nieuwe technieken in te zetten bij implementatie van wetten en door middel van digitalisering interne bedrijfssystemen te stroomlijnen, zodat tijd en kosten bespaard worden en de betrouwbaarheid van de dienstverlening vergroot.

Een dergelijke proactieve en ook preventieve vorm van betrokkenheid van een centrale overheidsinstantie voorkomt teleurstellingen en ongewenste ontwikkeling die achteraf weer gecorrigeerd moeten worden.

Wetgeving die beleidsdoelen uit NL DIGIbeter raakt

Bijlage F

In deze bijlage beschrijven we, niet limitatief, ontwikkelingen van nationale en Europese wetgeving waaruit standaardisatie kan voortkomen en die aansluiten bij één of meerdere beleidsdoelen uit NL DIGIbeter.

F.1 E-overheid in Europa (Tallinnverklaring)

In deze verklaring, getekend in oktober 2017, hebben de Ministers van de Europese lidstaten afspraken gemaakt over een gezamenlijke richting voor de digitale overheid en waar de Europese Commissie zich aan zal committeren.

Zo is opgenomen dat burgers en bedrijven digitaal kunnen communiceren met de overheid en dat bij het ontwikkelingen van digitale diensten de burgers en bedrijven centraal dienen te staan. Daarbij dient aandacht te zijn voor het verbeteren van de dienstverlening waaronder een meer proactieve dienstverlening, vaardigheden en toegankelijkheid. Elementen die in de Tallinnverklaring worden genoemd zijn:

- Identificeren van opties voor eenmalige gegevensverstrekking tussen lidstaten;

- De mogelijkheid tot inzage en correctie van persoonlijke gegevens;
  - Hierin speelt de Europese Algemene Verordening Gegevensbescherming (AVG) een belangrijke rol.

- De kwaliteit van open data vergroten.
  - Voor de Nederlandse overheid is hiervoor onder andere relevant de Wet hergebruik van overheidsinformatie. Dit betekent dat overheidsinformatie ter beschikking moet worden gesteld. In de wet en de richtlijn[30] is opgenomen dat zoveel mogelijk aan formele en open standaardisatie moet worden gebruikt ten aanzien van het formaat en de metadata.

- Passende aandacht voor vertrouwen en veiligheid waarbij een risico gerichte aanpak gevolgd wordt.
  - Vanaf 1 januari 2020 wordt de Baseline Informatiebeveiliging Overheid (BIO) van kracht. Deze vervangt de BIG, BIR, IBI en BIWA. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek.

De Tallinnverklaring sluit aan bij de volgende NL DIGIbeter beleidsdoelen:

- Er wordt gezorgd voor veilige informatie en dienstverlening;
- Burgers en ondernemers krijgen recht op digitale dienstverlening;
- Burgers en ondernemers kunnen zelf de regie voeren op hun (persoons)gegevens.

30 Richtlijn 2003/98/EG.

F.2 Wetsvoorstel modernisering elektronisch bestuurlijk verkeer

In januari 2021 moet de wet modernisering elektronisch bestuurlijk verkeer inwerkingtreden. Met het wetsvoorstel modernisering elektronisch bestuurlijk verkeer wijzigt de wetgever de Algemene wet bestuursrecht (Awb). De Awb bevat de algemene regels voor de verhouding tussen de overheid en individuele burgers en bedrijven.[31] Het wetsvoorstel regelt dat burgers en bedrijven het recht krijgen om elektronisch zaken te doen met de overheid. Dat heeft voor bestuursorganen twee concrete gevolgen:

1. Zij moeten verplicht digitale kanalen open stellen voor ieder elektronisch formeel bericht gericht aan het bestuursorgaan. Onder een formeel bericht wordt verstaan: elk bericht dat deel uitmaakt van een procedure inzake een besluit, voorgeschreven melding of klacht.
2. Zij moeten digitale kanalen zo aanpassen dat aan de wettelijke eisen wordt voldaan (alleen noodzakelijk gegevens vragen, ontvangstbevestiging sturen, e-formulier beschikbaar stellen, bewijslast bij bestuursorgaan, mededeling bij weigering verkeerd ingezonden bericht).[32]

In de Awb, noch in het wetsvoorstel, worden open standaarden verplicht gesteld. Wel vereist de Awb dat elektronisch verkeer tussen burger en bestuursorgaan 'voldoende betrouwbaar en vertrouwelijk' geschiedt. Welk betrouwbaarheidsniveau voor welk soort elektronisch bericht moet worden ingeregeld en of standaarden verplicht zijn, wordt daarbij opengelaten. Het is niet de verwachting dat in de Awb standaarden verplicht worden gesteld. Het is wel mogelijk dat de wetgever, om naleving te bevorderen, de toepassing van open standaarden gaat stimuleren of verplichten.

Het Wetsvoorstel modernisering elektronisch bestuurlijk verkeer sluit aan bij de volgende NL DIGIbeter beleidsdoelen:

- Burgers en ondernemers krijgen recht op digitale dienstverlening;
- Overheidsportalen worden gemoderniseerd.

31 https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2017/04/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer.pdf, p. 4.

32 https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2017/04/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer.pdf, p. 4 en 5.

F.3 Algemene verordening Gegevensbescherming (AVG)

In mei 2018 is de Algemene verordening Gegevensbescherming in werking getreden en heeft in Nederland de Wet bescherming persoonsgegevens (Wbp) vervangen. Met de AVG is in de hele Europese Unie dezelfde privacywetgeving gaan gelden. De AVG legt voor iedereen die persoonsgegevens verwerkt, dus ook aan overheden, eisen en verplichtingen op zodat op een zorgvuldige en veilige manier wordt omgegaan met persoonsgegevens. De Autoriteit Persoonsgegevens (AP), onderdeel van het ministerie van J&V, houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert gevraagd en ongevraagd ministeries, regering en parlement over (nieuwe) regelgeving.

De huidige AVG legt geen specifieke standaardisatie op ten aanzien van informatieveiligheid of de juiste verwerking van persoonsgegevens. De AVG stelt dat technische en organisatorische maatregelen moeten worden getroffen ten aanzien van het veilig omgaan met persoonsgegevens en het voldoen aan de AVG. AP stelt in haar huidige beleidsregels Beveiliging van persoonsgegevens dat verantwoordelijken de beveiligingsstandaarden moeten volgen. Als voorbeeld van zo'n standaard adviseert AP voor de zorgsector specifieke de NEN 7510 beveiligingsstandaard.[33] Deze standaard wordt echter niet wettelijk verplicht.

Voor het voldoen aan de AVG is nog geen officiële norm of standaardisatie vastgesteld. Dit zien we ook bevestigd worden in de bijlage van het jaarverslag van de Autoriteit Persoonsgegevens uit 2018.[34] De toezichthouder geeft daarbij aan dat er op dit moment nog geen instellingen geaccrediteerd zijn door de Raad voor de accreditatie voor het afgeven van AVG-certificaten

De AVG en Nederlandse uitvoeringwet AVG sluiten aan bij de volgende NL DIGIbeter beleidsdoelen:

- Wetgeving om rechten en waarden te borgen wordt toekomstbestendig gemaakt;
- Burgers en ondernemers krijgen recht op digitale dienstverlening;
- Burgers en ondernemers kunnen zelf de regie voeren op hun (persoons)gegevens;
- Er wordt gezorgd voor veilige informatie en dienstverlening.

F.4 Verordening: Single digital Gateway (EU 2018/1724)

De Verordening Single Digital Gateway voorziet in een Europese toegangspoort die Europeanen toegang geeft tot informatie en procedures. De verordening is in december 2018 in werking getreden.

Vanuit de EU komt er een toegangspoort voor integratie van verschillende netwerken en diensten op nationaal en EU-niveau om burgers en bedrijven te ondersteunen bij hun grensoverschrijdende activiteiten. Dit geeft EU-burgers en bedrijven toegang tot informatie die zij nodig hebben om hun recht op mobiliteit in de EU uit te oefenen en verzekert dat zij op niet-discriminerende wijze volledige toegang krijgen tot online procedures. Het gaat hier onder andere om digitale toegang tot procedures zoals: werken, studeren, verhuizen, registratie van motorvoertuigen, aanvragen voor een verblijfsattest, studieleningen, subsidies, erkenning van academische titels, Europese ziekteverzekeringskaart, pensioenuitkeringen en de registratie van werknemers voor pensioen- en verzekeringsstelsels. Burgers en ondernemers krijgen voor deze diensten het recht om eenmalig gegevens aan te leveren binnen de EU (het eenmaligheidsbeginsel).

Aanvullend stelt de Commissie uiterlijk op 12 juni 2021 uitvoeringshandelingen vast die gaan over het technisch systeem voor de grensoverschrijdende geautomatiseerde uitwisseling van bewijs en de toepassing van het „eenmaligheidsbeginsel'. In de uitvoeringshandelingen worden de benodigde technische en operationele specificaties van het technische systeem bepaald. De Commissie houdt daarbij rekening met de normen en technische kenmerken die zijn opgesteld door Europese en internationale organisaties en organen voor normalisatie, in het bijzonder het Europees Comité voor Normalisatie (CEN), het Europees Instituut voor telecommunicatienormen (ETSI), de Internationale Organisatie voor normalisatie (ISO), en de Internationale Telecommunicatie-unie (ITU), alsook de in artikel 32 van Verordening (EU) 2016/679 en artikel 22 van Verordening (EU) 2018/1725 bedoelde veiligheidsnormen.

De verordening geeft alle nationale, regionale en lokale overheden voor de verschillende onderdelen twee tot vijf jaar de tijd om de implementatie voor te bereiden. Binnen twee jaar moeten de centrale overheden hun informatievoorziening aangepast hebben voor EU-burgers en bedrijven. Voor lokale overheden geldt een termijn van vier jaar.

33 De NEN7510:2017 norm is gebaseerd op de ISO/ IEC 27001:2013.
34 Bijlage jaarverslag Autoriteit Persoonsgegevens 2018, 4 april 2019.

Het is de bedoeling dat vijf jaar na de inwerkingtreding alle relevante procedures voor EU-burgers en bedrijven toegankelijk zijn en voorzien van vertaalde toelichtingen. In die vijf jaar moeten de lidstaten daarvoor ook een uitwisseling op gang brengen waarin bewijsstukken onderling worden uitgewisseld: als een burger of bedrijf een aanvraag indient bij een overheidsorganisatie moet de laatste de relevante gegevens bij de lidstaat opvragen waar de aanvrager vandaan komt.

De Single Digital Gateway sluit aan bij de volgende NL DIGIbeter beleidsdoelen:

- Overheidsportalen worden gemoderniseerd;
- Digitale identificatiemiddelen en digitaal machtigen worden doorontwikkeld;
- Burgers en ondernemers krijgen recht op digitale dienstverlening;
- Informatie en dienstverlening worden begrijpelijk en toegankelijk.

eIDAS-Verordening

Met de Europese eIDAS-Verordening hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Per 29 september 2018 moeten overheden en privaatrechtelijke organisaties met een publieke taak Europees erkende inlogmiddelen accepteren binnen de digitale dienstverlening. Deze verplichting geldt onder andere voor organisaties die gebruik maken van DigiD en eHerkenning. De Europese Unie wil hiermee regelen dat het makkelijker en veiliger wordt om binnen Europa online zaken te regelen.

De eIDAS-Verordening schrijft in de inleiding het volgende over standaardisatie:

'Een op internationale normen gebaseerde IT-veiligheidscertificering, zoals ISO 15408 en verwante evaluatiemethoden en regelingen voor wederzijdse erkenning, is een belangrijk instrument voor de verificatie van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen, en dient te worden gestimuleerd. Innovatieve oplossingen en diensten zoals mobiel ondertekenen en ondertekenen in de cloud berusten echter op technische en organisatorische oplossingen voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen waarvoor nog geen beveiligingsstandaarden voorhanden zijn of waarvoor de eerste IT-veiligheidscertificeringsprocedure nog loopt. Het beveiligingsniveau van dergelijke gekwalificeerde apparatuur voor het aanmaken van elektronische handtekeningen kan worden geëvalueerd door gebruik te maken van alternatieve processen, maar enkel indien dergelijke veiligheidsnormen niet beschikbaar zijn of indien de eerste IT-veiligheidsbeoordeling aan de gang is. Deze processen dienen vergelijkbaar te zijn met de standaarden voor IT-veiligheidscertificering, voor zover het om gelijke beveiligingsniveaus gaat. Deze processen zouden baat kunnen hebben bij onderlinge evaluatie.'

De eIDAS-Verordening sluit aan bij de volgende NL DIGIbeter beleidsdoelen:

- Digitale identificatiemiddelen en digitaal machtigen worden doorontwikkeld;
- Door middel van standaardisatie toegankelijkheid, veiligheid en betrouwbaarheid van digitale dienstverlening waarborgen;
- Er wordt gezorgd voor veilige informatie en dienstverlening.

F.5 Wet basisregistratie personen (Wet BRP)

De Wet Basisregistratie Personen (Wet BRP) vormt sinds 2014 de basis voor de registratie van persoonsgegevens in de Basisregistratie Personen (BRP). Alle overheidsinstellingen en bestuursorganen (zoals de Belastingdienst) zijn verplicht voor hun taken gebruik te maken van de BRP. De wet beschrijft aan welke eisen beheerders en gebruikers van de BRP moeten voldoen. Ook geeft de wet aan voor welke doelen die informatie gebruikt mag worden.

Ook de technische systemen waarin persoonsgegevens worden opgeslagen vallen onder de Wet BRP. Daarbij gaat het om de beveiligde opslag van de informatie. Maar ook om de uitwisseling van gegevens tussen beheerders en afnemers. Deze wettelijke eisen worden uitgewerkt in technische specificaties voor de systemen van gemeenten en afnemers. Deze technische specificaties staan omschreven in het Logisch Ontwerp GBA 3.11 (LO GBA). Het Logisch Ontwerp beschrijft de minimaal te stellen functionele eisen aan de aangesloten systemen en aan het GBA-netwerk. In het Logisch Ontwerp wordt bijvoorbeeld minimaal de Teletex-standaard[35] en de X.400 standaard vereist voor elektronische berichtenuitwisseling.

De Wet basisregistratie personen sluit aan bij de volgende NL DIGIbeter beleidsdoelen:

- Burgers en ondernemers kunnen zelf de regie voeren op hun (persoons)gegevens;
- De overheid gaat met de tijd mee.

F.6 ePrivacy Verordening

Op 10 januari 2017 heeft de Commissie een voorstel voor een verordening betreffende privacy en elektronische communicatie ingediend, om de huidige regels aan te passen aan de technische ontwikkelingen en aan de Algemene Verordening Gegevensbescherming. Het wetsvoorstel is nog niet aangenomen en daarmee is ook onduidelijk wanneer de verordening in werking zal treden.

Het doel is het vertrouwen in en de veiligheid van de digitale eengemaakte markt te versterken. De huidige e-privacyregels gelden namelijk alleen voor traditionele telecomaanbieders en niet voor diensten als Skype, WhatsApp, Facebook Messenger en Gmail. Om te waarborgen dat de elektronische communicatie vertrouwelijk wordt behandeld, ongeacht de gebruikte technologie, gelden de voorgestelde regels ook voor op internet gebaseerde spraakdiensten en chatten via internet. Tegelijkertijd beoogt de Commissie nieuwe kansen te creëren voor het bedrijfsleven.

In de verordening worden geen standaarden geadviseerd of verplicht gesteld.

De ePrivacy Verordening sluit aan bij de volgende NL DIGIbeter beleidsdoelen:

- Wetgeving om rechten en waarden te borgen wordt toekomstbestendig gemaakt;
- Burgers en ondernemers kunnen zelf de regie voeren op hun (persoons)gegevens;
- Beschermen van grondrechten en publieke waarden.

35 Gebaseerd op CCITT-aanbeveling Rec. T.61

VERDONCK KLOOSTER & ASSOCIATES

VKA combineert technische kennis met organisatorische ervaring

Als medewerkers van VKA hebben we een ding gemeen: we willen ICT projecten laten slagen. Als het moet zetten we daar alles voor opzij. We houden dan ook niet van politiek bedrijven, stoelen warm houden, meehuilen of klagen. Maar een groot ICT project tot een goed einde brengen, dat ervaren wij als succes. Voor u en voor onszelf. Door onze gedrevenheid en onze expertise is VKA een toonaangevend adviesbureau voor strategische ICT projecten geworden. Dat is een positie die we in de loop der jaren hebben veroverd. Een advies van VKA is onbetwistbaar goed, gebaseerd op gedegen kennis en het wordt uitgebracht door vaardige professionals.

ICT dient de mens. Dat is kort gezegd de opvatting van Verdonck, Klooster & Associates. En als strategisch ICT adviesbureau hebben we de technische kennis én de organisatorische ervaring om dat ook echt waar te maken. Het maakt ons een unieke partner voor opdrachtgevers die het hoogste rendement uit hun ICT investeringen willen halen.

Bij VKA zijn we er van overtuigd dat Nederland door een goede inzet van ICT nog sterker kan worden. De dienstverlening aan burgers en bedrijven kan sneller, beter en eenvoudiger. De duurzaamheid kan worden verbeterd. En er zijn uitstekende kansen voor innovatieve nieuwe concepten die we nog beter kunnen benutten. Om grote projecten te laten slagen, moet volgens ons vooraf de strategische impact beter worden onderkend. Want ICT overstijgt al lang het technische domein van de afdeling automatisering. Bedrijven en organisaties zijn zo afhankelijk geworden van een goed werkende informatievoorziening, dat het vaak een van de belangrijkste strategische onderwerpen op de agenda is geworden. Dat maakt ICT tot een multidisciplinair vakgebied waar technologie, bedrijfsprocessen en organisatie bij elkaar komen.

Verdonck Klooster & Associates
Baron de Coubertinlaan 1, 2719 EN Zoetermeer
Postbus 7360, 2701 AJ Zoetermeer
079 368 1000
www.vka.nl

Berenschot is een onafhankelijk organisatieadviesbureau met 350 medewerkers wereldwijd. Al 80 jaar verrassen wij onze opdrachtgevers in de publieke sector en het bedrijfsleven met slimme en nieuwe inzichten. We verwerven ze en maken ze toepasbaar. Dit door innovatie te koppelen aan creativiteit. Steeds opnieuw. Klanten kiezen voor Berenschot omdat onze adviezen hen op een voorsprong zetten.

Ons bureau zit vol inspirerende en eigenwijze individuen die allen dezelfde passie delen: organiseren. Ingewikkelde vraagstukken omzetten in werkbare constructies. Door ons brede werkterrein en onze brede expertise kunnen opdrachtgevers ons inschakelen voor uiteenlopende opdrachten. En zijn we in staat om met multidisciplinaire teams alle aspecten van een vraagstuk aan te pakken.

Berenschot Groep B.V.
Europalaan 40, 3526 KS Utrecht
Postbus 8039, 3503 RA Utrecht
030 2 916 916
www.berenschot.nl
/berenschot

Berenschot