Wettelijk kader e-Overheid

Juridische eisen ten aanzien van de e-Overheid en ten aanzien van een interoperabiliteitsraamwerk

Versie 1.1

augustus 2008

Universiteit van Tilburg **TILT – Centrum voor Recht, Technologie en Samenleving**	**Duthler Associates**
Postbus 90153 5000 LE Tilburg	Frankenslag 137 2582 HH 's-Gravenhage
<j.e.j.prins@uvt.nl>	<a.w.duthler@duthler.nl>

INHOUDSOPGAVE

1 Inleiding

1.1 Introductie

Dit rapport is opgesteld door TILT, het Centrum voor Recht Technologie en Samenleving van de Universiteit van Tilburg, en Duthler Associates, adviseurs voor bestuur, recht en ICT. Het bevat een analyse van het wettelijk kader dat randvoorwaardelijk is voor de invulling van het functioneren van de e-Overheid in het algemeen, en het op te stellen interoperabiliteitsraamwerk in het bijzonder.

1.2 Aanleiding

De staatssecretaris van Economische Zaken heeft het Forum Standaardisatie verzocht een interoperabiliteitsraamwerk te ontwikkelen. Het interoperabiliteitsraamwerk beschrijft de principes en samenstellende bestanddelen die randvoorwaardelijk zijn voor de bouw van de e-Overheid. Doelstelling van dit raamwerk is sturing op interoperabiliteit mogelijk te maken. Eén van de onderdelen van het interoperabiliteitsraamwerk betreft afspraken over te gebruiken standaarden. De afspraken moeten passen binnen het wettelijk kader dat op de e-Overheid van toepassing is.

1.3 Opdracht en onderzoeksvragen

De opdrachtomschrijving luidt als volgt:

- Stel een indicatief overzicht op van de belangrijkste Nederlandse en Europese wet- en regelgeving die randvoorwaardelijk zijn voor de invulling en het functioneren van de e-Overheid in Nederland. Betrek daarbij ook de belangrijkste sectorale wetgeving op hoofdlijnen.
- Inventariseer welke (deel)studies er zijn over dit onderwerp, zowel gericht op Nederland als op Europa.
- Analyseer welke eisen op basis van de gevonden wet- en regelgeving gesteld moeten worden aan de inrichting van de e-Overheid in het algemeen en aan het op te stellen interoperabiliteitsraamwerk in het bijzonder.
- Stel vast wat de mogelijke knelpunten en hiaten zijn met betrekking tot deze eisen.

Naar aanleiding van de opdrachtomschrijving is de volgende **centrale vraag** geformuleerd: Welke randvoorwaarden voor het interoperabiliteitsraamwerk zijn af te leiden uit de nationale en Europese wettelijke regelingen, zoals van toepassing op e-overheidsdiensten en –handelingen? Welke knelpunten en hiaten zijn waar te nemen? De volgende **onderzoeksvragen** vloeien voort uit de centrale vraagstelling:

1. Welke wet- en regelgeving is randvoorwaardelijk voor de elektronische overheid, en in het bijzonder het op te stellen interoperabiliteitsraamwerk?
2. Welke voor het onderwerp relevante deelstudies zijn er reeds verschenen in Nederland en Europa?
3. Hoe werkt de geïnventariseerde wet- en regelgeving uit ten aanzien van rechten/plichten, taken/verantwoordelijkheden en eisen/randvoorwaarden op de terreinen van vergaring, gebruik/verstrekking en bewaring/vernietiging van gegevens?
4. Wat zijn knelpunten en hiaten in de geïnventariseerde wet- en regelgeving voor de elektronische overheid, en in het bijzonder het interoperabiliteitsraamwerk?
5. Welke conclusies en aanbevelingen kunnen worden geformuleerd op basis van de antwoorden op voorgaande deelvragen?

1.4 e-Overheid en interoperabiliteit

Bij het uitvoeren van een onderzoek naar de juridische randvoorwaarden ten aanzien van de e-Overheid en een interoperabiliteitsraamwerk, is het van belang eerst vast te stellen wat er onder 'e-Overheid' en 'interoperabiliteit' dient te worden verstaan.

Onder e-Overheid kan kortweg worden verstaan dat langs elektronische weg door of met de overheid (in verschillende hoedanigheden) kan worden gecommuniceerd. Het gebruik van de zinsnede 'de e-Overheid' is enigszins misleidend omdat het suggereert dat er sprake is van één centrale 'elektronische overheid'. Toch is de zinsnede 'de e-Overheid' inmiddels ingeburgerd. Daarom wordt in dit rapport ook gesproken van 'de e-Overheid'.

Met betrekking tot de betekenis van de term 'interoperabiliteit' kan worden gewezen op het recente rapport met betrekking tot een Nederlands interoperabiliteitsraamwerk, opgesteld door RAND Europe in opdracht van het Forum Standaardisatie.[1] In dit rapport wordt interoperabiliteit omschreven als:

> 'The ability of distinct systems to communicate and share semantically compatible information, perform compatible transactions, and to interact in ways that support compatible business processes to enable users to perform desired tasks.'[2]

Met deze definitie komen de volgende elementen aan de orde:

- het gaat om communicatie en het delen van informatie;
- het gaat om semantische *compatibility*, *compatible* transacties en *compatible* processen;
- interoperabiliteit is erop gericht gebruikers in staat te stellen gewenste taken uit te voeren.

De vraag rijst echter wat de betekenis is van de term '*compatible*'. Hierdoor is het mogelijk dat de vraag naar de betekenis van de term 'interoperabiliteit' wordt beantwoord, maar dat daarvoor een nieuwe vraag in de plaats komt, namelijk de vraag naar de betekenis van '*compatible*'.

In de NORA 2.0 wordt het volgende opgemerkt over interoperabiliteit:

> 'Bedrijfsprocessen en hun ondersteunende ICT systemen zijn interoperabel als ze digitaal data en kennis kunnen uitwisselen. Standaarden zijn afspraken over de vorm van de uitwisseling van gegevens. Standaarden bestaan naast afspraken over architectuur.
> Het EIF (European Interoperability Framework – red) maakt voor interoperabiliteit een onderverdeling in drie niveaus:
>
> - Organisatorisch: afspraken over regelgeving, bedrijfsprocessen en uitvraagmomenten
> - Semantisch: afspraken over de betekenis van de gegevens
> - Technisch: afspraken over transport en logistiek van de uitwisseling'[3]

Blijkens deze omschrijving draait het bij interoperabiliteit om:

- het uitwisselen van informatie (data en kennis);

[1] RAND Europe & GNKS Consult, *Towards a Dutch Interoperability Framework. Recommendations to the Forum Standaardisatie*, 2007 (hierna: RAND 2007).
[2] RAND 2007, p. 6.
[3] NORA 2.0, p. 57.

- drie niveaus: organisatorisch, semantisch en technisch;

Deze twee elementen komen inhoudelijk overeen met de eerste twee elementen van de RAND-omschrijving, ook al is de formulering anders. Een verschil lijkt eruit te bestaan dat de RAND-omschrijving uitgaat van een gerichtheid op het uitvoeren van gewenste taken. Een 'gerichtheid' wordt in de NORA-omschrijving niet expliciet genoemd, maar blijkt wel impliciet. Er wordt immers gesproken van *uitwisselen* en *afspraken*, en er wordt gesuggereerd dat er sprake is van verschillende bedrijfsprocessen waarover afspraken dienen te worden gemaakt, kennelijk met als doel ze beter op elkaar af te stemmen. Hieruit blijkt dat er sprake is van een gerichtheid op *samenwerken*. De NORA-omschrijving is hiermee iets specifieker dan de RAND-omschrijving, waarin immers wordt uitgegaan van het ruimere 'uitvoeren van gewenste taken'.

Aan de hand van bovenstaande korte vergelijking, wordt in dit rapport uitgegaan van de volgende omschrijving van interoperabiliteit, waarbij samenwerking de centrale doelstelling is:

> *Interoperabiliteit is het vermogen (organisatorisch, semantisch en technisch) om gegevens uit te wisselen en processen op elkaar af te stemmen met het oog op samenwerking.*

Een *interoperabiliteitsraamwerk* kan uit verschillende, meerdere, componenten bestaan, bijvoorbeeld uit:

- beleidsbeginselen ten aanzien van interoperabiliteit;
- een referentiearchitectuur;
- een semantisch raamwerk (ontologieën e.d.);
- technische standaarden.[4]

Omdat een interoperabiliteitsraamwerk uit verschillende specifieke componenten kan bestaan, worden in dit onderzoek de juridische randvoorwaarden ten aanzien van interoperabiliteit in het algemeen geschetst. Indien het onderzoek op één of meerdere mogelijke onderdelen van een interoperabiliteitsraamwerk zou worden gericht, zou de toegevoegde waarde ervan beperkt zijn. De randvoorwaarden kunnen in een later stadium worden toegepast bij het opstellen van een interoperabiliteitsraamwerk.

1.5 Werkwijze

Ter uitvoering van het onderzoek is de volgende werkwijze gehanteerd.

Stap 1
In de eerste plaats is er een indicatief overzicht van wet- en regelgeving opgesteld en zijn de relevante (deel)studies geïnventariseerd.

Stap 2
In de tweede plaats is de relevante wet- en regelgeving geanalyseerd.

De analyse heeft ook plaats gevonden door in een viertal cases schriftelijke en deels mondelinge interviews te houden. Dit is gebeurd ten aanzien van de volgende cases:

1. het elektronisch bouwloket/omgevingsloket;
2. het digitaal klantdossier (DKD);
3. het elektronisch proces-verbaal (ePV); en
4. het uitwisselen van geo-informatie.

[4] Vgl. RAND 2007, p. 13-14.

De keuze voor deze vier cases vloeit voort uit het oogmerk diverse niveaus en organisaties te bestrijken (lokaal, regionaal en nationaal; gemeenten, uitvoeringsorganisaties, centrale overheidsdiensten en -organisaties). De vier cases voldoen aan de volgende criteria.

- De cases betreffen elektronische dienstverlening en gegevensuitwisseling in *verschillende beleidsdomeinen*. Zo kan een divers palet aan de toepassing van de belangrijkste relevante wet- en regelgeving worden bestudeerd. Het gaat hierbij zowel om de uitleg van wet- en regelgeving als de toepassing ervan.
- Bij de cases is sprake van *interorganisatorische- dan wel keten-samenwerking*, d.w.z. verschillende publieke organisaties zijn betrokken bij de elektronische dienstverlening en gegevensuitwisseling. Dit is van belang met het oog op het op te stellen interoperabiliteitsraamwerk.
- Ten slotte zijn de cases *voldoende operationeel* om daadwerkelijke effecten en consequenties van de uitwerking van wet- en regelgeving in de praktijk van de elektronische overheid te kunnen bestuderen en analyseren. ‘Voldoende’ operationeel wil zeggen dat er tenminste een aantal pilots heeft plaatsgevonden.

Stap 3
Aan de hand van de analyse en de *case studies* die plaatsvonden in stap 2, zijn knelpunten en hiaten, eisen en randvoorwaarden, en conclusies en aanbevelingen geformuleerd.

1.6 Leeswijzer

De resultaten van de hierboven genoemde stappen, zijn als volgt in het rapport opgenomen. Het indicatieve overzicht van wet- en regelgeving en de inventarisatie van de relevante (deel)studies (stap 1) opgenomen in bijlage 1 respectievelijk bijlage 2. Hoofdstuk 2 bevat de analyse van de relevante wet- en regelgeving (stap 2). In hoofdstuk 3 komen de cases aan de orde. De knelpunten en hiaten, de eisen en randvoorwaarden, en de conclusies en aanbevelingen zijn opgenomen in respectievelijk hoofdstuk 4, 5 en 6.

2 Het wettelijk kader van de e-Overheid

2.1 Inleiding

In de nu volgende paragrafen wordt het wettelijk kader voor de elektronische overheid nader toegelicht.

Er is niet één, overkoepelend wettelijke regeling ten aanzien van de elektronische overheid. De relevante wettelijke regels zijn in vele verschillende wetten te vinden. In dit onderzoek worden de volgende wetten toegelicht:

- de Wet elektronisch bestuurlijk verkeer (Webv);
- de Wet elektronische handtekeningen (Weh);
- de Wet bescherming persoonsgegevens (Wbp);
- de Wet algemene bepalingen burgerservicenummer (Wabb);
- de wetgeving inzake de basisregistraties, waaronder de Wet Gemeentelijk Basisadministratie (WGBA);
- de Wet openbaarheid van bestuur (Wob);
- de Auteurswet (Aw);
- de Databankenwet (Dw);
- de Archiefwet 1995;
- de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), in samenhang met de Wet eenmalige gegevensuitvraag werk en inkomen (WEU);
- het Wetboek van Strafvordering (Sv) voor wat betreft het elektronisch proces-verbaal;
- het wetsvoorstel Wet algemene bepalingen omgevingsrecht (Wabo)

Naast deze Nederlandse wet- en regelgeving, is ook de volgende Europese regelgeving relevant:[5]

- de Dienstenrichtlijn;
- de INSPIRE-richtlijn.

De genoemde wetten en regelingen worden hierna in hoofdlijnen besproken.

2.2 Wet elektronisch bestuurlijk verkeer (Webv)

Met de Wet elektronisch bestuurlijk verkeer[6] (Webv) zijn bepalingen toegevoegd aan de Algemene wet bestuursrecht. De Webv bevat algemene regels betreffende het verkeer langs elektronische weg tussen burgers en bestuursorganen en tussen bestuursorganen onderling.[7] Uit deze formulering blijkt dat de Webv niet van toepassing is op het verkeer met de rechter.[8]

Nevenschikking

Eén van de achterliggende gedachten bij de Webv, is dat de elektronisering van de samenleving niet ten koste mag gaan van hen die (nog) geen toegang hebben tot het

[5] Hier wordt Europese wet- en regelgeving genoemd die nog niet is geïmplementeerd met in de genoemde Nederlandse wet- en regelgeving.

[6] *Stb.* 2004, 214. Inwerkingtreding met ingang van 1 juli 2004, *Stb.* 2004, 260. Zie voor een overzicht van de praktijk en de jurisprudentie met betrekking tot de Wet elektronisch bestuurlijk verkeer M.M. Groothuis, 'De elektronische overheid twee jaar na de inwerkingtreding van de Wet elektronisch bestuurlijk verkeer', *Computerrecht* 2006/4, p 193-199; en G. Overkleeft-Verburg, 'Elektronisch bestuurlijk verkeer in de Awb. Rechtspraktijk en rechtspraak', *JBplus* 2008, p. 20-38.

[7] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 3.

[8] Naar verwachting zal op den duur de Webv ook van toepassing zijn op het verkeer met de bestuursrechter. In december 2007 heeft de Commissie wetgeving algemene regels van bestuursrecht een voorontwerp van een wet met die strekking aangeboden aan de ministers van Justitie en BZK.

elektronisch verkeer. Deze gedachte heeft geleid tot het beginsel van *nevenschikking*. Dit beginsel houdt in dat het conventionele, 'papieren' verkeer niet mag worden verdrongen door elektronisch verkeer. De Webv bevat dan ook de volgende uitgangspunten:

- de burger bepaalt in welke vorm het verkeer plaatsvindt indien het bestuursorgaan over beide mogelijkheden beschikt;
- voor zover het bestuursorgaan over bepaalde zaken alleen maar op conventionele wijze communiceert, heeft de burger geen keus; hij kan elektronisch verkeer niet afdwingen;
- het is het bestuursorgaan niet toegestaan bepaalde zaken alleen nog maar langs elektronische weg te doen, tenzij alle betrokkenen hiermee instemmen.[9]

Er zijn uitzonderingssituaties op bovenstaande uitgangspunten mogelijk, waarin de burger wel wordt verplicht langs elektronische weg te communiceren. Zo'n uitzonderingssituatie moet dan wel een grondslag hebben in een formele wet.[10] Het gaat bijvoorbeeld om de volgende situaties.

- In sommige gevallen dienen bedrijven op elektronische wijze aangifte te doen inzake de volgende belastingen:
  - de inkomstenbelasting;
  - de vennootschapsbelasting;
  - de omzetbelasting;
  - de loonbelasting;
  - de verpakkingenbelasting.[11]
- De zogenaamde Eerstedagsmelding dient langs elektronische weg te worden gedaan.[12]
- Ten aanzien van de omgevingsvergunningen wordt er gestreefd naar de situatie dat bedrijven slechts op elektronische wijze een vergunningsaanvraag kunnen doen, wat op den duur kan leiden tot het uitsluiten van de schriftelijke aanvraag.[13]

Kenbaarmaking

Zowel de burger als het bestuursorgaan dienen kenbaar te maken dat de elektronische weg is opengesteld.[14] De kenbaarmaking door het bestuursorgaan dat de elektronische weg is geopend, kan zowel geschieden in een algemene regeling, als in een bericht aan één of meer geadresseerden. Kenbaarmaking kan bijvoorbeeld plaatsvinden doordat in een brochure, huis-aan-huis-blad of op een website te kennen wordt gegeven waar op het internet aanvragen voor een bepaald soort vergunning kunnen worden gedaan, klachten kunnen worden ingediend, en dergelijke. De enkele beschikbaarheid van een elektronisch adres, betekent nog niet dat daarmee voor alle mogelijke handelingen de elektronisch weg openstaat.[15]

---

[9] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 8, artikel 2:14 lid 1 en 2:15 lid 1 Awb.
[10] Dit uitgangspunt, inhoudende dat verplicht gebruik van de elektronische weg mogelijk is bij of krachtens de wet, kan worden gegrond op artikel 2:13 lid 1 juncto lid 2 sub a Awb.
[11] Artikel 8 lid 2 sub a Awr juncto artikel 20 lid 2 Uitvoeringsregeling Awr 1994. Vgl. Rb. Arnhem 25 april 2007, *LJN* BA4054.
[12] Artikel 28 sub f Wet op de loonbelasting 1964 juncto artikel 66a lid 1 Uitvoeringsregeling loonbelasting 2001.
[13] *Kamerstukken II*, 2006/07, 30 844, nr. 3, p. 63. Zie ook de concept-voorontwerpen van het BOR (Besluit omgevingsrecht) en het MOR (Ministeriële regeling omgevingsrecht). Op het moment van schrijven ligt het wetsvoorstel Wet algemene bepalingen omgevingsvergunning (Wabo) ter beoordeling voor aan de Eerste Kamer. De Wabo, het BOR en het MOR worden behandeld in paragraaf 2.12.
[14] Respectievelijk artikel 2:14 lid 1 en 2:15 lid 1 Awb.
[15] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 13.

Nadere eisen
Het bestuursorgaan kan *nadere eisen* stellen aan het gebruik van de elektronische weg.[16] De nadere eisen kunnen betrekking hebben op uniforme behandeling en een veilig dataverkeer. Zo kan in het kader van een uniforme behandeling een bestuursorgaan stellen dat er gebruik dient te worden gemaakt van een bepaald elektronisch postadres, of van een bepaald 'format' van documenten. Voor massale processen kan een specifiek kanaal voor een specifieke berichtensoort met specifieke eisen worden opengesteld. Deze eisen kunnen worden vastgesteld in overleg met betrokkenen. De in overleg gemaakte afspraken kunnen worden vastgelegd in een uitwisselingsprotocol. Een uitwisselingsprotocol bevat onder meer de normen en standaarden die nodig zijn voor de communicatie en berichtdefinities die noodzakelijk zijn voor de automatische verwerking van de gegevens.[17]

De enkele verklaring dat een bestuursorgaan de elektronische weg heeft opengesteld, betekent op zichzelf niet zoveel. De vraag rijst dan op welke wijze, en ten behoeve van welke communicatiemiddelen de elektronische weg is opengesteld. De openstelling van de elektronische weg brengt daarom vrijwel automatisch met zich mee dat het bestuursorgaan ook beleid moet vaststellen in de vorm van de 'nadere eisen' waar de Awb over spreekt. De nadere eisen die het bestuursorgaan kan stellen, zijn waarschijnlijk aan te merken als een *beleidsregel* in de zin van de Awb.[18] Een voorbeeld van zo'n beleidsregel is het openstellingsbesluit van de Belastingdienst.[19]

Voldoende betrouwbare en vertrouwelijke communicatie
Eén van de belangrijkste onderdelen van de wettelijke regeling van het elektronisch verkeer tussen burger en bestuursorgaan, is de norm van een voldoende betrouwbare en vertrouwelijke communicatie. Deze norm houdt in dat:

- indien een bestuursorgaan een bericht elektronisch verzendt, dan dient dit op een voldoende betrouwbare en vertrouwelijke manier te geschieden, gelet op de aard en inhoud van het bericht en het doel waarvoor het wordt gebruikt;[20]
- een bestuursorgaan een elektronisch verzonden bericht kan weigeren voor zover de betrouwbaarheid en de vertrouwelijkheid van dit bericht onvoldoende is gewaarborgd, gelet op de aard en inhoud van het bericht en het doel waarvoor het wordt gebruikt.[21] De weigering moet het bestuursorgaan ook melden aan de burger.[22]

Volgens de wetgever zijn in theorie drie maten van betrouwbaarheid en vertrouwelijkheid te onderscheiden:

- *maximale betrouwbaarheid en vertrouwelijkheid*, hiervan is sprake indien de beveiliging geheel conform de maximaal (technische) mogelijkheden plaatsvindt;
- *voldoende betrouwbaarheid en vertrouwelijkheid*, hiervan is sprake indien de veiligheid even groot is vergeleken met de situatie dat er uitsluitend van conventioneel verkeer gebruik zou worden gemaakt; en
- *pro forma betrouwbaarheid en vertrouwelijkheid,* hiervan is sprake indien de beveiliging slechts één stap verwijderd is van het bieden van geen enkele beveiliging; zij bestaat bijvoorbeeld uit de (elektronische) mededeling 'verboden toegang'.[23]

---

[16] Artikel 2:15 lid 1 Awb.
[17] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 13.
[18] Artikel 1:3 lid 4 Awb.
[19] 'Openstelling elektronisch bestuurlijk verkeer met de belastingdienst', 27 april 2005, nr. CPP 2004/2807M, *Stcrt.* 9 mei 2005, nr. 87, p. 12 e.v.
[20] Artikel 2:14 lid 3 Awb.
[21] Artikel 2:15 lid 3 Awb.
[22] Artikel 2:15 lid 4 Awb.
[23] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 16-17.

Volgens de wetgever moet worden gestreefd naar de middelste optie van een *voldoende betrouwbaarheid en vertrouwelijkheid*. Er dient te worden beoogd vergelijkbare waarborgen te bieden, als de waarborgen die het 'papieren verkeer' biedt. Bepalend is dat *elektronisch verkeer even betrouwbaar en vertrouwelijk moet zijn als conventioneel verkeer*. De wetgever wijst er ook op dat het niet gewenst is om in de elektronische situatie een hogere mate van betrouwbaarheid en vertrouwelijkheid te eisen dan bij conventionele communicatie. Voorts beoogt de wetgever met de eis van betrouwbaarheid en vertrouwelijkheid uitdrukking te geven aan de zogenaamde *algemene beginselen van behoorlijk IT-gebruik*. Hieronder worden verstaan de beginselen van authenticiteit, integriteit, onweerlegbaarheid, transparantie, beschikbaarheid, flexibiliteit en vertrouwelijkheid. Concreet kunnen deze beginselen bijvoorbeeld worden gewaarborgd met techniek waarmee een elektronische handtekening kan worden gezet, met een tijdsstempel of met behulp van cryptografische technieken.
Wanneer precies sprake is van een voldoende mate van betrouwbaarheid en vertrouwelijkheid, is in algemene zin moeilijk te zeggen. Uit bovenstaande blijkt, dat de hoofdregel is dat aard en inhoud van een bericht en het doel waarvoor het wordt gebruikt, bepalend zijn voor de mate van betrouwbaarheid en vertrouwelijkheid die vereist is. Hier dient steeds een vergelijking gemaakt te worden met het conventionele, papieren, verkeer: de mate van betrouwbaarheid en vertrouwelijkheid dient even groot te zijn als in het conventionele verkeer. Bijvoorbeeld aan de verlening van een vergunning dienen hogere eisen te worden gesteld dan aan het verstrekken van algemene inlichtingen.[24] Praktisch gezien betekent een en ander dat het bestuursorgaan de norm van een betrouwbare en vertrouwelijke communicatie in zijn beleid (de 'nadere regels') zal moeten uitwerken.[25]

2.3 Wet elektronische handtekeningen (Weh)

Met de Wet elektronische handtekeningen[26] (hierna: Weh) is de Europese richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen geïmplementeerd.[27] De richtlijn beoogt het gebruik van elektronische handtekeningen te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. De Weh bevat bepalingen betreffende de rechtsgevolgen van elektronische handtekeningen en de vereisten waaraan voldaan moet zijn, willen die rechtsgevolgen intreden. Daarnaast wordt de aansprakelijkheid van certificatiedienstverleners, het toezicht op certificatiedienstverleners en de vrijwillige accreditatie van certificatiedienstverleners geregeld. De Weh is een privaatrechtelijke regeling. De Wet elektronisch bestuurlijk verkeer verklaart echter delen van de Weh van overeenkomstige toepassing. Hierop wordt straks ingegaan.

De Weh verstaat onder een elektronische handtekening een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie.[28] Deze definitie is behoorlijk ruim. Bijvoorbeeld de ingescande handgeschreven handtekening kan hiermee als elektronische handtekening worden gekwalificeerd.[29] Zo'n ingescande handtekening zou bijvoorbeeld onder aan een e-mail bericht geplaatst kunnen worden. De handtekening is dan 'vastgehecht' aan andere elektronische gegevens, namelijk het e-mailbericht. Bovendien wordt

[24] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 14-17.
[25] Zie ter illustratie bijvoorbeeld het openstellingsbesluit van de Belastingdienst, zie noot 19.
[26] *Stb.* 2003, 199.
[27] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PbEG* 19-1-2000, L13/12. De bijlagen van de richtlijn zijn geïmplementeerd in het Besluit elektronische handtekeningen, Besluit van 8 mei 2003, *Stb.* 2003, 200.
[28] Artikel 3:15a lid 4 BW.
[29] *Kamerstukken II* 2000/01, 27 743, nr. 3, p. 2.

de handtekening dan gebruikt voor authentificatie. Onder authentificatie wordt waarschijnlijk verstaan dat de handtekening ertoe dient te stellen dat het bericht daadwerkelijk afkomstig is van de ondertekenaar en misschien ook dat de ondertekenaar is wie hij zegt te zijn.[30] Dit specifieke voorbeeld is overigens uiteraard niet bijzonder geschikt ter authentificatie, iedereen kan immers de handtekening van een ander inscannen en onder e-mailberichten plaatsen. De definitie van de elektronische handtekening is overigens zo ruim dat zelfs het plaatsen van een naam onder een e-mailbericht als elektronische handtekening kan worden aangemerkt. De vermelding van de naam dient immers ter authentificatie.

De Weh bevat een gelijkstellingsbepaling:

> 'een elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, indien de methode die daarbij is gebruikt voor authentificatie *voldoende betrouwbaar* is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval.'[31]

Onderdeel van de gelijkstellingsbepaling is dus een *betrouwbaarheidstoets*: de methode voor authentificatie moet voldoende betrouwbaar zijn. De wet bevat vervolgens een regel op grond waarvan een methode voor authentificatie wordt *vermoed* voldoende betrouwbaar te zijn. De gebruikte elektronische handtekening dient dan aan de volgende eisen te voldoen:

- zij is op unieke wijze aan de ondertekenaar verbonden;
- zij maakt het mogelijk de ondertekenaar te identificeren;
- zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
- zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
- zij is gebaseerd op een gekwalificeerd certificaat[32];
- zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen[33].[34]

Er zijn twee punten van kritiek uit te oefenen op de Weh. In de eerste plaats bepaalt de Weh dat een elektronische handtekening dezelfde 'rechtsgevolgen' heeft als de handgeschreven handtekening. Het is echter niet duidelijk welke rechtsgevolgen het betreft.[35] In de tweede plaats blijft er (ondanks de doelstelling van de Weh) een grote mate van rechtsonzekerheid bestaan vanwege de ruime definitie van de elektronische handtekening en vanwege de vraag hoe in de praktijk de betrouwbaarheidstoets dient te worden ingevuld

Evaluatie van de samenhang tussen de Wet elektronische handtekening en de Wet elektronisch bestuurlijk verkeer
Hierboven is in paragraaf 2.2 de norm van een betrouwbare en vertrouwelijk communicatie van de Wet elektronisch bestuurlijk verkeer (Webv) behandeld. Deze norm biedt voor

---

[30] In de Memorie van Toelichting bij het wetsvoorstel elektronisch bestuurlijk verkeer wordt overigens gesteld dat "met de term "authentificatie" uitdrukking [wordt] gegeven aan het beginsel van de authenticiteit", *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 41. Authenticiteit betreft volgens de Memorie van Toelichting de vraag of de inhoud van een bericht daadwerkelijk van de afzender afkomstig is, p. 15.
[31] Artikel 3:15a lid 1 BW.
[32] Als bedoeld in artikel 1.1, onderdeel *ss* van de Telecommunicatiewet.
[33] Als bedoeld in artikel 1.1, onderdeel *vv* van de Telecommunicatiewet.
[34] Artikel 3:15a lid 2 BW.
[35] Vgl. *kamerstukken I*, 2002/03, 27 743, nr. 35, p. 10, waar de Minister suggereert dat er voor de totstandkoming van de koopovereenkomst en van de huurovereenkomst een handtekening vereist is.

bestuursorganen het kader om het beleid inzake het gebruik van elektronische handtekeningen vast te stellen. De Webv bevat ook een gelijkstellingsbepaling, weliswaar anders geformuleerd dan de civielrechtelijke variant. De bepaling stelt:

> 'Aan het vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die daarbij voor authentificatie is gebruikt voldoende betrouwbaar is, gelet op de aard en de inhoud van het elektronische bericht en het doel waarvoor het wordt gebruikt. (…)'[36]

Deze bepaling bevat dus, net zoals de civielrechtelijke variant, een betrouwbaarheidstoets. De regeling inzake het wettelijk vermoeden dat een elektronische handtekening voldoende betrouwbaar is, indien is voldaan aan de betreffende vereisten, wordt van overeenkomstige toepassing verklaard.[37]

Het is nu de vraag hoe de norm van een betrouwbare en vertrouwelijke communicatie zich verhoudt tot de gelijkstellingsbepaling. De norm van een betrouwbare en vertrouwelijke communicatie moet door een bestuursorgaan worden ingevuld. Volgens de wetgever heeft de gelijkstellingsbepaling betrekking op een methode, op een bepaalde manier die bijdraagt aan de realisatie van de norm.[38] Met de norm kunnen dus de randvoorwaarden voor het elektronisch verkeer met een bestuursorgaan worden vastgesteld. Er kan daarbij ook worden vastgesteld hoe op elektronische wijze met vormvereisten worden omgegaan. De gelijkstellingsbepaling en het vermoeden van voldoende betrouwbaarheid hebben betrekking op één van de mogelijke manieren om invulling te geven aan de norm.

Er zijn twee toepassingen waarmee de overheid binnen de kaders van de Webv en de Weh te werk gaat: PKIoverheid en DigiD.

PKIoverheid
De Nederlandse overheid heeft een *Public Key Infrastructure* ingericht onder de naam *PKIoverheid*.
PKIoverheid is een infrastructuur onder verantwoordelijkheid van het Ministerie van Binnenlandse Zaken welke betrouwbare overheidscommunicatie realiseert. 'PKIoverheid kent één infrastructuur met één niveau van betrouwbaarheid. Met één elektronische identiteit van PKIoverheid kunnen eindgebruikers meerdere elektronische diensten van verschillende aanbieders afnemen.'[39] De Public Key Infrastructure (PKI) van de overheid is gebaseerd op Nederlandse en Europese standaarden (ETSI) en wetgeving (Weh).[40] De website van PKIoverheid verwijst naar de gelijksstellingsregel van de Weh, zoals neergelegd in het Burgerlijk Wetboek: 'Let er wel op dat het ondertekenen inhoudt dat u instemt met de inhoud van het document. Als u gebruik maakt van een gekwalificeerd certificaat dan zijn de rechtsgevolgen van de elektronische ondertekening gelijk aan die van een handgeschreven handtekening'.[41] Onder het kopje 'Wat is de juridische status van een ondertekend document' meldt de website: 'Voor formele stukken en contracten is rechtsgeldigheid van de handtekening cruciaal.'[42] Ook wordt gesteld dat certificaten worden gebruikt bij 'het zetten van een rechtsgeldige elektronische handtekening'.[43]

---

[36] Artikel 2:16 Awb.
[37] Voor zover de aard van een bericht zich daartegen niet verzet. Er kunnen bij wettelijk voorschrift aanvullende eisen worden gesteld, artikel 2:16 Awb.
[38] *Kamerstukken II*, 2001/02, 28 483, nr. 3, p. 20-22.
[39] http://www.pkioverheid.nl/over-pkioverheid/achtergrond-pkioverheid/#c236
[40] http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2008/
[41] http://www.pkioverheid.nl/voor-eindgebruikers/voor-certificaathouders/een-handtekening-plaatsen/
[42] http://www.pkioverheid.nl/voor-eindgebruikers/algemene-informatie/een-ondertekend-document/
[43] http://www.pkioverheid.nl/. Een vergelijkbare opmerking is gemaakt door de Minister van VWS over de UZI-pas. Volgens de Minister kan het Agentschap CIBG (de uitvoeringsorganisatie ten aanzien van

Vanuit juridisch oogpunt zijn er vraagtekens te zetten bij de opmerkingen op de website van PKIoverheid. Het is de vraag wat onder een 'rechtsgeldige elektronische handtekening' wordt verstaan, en op welke rechtsgevolgen wordt gedoeld. Er zou kunnen worden gedoeld op het gebruik van een elektronische handtekening om aan een vormvereiste te voldoen. Bijvoorbeeld een aanvraag die wordt ingediend bij een bestuursorgaan dient te worden ondertekend.[44] In dat geval zou een elektronische handtekening echter alleen aan het vormvereiste voldoen indien het betreffende bestuursorgaan op die manier de elektronische weg heeft opengesteld. Uit het enkel opvolgen van de eisen van de Weh vloeit niet automatisch een rechtsgevolg voort. Het is voor bestuursorganen van belang om voor ogen te houden dat er dient te worden nagegaan voor welke doeleinden er een elektronische handtekening vereist is.

DigiD
DigiD is een generieke authenticatievoorziening van de overheid. Met behulp van DigiD realiseert de gebruiker (bezoeker) zijn of haar authenticatie waardoor toegang tot een beveiligde website wordt gerealiseerd. De website zelf wordt beveiligd met een PKIoverheid-certificaat om betrouwbaarheid te kunnen garanderen. Naast het inloggen in beveiligde elektronische omgevingen biedt DigiD tevens mogelijkheden voor het elektronisch tekenen van documenten waardoor het dienstverleningsproces geheel elektronisch kan worden.

De Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties (op het moment van schrijven: de Staatssecretaris) is belast met de zorg voor de instandhouding van DigiD.[45] Het beheer en de ontwikkeling van DigiD is een taak van het cluster *Identificatie en Authenticatie* van de Gemeenschappelijke Beheer Organisatie.[46]

De werking van DigiD brengt met zich mee dat er een persoonsnummer wordt teruggekoppeld naar het bestuursorgaan van wiens diensten de burger gebruik wenst te maken. Het persoonsnummer betreft de inloggende burger. Het kan gaan om het burgerservicenummer of het A-nummer. Deze werking brengt een verwerking in de zin van de Wbp van het persoonsnummer met zich mee. Er wordt in een juridische basis voor deze gegevensverwerking voorzien met het Tijdelijk besluit nummergebruik overheidstoegangsvoorziening.[47] Dit besluit bevat als doelomschrijving voor de gegevensbescherming dat het betreffende nummer kan worden gebruikt 'met het oog op het verifiëren van de identiteit van degene die met behulp van de voorziening toegang zoekt tot elektronisch bestuurlijk verkeer met een bestuursorgaan dat is aangesloten bij de voorziening'.

DigiD kent verschillende zekerheidsniveaus: *Basis*, *Midden* en *Hoog*. DigiD Basis bestaat uit een inlogcode (gebruikersnaam en wachtwoord). Bij zekerheidsniveau Midden wordt per transactie aan de gebruiker via sms een transactiecode verzonden. Met de code dient de gebruiker zich per transactie te authenticeren. Het toekomstige zekerheidsniveau Hoog houdt in dat gebruik zal worden gemaakt van een elektronische identiteitskaart (e-Nik).[48] De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties heeft een beleidsregel vastgesteld op grond waarvan burgers inzage kunnen krijgen in de eigen gegevens uit de gemeentelijke basisadministratie van persoonsgegevens via MijnOverheid.nl (de Persoonlijke

---

processen in de zorg) toetreden tot PKIoverheid en UZI-passen uitgeven waarmee een 'rechtgeldige' elektronische handtekening gezet kan worden, *Kamerstukken II*, 2004/05, 27 529, nr. 5, p. 3.
[44] Artikel 4:2 lid 1 Awb.
[45] Artikel 1 Besluit beheer DigiD.
[46] Artikel 14.2 Organisatiebesluit directoraat-generaal Bestuur (Organisatiebesluit DGB).
[47] *Stb.* 2004, 584.
[48] De invoering van de e-Nik is al diverse malen uitgesteld, de vraag is niet alleen wanneer, maar óf de e-Nik er nog wel gaat komen.

Internetpagina, PIP) met behulp van DigiD, met het zekerheidsniveau Basis.[49] Voor andere overheidstoepassingen kunnen gemeenten en uitvoeringsorganisaties zelf aangeven welk zekerheidsniveau zij passend achten. Dit kan worden vastgesteld met behulp van een soort stappenschema, om te voorkomen dat gevoelige gegevens niet afdoende worden afgeschermd. De IB-groep werkt bijvoorbeeld met DigiD Midden (ook wel plus genoemd), om zo de persoonsgegevens van de bij haar ingeschreven studenten afdoende te kunnen waarborgen. Deze keuze is er onder meer door ingegeven dat niet alleen NAW-gegevens worden verwerkt, maar ook financiële data. De keuze voor een zekerheidsniveau kan juridisch worden geduid als een invulling van de norm van een betrouwbare en vertrouwelijke communicatie.

2.4 Algemene wet rijksbelastingen (elektronische belastingaangifte)

De belastingwetgeving kent specifieke regels ten aanzien van de elektronische belastingaangifte.

Algemene wet rijksbelastingen

De Algemene wet rijksbelastingen (Awr) is een algemene wettelijke regeling betreffende de heffing van belastingen. De Awr bevat de volgende hoofdregels. De inspecteur van de belastingen kan degene die naar zijn mening vermoedelijk belastingplichtig of inhoudingsplichtig is, uitnodigen tot het doen van aangifte.[50] Degene die zelf daartoe een verzoek indient, wordt in elk geval uitgenodigd tot het doen van aangifte.[51] Een ieder die is uitgenodigd tot het doen van aangifte, is hiertoe gehouden.[52] In sommige situaties is de belastingplichtige of inhoudingsplichtige die niet is uitgenodigd tot het doen van aangifte, gehouden om tot een uitnodiging te verzoeken.[53]

In de Uitvoeringsregeling AWR is bepaald voor welke belastingen of groepen van belastingplichtigen of inhoudingsplichtigen het doen van aangifte *uitsluitend langs elektronische weg* kan geschieden.[54] Dit betreft verschillende categorieën belastingen zoals de inkomstenbelasting[55], vennootschapsbelasting[56], omzetbelasting[57], loonbelasting[58] en verpakkingenbelasting[59].

Er zijn op dit moment, volgens het openstellingsbesluit van de Belastingdienst,[60] drie manieren om elektronisch aangifte te doen:

- aangifte via de internetsite van de Belastingdienst;
- aangifte met de aangifte- of administratiesoftware; of
- aangifte door een fiscaal intermediair, zoals een accountant of een belastingadviseur.

---

[49] Beleidsregel tot vaststelling niveau DigiD voor inzage in GBA persoonsgegevens via MijnOverheid.nl, *Stcrt*. 14 februari 2008, nr. 32, p. 6.
[50] Artikel 6 lid 1 AWR.
[51] Artikel 6 lid 2 AWR.
[52] Artikel 8 lid 1, 3 AWR.
[53] Artikel 2 UR AWR.
[54] Artikel 8 lid 2 sub a AWR.
[55] Artikel 20, lid 2 sub a Uitvoeringsregeling AWR.
[56] Artikel 20, lid 2 sub b Uitvoeringsregeling AWR.
[57] Artikel 20, lid 2 sub c Uitvoeringsregeling AWR.
[58] Artikel 20, lid 2 sub d Uitvoeringsregeling AWR.
[59] Artikel 20, lid 2 sub e Uitvoeringsregeling AWR.
[60] Besluit van 27 april 2005, nr. CPP2004/2807M, *Stcrt.* 2005, nr. 87, p. 12.

2.5 Wetboek van Strafvordering (elektronisch proces verbaal en de elektronische aangifte)

Het Wetboek van Strafvordering (Sv) bevat het formele strafrecht, dat wil zeggen de wijze waarop vervolging naar aanleiding van strafbare feiten geschiedt. In deze paragraaf worden de bepalingen behandeld die betrekking hebben op het elektronisch proces-verbaal en op de elektronische aangifte.

Met de Wet van tot wijziging van het Wetboek van Strafvordering (elektronische aangiften en processenverbaal) (hierna: de wijzigingswet)[61] zijn het elektronisch proces-verbaal en de elektronische aangifte in het Wetboek van Strafvordering opgenomen. De wijzigingen ten aanzien van de aangifte zijn per 1 januari 2007 in werking getreden.[62] De wijzigingen ten aanzien van het proces-verbaal zijn nog niet in werking getreden. De elektronische aangifte wordt geregeld in artikel 163 Sv. Het elektronisch proces-verbaal zal worden geregeld in artikel 153 Sv.

Het proces-verbaal (PV) wordt geregeld door de artikelen 152 tot en met 159 Sv. Artikel 153 stelt onder meer dat een PV *persoonlijk, gedagtekend en ondertekend wordt opgemaakt*. De wijzigingswet voegt de volgende volzin toe aan artikel 153: 'Met een ondertekend proces-verbaal wordt gelijkgesteld een proces-verbaal dat langs elektronische weg is opgemaakt en verzonden, mits dit voldoet aan de bij of krachtens algemene maatregel van bestuur gestelde eisen'. Hiermee wordt een elektronisch PV (ePV) mogelijk. De mogelijkheid van een ePV is beperkt tot de processen-verbaal die door opsporingsambtenaren moeten worden opgemaakt 'van het door hen opgespoorde strafbare feit of van hetgeen door hen tot opsporing is verricht of bevonden.'[63] Uit de nieuwe wettekst blijkt dat er een belangrijke rol is weggelegd voor een nader vast te stellen algemene maatregel van bestuur (AMvB).

Met de nieuwe wettekst is gekozen voor de juridische figuur van de gelijkstelling: het langs elektronische weg opgemaakt en verzonden stuk wordt gelijkgesteld met een klassiek opgemaakt en ondertekend stuk, mits er wordt voldaan aan een aantal nader te stellen technische eisen. Er is gekozen voor een AMvB, en niet voor een formele wet, vanwege het technische karakter van deze eisen en vanwege de snelle ontwikkelingen in de techniek.[64] Bij het PV is in beginsel een beperkt aantal actoren betrokken die veelvuldig contact met elkaar hebben (politie, openbaar ministerie en rechter). De wetgever heeft aangekondigd bij het opstellen van de AMvB hiermee rekening te houden.[65] Op het moment van schrijven is deze AMvB nog niet vastgesteld. Naar verwachting zullen de eisen die in de AMvB worden opgenomen, betrekking hebben op de volgende punten.

- Er zal moeten kunnen worden vastgesteld *welke opsporingsambtenaar* het PV heeft opgesteld. De in het AMvB te stellen eisen zullen erin moeten voorzien dat degene wiens naam en functie vermeld worden, ook daadwerkelijk degene is die het PV heeft opgesteld.
- De betrouwbaarheid van het PV. Dit houdt in dat de tekst van het PV zoals deze wordt vastgelegd en ingezonden, dezelfde is als die de opsporingsambtenaar heeft opgesteld. Er zal moeten worden voorzien in afdoende beveiligingseisen. Ook zal verzekerd dienen te zijn dat de tekst in oorspronkelijke versie bewaard kan worden. Een strafzaak kan vele jaren duren, ook na verloop van jaren kan er daarom de behoefte bestaan aan de beschikbaarheid van het PV. Hiermee is het denkbaar er bij

[61] *Stb.* 2005, 470.
[62] *Stb.* 2006, 728.
[63] Artikel 152 Sv; *Kamerstukken II*, 2003/04, 29 438, nr. 3, p. 9.
[64] *Kamerstukken II*, 2003/04, 29 438, nr. 3, p. 1.
[65] *Kamerstukken II*, 2003/04, 29 438, nr. 3, p. 7.

> de AMvB regels zullen worden gesteld inzake het beschikbaar houden van de programmatuur of dat een maximumtermijn wordt vastgelegd, na verloop waarvan een fysieke (authentieke) versie wordt vervaardigd.[66]

De aangifte wordt geregeld door de artikelen 160 tot en met 163 Sv. De wet maakt daarbij een onderscheid tussen de mondelinge aangifte en de schriftelijke aangifte. Artikel 163 lid 3 Sv stelt: 'de *schriftelijke* aangifte wordt door den aangever of diens gemachtigde *onderteekend*.' De Wijzigingswet heeft hieraan toegevoegd:

> 'Met een ondertekende aangifte wordt gelijkgesteld de aangifte die langs elektronische weg is gedaan, mits deze voldoet aan de bij of krachtens algemene maatregel van bestuur gestelde eisen. Bij algemene maatregel van bestuur kunnen beperkingen worden aangebracht in de gevallen waarin aangifte langs elektronische weg kan worden gedaan.'

Ook hier is er dus sprake van gelijkstelling en een AMvB waarbij nadere eisen worden gesteld. In de Memorie van Toelichting bij de Wijzigingswet worden aangegeven dat de nadere eisen betrekking moeten hebben op:

- De identificeerbaarheid en traceerbaarheid van de aangever. Zo ligt het voor de hand dat de aangever zijn naam, adres en zo mogelijk telefoonnummer moet opgeven. Ook andere gegevens zouden in dat verband kunnen worden voorgeschreven. Denkbaar is ook een systeem waarin de aangever die gebruik maakt van e-mail, de gegevens beschikbaar stelt waarmee kan worden vastgesteld of hij de rechtmatige gebruiker van het betrokken e-mail-adres is.
- De betrouwbaarheid van de inhoud van de aangifte, ook in de zin van beveiliging tegen onbevoegde kennisneming en onbevoegde wijziging. Hierbij kan worden gedacht aan technische voorzieningen of aan voorzieningen van organisatorische aard. Ook een combinatie is denkbaar, in die zin dat degene die elektronisch aangifte doet een bevestiging dient te geven van de aangifte zoals deze door de opsporingsambtenaar is ontvangen.[67]

De AMvB inzake de elektronische aangifte, het Besluit elektronische aangifte, is per 1 januari 2007 in werking getreden.[68] In het Besluit staat de aangiftevoorziening centraal: de elektronische aangifte kan plaatsvinden met een aangiftevoorziening die door de minister van Justitie is goedgekeurd. Het Besluit bevat een aantal functionele eisen waar de aangiftevoorziening aan dient te voldoen, alvorens de minister (middels een keuringsinstantie) kan overgaan tot goedkeuring.[69]

Op grond van het Besluit elektronisch aangifte dient de aangiftevoorziening aan de volgende functionele eisen te voldoen:

a. iedere aangifte wordt automatisch voorzien van een uniek nummer en van de datum en het tijdstip waarop deze is ontvangen;
b. de transmissie van de aangifte vindt op zodanige wijze plaats, dat de inhoud van de ontvangen aangifte gelijk is aan de inhoud van de door de aangever verstuurde aangifte;

---

[66] *Kamerstukken II*, 2003/04, 29 438, nr. 3, p. 10.
[67] *Kamerstukken II*, 2003/04, 29 438, nr. 3, p. 11.
[68] *Stb.* 2006, 728.
[69] Artikel 7 Besluit elektronische aangifte.

c. de aangever wordt in de gelegenheid gesteld de aangifte zoals deze is ontvangen, langs elektronische weg te controleren en zonodig te wijzigen alvorens de aangifte te bevestigen;
d. indien in de ontvangen aangifte nadien wijzigingen worden aangebracht, is dit achteraf vast te stellen;
e. er zijn passende maatregelen genomen ter beveiliging van de gegevens en tegen kennisneming door onbevoegden.[70]

Voorts dient de aangiftevoorziening de aangever te verplichten tot het invullen van ten minste de volgende gegevens:
a. naam, voornamen, geboortedatum en geboorteplaats van de aangever;
b. het adres waarop de aangever als ingezetene is ingeschreven onderscheidenlijk zijn feitelijke woon- of verblijfplaats;
c. een aanduiding van het feit waarvan aangifte wordt gedaan;
d. een aanduiding van de plaats waar en het tijdstip waarop het feit heeft plaatsgevonden;
e. indien de aangever niet tevens het slachtoffer is, indien bekend de persoonsgegevens van het slachtoffer overeenkomstig de onderdelen a en b;
f. de wijze waarop de aangever een bevestiging van de aangifte wenst te ontvangen;
g. een aanduiding waaruit blijkt dat het de aangever bekend is dat het doen van een valse aangifte een strafbaar feit is.[71]

2.6 Wet bescherming persoonsgegevens (Wbp)

Hoofdregels

De Wet bescherming persoonsgegevens stelt eisen aan de wijze waarop met persoonsgegevens mag worden omgegaan. De Wbp is een kaderwet die algemene regels stelt aan de verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens die een geïdentificeerde of identificeerbare natuurlijke persoon betreffen.[72] Degene op wie een persoonsgegeven betrekking heeft, is de *betrokkene*.[73] Onder de verwerking van persoonsgegevens wordt verstaan elke handeling met betrekking tot die persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen,ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of anderszins ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.[74]

De Wbp richt zich in eerste instantie tot de verantwoordelijke. Dit is degene die, alleen of tezamen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit kan een natuurlijk persoon, rechtpersoon, bestuursorgaan of ieder ander betreffen.[75] De verantwoordelijke kan een verwerking uitbesteden aan een bewerker. Dat is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan het rechtstreeks gezag van de verantwoordelijke onderworpen te zijn.[76]

---

[70] Artikel 4 Besluit elektronische aangifte.
[71] Artikel 5 Besluit elektronische aangifte.
[72] Artikel 1 sub a Wbp. De Wbp bevat overigens aanvullende regels ten aanzien van *bijzondere persoonsgegevens*, strafrechtelijke gegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag. Bijzondere persoonsgegevens zijn persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, artikel 16 e.v. Wbp.
[73] Artikel 1 sub f Wbp.
[74] Artikel 1 sub b Wbp.
[75] Artikel 1 sub d Wbp.
[76] Artikel 1 sub e Wbp.

De Wbp kent het *doelbindingsbeginsel*: persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.[77] Het is dus van belang dat de verantwoordelijke de gerechtvaardigde doeleinden van de verwerking vaststelt en deze uitdrukkelijk omschrijft. Daarnaast kent de Wbp een aantal *zorgvuldigheidsnormen*: persoonsgegevens dienen in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze te worden verwerkt.[78] Voorts mogen persoonsgegevens alleen worden verwerkt, voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.[79] De verantwoordelijke dient de nodige maatregelen te treffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.[80] Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.[81] Dit alles brengt met zich mee dat de verantwoordelijke aandacht moet besteden aan het onderhoud van zijn gegevensbestanden en af en toe kritisch moet bezien welke persoonsgegevens voor wat voor periode nu precies noodzakelijk zijn. Een derde belangrijk uitgangspunt van de Wbp is *transparantie*: de verantwoordelijke voor de gegevensverwerking dient jegens de betrokkene inzichtelijk te maken wat hij met diens persoonsgegevens doet. Dit beginsel is uitwerkt in de informatieplicht jegens de betrokkene en in de rechten van de betrokkene (inzage, correctie, verzet).

De bovenstaande open normen van de Wbp zijn in de wet nader aangescherpt. De Wbp noemt namelijk een limitatief aantal gronden op grond waarvan persoonsgegevens mogen worden verwerkt. Dat mag indien:

a. er sprake is van de ondubbelzinnige toestemming van de betrokkene;
b. de verwerking noodzakelijk is ter uitvoering van een overeenkomst, dan wel in het kader van het sluiten daarvan;
c. de verwerking noodzakelijk is om een wettelijke verplichting na te komen;
d. de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de verwerking noodzakelijk is voor een goede vervulling van de publiekrechtelijke taak door het desbetreffende bestuursorgaan, dan wel het bestuursorgaan waaraan de gegevens worden verstrekt;
f. de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang van de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijk levenssfeer, prevaleert.[82]

Nadat persoonsgegevens eenmaal zijn verkregen, mogen ze niet verder worden verwerkt op een wijze die *onverenigbaar* is met de doeleinden waarvoor ze zijn verkregen.[83] Bij de beoordeling of er sprake is van onverenigbaarheid, houdt de verantwoordelijke in elk geval rekening met:

a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;

[77] Artikel 7 Wbp.
[78] Artikel 6 Wbp.
[79] Artikel 11 lid 1 Wbp.
[80] Artikel 11 lid 2 Wbp.
[81] Artikel 10 lid 1 Wbp.
[82] Artikel 8 Wbp.
[83] Artikel 9 lid 1 Wbp.

b. de aard van de betreffende gegevens;
c. de gevolgen van de beoogde verwerking voor de betrokkene;
d. de wijze waarop de gegevens zijn verkregen; en
e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.[84]

Meldingsplicht
Op de verantwoordelijke kan een *meldingsplicht* rusten wanneer hij op geheel of gedeeltelijk geautomatiseerde wijze persoonsgegevens verwerkt, en waarbij de verwerking voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is. De meldingsplicht houdt in dat de verantwoordelijke de voorgenomen verwerkingen moet melden bij het College bescherming persoonsgegevens.[85]

De Nederlandse wetgever heeft een lijst opgesteld van veel voorkomende verwerkingen die zijn vrijgesteld van de meldingsplicht. Deze lijst is opgenomen in het Vrijstellingsbesluit Wbp.[86]

Informatieverstrekking aan de betrokkene
Soms moet de verantwoordelijke de betrokkene op de hoogte stellen van het feit dat 'zijn' persoonsgegevens worden verwerkt. De verantwoordelijke is dan verplicht om bepaalde informatie te verstrekken aan de betrokkene. Voor wat betreft het *moment* waarop deze informatie moet worden verstrekt, maakt de Wbp onderscheid tussen de situatie waarin persoonsgegevens van de betrokkene worden verkregen, en de situatie waarin persoonsgegevens op een andere wijze worden verkregen.

Het moment van informatieverstrekking
Wanneer de persoonsgegevens van de betrokkene worden verkregen, dan dient de verantwoordelijke vóór het moment van verkrijging van de persoonsgegevens, de betrokkene informatie te verstrekken, tenzij de betrokkene daarvan reeds op de hoogte is.[87] Wanneer de persoonsgegevens op een andere wijze worden verkregen, dan dient de verantwoordelijke de betrokkene informatie te verstrekken op het moment van de vastlegging van de gegevens, of, indien de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van eerste verstrekking.[88]

De te verstrekken informatie
De informatie die de verantwoordelijke dient te verstrekken, bestaat uit:
- de identiteit van de verantwoordelijke; en
- de doeleinden van de verwerking waarvoor de gegevens zijn bestemd.

Deze informatie hoeft weer niet te worden verstrekt, indien de betrokkene er al van op de hoogte is. [89]

Daarnaast dient de verantwoordelijke aanvullende informatie te verstrekken 'voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.'[90]

---

[84] Artikel 9 lid 2 Wbp.
[85] Artikel 27 Wbp.
[86] *Stb.* 2001, 250. Zie ook artikel 29 lid 1 Wbp.
[87] Artikel 33 lid 1 Wbp.
[88] Artikel 34 lid 1 Wbp.
[89] Artikel 33 lid 2, 34 lid 2 Wbp.
[90] Artikel 33 lid 3, 34 lid 3 Wbp.

Uitzonderingen
Ten aanzien van de situatie dat de persoonsgegevens op een andere wijze worden verkregen dan van de betrokkene zelf, gelden er twee uitzonderingen. Ten eerste is de informatieverplichting niet van toepassing indien het meedelen van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval moet de verantwoordelijke wel de herkomst van de gegevens vastleggen.[91] Ten tweede is de informatieverplichting niet van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval moet de verantwoordelijke de betrokkene op zijn verzoek informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.[92]

Rechten van de betrokkene
De Wbp kent aan de betrokkene een aantal rechten toe. Het gaat om het recht op kennisneming, het recht op correctie of verwijdering, en het recht op verzet. De verantwoordelijke dient in het kader van de uitoefening van deze rechten zorg te dragen voor een deugdelijke vaststelling van de identiteit van de verzoeker.[93] Hiermee moet worden voorkomen iemand door gebruik te maken van de naam van een ander, gegevens over die ander kan verkrijgen.[94]

Recht op kennisneming
Het recht op kennisneming houdt in dat de betrokkene zich tot de verantwoordelijke kan wenden met de vraag hem mee te delen of er persoonsgegevens worden verwerkt die op hem betrekking hebben. De verantwoordelijke dient hier binnen vier weken schriftelijk op te reageren.[95] Als de verantwoordelijke inderdaad persoonsgegevens verwerkt die de aanvrager betreffen, dan dient de mededeling de volgende informatie te bevatten:

- een volledig overzicht van de persoonsgegevens in begrijpelijke vorm;
- een omschrijving van het doel of de doeleinden van de verwerking
- de categorieën van gegevens waarop de verwerking betrekking heeft;
- de ontvangers of categorieën van ontvangers;
- de beschikbare informatie over de herkomst van de gegevens.[96]

De verantwoordelijke moet ook informatie verstrekken over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van persoonsgegevens, indien de betrokkene daarom vraagt.[97]

Recht op correctie
Het recht op correctie of verwijdering houdt in dat de betrokkene, nadat gevolg is gegeven aan het recht op kennisgeving, de verantwoordelijke kan verzoeken de persoonsgegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen. De betrokkene komt dit recht toe indien de persoonsgegevens feitelijk onjuist zijn, of indien zij voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, of anderszins in strijd met de wet worden verwerkt.[98] De verantwoordelijke moet binnen vier weken het verzoek beantwoorden. Indien hij het verzoek weigert, dient hij dit te onderbouwen.[99]

---

[91] Artikel 34 lid 4 Wbp.
[92] Artikel 34 lid 5 Wbp.
[93] Artikel 37 lid 2 Wbp.
[94] *Kamerstukken II*, 1997/98, 25 862, nr. 3, p. 161.
[95] Artikel 35 lid 1 Wbp.
[96] Artikel 35 lid 2 Wbp.
[97] Artikel 35 lid 3 Wbp.
[98] Artikel 36 lid 1 Wbp.
[99] Artikel 36 lid 2 Wbp.

Recht op verzet
Hierboven is erop gewezen dat aan de verwerking van persoonsgegevens een gerechtvaardigd doel ten grondslag moet liggen. Wanneer de volgende twee gronden worden aangevoerd als gerechtvaardigd doel, dan kan de betrokkene verzet aantekenen tegen de verwerking van persoonsgegevens die op hem betrekking hebben. Het gaat om:

- de gegevensverwerking die noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt; en
- de gegevensverwerking die noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.[100]

De wijze waarop de betrokkene het verzet aantekent is niet aan enige vorm gebonden. Dit kan dus bijvoorbeeld mondeling, schriftelijk of via e-mail. Wel moet duidelijk uit het aangetekende verzet blijken op grond van welke persoonlijke omstandigheden, welke handeling of geheel van handelingen ten aanzien van welke persoon zou moeten worden beëindigd. De verantwoordelijke kan overigens voor het in behandeling nemen van het verzet een vergoeding van de eventuele kosten verlangen. Deze vergoeding mag niet hoger zijn dan € 4,50.[101]

Naar aanleiding van het verzet, dient de verantwoordelijke na te gaan of in de huidige omstandigheden deze doelen nog steeds als gerechtvaardigde doelen kunnen gelden.[102] Is dat niet het geval, dan is het verzet gerechtvaardigd. De beoordeling van het verzet dient binnen vier weken te geschieden.[103]

Het College Bescherming Persoonsgegevens (CBP) en de functionaris voor de gegevensbescherming (FG)
Het toezicht op de toepassing van de Wbp geschiedt door het College bescherming persoonsgegevens (CBP). Wanneer het CBP onrechtmatige gedragingen constateert, bijvoorbeeld het niet voldoen aan de meldingsplicht of het verwerken van persoonsgegevens zonder dat daar een grondslag voor is, kan het onder meer een boete opleggen[104] of bestuursdwang toepassen.[105]
De functionaris voor de gegevensbescherming (FG) fungeert ook als toezichthouder. Een organisatie waarin persoonsgegevens worden verwerkt, kan een FG benoemen. De FG functioneert als een toezichthouder *binnen* de betreffende organisatie. Binnen de organisatie fungeert de FG als vraagbaak. Ten opzichte van het CBP vervult de FG de rol van intermediair. De waarde van de FG is erin gelegen dat taken van het CBP door de FG kunnen worden verricht, op een voor de betreffende organisatie geëigende wijze.[106] Bijvoorbeeld het melden van verwerkingen van persoonsgegevens geschiedt dan niet bij het CBP, maar bij de FG.[107]

---

[100] Artikel 40 lid 1 juncto artikel 8 sub e en f Wbp.
[101] Artikel 40 lid 3 Wbp juncto artikel 4 Besluit kostenvergoeding rechten betrokkene Wbp.
[102] *Kamerstukken II*, 1997-1998, 25 892, nr. 3, p. 163.
[103] Artikel 40 lid 2 Wbp.
[104] Artikelen 66-74 Wbp.
[105] Artikel 65 Wbp.
[106] *Kamerstukken II*, 1997-1998, 25 892, nr. 3, p. 29.
[107] Artikel 27 lid 1 Wbp.

2.7 Wet algemene bepalingen burgerservicenummer (Wabb)

De Wet algemene bepalingen burgerservicenummer (Wabb) stelt algemene regels omtrent het burgerservicenummer (hierna: BSN) en geeft daarbij enkele kaders aan waarbinnen het mag of moet worden gebruikt.

Een BSN wordt omschreven als het als zodanig overeenkomstig de Wabb aan een natuurlijke persoon toegekend nummer.[108] Het BSN is een nummer van negen cijfers dat voldoet aan de zogenaamde elfproef.[109] Het BSN is een informatieloos nummer; het bevat geen informatie over de persoon aan wie het is toegekend. Deze informatieloosheid is om twee redenen opgenomen in de Wabb. In de eerste plaats dient het kenbaar maken van persoonsgegevens zonder noodzaak te worden voorkomen. In een identificatienummer kan bijvoorbeeld een geboortedatum of het geslacht van de betreffende persoon worden opgenomen. Bij het gebruik van zo'n nummer zou dan het geslacht en/of geboortedatum kenbaar worden gemaakt, wat onwenselijk wordt geacht.[110] De tweede reden is dat het toevoegen van zulke informatie aan het BSN, het BSN langer zou maken dan efficiënt zou zijn voor het gebruik. Dit zou ook de kans op fouten kunnen vergroten.[111]

Of een persoon, instelling of organisatie gebruik mag maken van het BSN, hangt af van de vraag of die persoon, instelling of organisatie als *gebruiker* kan worden aangemerkt. Een gebruiker kan het BSN voor het volgende gebruiken:

- voor de opname in de eigen registratie van de gebruiker, zodat de gegevens van een persoon doeltreffend zijn terug te vinden;
- als hulpmiddel bij het raadplegen van gegevens die in andere registraties zijn opgeslagen, bijvoorbeeld op het gebied van inkomens of opgebouwde verzekeringsrechten.[112]

De Wabb noemt alleen degene die bevoegd, dan wel verplicht is het BSN te gebruiken *gebruiker*. Een gebruiker kan zijn een overheidsorgaan[113], of een niet-overheidsorgaan.[114] Voor overheidsorganen bevat de Wabb in artikel 10 een wettelijke grondslag voor het gebruik van het BSN. Zij kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik maken van het BSN. Een niet-overheidsorgaan wordt als gebruiker aangemerkt voor zover het werkzaamheden verricht waarbij het gebruik van het BSN bij of krachtens wet is voorgeschreven.[115] Voor niet-overheidsorganen zal er dus een wettelijke basis moeten zijn, willen zij als gebruiker van het BSN kunnen handelen.

---

[108] Artikel 1 sub b Wabb.

[109] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 11. De elfproef houdt het volgende in: het burgerservicenummer bestaat uit 8 of 9 cijfers (bij 8 cijfers voorloopnul toevoegen). Het meest rechtse cijfer is het controlegetal, vermenigvuldig het meest linkse cijfer van het nummer met 9, vermenigvuldig het cijfer daarnaast met 8, het cijfer daarnaast met 7, enzovoorts, tot het achtste cijfer met 2 is vermenigvuldigd. Tel de uitkomsten van de vermenigvuldigingen bij elkaar op, deel deze som door 11. Het restgetal, indien niet 10, is gelijk aan het controlecijfer.

[110] Niet alle EU-lidstaten zijn het eens met deze opvatting. België werkt bijvoorbeeld met het Rijksregisternummer, bestaande uit elf cijfers, waarvan de eerste zes cijfers de geboortedatum vormen.

[111] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 9.

[112] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 13-14.

[113] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 31; artikel 1 lid 1 Awb, een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of enig ander persoon of college met enig openbaar gezag bekleed.

[114] Artikel 1 sub d Wabb. Er is nog een derde categorie van personen denkbaar die bevoegd zijn het burgerservicenummer te gebruiken, te weten die niet-overheidsorganen die op grond van een AMvB bevoegd worden om het burgerservicenummer te gebruiken, artikel 24 lid 2 Wbp.

[115] Artikel 1 sub d Wabb.

Voorbeelden van niet-overheidsgebruikers zijn zorginstellingen (op grond van de Wet BSN in de Zorg) en onderwijsinstellingen (onder de noemer onderwijsnummer).

De gebruikers dienen bij het gebruik van het BSN wel de regels die bij of krachtens hoofdstuk 4 van de Wabb zijn gesteld, in acht te nemen. Deze regels houden onder meer het volgende in:

- bij het uitwisselen van persoonsgegevens tussen gebruikers onderling waarbij een persoonsnummer wordt gebruikt, wordt het BSN vermeld. Deze regel gaat niet op indien het gebruik van een ander persoonsnummer is voorgeschreven of er bijzondere omstandigheden zijn waarin het gebruik van het BSN in een individueel geval onwenselijk is gelet op de privacy van betrokkene, de opsporing en vervolging van strafbare feiten , dan wel de veiligheid van de staat;[116]
- bij het gebruik van het BSN dient de gebruiker zich ervan te vergewissen dat het betreffende BSN daadwerkelijk betrekking heeft op de persoon wiens persoonsgegevens hij verwerkt (de *vergewisplicht*);[117]
- degene aan wie een BSN is toegekend kan bij het verstrekken van persoonsgegevens aan een gebruiker, niet worden verplicht om een ander persoonsnummer dan zijn BSN te verstrekken.[118]

Wanneer een persoon, instelling of organisatie eenmaal als gebruiker wordt aangemerkt, dan staat in principe de mogelijkheid open om aan te sluiten bij de Beheervoorziening BSN. De Beheervoorziening BSN komt hieronder bij de behandeling van het BSN-stelsel aan de orde.

Sectorale wetgeving
In de sectoren zorg en onderwijs wordt het gebruik van het BSN voorgeschreven door middel van sectorale wetgeving. Het gebruik van een algemeen persoonsnummer als het BSN is slechts toegestaan ter uitvoering van de wet waarmee het gebruik van dat nummer is voorgeschreven, dan wel voor de doeleinden bij de wet bepaald.[119] Wordt er voor een sector het gebruik van het BSN voorgeschreven, dan is het van belang om vast te stellen wat de doeleinden zijn van het gebruik van het nummer in de betreffende sector.

Het gebruik van het BSN in de zorgsector wordt voornamelijk geregeld door de Wet gebruik BSN in de zorg. Er worden drie partijen aangewezen die bevoegd zijn het BSN te gebruiken. Het gaat om de zorgaanbieder, de zorgverzekeraar en het indicatieorgaan. Deze partijen gebruiken het BSN om te waarborgen dat de persoonsgegevens die zij verwerken, betrekking hebben op de juiste persoon.[120] Als voorwaarde voor gebruik van het BSN in de zorg, geldt dan ook dat het BSN slechts voor deze doelstelling gebruikt mag worden.

In (een deel van) de sector onderwijs wordt reeds enige tijd gebruik gemaakt van een persoonsgebonden nummer.[121] Het persoonsgebonden nummer in het onderwijs kan onder omstandigheden worden gebruikt door onderwijsinstellingen, de Informatie Beheergroep en het betreffende bevoegde gezag. Het gebruik van een persoonsgebonden nummer in het onderwijs dient de volgende doeleinden:

- de controle op de rechtmatigheid van bestedingen;

[116] Artikel 11 Wabb.
[117] Artikel 12 Wabb.
[118] Artikel 13 Wabb.
[119] Artikel 24 Wbp.
[120] Artikel 4 Wet BSN in de zorg; artikel 86 lid 3 Zorgverzekeringswet; artikel 52 lid 3 AWBZ; *Kamerstukken II*, 2005-2006, 30 380, nr. 3, p. 18-19.
[121] Wet tot wijziging van enkele onderwijswetten in verband met de invoering van persoonsgebonden nummers in het onderwijs, *Stb*. 2001, 681; *Kamerstukken II*, 2005-2006, 30 404, nr. 1-6.

- het verlichten van de administratieve belasting van scholen en instellingen;
- het verbeteren van beleidsinformatie.[122]

De vergewisplicht
De gebruiker mag er niet klakkeloos van uitgaan dat het BSN dat hij gebruikt, betrekking heeft op de juiste persoon. Een burger kan namelijk bepaalde risico's lopen, zoals:

- De schending van de privacy van de burger doordat het BSN ten onrechte wordt gebruikt;
- Het plegen van fraude omdat van de gegevens van een andere burger gebruik wordt gemaakt bij het toekennen van een recht;
- De benadeling van de burger omdat voor het nemen van een besluit onjuiste gegevens worden gebruikt.

Om zorg te dragen voor het juist en nauwkeurig gebruik van het BSN, zodat bovenstaande risico's worden beperkt, geldt voor gebruikers daarom de vergewisplicht. Gebruikers dienen zich ervan te vergewissen dat het BSN betrekking heeft op de persoon wiens persoonsgegevens zij verwerken. Het gaat met andere woorden om het controleren van de juistheid van de combinatie van een persoon met een BSN.[123] Deze controle geschiedt over het algemeen met behulp van een wettelijk identiteitsbewijs, omdat daarop naam, pasfoto én aanvullende gegevens staan die identificatie kunnen realiseren. De vergewisplicht brengt overigens niet mee dat een gebruiker vaker de identiteit van een burger moet vaststellen dan reeds het geval is. Het is voor de burger niet een nieuwe identificatieplicht. Mocht er echter in een bepaalde situatie een identificatieplicht zijn, op grond waarvan de burger zich jegens de gebruiker dient te identificeren, dan kan de gebruiker aansluitend op de identificatie aan de vergewisplicht voldoen.

Het BSN-stelsel
Het gebruik van het BSN wordt praktisch mogelijk gemaakt door het BSN-stelsel. Het BSN-stelsel bestaat uit de volgende drie onderdelen:

- De Beheervoorziening BSN; deze bestaat uit zijn beurt weer uit:
  - voorzieningen die nodig zijn voor het aanmaken, distribueren, toekennen en beheren van burgerservicenummers
  - het nummerregister;
  - voorzieningen waarmee het nummerregister geraadpleegd kan worden;
  - voorzieningen waarmee bepaalde verificatievragen gesteld kunnen worden.[124]
- voorzieningen die nodig zijn voor het overige gebruik van BSNs;
- regels betreffende de relatie met andere persoonsnummers.[125]

De Beheervoorziening BSN
De Beheervoorziening BSN wordt beheerd door het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelatie ziet toe op de juiste toekenning van het BSN.[126] Voorts dient de Minister eens per drie jaar een onderzoek uit te voeren naar de inrichting, werking en de beveiliging van de Beheervoorziening BSN.[127]

---

[122] *Kamerstukken II*, 1997-1998, 25 828, nr. 3, p. 1-9.
[123] Artikel 12 Wabb.
[124] Artikel 3 lid 1 Wabb.
[125] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 10, 13-14.
[126] Artikel 20 Wabb.
[127] Artikel 21 Wabb.

Voordat een nummer als BSN wordt toegekend, wordt het eerst aangemaakt en gedistribueerd door de Beheervoorziening BSN. De Beheervoorziening BSN maakt nummers aan van negen cijfers die voldoen aan de elfproef.[128] De aangemaakte nummers worden vastgelegd in een nummerregister. Vanuit het nummerregister worden de nummers gedistribueerd aan de instanties die bevoegd zijn het nummer toe te kennen. In het nummerregister wordt bijgehouden aan welke instantie het nummer is gedistribueerd. Het algemene beheer na distributie bestaat uit het permanent vasthouden van het nummer en een aantal administratieve gegevens over het nummer in het nummerregister. Ook bestaat beheer uit het wijzigen van de status van een nummer. Een status kan bijvoorbeeld zijn 'aangemaakt', 'beschikbaar gesteld' en 'toegekend'.[129] De status geeft zodoende weer of een nummer is aangemaakt, is gedistribueerd of aan een persoon is toegekend. Bij de aanmaak en distributie draagt de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties er zorg voor dat een nummer dat als BSN kan worden toegekend, slechts éénmaal wordt aangemaakt en gedistribueerd.[130] Een aangemaakt en gedistribueerd nummer wordt vervolgens door het college van burgemeester en wethouders als BSN toegekend op het moment dat een persoon wordt ingeschreven in de Gemeentelijke basisadministratie persoonsgegevens (GBA) en deze persoon nog niet over een BSN beschikt.[131] De colleges van burgemeester en wethouders zijn verplicht om aan de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties inlichtingen te verschaffen omtrent de toekenning van het BSN, die voor de Minister het bijhouden van het nummerregister van belang zijn.[132] Deze verplichting rust op het college van burgemeester en wethouder omdat juist dat orgaan belast is met het toekennen van het BSN en daarom als enige in staat is om informatie daarover te verstrekken.[133] Ook kunnen andere overheidsorganen worden verplicht om aan de Minister informatie te verstrekken die voor het bijhouden van het nummerregister van belang zijn.[134]

Het college van burgemeester en wethouders draagt de zorg dat een BSN slechts éénmaal en foutloos wordt toegekend.[135] Bij de toekenning van een BSN na inschrijving in de GBA, dient het college van burgemeester en wethouders de *presentievraag* te stellen. Dat betekent dat het college met behulp van de Beheervoorziening BSN dient na te gaan:

- of aan de betreffende persoon al een BSN dan wel een sofi-nummer is toegekend;
- aan welke persoon een bepaald BSN is toegekend;
- of het Nederlandse identiteitsdocument een geldig document is;[136]
- of er misschien elders een inschrijvingsprocedure loopt.

De betrokken registers
Eén van de belangrijkste functionaliteiten die het BSN-stelsel biedt, is dat via de Beheervoorziening BSN bepaalde registers kunnen worden geraadpleegd in verband met de juiste toekenning of het juiste gebruik van het BSN. Het gaat in de eerste plaats om het nummerregister. In het nummerregister wordt bijgehouden wanneer welk nummer is aangemaakt, aan welk bestuursorgaan het is gedistribueerd, en door welke toekennende

[128] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 11.
[129] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 13.
[130] Artikel 7 Wabb.
[131] Artikel 8 lid 1 Wabb.
[132] Artikel 5 Wabb.
[133] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 33.
[134] Artikel 6 Wabb.
[135] Artikel 8 lid 3 Wabb.
[136] Artikel 8 lid 1 juncto 3 lid 1 onder c en d Wabb.

instantie[137] het is toegekend. Het nummerregister bevat dus geen informatie over de persoon aan wie het BSN uiteindelijk is toegekend. In de tweede plaats kan via de Beheervoorziening BSN een aantal registers betreffende identiteitsdocumenten worden geraadpleegd. Het betreft de reisdocumentenadministratie, het kaartregister vreemdelingen en het rijbewijsregister. De registers zijn van belang bij de hierna te behandelen verificatievragen. In de derde plaats is er via de Beheervoorziening BSN toegang tot de Gemeentelijke basisadministratie (GBA) en de toekomstige Registratie niet-ingezetenen (RNI). Toegang tot deze registers staat slechts open voor overheidsorganen en gebruikers-niet-overheidsorganen, indien daar een wettelijke grondslag voor bestaat.[138]

Verificatievragen
Eén van de belangrijkste praktische functies van het BSN-stelsel, is de mogelijkheid voor gebruikers om verificatievragen te stellen. Indien de gebruiker is aangesloten op de Beheervoorziening BSN, dan kan hij met de verificatievragen een BSN, een Nederlands identiteitsdocument of de identiteit van een persoon verifiëren. Dit kan door het stellen van vijf verificatievragen:

1. Is dit nummer een BSN?
2. Is dit een document als bedoeld in artikel 1 lid 1 onder 1, 2 of 4, van de Wet op de identificatieplicht?[139]
3. Wat zijn de identificerende gegevens bij dit BSN?[140]
4. Welk BSN hoort bij deze identificerende gegevens?[141]
5. Hoort deze combinatie van identificerende gegevens en BSN bij elkaar?

Verificatievragen 1 en 2 zijn de basisverificatievragen. Deze mogen door elke gebruiker worden gesteld, indien dat nodig is voor de uitvoering van de vergewisplicht. De overige verificatievragen mag een gebruiker-niet-overheidsorgaan alleen stellen als hij hiertoe bij of krachtens wet verplicht of bevoegd is.[142] Dit kan in sectorale wetgeving worden geregeld.

Relatie met andere persoonsnummers
Het BSN-stelsel maakt het niet onmogelijk dat naast het BSN andere persoonsnummers worden gebruikt. Het kan daarbij gaan om twee categorieën van andere nummers: *aanvullende nummers* en *sectornummers*.
Aanvullende nummers zijn bedoeld voor personen die niet over een BSN beschikken, sectornummers zijn bedoeld voor personen in een bepaalde sector, ongeacht of iemand over een BSN beschikt; aanvullende nummers zijn negencijferige nummers die niet zijn te onderscheiden van het BSN. Er is maar één soort aanvullende nummer: het sofi-nummer. Het sofi-nummer is nodig voor het heffen van belastingen van bepaalde categorieën van personen. Het sofi-nummer is cijfermatig gelijk aan het BSN, maar heet feitelijk anders bij gebruik in sociaal-fiscale situaties. Voor het gemak wordt overal de term BSN gevoerd.
Vanwege het gebruik van het sofi-nummer zijn er twee extra voorzieningen van het BSN-stelsel noodzakelijk. In de eerste plaats zal het naspeuren door de toekennende instanties van

[137] Een BSN wordt toegekend door het college van burgemeester en wethouders. Daarnaast kan in sommige gevallen de Belastingdienst nummers toekennen die door de Beheervoorziening BSN zijn aangemaakt. Ook de IB-groep kan, in uitzonderlijke gevallen, onderwijsnummers toekennen aan studenten teneinde de verwerking van hun gegevens ten behoeven van het onderwijs te realiseren. Denk hierbij bijvoorbeeld aan buitenlandse studenten of grens-studenten (wonende in de grensstreek, studerend in Nederland).
[138] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 13-14, 32.
[139] Artikel 15 lid 1 sub c Wabb.
[140] Artikel 15 lid 1 sub b Wabb.
[141] Artikel 15 lid 1 sub a Wabb.
[142] Artikel 15 Wabb.

het desbetreffende nummer niet alleen in de GBA en de toekomstige registratie van niet-ingezetenen, maar ook in het bestand beheer van relaties van de Belastingdienst moeten geschieden. In de tweede plaats moet een sofi-nummer kunnen worden omgezet in een BSN wanneer de betrokken persoon wordt ingeschreven in de GBA of geregistreerd wordt in de toekomstige Registratie niet-ingezetenen.
Sectornummers zijn niet gelijk aan het BSN. Zo zal in de strafrechtketen en de vreemdelingenketen binnen de sector Justitie bekend een eigen sectornummer worden gehanteerd.[143] Het is daarom noodzakelijk om te voorzien in een koppeling tussen het sectornummer en het BSN van een persoon om sectoroverstijgende gegevensuitwisseling mogelijk te maken, mede omdat de burger niet kan worden verplicht een ander nummer dan het BSN te verstrekken. De koppeling kan geschieden middels een koppeltabel.[144]

De Nationale Vertrouwensfunctie (NVF)
Om de burger erop te kunnen laten vertrouwen dat er zorgvuldig met het BSN wordt omgegaan, wordt er voorzien in een zogenaamde *Nationale Vertrouwensfunctie* (NVF). De NVF is niet een aparte instelling of organisatie maar een verzameling maatregelen die ervoor zorgt dat het BSN op de juiste manier wordt gebruikt. Voor wat betreft het BSN gaat het om de volgende drie voorzieningen:

- de Landkaart;
- het Toetsingskader;
- de Functionaris voor de Gegevensbescherming.

Landkaart
Eén van de manieren om het vertrouwen van de burger te bevorderen, houdt in dat er inzicht dient te worden gegeven in de categorieën persoonsgegevens die de overheid vastlegt en wat zij daarmee doet. In deze transparantie wordt onder meer voorzien door middel van de Landkaart[145]. De Landkaart is een voorziening in de vorm van een website. De Landkaart geeft onder meer inzicht in het gebruik van het BSN en biedt een overzicht van de verschillende gebruikers, van de (categorieën van) persoonsgegevens die worden vastgelegd en van de (categorieën van) persoonsgegevens die worden uitgewisseld met andere gebruikers, met inbegrip van gebruikers die geen overheidsorgaan zijn. Er wordt met de Landkaart geen inzicht gegeven in de persoonsgegevens van een individuele burger. Er wordt wel inzichtelijk gemaakt welke categorieën van gegevens organisaties volgens de wet mogen vastleggen en uitwisselen en welke wettelijke grondslag daarvoor bestaat. Met de landkaart krijgen burgers systematisch inzicht in de wijze waarop de overheid gegevens over haar burgers uitwisselt met behulp van het BSN.[146] Ook andere overheidsprojecten zijn aan de landkaart toegevoegd, om voor de burger inzichtelijk te maken wat de status is van de e-overheid projecten.

Het beheer van de Landkaart is ondergebracht bij het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR). Dit agentschap van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties beheert ook de GBA en de Beheervoorziening BSN. Om de inhoud van de Landkaart actueel te houden, zijn overheidsorganen verplicht informatie aan te leveren over gegevensverwerkingen waarbij het BSN wordt gebruikt. Niet-overheidsorganen die het BSN moeten gebruiken, hebben zelf geen informatieplicht met betrekking tot de Landkaart.[147] Echt transparant maakt de Landkaart het gebruik niet, er worden bij de diverse gemeenten wel verwijzingen gegeven naar de bestanden die gebruik

[143] Agentschap BPR, 'Beheervoorziening', WWW < http://www.bprbzk.n/>, geraadpleegd 3 juli 2008.
[144] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 14-15.
[145] Zie: www.landkaarte-overheid.nl.
[146] *Kamerstukken II*, 2005-2006, 30 312, nr. 3, p. 23.
[147] Artikel 18 Wabb.

maken van BSN, maar de inhoud van deze bestanden of het doel worden niet verklaard. Hoewel de kaart op het moment van schrijven alleen de status van BSN en DigiD goed laat zien, is het streven de landkaart snel up-to-date te maken. De verantwoordelijkheid voor het aanleveren van informatie voor de landkaart ligt echter bij de overheidsinstanties die de diverse projecten implementeren.

Toetsingskader
Een volgende onderdeel van de NVF is het toetsingskader. Het toetsingskader dient als handvat voor de goede uitvoering, als hulpmiddel van toezichthouders, als nadere uitwerking en operationalisering, als toelichting op de regels van de Wbp, als een handvat voor beveiliging en het geeft een overzicht van eisen voor gebruik van het BSN. Ook het toetsingskader draagt bij aan het vertrouwen in de wijze waarop de overheid met persoonsgegevens omgaat in het BSN-stelsel.

Functionaris voor de Gegevensbescherming
Bij de Beheervoorziening BSN is een Functionaris voor de Gegevensbescherming ingesteld.[148] Wat een Functionaris voor de Gegevensbescherming precies inhoudt, werd hierboven al bij de behandeling van de Wet bescherming persoonsgegevens (Wbp) besproken. De FG die is aangesteld ten behoeve van de Beheervoorziening BSN, kan uiteraard slechts toezien op de gegevensverwerkingen, voor zover deze onder de verantwoordelijkheid van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties vallen. Omdat deze minister verantwoordelijk is voor de centrale componenten van het BSN-stelsel (ondergebracht in de Beheervoorziening BSN) bevordert het toezicht dat de FG uitoefent in de praktijk de goede werking van het BSN-stelsel als geheel. De nadere regeling van taken en bevoegdheden van de FG vindt plaats op grond van de artikelen 62, 63 en 64 van de Wbp.
Burgers kunnen bij de FG bij de Beheervoorziening BSN terecht met eventuele klachten en vragen over het gebruik van het BSN door de Beheervoorziening BSN.

2.8 Wetgeving inzake basisregistraties, de Wet gemeentelijke basisadministratie persoonsgegevens (GBA) als voorbeeld

De overheid werkt aan een stelsel van basisregistraties. Deze registraties dienen als één stelsel te functioneren. Dit stelsel maakt het mogelijk gegevens eenmalig in te winnen en op meerdere plaatsen binnen de overheid te gebruiken. Overheden worden in de toekomst verplicht gebruik te maken van deze gegevens. Daarnaast verschaffen deze authentieke registraties kwalitatief betere informatie. Er zijn inmiddels 10 basisregistraties aangewezen:

- Gemeentelijke Basisadministratie Persoonsgegevens (GBA);
- Handelsregister (NHR);
- Basis Gebouwen Registratie (BGR);
- Basisregistratie Topografie (BRT);
- Basisregistratie Adressen (BRA);
- Basisregistratie Kadaster (BRK);
- Kentekenregistratie;
- Basisregistratie Lonen, Arbeidsverhoudingen en Uitkeringsverhoudingen;
- Basisregistratie Inkomen;
- Basisregistratie WOZ;

De GBA als basisregistratie
De Wet gemeentelijke basisadministratie persoonsgegevens (en de daarop gebaseerde regelgeving) bevat het kader inzake de gemeentelijke basisadministraties persoonsgegevens.

[148] De Wabb legt de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties de plicht op een FG te benoemen, artikel 19 Wabb.

Hieronder wordt dit kader geschetst. Ook wordt de wet- en regelgeving inzake de GBA opgevoerd als een voorbeeld van een juridisch kader met betrekking tot een basisregistratie. De GBA is een register van gegevens over de inwoners van Nederland. Het beheer van de GBA is een taak van de gemeente. De GBA dient echter als algemene administratie. Dat betekent dat ook anderen er gebruik van kunnen maken. Dit gebruik komt erop neer dat anderen gegevens kunnen opvragen uit de GBA. Dat is echter alleen mogelijk voor diegenen die daartoe bevoegd zijn. De Wet GBA maakt een onderscheid tussen (binnengemeentelijke en buitengemeentelijke) afnemers en derden. Afnemers zijn bestuursorganen, derden zijn elke andere persoon of instelling dan een afnemer of een ingeschrevene.[149] De betrokken afnemers zijn overheids- en semi-overheidsorganisaties, die voor de uitoefening van hun publiekrechtelijke taken persoonsgegevens nodig hebben. Voorbeelden zijn de Belastingdienst, waterschappen, de Sociale Verzekeringsbank en pensioenfondsen. In totaal gaat het om enkele honderden afnemers. Zij krijgen selecties uit de GBA-gegevens, al naar gelang hun behoefte en de afspraken die over levering van de GBA-gegevens zijn gemaakt. Er worden aan een afnemer alleen gegevens verstrekt uit de GBA als dat noodzakelijk is voor de vervulling van zijn taak.[150] Aan een derde worden alleen gegevens verstrekt in bij of krachtens de Wet GBA aangewezen gevallen.[151]

Rechten van de betrokkene in de Wet GBA
De Wet GBA bevat een specifieke privacyregeling die niet onder de werkingssfeer van de Wbp valt. De Wet GBA verklaart echter af en toe de Wbp van overeenkomstige toepassing, verder wordt de Wbp materieel gevolgd. De Wet GBA is van toepassing op de in de GBA opgenomen persoonsgegevens en de gegevensverstrekkingen hieruit. Wordt vervolgens iets anders gedaan met de GBA-gegevens (worden zij bijvoorbeeld in een andere registratie opgenomen of anderszins verder verwerkt), of worden extra gegevens verwerkt, dan is op verdere verwerkingen en gegevens de Wbp van toepassing.[152] Een en ander heeft tot gevolg dat de Wet GBA eigen regelingen bevat inzake de rechten van een betrokkenen op onder meer inzage in de GBA en de correctie van onjuiste gegevens in de GBA. Deze rechten worden hieronder beschreven.

Het recht op inzage
Een ieder kan zich tot het college van burgemeester en wethouders wenden met de vraag of er persoonsgegevens die op hem betrekking hebben, worden verwerkt in de GBA. Het college dient op dit verzoek binnen vier weken kosteloos schriftelijk op te antwoorden. Indien er daadwerkelijk gegevens worden verwerkt die op de verzoeker betrekking hebben, dan dient aan de verzoeker een schriftelijke mededeling te worden gedaan. De schriftelijke mededeling bevat onder meer de hoofdlijnen van de regels betreffende de GBA, de hoofdlijnen van de regels betreffende de identiteit van de voor de verwerking verantwoordelijke, de doeleinden van de GBA, de categorieën van ontvangers van gegevens en de rechten van de ingeschrevene.[153] Het college van burgemeester en wethouders dient binnen vier weken kosteloos inzage te verlenen aan degene wiens gegevens worden verwerkt.[154] Op verzoek wordt aan een betrokkene binnen vier weken een afschrift verstrekt van de hem betreffende gegevens die in de GBA worden verwerkt. Desgewenst wordt een gewaarmerkt afschrift

[149] Artikel 1 Wet GBA.
[150] Artikel 3 lid 1 en lid 2 Wet GBA.
[151] Artikel 3 lid 3 GBA.
[152] L.L.F.M. Mutsaers, 'De gemeentelijke basisadministratie persoonsgegevens', p. 164-165, In: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2002, p. 159-195.
[153] Artikel 79 lid 1 juncto 78 lid 3 Wet GBA.
[154] Artikel 79 lid 2 Wet GBA.

verstrekt.[155] Overigens wordt geen informatie medegedeeld over het verstrekken van gegevens uit de GBA aan afnemers, voor zover dit noodzakelijk is in het belang van de veiligheid van de staat of de voorkoming, opsporing en vervolging van strafbare feiten.[156] Wanneer een verzoek tot inzage worden gedaan, dient het college van burgemeester en wethouders zorg te dragen voor een deugdelijke vaststelling van de identiteit van de verzoeker.[157]

Het recht op correctie
Het kan voorkomen dat de gegevens in de GBA, feitelijk onjuist of onvolledig zijn of in strijd met een wettelijk voorschrift worden verwerkt. De betrokkene kan dan het college van burgemeester en wethouders verzoeken de hem betreffende gegevens te verbeteren, aan te vullen of te verwijderen.[158] Ook bij het recht op correctie dient het college van burgemeester en wethouders zorg te dragen voor een deugdelijke vaststelling van de identiteit van de verzoeker.[159] Van de uitvoering van het verzoek dient het college terstond schriftelijk mededeling te doen aan de verzoeker.[160] Naast het recht op correctie, bestaat er voor de burger ook de plicht tot het melden van onjuistheden in de GBA.[161] Denk hierbij aan het verplicht doorgeven van adreswijzigingen.[162]

Het melden van correctie aan afnemers en derden
Naar aanleiding van een verzoek van de betrokkene kunnen gegevens in de GBA worden gewijzigd. Daarnaast kan het voorkomen dat het college van burgemeester en wethouders ambtshalve gegevens van een betrokkene verbetert, aanvult of verwijdert. In beide gevallen dient op verzoek van de betrokkene het college melding te doen van de verbetering, aanvulling of verwijdering aan diegenen die gegevens afnemen van de GBA. Er hoeft dan alleen melding te worden gedaan aan die afnemers en derden aan wie in het jaar voorafgaand aan het verzoek van de betrokkene en in de periode die is verstreken sinds het verzoek, de betreffende gegevens zijn verstrekt. Mocht de melding aan de afnemers of derden onmogelijk blijken of een onevenredige inspanning te kosten, dan hoeft zij niet te worden gedaan.[163]

Met ingang van 7 februari 2007 is de Wet GBA gewijzigd door de Wet tot wijziging van de Wet gemeentelijke basisadministratie persoonsgegevens in verband met de aanpassing aan de eisen die gelden voor basisregistraties.[164] Dit heeft onder meer de volgende wijzigingen met zich meegebracht.[165]

Authentieke gegevens
Op grond van het nieuwe artikel 3a kan bij algemene maatregel van bestuur worden bepaald welke gegevens worden aangemerkt als authentieke gegevens. Dit is inmiddels gebeurd middels artikel 58a van het Besluit gemeentelijke basisadministratie persoonsgegevens.

---

[155] Artikel 79 lid 2 Wet GBA.
[156] Artikel 79 lid 1 juncto 78 lid 5 Wet GBA.
[157] Artikel 79 lid 4 Wet GBA.
[158] Artikel 82 lid 1 Wet GBA.
[159] Artikel 82 lid 4 juncto 79 lid 4 Wet GBA.
[160] Artikel 82 lid 5 Wet GBA.
[161] Artikelen 65 – 77 Wet GBA.
[162] Artikel 66 Wet GBA.
[163] Artikelen 82 en 104 Wet GBA.
[164] *Stb.* 2007, 76. Inwerkingtreding: *Stb.* 2007, 78.
[165] Een aantal van deze wijzigingen is tot 1 januari 2010 beperkt van toepassing, artikel 146b Wet GBA.

Verplicht gebruik
Een tweede wijziging houdt in dat een afnemer die bij de vervulling van zijn taak informatie over een ingeschrevene nodig heeft die als authentiek gegeven in de GBA beschikbaar is in beginsel verplicht is om voor die informatie gebruik te maken van dat gegeven.[166]

Eenmalige gegevensverstrekking
Een ingeschrevene mag weigeren om aan een afnemer een gegeven te verstrekken, indien die afnemer in het kader van het verplicht gebruik dit gegeven uit de GBA dient te betrekken. De ingeschrevene kan zich hier niet op beroepen voor zover het gegeven noodzakelijk wordt geacht voor een deugdelijke vaststelling van de identiteit van de betrokkene.[167]

Terugmeldplicht
Indien een afnemer *gerede twijfel* heeft over de juistheid van een authentiek gegeven dat hij verstrekt heeft gekregen uit de basisregistratie, dan dient hij daarvan mededeling te doen aan het college van burgemeester en wethouders.[168]

Bovenstaande vier elementen zijn typerend voor basisregistraties. Zij zijn ook te vinden in de wettelijke regelingen van de andere basisregistraties.

2.9 Wet openbaarheid van bestuur (Wob)
De Wet openbaarheid van bestuur (Wob) regelt de toegang tot overheidsinformatie en ook het hergebruik van deze informatie.

De Wob gaat zowel uit van de term 'document', dit is een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat,[169] als de term 'informatie'. Hoewel de laatste term niet wordt gedefinieerd in de WOB, mag worden uitgegaan van bestuurlijke informatie. De Wob regelt immers de openbaarheid van bestuur. Gegevens die een extreme verzamelings- of afleidingsinspanning versien van het betreffende bestuursorgaan, zouden in theorie niet als informatie in de zin van de Wob moeten worden gezien.[170] Een Wob-verzoek kan voorts worden omschreven als een verzoek om informatie neergelegd in documenten over een bestuurlijke aangelegenheid, dat gericht is tot een bestuursorgaan of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf.[171]

Wat betreft de toegang tot overheidsinformatie wordt er een onderscheid gemaakt tussen actieve en passieve informatieverstrekking. De actieve informatieverstrekking houdt in dat een bestuursorgaan bij de uitvoering van zijn taak overeenkomstig de Wob informatie verstrekt en daarbij uitgaat van het algemeen belang van openbaarheid van informatie.[172] Eén van de eisen die de Wob stelt aan het verstrekken van informatie houdt in dat het bestuursorgaan er zoveel mogelijk zorg voor dient te dragen dat de verstrekte informatie actueel, nauwkeurig en vergelijkbaar is.[173] Aan de actualiteitswaarde worden overigens ook weer niet al te hoge eisen gesteld. Dit valt af te leiden uit het feit dat het bestuursorgaan kan volstaan met het openbaar maken door de betreffende stukken op te nemen in een algemeen verkrijgbare uitgave, afzonderlijk uit te geven en algemeen verkrijgbaar te stellen, of ter inzage te leggen, in kopie te

[166] Artikel 3b Wet GBA.
[167] Artikel 3c Wet GBA.
[168] Artikel 62 lid 1 Wet GBA.
[169] Artikel 1 sub a Wob.
[170] Lodder e.a., 'Wob & ICT: over openbaarheid van bestuur in de informatiemaatschappij', WWW <http://appia.rechten.vu.nl/~lodder/papers/wob&ict.htm>.
[171] Artikel 3 lid 1 Wob.
[172] Artikel 2 lid 1 Wob.
[173] Artikel 2 lid 2 Wob.

verstrekken of uit te lenen.[174] Hieruit blijkt dat het bestuursorgaan bijvoorbeeld niet verplicht is *real-time* informatie te verstrekken.

De passieve informatieverstrekking houdt in dat het bestuursorgaan op verzoek informatie verstrekt. Een ieder kan een verzoek om informatie, neergelegd in documenten, over een bestuurlijke aangelegenheid richten tot een bestuursorgaan (of een daaronder werkzame instelling, dienst of bedrijf).[175] De verzoeker dient daarbij de bestuurlijke aangelegenheid of het document te noemen.[176] Hij hoeft niet te stellen zelf een bepaald belang te hebben.[177] Het bestuursorgaan verstrekt informatie uit de documenten door:

a. kopie ervan te geven of de letterlijke inhoud ervan in andere vorm te verstrekken;
b. kennisneming van de inhoud toe te staan;
c. een uittreksel of een samenvatting van de inhoud te geven, of
d. inlichtingen daaruit te verschaffen.[178]

Indien de verzoeker erom vraagt om de informatie in een bepaalde vorm te verschaffen, dan verstrekt het bestuursorgaan de informatie in de verzochte vorm, tenzij het verstrekken van de informatie in die vorm redelijkerwijs niet gevergd kan worden, en/of de informatie reeds in een andere, voor de verzoeker gemakkelijk toegankelijke vorm voor het publiek beschikbaar is.[179] Het verzoek wordt door het bestuursorgaan ingewilligd tenzij één van de uitzonderingsgronden of beperkingen zoals opgenomen in de Wob zich voordoet.[180]

Uit bovenstaande blijkt dat zowel bij de actieve als bij de passieve informatieverstrekking er geen verplichting is tot regelmatige of structurele informatieverstrekking. De burger kan met andere woorden geen ‘abonnement’ krijgen op overheidsinformatie (het regelmatig indienen van een Wob-verzoek daargelaten) of zelfstandig ‘inkijken’ in de informatiesystemen van de overheid.

De bepalingen in de Wob die het hergebruik van overheidsinformatie betreffen, gelden als (gedeeltelijke) implementatie van de Europese richtlijn inzake het hergebruik van overheidsinformatie.[181] Op grond van de Wob kan een ieder een verzoek om hergebruik richten tot een overheidsorgaan (of een onder verantwoordelijkheid daarvan werkzame instelling, dienst of bedrijf).[182] Onder ‘hergebruik’ verstaat de Wob ‘het gebruik van informatie die openbaar is (op grond van de Wob zelf of op grond van een andere wet) en die is neergelegd in documenten berustend bij een overheidsorgaan, voor andere doeleinden dan het oorspronkelijke doel binnen de publieke taak waarvoor de informatie is geproduceerd.’[183] De bepalingen van de Wob ten aanzien van toegang tot overheidsinformatie zijn voor de groot deel van overeenkomstige toepassing.[184] Specifiek ten aanzien van hergebruik bepaalt de Wob dat:

- voor hergebruik beschikbare document zoveel mogelijk langs elektronische weg beschikbaar worden gesteld;[185]

---

[174] Artikel 9 lid 3 Wob.
[175] Artikel 3 lid 1 Wob.
[176] Artikel 3 lid 2 Wob.
[177] Artikel 3 lid 3 Wob.
[178] Artikel 7 lid 1 Wob.
[179] Artikel 7 lid 2 Wob.
[180] Artikel 3 lid 5 Wob. Zie artikel 10 en 11 ten aanzien van deze gronden en beperkingen.
[181] Richtlijn 2003/98/EG, *PbEG* 2003 L 345/90.
[182] Artikel 11b lid 1 Wob.
[183] Artikel 1 sub h Wob.
[184] Artikel 11c Wob.
[185] Artikel 11d Wob.

- een overheidsorgaan niet verplicht is de vervaardiging van documenten voort te zetten, enkel met het oog op hergebruik;[186]
- de voorwaarden voor hergebruik voor vergelijkbare categorieën van hergebruik gelijk zijn;[187]
- een exclusief recht tot hergebruik niet wordt verleend, tenzij dat noodzakelijk is voor het verlenen van een dienst van algemeen belang. Indien er een exclusief recht worden verleend, dient elke drie jaar te worden bezien of de reden voor het verlenen van het exclusieve recht nog aanwezig is;[188]
- de totale inkomsten uit het verstrekken en het verlenen van toestemming voor hergebruik niet hoger mogen zijn dan de kosten van verzameling, productie, vermenigvuldiging en verspreiding van de informatie, vermeerderd met een redelijk rendement op investeringen.[189]

Het hergebruikregime van de Wob is niet van toepassing op informatie waarvan het overheidsorgaan niet auteursrechthebbende is, dan wel niet als producent in de zin van de Databankenwet geldt.[190]

2.10 Auteurswet (Aw)

Artikel 1 van de Auteurswet (Aw) geeft bondig de essentie van het (subjectieve) auteursrecht weer: 'het auteursrecht is het uitsluitend recht van de maker van een werk (…) om dit openbaar te maken en te verveelvoudigen, behoudens beperkingen bij de wet gesteld'. Onder 'werk' verstaan de Auteurswet 'ieder voortbrengsel van letterkunde, wetenschap of kunst, op welke wijze of in welke vorm het ook tot uitdrukking zij gebracht'. Voorbeelden van werken zijn boeken, brochures, nieuwsbladen, tijdschriften en alle andere geschriften, mondelinge voordrachten, aardrijkskundige kaarten, ontwerpen, schetsen en plastische werken met betrekking tot bouwkunde, aardrijkskunde, plaatsbeschrijving of andere wetenschappen, fotografische werken, filmwerken, tekeningen en modellen van nijverheid, computerprogramma's en het voorbereidend materiaal.[191]

De Aw bevat twee specifieke bepalingen ten aanzien van de overheid. De Auteurswet spreekt dan van de 'openbare macht'. Artikel 11 Aw bepaalt dat er geen auteursrecht rust op 'wetten, besluiten en verordeningen, door de openbare macht uitgevaardigd, noch op rechterlijke uitspraken en administratieve beslissingen'. De achterliggende gedachte hierbij is de democratische eis die meebrengt dat werken als deze zonder (verdere) overheidsbemoeienis zo ruim mogelijk verspreid moeten kunnen worden, en met name geen voorwerp kunnen zijn van geheimhouding door diezelfde overheid, of voorwerp van selectieve openbaarmaking.[192]

Ten aanzien van andere werken dan die door artikel 11 worden bestreken, die door (of vanwege) de openbare macht openbaar worden gemaakt en waarvan de openbare macht de auteursrechthebbende is, bepaalt artikel 15b Aw dat in beginsel iedere openbaarmaking of verveelvoudiging daarvan is toegestaan, tenzij het auteursrecht is voorbehouden.

---

[186] Artikel 11e Wob.
[187] Artikel 11f Wob.
[188] Artikel 11g Wob.
[189] Artikel 11h Wob.
[190] Artikel 11a lid 1 sub a Wob.
[191] Artikel 10 lid 1 Auteurswet.
[192] J.H. Spoor, D.W.F. Verkade & D.J.G. Visser, *Auteursrecht. Auteursrecht, naburige rechten en databankenrecht*, Deventer: Kluwer 2005, p. 137.

2.11 Databankenwet

Met de Databankenwet (Dw) heeft de Nederlandse wetgever in 1999 de Europese Databankenrichtlijn[193] geïmplementeerd. De Dw geeft producenten van databanken een eigen recht (het sui generis-recht). Onder een databank wordt verstaan:

- een verzameling van werken, gegevens of andere zelfstandige elementen;
- die systematisch of methodisch geordend zijn; en
- die afzonderlijk met elektronische middelen of anderszins toegankelijk zijn; en
- waarvan de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een *substantiële investering*.[194]

Een cruciale vraag is wanneer een investering als *substantieel* kan worden gezien. Een investering zou gezien kunnen worden als substantieel, indien zij eerst na geruime tijd door exploitatie van de databank kan worden terugverdiend. In die gedachtegang is juridische bescherming van de databank noodzakelijk om de databank economisch gezien verantwoord tot stand te kunnen brengen.[195] De wet verstaat onder *producent* van een databank degene die het risico draagt van de voor de databank te maken investering.[196] De roept ten aanzien van databank die worden gerealiseerd door de overheid de vraag op of er sprake kan zijn van een investering waarvoor een risico wordt gedragen. De vraag komt hierna kort aan de orde bij de behandeling van een vonnis van de Rechtbank Amsterdam.

Het eigen recht houdt in dat de producent het uitsluitend recht heeft toestemming te verlenen voor de volgende handelingen:

1. het opvragen en hergebruiken van het geheel of van een substantieel deel (in kwalitatief of kwantitatief opzicht) van de inhoud van de databank;
2. het herhaald en systematisch opvragen of hergebruiken van niet-substantiële delen (in kwalitatief of kwantitatief opzicht) van de inhoud van een databank, voorzover dit:
    - in strijd is met de normale exploitatie van die databank; of
    - ongerechtvaardigde schade toebrengt aan de rechtmatige belangen van de producent van de databank.[197]

Net zoals de Auteurswet bevat ook de Dw specifieke bepalingen ten aanzien van de openbare macht (de overheid). In de eerste plaats is het hierboven genoemde eerste recht niet van toepassing ten aanzien van databanken waarvan zij de openbare macht de producent is, tenzij dit recht uitdrukkelijk is voorbehouden. Dit voorbehoud kan geschieden in het algemeen bij de wet, besluit of verordening, in een bepaald geval blijkens mededeling op de databank zelf of bij de terbeschikkingstelling aan het publiek van de databank.[198] In de tweede plaats bezit de openbare macht het hierboven genoemde eerste recht *niet* ten aanzien van databanken waarvan zij de producent is en waarvan de inhoud gevormd wordt door wetten, besluiten en verordeningen, door haar uitgevaardigd, of door rechterlijke uitspraken en administratieve beslissingen.[199]

---

[193] *PbEG* 1996 L 77/20.
[194] Artikel 1 sub a Dw.
[195] Spoor, Verkade & Visser 2005, p. 621-623 (zie noot 192).
[196] Artikel 1 sub b Dw.
[197] Artikel 2 lid 1 Dw.
[198] Artikel 8 lid 2 Dw.
[199] Artikel 8 lid 1 Dw.

De rechtbank Amsterdam heeft zich recentelijk gebogen over de vraag of de gemeente Amsterdam zich kan beroepen op de Dw.[200] Het betrof een geschil waarbij de eiseres bepaalde gegevens van de gemeente wenste te verkrijgen. De gemeente beriep zich op de Dw en op de hergebruikregeling van de Wob om zo een vergoeding te kunnen vragen voor de gegevensverstrekking en om voorwaarden aan de verstrekking te kunnen stellen (in de vorm van een licentieovereenkomst). De rechtbank heeft besloten dat de gemeente zich niet kan beroepen op de Dw. Wil men worden aangemerkt als een producent van een databank, dan dient men het risico te dragen van de voor de databank te maken investering, zoals hierboven wordt beschreven. Volgens de rechtbank had de gemeente publieke middelen tot haar beschikking, waardoor er geen sprake is van een risicodragende investering. Omdat daar volgens de rechtbank geen sprake van was, kwam aan de gemeente geen databankenrecht toe, en is de hergebruikregeling van de Wob ook niet van toepassing.

De redenering van de rechtbank Amsterdam heeft tot gevolg dat de overheid slechts zelden als producent van een databank zal kunnen worden aangemerkt. De meeste databanken, geproduceerd door de overheid, zullen immers zijn geproduceerd met publieke middelen. In lijn met de redering van de rechtbank zou een overheidsorgaan wellicht wél een databankenrecht kunnen toekomen indien hij het risico draagt van de voor de databank te maken investering. Daar zou bijvoorbeeld sprake van kunnen zijn indien een overheidsorgaan niet wordt gefinancierd door overheidsgelden én indien het zichzelf dient te bedruipen. In dat geval draagt het overheidsorgaan immers daadwerkelijk het risico van de investering die is gedaan om tot de databank te komen.[201]

2.12 Wetsvoorstel Wet algemene bepalingen omgevingsrecht (Wabo)

De wetgever beoogt met het wetsvoorstel Wet algemene bepalingen omgevingsrecht (Wabo) één geïntegreerde vergunning voor bouwen, wonen, monumenten, ruimte, natuur en milieu mogelijk te maken. Het wetsvoorstel Wabo is in december 2007 plenair in de Tweede Kamer besproken, waarna de Kamer in grote meerderheid met het voorstel heeft ingestemd. Halverwege december is het wetsvoorstel naar de Eerste Kamer gestuurd. Naar verwachting treedt de Wabo op 1 januari 2009 in werking.

Hierna wordt uitgegaan van de volgende wet- en regelgeving:

- De Algemene wet bestuursrecht (Awb);
- het wetsvoorstel Wet algemene bepalingen omgevingsrecht (Wabo);[202]
- het voorontwerp Besluit omgevingsrecht (BOR);[203]
- het voorontwerp Ministeriële regeling omgevingsrecht (MOR);[204] en
- de Wet ruimtelijke ordening (Wro).[205]

De Wabo bevat twee hoofdregels met betrekking tot de vraag welke werkzaamheden vergunningsplichtig zijn. Volgens de eerste hoofdregel is het verboden zonder vergunning bepaalde projecten uit te voeren.[206] Het gaat dan bijvoorbeeld om het bouwen van een bouwwerk. Volgens de tweede hoofdregel is een omgevingsvergunning nodig voorzover bij

---

[200] Rb. Amsterdam, 6 februari 2008, AWB 07/786 WET (Landmark Nederland B.V./College van B&W Gemeente Amsterdam).
[201] Zie H.W. Wefers Bettink, 'Intellectuele eigendomsrechten op geo-informatie', in: L. van der Wees & S. Nouwt (red.), *Recht en locatie. Geo-informatie in een juridische context* (Nederlandse Vereniging voor Informatietechnologie en Recht), Den Haag: Reed Business BV 2008, p. 85-89.
[202] *Kamerstukken II* 2006/07-2007/08, 30 844, nr. 1-40; *Kamerstukken I* 2007/08, 30 844, A-C.
[203] Versie 6 december 2006.
[204] Versie 6 december 2006.
[205] *Stb.* 2006, 566.
[206] Artikel 2.1 lid 1 Wabo.

een provinciale of gemeentelijke verordening is bepaald dat het verboden is zonder vergunning bepaalde werkzaamheden te verrichten.[207]

'Bevoegd gezag'
De Wabo gaat ervan uit dat één bestuursorgaan één integraal besluit neemt met betrekking tot de vergunningverlening. De hoofdregel is dat het college van burgemeester en wethouders van een gemeente als bevoegd gezag worden aangemerkt.[208] Bij AMvB kan worden bepaald dat gedeputeerde staten voor projecten die van provinciaal belang zijn, als bevoegd gezag worden aangemerkt, of dat een aangewezen minister voor projecten die van nationaal belang zijn als bevoegd gezag wordt aangemerkt.[209] De minister van VROM kan in afwijking van deze hoofdregels bepalen dat hij als bevoegd gezag wordt aangemerkt indien dat geboden is in het algemeen belang.[210]

Waar dient de vergunningaanvraag aan te voldoen?
Een aanvraag dient te worden ondertekend en bevat ten minste:
- de naam en het adres van de aanvrager;
- de dagtekening;
- een aanduiding van de beschikking die wordt gevraagd;[211]

De aanvrager verschaft voorts de gegevens en bescheiden die voor de beslissing op de aanvraag nodig zijn en waarover hij redelijkerwijs de beschikking kan krijgen.[212]

Aantal exemplaren dat moet worden ingediend ingeval van schriftelijke aanvraag
De aanvraag kan schriftelijk of elektronisch worden gedaan.[213] Bedrijven (rechtspersonen of natuurlijke personen die een bedrijf of zelfstandig beroep uitoefenen) kunnen uitsluitend op elektronische wijze een aanvraag doen.[214] Het bevoegd gezag kan bepalen hoeveel exemplaren van de aanvraag en de bijbehorende gegevens en bescheiden dienen te worden ingediend, maar dit kan maximaal vier exemplaren bedragen.[215]

Algemene indieningsvereisten
In een aanvraag om een vergunning vermeldt de aanvrager:
a. de naam, het adres en de woonplaats van de aanvrager, alsmede het elektronisch adres van de aanvrager indien de aanvraag op een e-formulier wordt ingediend;
b. het adres, de kadastrale aanduiding dan wel de ligging van het project;
c. een omschrijving van de aard en de reden van het project;
d. een omschrijving van de aard, de omvang en de effecten[216] van de activiteiten die worden aangevraagd;

---

[207] Artikel 2.2 lid 1 Wabo.
[208] Artikel 2.5 lid 1 Wabo.
[209] Respectievelijk artikel 2.5 lid 2 en 3 Wabo.
[210] Artikel 2.5 lid 4 Wabo.
[211] Artikel 4:2 lid 1 Awb.
[212] Artikel 4:2 lid 2 Awb.
[213] Artikel 4.1 lid 1 BOR.
[214] Artikel 4.1 lid 2 BOR.
[215] Artikel 4.2 lid 1 BOR. Indien er meer dan twee adviseurs zijn aangewezen in de situatie dat burgemeester en wethouders als adviseur zijn aangewezen indien zij niet het bevoegd gezag zijn, verstrekt de aanvrager op verzoek van het bevoegd gezag evenzoveel meer exemplaren, artikel 4.2 lid 2 juncto 6.1 BOR.
[216] Met 'effecten' wordt bedoeld een beschrijving van de gevolgen van de activiteit voor de fysieke leefomgeving, voor zover die gevolgen relevant zijn voor de beoordeling van de aanvraag om een omgevingsvergunning.

e. indien de aanvraag wordt ingediend door een gemachtigde: zijn naam, adres en woonplaats, alsmede het elektronisch adres van de gemachtigde indien de aanvraag op een e-formulier wordt ingediend;
f. indien het project wordt uitgevoerd door een ander dan de aanvrager: zijn naam, adres en woonplaats.[217]

De aanvrager voorziet de aanvraag van een aanduiding waaruit de plaats en de omvang van de aangevraagde activiteit of activiteiten kan worden opgemaakt.[218] De aanvrager doet bij de aanvraag een gespecificeerde opgave van de kosten van de te verrichten werkzaamheden, in verband met de berekening van de leges, tenzij geen leges worden geheven.[219]

Bovenstaande vereisten zijn de algemene indieningsvereisten. Naast deze vereisten, dient een aanvraag te voldoen aan de specifieke eisen die worden gesteld ingeval van specifieke activiteiten.[220] Zo gelden er bijvoorbeeld aanvullende vereisten voor aanvragen inzake bouwen en huisvesten, inzake het uitvoeren van een werk of werkzaamheden, inzake sloopactiviteiten en inzake het gebruiken van gronden, gebouwen, monumenten of andere objecten.

Elektronische indiening
Ingeval de vergunningsaanvraag op elektronische wijze worden gedaan, dan nemen burgemeester en wethouders van de gemeente waar het project geheel of in hoofdzaak wordt of zal worden uitgevoerd of het bevoegd gezag, indien burgemeester en wethouders niet bevoegd zijn op de aanvraag te beslissen, nemen een aanvraag die langs elektronische weg wordt gedaan, in ontvangst.[221]
Ingeval van een elektronische vergunningsaanvraag, dienen ook de daarbij te verstrekken gegevens en bescheiden langs elektronische weg te worden verstrekt. De aanvrager kan de gegevens en bescheiden op schriftelijke wijze verstrekken, voor zover het bevoegd gezag te kennen heeft gegeven dat dit mogelijk is.[222] Het bestuursorgaan dient de ontvangst van een elektronisch ingediende aanvraag te bevestigen.[223]

Algemene eisen aan elektronische indiening
Algemene gegevens, rapportages en berekeningen dienen aangeleverd te worden in een van de volgende bestandsformaten:

- .pdf;
- .doc;
- .xls.[224]

Tekeningen dienen aangeleverd te worden in een van de volgende bestandsformaten:

- .jpg
- .tiff
- .pdf
- .dwf formaat, indien de gemeente heeft aangegeven dat het dit formaat accepteert.[225]

[217] Artikel 1.1 lid 1 MOR.
[218] Artikel 1.1 lid 2 MOR. Met ‘aanduiding’ is bedoeld een situatieschets, foto of afbeelding. De gekozen vorm en de maatvoering zijn in beginsel vormvrij.
[219] Artikel 1.1 lid 3 MOR.
[220] Artikel 4.4 lid 1 BOR.
[221] Artikel 4.3 lid 1 BOR.
[222] Artikel 4.3 lid 2 BOR.
[223] Artikel 4:3a Awb.
[224] Artikel 1.2 lid 1 MOR.
[225] Artikel 1.2 lid 2 MOR.

Indien de digitale bestanden worden ingediend op een opslagmedium, dient deze slechts bruikbaar te zijn voor het alleen lezen van die bestanden, zogenoemde 'read-only'-bestanden. Indien de bestanden langs elektronische weg worden aangeleverd dienen deze als 'read-only' (alleen lezen) te zijn gekenmerkt.[226]

Het MOR bevat voorts aanvullende vereisten ten aanzien van de indiening van aanvragen voor de verschillende categorieën van projecten.

2.13 Archiefwet 1995

De Archiefwet 1995 regelt onder meer de vorming, selectie, het behoud, de openbaarheid en ook de vernietiging van archiefbescheiden, en de bestuurlijke verhoudingen hieromtrent.

Eén van de hoofdregels van de Archiefwet 1995 houdt in dat overheidsorganen verplicht zijn de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren. Ook moeten zij zorgdragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden.[227] Onder *overheidsorgaan* wordt verstaan een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of een ander persoon of college met enig openbaar gezag bekleed.[228] Naast het overheidsorgaan richt de Archiefwet 1995 zich tot de zogenaamde zorgdrager, dit is degene die bij of krachtens de wet is belast met de zorg voor de archiefbescheiden.[229]

De zorgdrager dient selectielijsten te ontwerpen waarin tenminste wordt aangegeven welke archiefbescheid voor vernietiging in aanmerking komen.[230] Het Archiefbesluit 1995 schrijft voor op welke wijze een selectielijst moet worden opgesteld en welke inhoud het tenminste moet bevatten.

De Regeling geordende en toegankelijke staat archiefbescheiden[231] (hierna: de Regeling) bevat regels ten aanzien van de wijze waarop archiefbescheiden dienen te worden bewaard. De Regeling geeft een aantal hoofdregels ten aanzien van de geordende en toegankelijke staat van archiefbescheiden.[232] Indien een gerede kans bestaat dat, als gevolg van wijziging van besturingsprogrammatuur, toepassingsprogrammatuur of andere apparatuur,niet aan deze hoofdregels kan worden voldaan, zorgt de zorgdrager ervoor dat conversie dan wel migratie van digitale archiefbescheiden plaatsvindt.[233] Onder conversie wordt verstaan het omzetten in of het overzetten van gegevens in een ander opslagformaat.[234] Onder migratie wordt verstaan het overzetten van gegevens en toepassingsprogrammatuur naar een ander platform.[235]

De zorgdrager dient archiefbescheiden die niet voor vernietiging in aanmerking komen en die ouder zijn dan twintig jaar over te brengen naar een archiefbewaarplaats.[236] Archiefbescheiden die niet voor vernietiging in aanmerking komen en die jonger zijn dan twintig jaar, kunnen door

---

[226] Artikel 1.2 lid 3 MOR.
[227] Artikel 3 Archiefwet 1995.
[228] Artikel 1 sub b Archiefwet 1995.
[229] Artikel 1 sub d Archiefwet 1995.
[230] Artikel 5 lid 1 Archiefwet 1995.
[231] *Stcrt.* 1 maart 2002, nr. 43, p. 8.
[232] Artikelen 2 t/m 4 van de Regeling.
[233] Artikel 5 lid 1 van de Regeling.
[234] Artikel 1 sub e van de Regeling.
[235] Artikel 1 sub i van de Regeling
[236] Artikel 12 lid 1 Archiefwet 1995.

de zorgdrager naar een archiefbewaarplaats worden overgebracht indien de beheerder van de archiefbewaarplaats van oordeel is dat er voldoende aanleiding bestaat ruimte beschikbaar te stellen.[237] Digitale archiefbescheiden dienen uiterlijk op het tijdstip van overbrenging te worden opgeslagen volgens de volgende standaarden:

a. voor character sets: ASCII (ISO/IEC 8859-1) of Unicode (ISO/IEC 10646-1);
b. voor tekstbestanden: Portable document format (PDF) of SGML dan wel XML vergezeld van een stylesheet (XSL, CSS) dan wel TIFF of PDF met de metadata in een XML-wrapper;
c. voor CAD/CAM bestanden; Portable document format (PDF) en STEP (Standard for the exchange of product data) als metadata standaard (ISO 10303);
d. voor images/beelden (bitmapped): Portable document format (PDF) en, indien gebruik gemaakt wordt van compressie: ITU T4 of ITU T6;
e. voor databases: het oorspronkelijke opslagformaat of ASCII (flatfile, met veldscheidingstekens), vergezeld van documentatie bij voorkeur in XML-DTD over de structuur van de database, tenminste omvattende een compleet logisch datamodel met beschrijving van de entiteiten; queries dienen in de vraagtaal SQL (SQL2) te worden vastgelegd.[238]

2.14 Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI) en de Wet eenmalige gegevensuitvraag werk en inkomen (WEU)

Voor de keten werk en inkomen zijn met name de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI) en de Wet eenmalige gegevensuitvraag werk en inkomen (WEU) relevant voor de e-Overheid. De keten werk en inkomen vormt een voorbeeld van een keten waarin de samenwerking wettelijk is afgebakend en waarin de burger centraal staat. In deze paragraaf zullen beide wetten besproken worden.

Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI)

De Wet SUWI[239], van kracht sinds 2002 regelt de structuur voor de uitvoeringsorganisatie in de keten werk en inkomen. Hierbij staat de klant centraal[240] en is er een onderscheid gemaakt tussen de publieke en private uitvoering van taken in de keten. De publieke uitvoering ligt bij de ketenpartners; gemeenten, UWV, SVB, CWI, de private uitvoering in samenwerking met werkgevers en reïntegratiebedrijven. De Wet SUWI heeft geleid tot een verplichte samenwerking tussen ketenpartners, waardoor gedeelde verantwoordelijkheid en betrokkenheid (wettelijk) worden erkend. De memorie van toelichting beschrijft de criteria waaraan het nieuwe stelsel voor werk en inkomen moet voldoen:

- Effectiviteit: helderheid over taken en verantwoordelijkheden;
- Klantgerichtheid: één-loketgedacht (uitvoering in DKD);
- Doelmatigheid: bundeling van taken zorgt voor schaalvoordelen en vermindering van bestuurslagen;
- Publieke waarborgen: scherp onderscheid tussen publiek en privaat;
- Beleidsmatige aansturingsmogelijkheden: de mogelijkheid tot Ministeriële an- en bijsturing;
- Toezichtbaarheid: transparantie en duidelijkheid zorgen voor vergroot toezicht;
- Reorganisatielasten: uiteindelijke lastenvermindering door schaalvoordelen.[241]

---

[237] Artikel 13 lid 1 Archiefwet 1995.
[238] Artikel 6 van de Regeling.
[239] *Stb.* 2001, 624,
[240] De memorie van toelichting bij de Wet SUWI, *Kamerstukken II* 2000-2001, 27 588, nr. 3, benadrukt dit herhaaldelijk (p. 2, 7, 8 e.v.). Alleen door de klant centraal te stellen kan de keten effectief zorg dragen de waarborgfunctie van de overheid in het kader van uitkeringen en het bevorderen van de arbeidsparticipatie.
[241] *Kamerstukken II* 2000-2001, 27 588, nr. 3 p. 12 – 16.

Wet eenmalige gegevensuitvraag werk en inkomen (WEU)
De Wet eenmalige gegevensuitvraag werk en inkomen (WEU)[242], van kracht sinds 1 januari 2008, is een uitvloeisel van de wet Walvis. [243] De WEU regelt de wijzing van diverse sociale zekerheidswetten met als doel administratieve lastenverlichting en verbetering van effectiviteit in de keten werk en inkomen. 'Uit een oogpunt van optimale dienstverlening aan de burger wordt via dit wetsvoorstel geregeld dat elk gegeven dat de ketenpartners werk en inkomen nodig hebben voor hun werk slechts eenmaal mag worden uitgevraagd. Bij het concept van bij wet in te stellen 'basisregistraties' hoort dat afnemers belast met een publieke taak verplicht zijn van de gegevens uit die basisregistraties gebruik te maken. In een basisregistratie worden gegevens die logisch bij elkaar horen en die voor de hele overheid van belang zijn (bijvoorbeeld over bedrijven, personen, etc.), beheerd.'[244] De WEU geeft hiermee ook het e-overheidproject DKD (Digitaal Klantdossier) een wettelijke basis. In feite zorgt het DKD voor uitvoering van de WEU in de keten werk en inkomen.

Het wettelijk kader dat gewijzigd wordt op grond van de WEU bestaat uit de volgende wetten:
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI)
- Wet werk en bijstand (WWB) (voorheen Algemene Bijstandswet, AWB)
- Werkloosheidswet (WW)
- Toeslagenwet
- Ziektewet
- Wet werk en inkomen naar arbeidsvermogen
- Wet op de arbeidsongeschiktheidsverzekering (WAO)
- Wet arbeidsongeschiktheidsvoorziening jonggehandicapten (WAJONG)
- Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers
- Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen
- Wet werk en inkomen kunstenaars
- Algemene Kinderbijslagwet
- Algemene Ouderdomswet (AOW)
- Algemene nabestaandenwet
- Wet verzelfstandiging Informatiseringsbank
- Invoeringswet Wet financiering sociale verzekeringen

Niet alle bovengenoemde wetten worden op even structurele wijze gewijzigd. In alle wetten wordt weliswaar het wettelijk verbod op meermalige gegevensuitvraag opgenomen, maar het is met name de Wet SUWI die een aanzienlijke wijziging ondergaat als gevolg van de invoering van de WEU. Het is immers de Wet SUWI die onder de WEU een nieuwe taak krijgt en nog verdere structuur in de keten werk en inkomen aanbrengt.

[242] Wet van 12 december 2007, *Stb.* 2007, 555, houdende wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen, de Wet werk en bijstand, de Werkloosheidswet en enige andere wetten in verband met eenmalige gegevensuitvraag aan burgers (*Wet eenmalige gegevensuitvraag werk en inkomen*). Inwerkingtreding: 1 januari 2008 (*Stb.* 2007, 556).
[243] Wet Administratieve Lastenverlichting en Vereenvoudiging Socialeverzekeringswetten, Stb. 2004, 311
[244] *Kamerstukken II* 2006-2007, 30 970, nr. 3, Memorie van toelichting bij de Wet Eenmalige Gegevensuitvraag Werk en Inkomen, p. 3.

Eenmalig uitvragen van gegevens
De wet regelt dat burgers slechts eenmaal gegevens hoeven te verstrekken aan een van de ketenpartners in de keten werk en inkomen en dat een andere ketenpartner niet nogmaals om *dezelfde* gegevens mag vragen. De klant staat hiermee centraal. Het zijn de ketenpartners die zorg moeten dragen voor overdracht van gegevens vanuit de diverse bronnen waar de klant zich als eerste heeft gemeld.

Privacy
Dat gegevens slechts eenmaal mogen worden uitgevraagd betekend niet dat de gegevensuitwisseling onbeperkt kan plaatsvinden. Het is immers belangrijk dat de privacy van de klant in het oog gehouden wordt en dat voldaan wordt aan de privacy regels zoals deze in Nederland gelden. De Wet SUWI, het daarbij behorende Besluit SUWI[245] en het Besluit Inlichtingenbureau[246] vormen de lex specialis rondom de bescherming van de privacy en overstijgen daarmee de Wbp. Het CBP (voorheen: de Registratiekamer) heeft wel inspraak gehad in de inrichting van deze regels door commentaar te leveren op de voorlopige wetteksten. Eerder commentaar[247] op de inrichting van deze regels vanuit de registratiekamer zag vooral op de te ruime omschrijving van de doelen waarop gegevensverzameling en uitwisseling was gestoeld. Met andere woorden, er werd niet voldoende voldaan aan het doelbindingsbeginsel van de Wbp. Ook op het conceptvoorstel voor de WEU was behoorlijk wat commentaar[248]. Het CBP gaf hierbij aan dat de verantwoordelijkheidsverdeling in de SUWI-keten zeer helder moest worden belegd, dat noodzakelijkheid en doelbinding uitgangspunten dienen te zijn en blijven en dat kwaliteit dient te worden gewaarborgd, dit laatste werkt dan ook uit op het accepteren van gelijke niveaus van beveiliging van data. Bovendien staat transparantie voor de burger voorop en kan de burger actief zijn rechten uitoefenen rondom de informatie-uitwisseling (verzet, correctie, verwijdering enz.).

2.15 Dienstenrichtlijn
De Dienstenrichtlijn[249] regelt de vrije vestiging van dienstverrichters en het vrije verkeer van diensten binnen de EU.[250] De richtlijn verplicht de lidstaten om een zogenaamd ‘één-loket’ te realiseren. De lidstaten van de EU moeten vóór 28 december 2009 aan de eisen van de richtlijn hebben voldaan.[251]

De Dienstenrichtlijn verstaat onder ‘dienstverrichter’ iedere natuurlijke persoon die onderdaan is van een lidstaat of iedere rechtspersoon[252] die in een lidstaat is gevestigd en een dienst aanbiedt of verricht.[253] De richtlijn spreekt ook van de ‘afnemer’, hieronder wordt verstaan

[245] Besluit van 20 december 2001 tot vaststelling van een algemene maatregel van bestuur ter uitvoering van de Wet structuur uitvoeringsorganisatie werk en inkomen, en in verband daarmee van enige andere socialezekerheidswetten (Besluit SUWI), *Stb.* 2001, 68, gewijzigd bij *Stb.* 2003, 333, *Stb.* 2004, 327, *Stb.* 2005, 351, *Stb.* 2005, 724, *Stb.* 2008, 104.
[246] Besluit Inlichtingenbureau Gemeenten, 13 december 2001, *Stb.* 2001, 686 (Besluit van 13 december 2001, houdende nadere regels omtrent de coördinatie en dienstverlening door het Inlichtingenbureau ten behoeve van de gemeenten bij de gegevensverstrekking op grond van zowel de Wet SUWI als de Abw, de IOAW en de IOAZ, alsmede omtrent de financiering van het Inlichtingenbureau).
[247] Registratiekamer, ‘nader advies concept-besluit Inlichtingenbureau en SUWI’, z2001-0762, 1 augustus 2001, p. 5
[248] CBP, Adviesaanvraag Wet eenmalige gegevensuitvraag werk en inkomen, 28 augustus 2006 z2006-00896.
[249] *PbEG* 2006 L 376/36.
[250] Artikel 1 lid 1 Dienstenrichtlijn.
[251] Artikel 44 lid 1 Dienstenrichtlijn.
[252] In de zin van artikel 48 van het Verdrag tot oprichting van de Europese Gemeenschap.
[253] Artikel 4 lid 2 Dienstenrichtlijn.

iedere natuurlijke persoon die onderdaan is van een lidstaat,[254] of iedere rechtspersoon[255] die in een lidstaat is gevestigd en, al dan niet voor beroepsdoeleinden, van een dienst gebruik maakt of wil maken.[256]

Procedures en formaliteiten via het 'één-loket'
Eén van de doelstelling van de Dienstenrichtlijn is het vereenvoudigen van administratieve procedures. De Europese wetgever vindt het daarom passend om te verzekeren dat elke dienstverrichter via één aanspreekpunt alle procedures en formaliteiten kan afhandelen. Dit ene aanspreekpunt is het 'één-loket'.[257] De lidstaten dienen er op toe te zien dat een dienstverrichter via het één-loket de volgende procedures en formaliteiten kan afwikkelen:

a. alle procedures en formaliteiten die nodig zijn voor de toegang tot zijn dienstenactiviteiten, in het bijzonder alle voor de vergunning nodige verklaringen, kennisgevingen en aanvragen bij de bevoegde instanties, met inbegrip van aanvragen tot inschrijving in een register, op een rol, in een databank of bij een beroepsorde of beroepsvereniging;
b. alle vergunningaanvragen die nodig zijn voor de uitoefening van zijn dienstenactiviteiten.[258]

Informatie en bijstand aangeboden via het één-loket
De lidstaten zien erop toe dat de volgende informatie voor dienstverrichters en afnemers gemakkelijk via het één-loket toegankelijk is:

a. de eisen die voor de op hun grondgebied gevestigde dienstverrichters gelden, in het bijzonder de eisen inzake de procedures en formaliteiten die afgewikkeld moeten worden om toegang te krijgen tot dienstenactiviteiten en deze uit te oefenen;
b. de adresgegevens van de bevoegde instanties, waaronder die welke bevoegd zijn op het gebied van de uitoefening van dienstenactiviteiten, zodat rechtstreeks contact met hen kan worden opgenomen;
c. de middelen en voorwaarden om toegang te krijgen tot openbare registers en databanken met gegevens over dienstverrichters en diensten;
d. de rechtsmiddelen die algemeen voorhanden zijn bij geschillen tussen de bevoegde instanties en de dienstverrichter of afnemer, tussen een dienstverrichter en een afnemer of tussen dienstverrichters onderling;
e. de adresgegevens van de verenigingen of organisaties, anders dan de bevoegde instanties, waarvan dienstverrichters of afnemers praktische bijstand kunnen krijgen.[259]

De lidstaten zien erop toe dat dienstverrichters en afnemers op hun verzoek van de bevoegde instanties bijstand kunnen krijgen. Die bijstand moet bestaan uit informatie die wordt verstrekt over de wijze waarop de hierboven onder a), bedoelde eisen doorgaans worden uitgelegd en toegepast. Waar passend omvat deze bijstand een handleiding met eenvoudige, stapsgewijze informatie. De informatie moet worden verstrekt in gewone en begrijpelijke taal.[260] De verplichting voor de bevoegde instanties om dienstverrichters en afnemers bij te staan, impliceert niet dat deze instanties in individuele gevallen juridisch advies moeten verstrekken,

[254] Of die rechten heeft die hem door communautaire besluiten zijn verleend.
[255] In de zin van artikel 48 van het Verdrag tot oprichting van de Europese Gemeenschap.
[256] Artikel 4 lid 3 Dienstenrichtlijn.
[257] Overweging 48 Dienstenrichtlijn.
[258] Artikel 6 lid 1 Dienstenrichtlijn.
[259] Artikel 7 lid 1 Dienstenrichtlijn.
[260] Artikel 7 lid 2 Dienstenrichtlijn.

maar heeft alleen betrekking op algemene informatie over de manier waarop de eisen gewoonlijk worden geïnterpreteerd of toegepast.[261]

De hierboven bedoelde informatie en bijstand moeten duidelijk en ondubbelzinnig worden verstrekt, zij moeten gemakkelijk op afstand en elektronisch toegankelijk zijn en de informatie moet actueel wordt gehouden.[262] De wijze waarop informatie aan dienstverrichters en afnemers wordt verstrekt, dient door elke lidstaat te worden vastgesteld. In het bijzonder kan aan de verplichting van de lidstaten om erop toe te zien dat relevante informatie gemakkelijk toegankelijk is voor dienstverrichters en afnemers en zonder hindernissen beschikbaar is voor het publiek, worden voldaan door deze informatie toegankelijk te maken via een website.[263] Het één-loket en de bevoegde instanties moeten zo snel mogelijk op elk verzoek om de informatie of bijstand reageren. Indien een verzoek ongegrond is, moet de aanvrager daarvan onverwijld in kennis worden gesteld.[264]

De lidstaten en de Commissie dienen flankerende maatregelen vast te stellen teneinde het één-loket aan te moedigen de bedoelde informatie in andere talen van de Gemeenschap beschikbaar te maken. Dit laat de wetgeving van lidstaten inzake het gebruik van talen onverlet.[265]

Procedures via elektronische middelen
Alle procedures en formaliteiten betreffende de toegang tot en de uitoefening van een dienstenactiviteit moeten eenvoudig, op afstand en met elektronische middelen via het betrokken één-loket en met de relevante bevoegde instanties kunnen worden afgewikkeld.[266] Deze eis is niet van toepassing op de inspectie van de plaats waar de dienst wordt verricht of van de door de dienstverrichter gebruikte uitrusting, en ook niet op de fysieke controle van de geschiktheid of de persoonlijke integriteit van de dienstverrichter of van zijn verantwoordelijke personeelsleden.[267]

De Dienstenrichtlijn bevat een procedure aan de hand waarvan de Europese Commissie gedetailleerde uitvoeringsbepalingen vaststelt, om de interoperabiliteit van de informatiesystemen en het gebruik van elektronische procedures tussen lidstaten te vergemakkelijken.[268]

---

[261] Artikel 7 lid 6 Dienstenrichtlijn.
[262] Artikel 7 lid 3 Dienstenrichtlijn.
[263] Overweging 50 Dienstenrichtlijn.
[264] Artikel 7 lid 4 Dienstenrichtlijn.
[265] Artikel 7 lid 5 Dienstenrichtlijn.
[266] Artikel 8 lid 1 Dienstenrichtlijn.
[267] Artikel 8 lid 2 Dienstenrichtlijn.
[268] Met inachtneming van op communautair niveau opgestelde gemeenschappelijke normen; artikel 8 lid 3 juncto artikel 40 lid 2 Dienstenrichtlijn. Onder interoperabiliteit wordt in de dienstenrichtlijn de definitie van het Europees interoperabiliteitskader (European Interoperability Framework – EIF) (Versie 1.0) aangehouden: *"de mogelijkheden van systemen op het gebied van informatie- en communicatietechnologie (ICT) en van de bedrijfsprocessen die zij ondersteunen om gegevens uit te wisselen en het delen van informatie en kennis mogelijk te maken"* (p. 5), <zie http://ec.europa.eu/idabc/en/document/2319/5644>. De richtlijn zelf geeft deze definitie niet, het handboek voor de implementatie van de dienstenrichtlijn wel. Beschikbaar via WWW <http://ec.europa.eu/internal_market/services/services-dir/index_en.htm>, zie p. 24 van het handboek, noot 56.

Vormgeving van het één-loket
Het aantal 'één-loketten' per Europese lidstaat kan variëren naargelang de regionale of lokale bevoegdheden of de betrokken activiteiten. De invoering van het één-loket mag geen afbreuk doen aan de verdeling van de taken en bevoegdheden tussen de verschillende instanties binnen de nationale systemen.[269] Als verschillende instanties op regionaal of lokaal niveau bevoegd zijn, kan één van hen als één-loket en coördinator fungeren. Het één-loket hoeft niet door bestuurlijke autoriteiten te worden opgericht, maar kan ook door een door de lidstaat met die taak belaste kamer van koophandel, beroepsorganisatie of particuliere instelling worden opgericht. Een belangrijke rol van het één-loket is het verlenen van bijstand aan dienstverrichters, hetzij als bevoegde instantie die zelf de nodige documenten kan afgeven voor de toegang tot een dienstenactiviteit, hetzij als tussenschakel tussen de dienstverrichter en de rechtstreeks bevoegde instanties.[270]

De vergoeding die het één-loket in rekening mag brengen, moet in verhouding staan tot de kosten van de procedures en formaliteiten waarmee het zich bezighoudt. Dit belet lidstaten niet het één-loket te belasten met de inning van andere administratieve vergoedingen, zoals die van toezichthoudende organen.[271]

2.16 INSPIRE-richtlijn

Het doel van de INSPIRE-richtlijn[272] is het vaststellen van algemene regels voor de oprichting van een infrastructuur voor ruimtelijke informatie in de Europese Gemeenschap. Dit dient ter ondersteuning van het communautaire milieubeleid en beleidsmaatregelen of activiteiten die van invloed kunnen zijn op het milieu.[273] De lidstaten dienen uiterlijk op 15 mei 2009 aan de richtlijn te voldoen.[274] De richtlijn laat het bestaan van intellectuele eigendomsrechten van overheidsinstanties onverlet.[275]

Onder 'infrastructuur voor ruimtelijke informatie' verstaat de richtlijn: metagegevens, verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens, netwerkdiensten en -technologieën, overeenkomsten betreffende de uitwisseling van, de toegang tot en het gebruik van de gegevens, en overeenkomstig de richtlijn ingestelde, beheerde of beschikbaar gemaakte mechanismen, processen en procedures voor coördinatie en monitoring.[276] 'Ruimtelijke informatie' wordt omschreven als gegevens die direct of indirect verwijzen naar een specifieke locatie of een specifiek geografisch gebied.[277]

De richtlijn heeft betrekking op verzamelingen ruimtelijke gegevens die aan de volgende voorwaarden voldoen:

a. ze hebben betrekking op een gebied waar een lidstaat rechten ten aanzien van de rechtsbevoegdheid heeft en/of uitoefent;
b. ze zijn beschikbaar in elektronisch formaat;
c. ze worden bewaard door of namens:

[269] Artikel 6 lid 2 Dienstenrichtlijn.
[270] Overweging 48 Dienstenrichtlijn.
[271] Overweging 49 Dienstenrichtlijn.
[272] Richtlijn 2007/2/EG tot oprichting van een infrastructuur voor ruimtelijke informatie in de Gemeenschap (Inspire), *PbEG* 2007 L 108/1.
[273] Artikel 1 richtlijn.
[274] Artikel 24 lid 1 richtlijn.
[275] Artikel 2 richtlijn.
[276] Artikel 3 lid 1 richtlijn.
[277] Artikel 3 lid 2 richtlijn.

   i. een overheidsinstantie, in de zin dat ze zijn geproduceerd of ontvangen dan wel worden beheerd of bijgewerkt door die instantie en binnen haar publieke taak vallen;
   ii. een derde partij waaraan het netwerk ter beschikking is gesteld overeenkomstig de richtlijn;
d. ze hebben betrekking op een of meer van de in de bijlagen van de richtlijn vermelde thematische categorieën.[278]

De bijlagen van de richtlijn bevatten de volgende thematische categorieën.

Thematische categorieën opgenomen in de bijlagen van de Inspire-richtlijn		
Bijlage I	**Bijlage II**	**Bijlage III**
1. Systemen voor verwijzing door middel van coördinaten 2. Geografisch rastersysteem 3. Geografische namen 4. Administratieve eenheden 5. Adressen 6. Kadastrale percelen 7. Vervoersnetwerken 8. Hydrografie 9. Beschermde gebieden	1. Hoogte 2. Bodemgebruik 3. Orthobeeldvorming 4. Geologie	1. Statistische eenheden 2. Gebouwen 3. Bodem 4. Landgebruik 5. Menselijke gezondheid en veiligheid 6. Nutsdiensten en overheidsdiensten 7. Milieubewakings-voorzieningen 8. Faciliteiten voor productie en industrie 9. Faciliteiten voor landbouw en aquacultuur 10. Spreiding van de bevolking - demografie 11. Gebiedsbeheer, gebieden waar beperkingen gelden, gereguleerde gebieden en rapportage-eenheden 12. Gebieden met natuurrisico's 13. Atmosferische omstandigheden 14. Meteorologische geografische kenmerken 15. Oceanografische geografische kenmerken 16. Zeegebieden 17. Biogeografische gebieden 18. Habitats en biotopen 19. Spreiding van soorten 20. Energiebronnen 21. Minerale bronnen

De richtlijn verplicht de lidstaten onder meer tot:
- het opstellen en bijwerken van metagegevens; en tot
- het oprichten en exploiteren van netwerkdiensten

Onder metagegevens verstaat de richtlijn ‘informatie waarin verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens worden beschreven en die het mogelijk maakt deze gegevens en diensten te zoeken, te inventariseren en te gebruiken.’[279]
De metagegevens dienen onder meer betrekking te hebben op:
a. de overeenstemming van verzamelingen ruimtelijke gegevens met de nader te bepalen uitvoeringsbepalingen;

[278] Artikel 4 lid 1 richtlijn.
[279] Artikel 3 lid 6 richtlijn.

b. de voorwaarden voor de toegang tot en het gebruik van verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens en, indien van toepassing, de daarmee samenhangende vergoedingen;
c. de kwaliteit en geldigheid van verzamelingen ruimtelijke gegevens;
d. de overheidsinstanties die verantwoordelijk zijn voor de oprichting, het beheer, het onderhoud en de verspreiding van verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens;
e. beperkingen voor de publieke toegang en de redenen voor deze beperkingen. De richtlijn bevat een regeling ten aanzien van de beperkingen die zijn toegestaan.[280]

De richtlijn verplicht de lidstaten tot de oprichting en exploitatie van een netwerk van de volgende diensten met betrekking tot verzamelingen ruimtelijke gegevens en de diensten met betrekking tot ruimtelijke gegevens waarvoor op grond van de richtlijn metagegevens zijn opgesteld:
a. zoekdiensten;
b. raadpleegdiensten;
c. downloaddiensten;
d. verwerkingsdiensten;
e. diensten die het mogelijk maken diensten met betrekking tot ruimtelijke gegevens op te vragen.[281]

Deze diensten moeten rekening houden met relevante gebruikerseisen en gemakkelijk bruikbaar, beschikbaar voor het publiek en via het internet of via andere telecommunicatiemiddelen toegankelijk zijn.[282]

De zoekdiensten moeten tenminste de volgende zoekcriteria omvatten:
a. trefwoorden;
b. classificering van ruimtelijke gegevens en diensten;
c. de kwaliteit en geldigheid van verzamelingen ruimtelijke gegevens;
d. mate van overeenstemming met de nader vast te stellen uitvoeringsbepalingen;
e. geografische locatie;
f. voorwaarden voor de toegang tot en het gebruik van verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens;
g. de overheidsinstanties die verantwoordelijk zijn voor de oprichting, het beheer, het onderhoud en de verspreiding van verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens.[283]

De richtlijn bevat enkele bepalingen die randvoorwaarden stellen aan het beschikbaar stellen van diensten en gegevens. De lidstaten dienen er voor te zorgen dat het publiek in beginsel kosteloos gebruik kan maken van de zoekdiensten en de raadpleegdiensten.[284] De lidstaten mogen het een openbare autoriteit die raadpleegdiensten aanbiedt, toestaan vergoedingen in rekening te brengen indien de vergoedingen ervoor zorgen dat de verzamelingen ruimtelijke gegevens en de overeenkomstige diensten met betrekking tot gegevens in stand worden gehouden, met name ingeval van zeer grote hoeveelheden *real time* gegevens.[285] Voorts

[280] Artikel 5 lid 1 richtlijn.
[281] Artikel 11 lid 1 richtlijn.
[282] Artikel 11 lid 1 richtlijn.
[283] Artikel 11 lid 2 richtlijn.
[284] Artikel 14 lid 1 richtlijn.
[285] Artikel 14 lid 2 richtlijn.

mogen de gegevens die via de raadpleegdiensten beschikbaar worden gesteld, worden geleverd in een vorm die het hergebruik voor commerciële doeleinden verhindert.[286]

Ten aanzien van de uitwisseling van ruimtelijke informatie stelt de INSPIRE-richtlijn dat overheden van andere overheidsinstanties een vergunning en/of een vergoeding kunnen verlangen. Ingeval een vergoeding wordt gevraagd, dient deze beperkt te blijven tot het minimum dat nodig is om de noodzakelijke kwaliteit en beschikbaarheid van verzamelingen ruimtelijke informatie en de diensten te garanderen. Dit minimum mag worden vermeerder met een redelijk rendement op de investering, in voorkomend geval met inachtneming van de vereisten inzake zelffinanciering van de overheidsdiensten die verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens verstrekken. Er mag in geen geval betaling worden verlangd voor ruimtelijke informatie die overheidsinstanties nodig hebben ter vervulling van hun verplichtingen inzake verslaglegging op grond van EU-wetgeving inzake het milieu.[287]

De richtlijn regelt verder de instelling van een *geoportaal*. De Europese Commissie zal namelijk op communautair niveau een Inspire-geoportaal opzetten en exploiteren.[288] Onder een 'Inspire-geoportaal' wordt verstaan een internetsite, of een equivalent daarvan, die toegang verschaft tot de hierboven genoemd diensten.[289] De lidstaten dienen via het Inspire-geoportaal toegang te verlenen tot de nationale diensten. De lidstaten mogen ook via hun eigen toegangspunten toegang verlenen tot deze diensten.[290]

Hierboven is al een paar keer ter sprake gekomen dat naar aanleiding van de richtlijn uitvoeringsbepalingen zullen worden vastgesteld. In mei 2008 is inmiddels de eerste invoeringsregeling (betreffende meta-informatie) aangenomen. De uitvoeringbepalingen beogen de niet-essentiële onderdelen van de richtlijn 'te wijzigen door haar aan te vullen', en betreffen de technische voorschriften voor de interoperabiliteit en, waar mogelijk, de harmonisatie van verzamelingen van ruimtelijke gegevens en diensten.[291] Onder interoperabiliteit verstaat de richtlijn de mogelijkheid dat, zonder terugkerende handmatige verrichtingen, verzamelingen ruimtelijke gegevens zodanig worden gecombineerd en dat diensten zodanig op elkaar inwerken dat het resultaat coherent is en de meerwaarde van de verzamelingen gegevens en de diensten wordt verhoogd.[292]

[286] Artikel 14 lid 3 richtlijn.
[287] Artikel 17 lid 3 richtlijn.
[288] Artikel 15 lid 1 richtlijn.
[289] Artikel 3 lid 8 richtlijn.
[290] Artikel 15 lid 2 richtlijn.
[291] Artikel 7 lid 1 richtlijn.
[292] Artikel 3 lid 7 richtlijn.

3 Onderzochte cases

3.1 Elektronisch bouwloket/omgevingsloket

Het Digitaal Bouwloket maakt het mogelijk bouwaanvragen met bijbehorende tekeningen en berekeningen digitaal in te dienen. Alle documenten die in de loop van de procedure ontstaan, worden digitaal aangemaakt en opgeslagen. Zo ontstaat een volledig digitaal dossier, dat onafhankelijk van tijd en plaats door verschillende partijen ingezien kan worden. Ook is een automatische bewaking van de wettelijke termijnen ingebouwd. Gekoppeld hieraan is de omgevingsvergunning. Door integratie van vergunningen kan men straks, na invoering van de Landelijke Voorziening Omgevingsloket, volstaan met één aanvraag bij één loket dat na het doorlopen van één procedure leidt tot één besluit (het al dan niet verlenen van een vergunning) en met één beroepsgang. Aan de basis van de omgevingsvergunning ligt het Wetsvoorstel algemene bepalingen omgevingsrecht (Wabo), zie hiervoor paragraaf 2.12.

Elektronische gegevensuitwisseling
Voor aanvragen en meldingen die via het e-Omgevingsloket zijn ingediend zijn er twee verzendmethoden waarmee de informatie elektronisch kan worden overgedragen aan het bevoegd gezag (Gemeente of provincie, afhankelijk van het soort aanvraag). Zowel burgers als bedrijven mogen een aanvraag indienen bij het Bouwloket. De twee manieren zijn:

1. Via e-mail
Direct na het indienen van de aanvraag stuurt het e-Omgevingsloket een e-mail naar het bevoegd gezag met de mededeling dat een aanvraag is ingediend. Als bijlage bij deze e-mail zitten een PDF-document en een XML-bericht met de aanvraaggegevens. Grote bijlagen als tekeningen die bij de aanvraag zijn gevoegd worden vanwege de omvang niet meegezonden. Wel zijn links naar deze bijlagen opgenomen.

2. Via webservice
Direct na het indienen van de aanvraag krijgt de webservice van het bevoegd gezag een service-aanroep van de webservice van het e-Omgevingsloket. Als de webservice van het bevoegd gezag deze aanroep beantwoordt, wordt een PDF-document en een XML-bericht met de aanvraaggegevens verzonden. Grote bijlagen als tekeningen die bij de aanvraag zijn gevoegd worden vanwege de omvang niet meegezonden. In de e-mail zijn wel links naar deze bijlagen opgenomen.[293]

Gemeenten hanteren ook nog een mogelijkheid om documenten en aanvragen niet-digitaal in te zien. Er zijn dan echter wel kosten verbonden aan het verschaffen van kopieën. Op gemeentelijk niveau worden door middel van Collegebesluiten afspraken gemaakt omtrent dienstverleningswensen. In die afspraken wordt zoveel mogelijk gebruik gemaakt van standaarden. Deze standaarden zijn openbaar en vastgelegd door het Rijk in het kader van de Wabo.

De gegevens die hoe dan ook worden uitgewisseld zijn de digitale vergunningaanvragen zelf en, indien het bevoegd gezag deze informatie in de Landelijke Voorziening Omgevingsloket (LVO) bijhoudt, de statusinformatie over de vergunningaanvraag. Dit betreft de uitwisseling tussen overheidsdiensten onderling.
Frequente aanvragers kunnen een code invoeren om sneller tot het juiste formulier te komen. Het gaat dan bijvoorbeeld om projectontwikkelaars die regelmatig een aanvraag indienen. De

[293] Infoblad Landelijke Voorziening Omgevingsloket, Informatie voor ICT-professionals, februari 2008.

code is samengesteld op basis van de keuzes die een invuller maakt in de vragenboom. De code heeft dus betrekking op het type formulier (reguliere bouwvergunning, lichte bouwvergunning, etc.) en niet op de aanvrager. Door het gebruik van de code wordt de vragenboom omzeild. Waar mogelijk worden bekende gegevens omtrent de aanvrager op het digitale én op het papieren formulier al vooraf ingevuld op basis van DigiD.

De overheidsorganisaties kunnen naast statusinformatie ook elektronisch NAW-gegevens uitwisselen. Zo kan bekeken worden of er bij verschillende overheidsinstanties aanvragen lopen voor dezelfde percelen of van dezelfde personen.

Landelijke Voorziening Omgevingsloket
VROM ontwikkelt een Landelijke Voorziening Omgevingsloket (LVO) waarmee zowel de omgevingsvergunning als de watervergunning aangevraagd kunnen worden. Deze digitale voorziening bestaat uit een aanvraaggedeelte en een dossiergedeelte.

De aanvraagmodule van de LVO bestaat uit een vragenboom en een aanvraagformulier op maat. De vragenboom stelt automatisch vast of iemand een vergunning nodig heeft en, zo ja, voor welke activiteiten (commerciële activiteiten, parkeerontheffingen, etc.). Met het digitale of papieren aanvraagformulier kan de burger of ondernemer de aanvraag of melding indienen. De definitieve aanvraagmodule komt beschikbaar op 1 januari 2009 en wordt voor alle gemeenten verplicht gesteld. Aanbieding vindt plaats via de gemeentelijke website.

Op de dossiermodule kunnen overheden de vergunningaanvraag of –melding opslaan, raadplegen en invullen. Het bevoegd gezag, adviseurs en aanvragers hebben altijd toegang tot de actuele documenten. Zonodig kan de aanvrager later nog documenten toevoegen of vervangen. De definitieve dossiermodule komt ook beschikbaar op 1 januari 2009. De aansluiting op deze module is facultatief.[294]
In Nijmegen betreft de uitwisseling gegevens betreffende bouwaanvragen, beschikkingen en bouwtekeningen. De uitwisseling geschiedt hier zowel met burgers en bedrijven als met het Ministerie van BZK (ICTU) in het kader van Vergunningen op Internet. De informatie is op Internet voor iedereen beschikbaar. De wettelijke grondslag daarvoor ligt in de WOB en de Woningwet. In Rotterdam is het momenteel nog beperkt. Het gaat daar vooralsnog uitsluitend om beoordeling van aspecten in een bouwplan (breedte van een gang in overleg met de brandweer e.d.) en de communicatie van de uiteindelijke beschikking met de aanvrager. Met de invoering van de Omgevingsvergunning zullen ook statusgegevens uitgewisseld worden. Uitwisseling met private partijen vindt ook plaats, bijvoorbeeld met architectenbureaus. De uitwisseling is veelal op vrijwillige basis. De uitwisseling vindt plaats omdat de gemeente is aangewezen om de aanvraag van een bouwvergunning te beoordelen.

Bij de gemeente Nijmegen zijn de gegevens in principe met een ieder uitwisselbaar, waarmee vergaring, gebruik en verstrekking dus onbeperkt zijn. De gegevens worden niet vernietigd en dus bewaard. Gedurende het vergunningsproces kunnen wijzigingen aangebracht worden, maar daarna niet meer.
Bij de gemeente Rotterdam wordt aangegeven dat het de vraag is of na invoering van de omgevingsvergunning bewaring nog bij hun organisatie blijft liggen.

In Rotterdam is nog geen toegang mogelijk tot gearchiveerde eigen persoonsgegevens. Huidige gegevensdeling vindt nog grotendeels op analoge wijze plaats (mondeling, schriftelijk,

[294] www <http://omgevingsvergunning.vrom.nl/index.cfm/t/Landelijke_Voorziening__LVO_/vid/518D4ED0-1438-5103-71D8A50ECDFBAFEB>.

eventueel e-mail). Met de invoering van de omgevingsvergunning zullen daar ook xml-berichten bij komen, met name in het traject van de omgevingsvergunning zelf (tussen landelijke voorziening, provincie en gemeentelijke diensten).
In Nijmegen worden de gegevens digitaal via Internet uitgewisseld. Voor deze gemeente gaat het om ongeveer 45.000 adressen met meerdere vergunningen per adres.

Bij statusinformatie omtrent de aanvraag gaat het om optionele uitwisseling, daar deze uitwisseling afhankelijk is van het bijhouden in het LVO door het bevoegd gezag.

De aanvraagmodule is een verplicht onderdeel van LVO, maar er is wel ruimte voor differentiatie in het formulier door bijvoorbeeld vragen toe te voegen of weg te laten indien een gemeente een bepaalde dienst niet aanbiedt. Het formulier is dus niet in het gehele land hetzelfde.

Zoals gezegd gaat het in Rotterdam nog hoofdzakelijk om analoge uitwisseling. In Nijmegen worden data en processtappen vastgelegd in een workflowsysteem voor bouwvergunningen. De bijbehorende documenten worden ingescand, aan adressen en vergunningnummers gekoppeld, en via internet getoond. Het digitaal bouwarchief en procedures online worden in Nijmegen ook gebruikt door de brandweer (digitale aanvalsplannen) en de afdeling WOZ (voor taxaties).

In Rotterdam worden de gegevens op papier bewaard zonder echte risicoclassificatie. De gegevens zijn openbaar, maar bij een verzoek om inzage wordt persoonsidentificatie gevraagd. In Nijmegen worden alle gegevens die op de bouwaanvraag staan vermeld, met uitzondering van het BSN, verwerkt en bewaard. Op internet is deze informatie vrij toegankelijk. Er zijn echter wel documenten die alleen binnen de gemeente door bepaalde ambtenaren mogen worden ingezien. Informatie over risicovolle panden, zoals banken en gevangenissen, wordt niet openbaar gemaakt en niet op internet geplaatst. In principe hebben alle burgers toegang tot de aanvragen, beschikkingen en bouwtekeningen die op internet zijn geplaatst. Interne adviezen en correspondentie zijn niet openbaar. Bij beide gemeenten wordt geen gebruik gemaakt van geanonimiseerde gegevens.

Binnen de LVO wordt DigiD gebruikt (één inlogcode voor alle elektronische overheidsinstanties) en LDAP (een voorziening om gebruikersnamen en wachtwoorden te beheren en toegang tot een applicatie te verlenen). Op deze manier zijn sommige gegevens al vooraf ingevuld. Gebruikers van het digitale formulier kunnen het formulier tussentijds opslaan. Dat is alleen mogelijk als zij geauthenticeerd zijn. Een belangrijk punt in het gebruik van LDAP is dat het ook gebruikt wordt voor het autoriseren van de betrokken overheden. Daarbij is elk bevoegd gezag verantwoordelijk voor het beheer van de eigen gebruikers. Allereerst zijn er centraal beheerders, op centraal niveau worden vervolgens decentraal beheerders van de overheidsinstellingen (gemeenten, provincie, het Rijk) toegevoegd. Deze maken weer overige beheerders, loketbeambten, vergunningverleners, inspecteurs en adviseurs aan.[295]

Omdat de LVO nog niet is ingevoerd is het nog lastig om wijzen van authenticatie te beschrijven. Wel blijkt al uit de respons van verschillende overheidsinstanties dat niet overal gebruik wordt gemaakt van geanonimiseerde gegevens. Welke gegevens worden opgevraagd en hoe lang deze worden bewaard is ook onduidelijk. Waar mogelijk wordt met DigiD gewerkt en worden op basis daarvan persoonsgegevens ingevuld in de formulieren.

[295] Infoblad Landelijke Voorziening Omgevingsloket, Informatie voor ICT-professionals, februari 2008.

Specifieke eisen en randvoorwaarden met betrekking tot interoperabiliteit.
Er worden geen eisen en randvoorwaarden gesteld ten aanzien van interoperabiliteit. Een respondent geeft aan zoveel mogelijk aan te sturen op het uitwisselen via bestaande standaarden, bij voorkeur gebaseerd op een XML berichtenverkeer. Daarmee doelt men met name op draagvlak vooraf bij alle betrokkenen als randvoorwaarde. “Voldoende draagvlak bij de verschillende partners staat op nummer één. Hierbij dienen de belangrijkste partners betrokken te worden in het op- en vaststellen van de standaard, het versiebeheer en de procedures. Het eenzijdig opstellen van een standaard door de rijksoverheid, zoals bij de LV BAG[296], leidt tot vele bijstellingen achteraf. Het implementeren hiervan heeft geleid tot zeer hoge kosten, die doorberekend worden in de licentiekosten van de software. Nog voordat de standaard echt in productie is genomen, lijkt er alweer een nieuwe, betere, standaard te komen. Al wordt de oude standaard nog wel een bepaalde tijd gegarandeerd, het leidt ertoe dat sommige marktpartijen zo laat mogelijk een standaard gaan implementeren.
De standaard StUF WOZ,[297] onder leiding van de Waarderingskamer verloopt geheel anders. De standaard is opgesteld in nauwe samenwerking met expertise van de softwareleveranciers. Voor het implementeren van deze standaard de komende jaren wordt door alle betrokken partijen een convenant ondertekend.
Een wettelijke regeling geeft meestal voldoende druk bij overheden om standaarden ook daadwerkelijk af te nemen en te implementeren. Het voorbeeld van StUF WOZ geeft aan dat een goede samenwerking en betrokkenheid vooraf belangrijker is.”

Ook VROM refereert aan een standaard uitwisselingsformaat als voorbeeld: ‘LVO draagt bij aan interoperabiliteit door een hoge mate van standaardisatie: StUF 3.0 en aansluiting op OSB (overheidsservicebus).’ Aangezien LVO gegevens moet uitwisselen met 500 overheidsorganisaties is standaardisatie volgens VROM een essentiële randvoorwaarde.

Opgemerkt dient te worden dat StUF een open standaard is. De StUF standaard beschrijft de kaders en de syntax waarbinnen XML berichten uitgewisseld kunnen worden. Een sectormodel beschrijft de berichten en de gegevens die hiermee uitgewisseld worden. Bij de open standaarden kan een onderscheid worden gemaakt in:

1. Open standaarden die binnengemeentelijk worden gebruikt, zoals ‘Binnengemeentelijke’ (BG), ‘Zaken’, ‘E-formulieren’. Deze standaarden zijn in beheer bij EGEM.
2. Open standaarden die worden gebruikt tussen gemeenten en landelijke voorzieningen, zoals ‘Basisregistratie Adressen en Gebouwen’ (BAG), Wet kenbaarheid publiekrechtelijke beperkingen’ (Wkpb), ‘Modernisering Gemeentelijke Basis Administratie’ (mGBA), ‘Waardering Onroerende Zaken’ (WOZ). Deze standaarden zijn in beheer bij de betreffende sector, zoals VROM, BZK, Waarderingskamer.

Een indirect bij het bouwloket betrokken respondent, stelt dat het vastleggen van standaarden uiteindelijk resulteert in meer snelheid in realisatie bij lokale overheden. Op dit moment worden afspraken omtrent interoperabiliteit gemaakt tussen benoemde partijen. Dit staat echter haaks op de gewenste marktwerking in het actieplan ‘Open in verbinding’. Een wettelijk kader voor interoperabiliteit zal de marktwerking dan ook versterken.

[296] Landelijke Voorziening Basisregistraties voor Adressen en Gebouwen.
[297] In de Regeling Stuf-WOZ is het uitwisselingsformaat geformuleerd bedoeld in artikel 9 van het Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet waardering onroerende zaken.

Gemeenten uiten sterk de wens om alle randvoorwaarden wettelijk vast te leggen. Omdat het om grote aantallen gegevens gaat die tussen een veelheid aan instanties worden uitgewisseld, is het wenselijk om op wettelijke regelgeving terug te kunnen vallen. De afspraken lopen over veel verschillende partijen en veel verschillende bestuurslagen. Elke relatie via contractuele verplichtingen regelen is veel werk met een grote kans op blijvende onduidelijkheid doordat zaken op de ene plek net anders worden beschreven dan op de andere plek.

Conclusie
1. Een belangrijk aandachtspunt is dat in een aantal regelingen, waaronder het voor deze case relevante voorontwerp Ministeriële regeling omgevingsrecht (MOR), verwezen wordt naar gesloten standaarden. De MOR somt een aantal formats op. Vergunningaanvragen moeten in een van deze formats ingediend worden. De relevante rechtsregels gaan op het moment dus niet uit van open standaarden.

De gemeente Tilburg wijkt overigens af van het MOR, de volgende bestandsformaten zijn toegestaan, (waarbij overleg gewenst is voordat een aanvraag in aan afwijkende format wordt ingediend):

- DXF-bestanden (Drawing eXchange Format) zijn bestanden die zijn geschreven volgens AutoCad specificaties.
- TSA (Tech Soft America) is een open platform voor het uitwisselen van data, met name gevisualiseerde ontwerpgegevens.
- CCD-bestanden zijn database bestanden met een TXT extensie in MS-DOS. Het betreft door komma begrensde database bestanden, ASCII, met CR/LF (MS-DOS).
- Het is toegestaan om de gegevens en bescheiden in andere formats aan te leveren. Wij raden u dan wel aan eerst met de gemeente te overleggen.[298]

2. Daarnaast is het maken van een kopie van een bouwtekening mogelijk op grond van de WOB, zonder dat er sprake is van een auteursrechtinbreuk. De kopie moet dan echter wel voor eigen/privégebruik zijn. In het geval dat de bouwtekeningen in een digitale aanvraag op het web gepubliceerd worden is er echter geen sprake meer van privégebruik. Het gaat dan om een kopie en openbaarmaking, zonder onderscheid naar wie openbaar wordt gemaakt. Een eventuele directe auteursrechtinbreuk kan afhangen van het gebruik dat gemaakt wordt van een tekening (zoals namaken van het bouwwerk), maar er is hier toch zeker enige verantwoordelijkheid voor de overheidsinstantie die de tekening op het web plaatst. Wanneer het digitale bouwloket wordt toegepast is dus ook een herziening van de toepasbaarheid van de Auteurswet vereist.

3. De verschillende Standaard Uitwisselingsformaten en sectormodellen ontwikkelen zich allemaal in hun eigen tempo. Voor de betrokken organisaties is het daardoor een uitdaging om alle gegevens te koppelen en interoperabiliteit te waarborgen.

4. Het Bouwloket vraagt om gespecialiseerde kennis. Mensen die ingezet worden voor het Bouwloket kunnen niet efficiënt ingezet worden voor een andere loketfunctie. De betreffende mensen werken vanuit en met gebiedsgebonden kennis, terwijl achter het loket een algemene blik wordt gevraagd.

5. Er is een discussie met het College Bescherming Persoonsgegevens over de inzage via Internet. Het blijkt problematisch om aanvragen en beschikkingen via Internet ter inzage te leggen, vanwege een gebrek aan afstemming tussen de WOB en de WBP.

[298] WWW <http://loket.tilburg.nl/SRVS/Data/Tilburg/Templatesets/Tilburg/documents/\vind/aanvraag_bouwvergunning.pdf>.

Overheidsinstanties worden dus gedwongen om een eigen afweging te maken, waarbij zij een wettelijke plicht laten prevaleren boven een andere wettelijke plicht.

VROM geeft als onzekerheid aan dat er vertraging voorkomt in de beschikbaarheid van verschillende e-overheid voorzieningen. De ontwikkeling van voorzieningen dient dus gewaarborgd te zijn en op schema gehouden te worden.

3.2 Digitaal klantdossier

Het Digitaal KlantDossier (DKD) is een gemeenschappelijk dossier waarin informatie gedeeld wordt door CWI, UWV en Gemeenten én klant, van en over de klant op het gebied van werk en inkomen. Het DKD is gepositioneerd in de keten werk en inkomen en bedoeld voor werkzoekenden en uitkeringsgerechtigden op grond van de Werkloosheidswet (WW) of Wet Werk en Bijstand (WWB). Het DKD biedt de burger het wettelijke recht op eenmalige gegevensaanlevering op grond van de WEU (per 1 januari 2008) en verzorgt vraaggerichte en ketenbrede dienstverlening via het internet (burgers) en SUWInet (medewerkers van de organisaties). [299] Deze eenmalige gegevensaanlevering is bedoeld om de administratieve lasten voor de burger te beperken en vind plaats tussen gemeenten (Gemeentelijke Sociale Dienst, GSD), CWI en UWV. De betrokken organisaties mogen de klant dus niet meer twee keer om dezelfde gegevens vragen. Hergebruik van gegevens (via vooringevulde informatie in online aanvraagformulieren[300]) staat voorop. Uiteindelijk moet het DKD een klantvolgsysteem worden, waarbij alle partijen de klant in het kader van werk en inkomen kunnen volgen (begeleiden).

Projectstatus

Sinds 3 januari 2008 is het DKD landelijk operationeel. Dit betekent dat gegevens worden geleverd door de ketenpartners (CWI, UWV, LRD, RDW en Gemeenten), dat medewerkers van CWI, UWV en gemeenten DKD gebruiken (inkijken, hergebruiken) en dat klanten DKD online kunnen gebruiken (inclusief vooringevulde informatie in online aanvraagformulieren E-WWb, E-Werk en E-WW.)[301]

Juridische setting

De juridische setting die wordt gevormd door eventuele contractuele dan wel andere afspraken die van toepassing zijn. Met name ook de vraag of er interne afspraken zijn ten aanzien van de interpretatie van wetgeving en de omgang met situaties waarin afwegingen gemaakt moeten worden tussen verschillende belangen die in wetgeving zijn verdisconteerd.

De Wet eenmalige gegevensuitvraag werk en inkomen (WEU)[302], van kracht sinds 1 januari 208 geeft het DKD een wettelijke basis en wijzigt de het wettelijk kader rondom DKD. De wet is een uitvloeisel van de wet Walvis[303].
Volgens het CBP dienen noodzakelijkheid en doelbinding (artikel 7 WBP) bij het verwerken van persoonsgegevens voorop te staan in de SUWI-keten, en zijn beveiliging en transparantie

[299] Rob Driehuis, Jaap Klapwijk, Ben Schepers, Team Implementatie DKD gemeenten, Versie 0.9, 5 december 2006
[300] E-WWB en E-WW
[301] Nieuwsbericht: Landelijke openstelling DKD een feit, 24 januari 2008, WWW <http://dkd.nl/home/nieuwsarchief/nieuwsitems/archive/2008/01/?tx_ttnews%5Btt_news%5D=13&cHash=b8c9509486>
[302] Wet van 12 december 2007, *Stb.* 2007, 555, houdende wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen, de Wet werk en bijstand, de Werkloosheidswet en enige andere wetten in verband met eenmalige gegevensuitvraag aan burgers (*Wet eenmalige gegevensuitvraag werk en inkomen*). Inwerkingtreding: 1 januari 2008 (*Stb.* 2007, 556).
[303] Wet Administratieve Lastenverlichting en Vereenvoudiging Socialeverzekeringswetten, Stb. 2004, 311

randvoorwaarden voor de inrichting van het DKD. Bovendien mag de wetgeving niet in strijd zijn artikel 9 WBP, verenigbaar gebruik, waarbij er een relatie bestaat tussen doel van verwerking en doel van verkrijging.[304]

Het wettelijk kader dat gewijzigd wordt op grond van de WEU bestaat uit de volgende wetten:

- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI)
- Wet werk en bijstand (WWB) (voorheen Algemene Bijstandswet, AWB)
- Werkloosheidswet (WW)
- Toeslagenwet
- Ziektewet
- Wet werk en inkomen naar arbeidsvermogen
- Wet op de arbeidsongeschiktheidsverzekering (WAO)
- Wet arbeidsongeschiktheidsvoorziening jonggehandicapten (WAJONG)
- Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers
- Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen
- Wet werk en inkomen kunstenaars
- Algemene Kinderbijslagwet
- Algemene Ouderdomswet (AOW)
- Algemene nabestaandenwet
- Wet verzelfstandiging Informatiseringsbank
- Invoeringswet Wet financiering sociale verzekeringen

Het wettelijk kader dat bepalend is voor DKD is de Wet SUWI. Deze wet bepaalt welke ketenpartners samenwerken in dit programma en de WEU. “Uit een oogpunt van optimale dienstverlening aan de burger wordt via dit wetsvoorstel geregeld dat elk gegeven dat de ketenpartners werk en inkomen nodig hebben voor hun werk slechts eenmaal mag worden uitgevraagd. Bij het concept van bij wet in te stellen "basisregistraties" hoort dat afnemers belast met een publieke taak verplicht zijn van de gegevens uit die basisregistraties gebruik te maken. In een basisregistratie worden gegevens die logisch bij elkaar horen en die voor de hele overheid van belang zijn (bijvoorbeeld over bedrijven, personen, etc.), beheerd.”[305] Sectoraal zijn op dit moment de WW en WWB het belangrijkste bij de uitvoering van taken binnen het DKD, omdat de e-functionaliteiten e-WW en e-WWB al geïmplementeerd zijn.

Naast de Wet SUWI is ook het Besluit Inlichtingenbureau[306] van toepassing. Dit besluit stelt de regels voor de coördinatie en dienstverlening van het inlichtingenbureau aan gemeenten. Hierbij wordt het Inlichtingenbureau opdracht gegeven gegevens te verschaffen aan gemeenten op grond van de Wet SUWI en wordt de gegevensverwerking door het Inlichtingenbureau geregeld. Bovendien zorgen de Wet SUWI, het Besluit SUWI en het Besluit Inlichtingenbureau als lex specialis voor de regels rondom bescherming van de privacy en overstijgen daarmee de WBP. Het commentaar van de Registratiekamer op het Besluit Inlichtingenbureau (huidig artikel 2 lid 2) was dat “de huidige ruime omschrijving van het

[304] College Bescherming Persoonsgegevens, ‘Adviesaanvraag Wet eenmalig gegevensuitvraag werk en inkomen’, z2006-00896, 19 oktober 2006.
[305] *Kamerstukken II* 2006/07, 30 970, nr. 3, p. 3.
[306] Besluit Inlichtingenbureau Gemeenten, 13 december 2001, *Stb.* 2001, 686 (Besluit van 13 december 2001, houdende nadere regels omtrent de coördinatie en dienstverlening door het Inlichtingenbureau ten behoeve van de gemeenten bij de gegevensverstrekking op grond van zowel de Wet SUWI als de Abw, de IOAW en de IOAZ, alsmede omtrent de financiering van het Inlichtingenbureau).

nevendoel, te weten diensten ten behoeve van gemeenten op het gebied van informatievoorziening en gegevensuitwisseling, onvoldoende bepaald is. De Registratiekamer betrekt hierbij de omstandigheid dat de gegevens waarover het IB [Inlichtingenbureau] beschikt door burgers verplicht aan de sociale diensten dienen te worden verstrekt en veelal gevoelig van aard zijn. In deze omstandigheid acht zij het noodzakelijk in de tekst van het besluit een dwingende koppeling aan te brengen tussen de kerntaken van het IB uit het eerste lid en de overige taken. Deze dienen niet alleen maar "in het verlengde" hiervan te liggen. Het criterium dient te zijn dat deze hiermee noodzakelijk zijn verbonden"[307], welk commentaar geleid heeft tot aanpassing van het concept van het Besluit Inlichtingenbureau.

Het Besluit IB wordt op korte termijn ingetrokken. Het IB wordt dan als (wettelijk) bewerker aangemerkt in plaats van de huidige positie als verantwoordelijke. Wie dan vervolgens de verantwoordelijke partij(en) word(t)(en) is niet duidelijk.[308]

Elektronische gegevensuitwisseling
Het kader van elektronische gegevensuitwisseling bestaan uit het ontwerp elektronische voorzieningen IB en het SUWI Gegeven Register (SGR), beide onderdeel van de Regeling Suwi. [309] Het SGR zorgt voor eenduidige gegevensuitwisseling zodat gegevensuitwisseling tussen de ketenpartners kan worden gerealiseerd. SGR beschrijft (cliënt)gegevens en legt de betekenis en de manier van het coderen van de "gegevens vast. Dit gebeurt in een gemeenschappelijke taal voor elektronische gegevensuitwisseling in het Suwidomein: SuwiML. Hierdoor zijn berichten gemakkelijk te begrijpen en maar voor één uitleg vatbaar. SuwiML is gebaseerd op het SGR en op de internet standaard XML (Extensible Markup Language). SuwiML is een XML-dialect."[310] "Alle gegevens in het SGR hebben een SuwiML-identificatie (een 'rugnummer', aangeduid als een SuwiML-tag) waarmee de gegevens in berichten voor elektronische gegevensuitwisseling worden geïdentificeerd. Bij uitwisseling op basis van SuwiML kunnen de gegevens op flexibele wijze in een browser aan gebruikers worden gepresenteerd en rechtstreeks door computersystemen worden verwerkt. Zo kan bijvoorbeeld het Intake-systeem van CWI, na het intoetsen van een burgerservicenummer (voorheen sofinummer), alle benodigde gegevens ophalen van inkijkservers van de verschillende partijen en deze automatisch inlezen. Het SuwiML Basisschema is in feite een één op één vertaling van SGR naar XML. [..] In de SuwiML berichtstandaard staat hoe de inhoudelijke structuur van informatie eruit moet zien. Hierdoor zijn ketenpartners in staat logisch berichten samen te stellen en optimaal gegevens uit te wisselen."[311]
Het SGR regelt de dienstverlening tussen SUWI-partijen in het kader van DKD. Afspraken met betrekking tot uniformiteit en standaardisaties worden vastgelegd in het SGR.

De gegevens in het DKD worden zowel met de klant (werkzoekende, uitkeringsgerechtigden) als onderling (uitvoeringsorganisaties) uitgewisseld.

Soorten gegevens
De gegevens die in het DKD zijn opgenomen of zullen worden opgenomen zijn onder meer:
- Financiële situatie (via gemeente)

[307] Registratiekamer, 'Nader advies concept-besluit Inlichtingenbureau en SUWI', z2001-0762, 1 augustus 2001, p. 5.
[308] Olf Kinkhorst, 'Uitvoeringstoets Besluit 30 mei 2007 UB/K/2007/127 IB07-052 eenmalige uitvraag (Beu)', brief aan het Ministerie van Sociale Zaken en Werkgelegenheid, 30-05-2007, onder punt 3. Beschikbaar via WWW <http://ikregeer.nl/static/pdf/BLG14121.pdf>.
[309] Het Ontwerp én SGR zijn bijlagen bij de SUWI-regeling van 2002; *Stcrt.* 2002, 2.
[310] WWW <http://www.bkwi.nl/suwinet/sgr_suwiml/>.
[311] WWW <http://www.bkwi.nl/suwinet/sgr_suwiml/wat_is_suwiml/>.

- Uitkeringen (via gemeente)
- Maatregelen (via gemeente en UWV)
- Vorderingen (via gemeente)
- Reïntegratie (via gemeente en UWV)
- Aanvragen (via gemeente)
- Gegevens polisadministratie (via UWV)
- Arbeidsgeschiktheid (via UWV)
- Dienstverlening (via CWI)
- Arbeidsbemiddeling (via CWI)
- Kentekenbewijzen, rijbewijzen (via RDW)
- Persoonsgegevens (via Landelijk Raadpleegbare Deelverzameling (LRD), landelijke GBA raadpleging)
- Nog niet opgenomen, maar op de planning:
- Diploma gegevens / opleidingen (via IB-groep)
- Gegevens over studieschuld, studiebeurzen (via IB-groep)
- Kinderbijslag (via SVB)

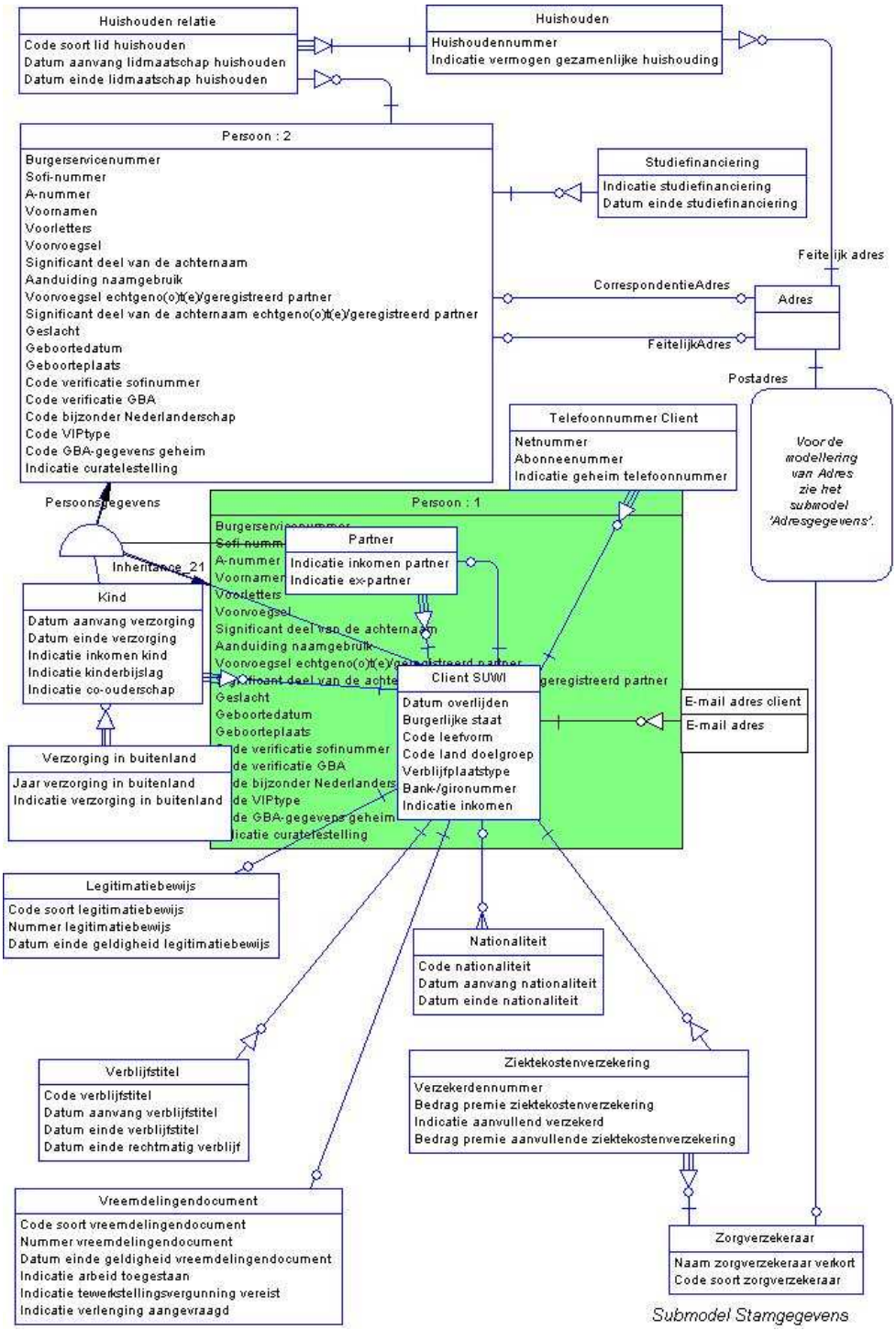
Implementatie van het DKD en de WEU uitvraag is de verantwoordelijkheid van de gemeenten. Aanlevering van gegevens geschiedde via:

- Het aanleveren van gegevens via bestandsaanlevering aan het inlichtingenbureau.
- Aanleveren van integrale bestanden aan het Inlichtingenbureau.
- Aanleveren van mutaties per sofinummer waarop wijziging heeft plaatsgevonden.
- Het realiseren van *real-time* berichtenverkeer webservices en een *upload* van indexerende gegevens naar een verwijsindex bij het Inlichtingenbureau.

Binnen de toegang tot gegevens zijn twee soorten groepen te onderscheiden. Allereerst de groep klanten, die toegang hebben tot hun eigen dossier via de website <http://www.werkeninkomen.nl>. Daarnaast de organisaties die toegang hebben tot het systeem via SUWInet-Inkijk óf organisaties die alleen gegevens aanleveren, maar niet uitgewisseld krijgen.

Het model van stamgegevens opgeslagen in het DKD ziet er als volgt uit:[312]

[312] WWW <http://www.bkwi.nl/fileadmin/suwiML/SGR%204_0.htm>



Figuur 1 - Model stamgegevens DKD

De klant heeft op de website toegang tot algemene informatie over werk en inkomen, en kan zich daarvoor elektronisch inschrijven. Eigen gegevens en status van het werk&inkomen proces zijn door de klant zelf in te zien nadat deze met DigiD toegang heeft gekregen. Zodra identiteit / authenticiteit van de klant is vastgesteld, heeft de klant toegang tot de eigen klantgegevens en kan hij/zij het klantproces (verwerkingen) volgen. Er is gekozen om de informatie alleen met DIGID te ontsluiten (laag niveau) en geen aanvullende beveiliging zoals sms verificatie te kiezen. De persoonlijke gegevens die voor de klant inzichtelijk zijn, zijn GBA-gegevens, gevolgde opleidingen, uitkeringsinformatie (voor zover beschikbaar), reïntegratie data en betalingen. Bij onjuiste gegevens kan de klant online een correctieverzoek doen. In sommige gevallen is het echt noodzakelijk dat de klant schriftelijk of via een balie een correctieverzoek doet (zoals foutief paspoortnummer). De klant kan ook een elektronische aanvraag indienen voor WW en WWB. Bij dit proces zijn de formulieren al deels vooraf ingevuld op basis van de gegevens die in het DKD bekend zijn over de klant (gemak voor de klant). Ook het werkbriefje WW kan online worden ingevuld door de klant.

Organisaties hebben inzicht in de gegevens door middel van toegang tot SUWInet-Inkijk of andere bedrijfsapplicaties. Doel van de toegang is het voldoen aan de WEU en het verminderen van bewijsstukken. De volledige klantdossiers zijn inzichtelijk voor de medewerkers van de betrokken organisaties. Doordat de systemen van de diverse actoren niet met elkaar zijn gecombineerd, maar aan elkaar zijn gekoppeld, is er sprake van ‘inkijk’ bij CWI, UWV, Gemeenten, RDW en GBA. Overdracht van klantgegevens (ook bewijsstukken) wordt zoveel mogelijk elektronisch gerealiseerd (via EKB). Tot slot is het mogelijk een zogenaamde omgekeerde intake te realiseren doordat gegevens over de klant kunnen worden verkregen uit de administraties van de ketenpartners.

Informatiebeveiliging & privacy
Partijen hebben allen eigen protocollen op het gebied van beveiliging en privacy. Gezamenlijke protocollen zijn daarom ontwikkeld om de keten gezamenlijk te kunnen beveiligen. De meeste beveiligingsrisico’s zitten nu op het gebied van de organisaties zelf en dienen opgelost te worden door middel van clean desk policies en dergelijke.[313]

Ontwikkeling van software
Hoewel de meeste ketenpartijen alle ICT aanbesteden, ontwikkelt BKWI veel software zelf. Dit betekent dus dat de verschillende software pakketten op elkaar aan moeten sluiten. Het BKWI is betrokken bij de uitwisseling van gegevens en via het SUWI gegevensregister (SGR) ook betrokken bij de ontwikkeling van gegevensvergelijkingsprocessen. “Het BKWI is betrokken bij de ontwikkeling van standaarden op het gebied van gegevensuitwisseling. Voor het DKD is daarvoor het SGR ingezet (meest recente versie: 4.0).[314] Algemeen informatiebeleid en/of procedures rondom het DKD worden via de stuurgroep en via andere vormen van overleg vastgesteld. Het BKWI heeft zelf de uitwisselstandaard, de gegevensstandaard, berichtdefinities, afspraken over IP-ranges en dergelijk opgesteld.

Om te voorkomen dat medewerkers een volledig nieuw systeem moesten gaan beheersen, is er gekozen om de inkijk in SUWInet zo aan te passen dat de nieuwe informatie extra raadpleegbaar is. Het bestaande systeem bood dus de benodigde nieuwe informatiestromen.

Ook wordt veel gemeentelijke software ontwikkeld door commerciële partijen, zoals Getronics Pink Roccade en Centric. Beide partijen ontwikkelen ICT oplossingen voor klanten in

[313] Inspectie Werk en Inkomen, ‘Samen onder één dak. Een gezamenlijk onderzoek van CBP en IWI naar het gebruik van persoonsgegevens in zes lokale samenwerkingsverbanden.’, november 2007, p. 10
[314] WWW <http://www.bkwi.nl/suwinet/sgr_suwiml/wat_is_sgr/>.

gemeenteland voor eigen rekening en risico. Vaste afspraken worden gemaakt met CP-ICT over uniformering, randvoorwaarden en tijdsplanning. De gebruikersvereniging van de betrokken gemeente(n) zijn ook betrokken bij het ontwikkelingsproces. Commerciële partijen zijn kennelijk niet betrokken bij de ontwikkeling van gegevensvergelijkingsprocessen, deze worden ontwikkeld op initiatief van het Ministerie.

Interoperabiliteit van gegevensuitwisseling
Tussen de ketenpartners wordt gebruik gemaakt van gezamenlijke Service Level Agreements, certificering en is er speciale aandacht voor terugmelding en correctie. Ketenpartners houden zich aan de bestaande structuren binnen de keten die zijn ingericht met behulp van de Ministeriële Regeling SUWI (SGR en andere ontwerpen), aan de NORA/OSB architectuur en de standaarden van de basisregistraties. NORA (Nederlandse Overheid Referentie Architectuur) geldt voor de hele Nederlandse overheid. De standaarden worden meer bepaald door SZW, de vertegenwoordiging van de gemeente waarbij ICT leveranciers gevraagd worden of deze ook mogelijk zijn. De gegevenssets worden vastgesteld en de wijze waarop gegevens worden getransporteerd. Er zijn ook leveranciers die zich naast al deze standaarden, nog conformeren aan open standaarden (OS) bij gegevensuitwisseling.

Conclusies
Interoperabiliteit wordt enerzijds beschouwd als organisatieprobleem en anderzijds als technisch probleem, afhankelijk van het perspectief dat aangehangen wordt. Interoperabiliteit wordt door geen van de partijen beschouwd als een juridisch vraagstuk. Regelgeving dient geen details te regelen, maar de algemene lijnen waarop de interoperabiliteit gebaseerd is. Een wettelijk kader heeft volgens sommigen slechts toegevoegde waarde op het niveau van gemak van aansluiting van relevante partijen. Anderen stellen echter dat wettelijke randvoorwaarden mogelijk leiden tot snellere realisatie en meer houvast bij de ontwikkeling van een interoperabiliteitsraamwerk. Ook wordt een wettelijk kader beschouwd als ‘drukmiddel’. Een gentlemen’s agreement zou ook mogelijk zijn, maar wettelijke kaders stimuleren marktwerking. Praktische randvoorwaarden bij interoperabiliteit zijn het beheer van vastgestelde standaarden, de eenduidige begeleiding bij uitrol en de betrokkenheid van alle partijen. Financieringsregelingen stimuleren interoperabiliteit, doordat er niet alleen sprake is van een wettelijke grondslag.

Het ontwikkelen van de gegevenssets en de wijze waarop uitwisseling zou moeten gaan plaatsvinden is een kwestie waar veel aandacht aan is besteed. De beschikbaarheid van kwalitatief goede gegevens was een voorwaarde voor ontsluiting van gegevens aan de burger, omdat er anders teveel vragen zouden worden opgeroepen. Uiteindelijk dienden de betrokken partijen voor 1 januari 2008 hun gegevenspakketten op orde te hebben, zodat de landelijke uitrol van het DKD plaats kon vinden. Er waren daarnaast veel vragen rondom de techniek en de verschillende standaarden en de gegevenssets. Zo zijn de standaarden volgens sommigen in een te beperkte club bepaald en waren ze nog niet ‘volwassen’ genoeg voor een landelijke uitrol. Ook waren er geen duidelijke afspraken over versiebeleid als het gaat om de specificaties van gegevensuitwisseling.

Privacywetgeving in de vorm van de Wbp wordt vaak als een knelpunt gezien. Dit ziet dan met name op de doelbinding van de Wbp en de transparantie van de processen van het DKD. Het doel van gegevensuitwisseling wordt vaak beschouwd als een doel op zich, wat niet afdoende is om te voldoen aan de Wbp doelbepaling. Aangegeven wordt wel dat de wetgever dit heeft opgelost dor de Wet SUWI aan te passen zodat de gegevensuitwisseling makkelijker realiseerbaar is.
Niettemin moet er gewaakt worden voor het beeld dat de Wbp de boosdoener is. Het is begrijpelijk dat organisaties zich soms beperkt voelen door de Wbp en het moeilijk vinden om

doelbinding en transparantie van processen te realiseren. Dit knelpunt zit dan echter niet in de Wbp, maar in het organisatieproces dat wellicht niet is ingericht op privacygericht werken. De wet kan partijen in de keten wel een handje helpen door de vastlegging van doelbepalingen zoals bij de Wet SUWI is gebeurd. Inhoudelijke belemmeringen die echt niet oplosbaar zijn door de invloed van het Wbp zijn niet waarschijnlijk. Bestaande kaders zijn toereikend of worden aangepast (Wet SUWI). Dit wordt nog eens bevestigd doordat er een goede dialoog plaats vindt met het CBP. De Wbp in een moderner jasje steken is een veelgehoorde wens. Dit neemt echter de (organisatorische) problemen rondom doelbinding en transparantie niet weg, omdat deze de kern vormen van de Wbp.

Wetgeving moet bovendien in een veel eerder stadium gerealiseerd worden om er voor te zorgen dat dit daadwerkelijk als drukmiddel kan worden ingezet. Hetzelfde geldt overigens voor alle procedures en handreikingen, deze moeten tijdig worden aangeleverd.

3.3 Elektronisch proces verbaal (ePV)

Inleiding en achtergrond

In 2002 heeft een pilotproject plaatsgevonden met betrekking tot de uitwisseling van een elektronisch Proces Verbaal (ePV) inzake artikel 8 van de Wegenverkeerswet (rijden onder invloed), tussen de politie, het OM (openbaar ministerie) en de ZM (zittende magistratuur).[315] Het pilotproject geldt als voorloper van het Programma Elektronische Berichtenuitwisseling in de Strafrechtsketen[316] (Programma ePV), dat in 2003 van start is gegaan. Per 1 mei 2007 is het Programma ePV overgegaan naar de ketenorganisatie Elektronisch Berichten Verkeer (EBV) en ondergebracht bij de Justitiële Informatiedienst. De achterliggende reden hiervoor is dat het project evolueerde van een ontwikkelprogramma naar een dienstenorganisatie. Deze ontstaansgeschiedenis heeft tot gevolg gehad dat de afkorting 'ePV', in eerste instantie werd gebruikt om elektronisch berichten verkeer in de gehele strafrechtketen aan te duiden.

In het kader van deze case zijn vragenlijsten uitgezet bij personen die specifiek bij het elektronisch proces-verbaal betrokken zijn. De reden om specifiek hiervoor te kiezen, en niet voor elektronisch berichtenverkeer in de gehele strafrechtsketen, is gebaseerd op de gedachte dat het met name wenselijk is om na te gaan hoe bij het elektronische proces-verbaal met het wettelijk vereiste van ondertekening wordt omgegaan. In het hiernavolgende wordt eerst in bredere zin ingegaan op elektronisch berichtenverkeer in de strafrechtketen.

Elektronische gegevensuitwisseling[317]

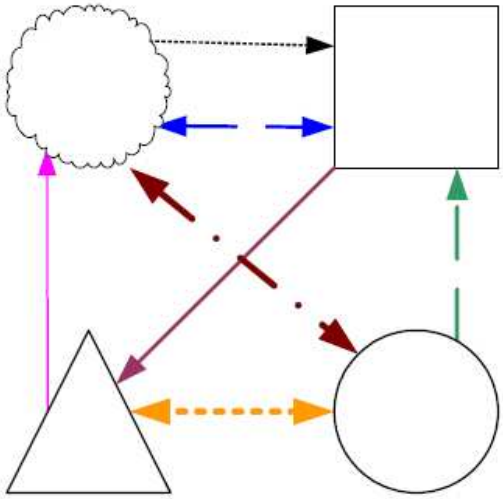
In de strafrechtsketen werd voorafgaand aan het ePV-programma reeds op elektronische wijze informatie uitgewisseld. Er vond daarbij slechts lokale standaardisatie plaats. Hierdoor waren processen, techniek en gegevens niet afgestemd tussen de verschillende interacties. Dit kan als volgt worden gevisualiseerd.

---

[315] *Kamerstukken II*, 2002/03, 28 684, nr. 3, p. 41.

[316] De strafrechtsketen is de keten gericht op het opsporen, vervolgen, berechten, ten uitvoer leggen van de straf en het begeleiden van personen die een strafbaar feit hebben gepleegd.

[317] B. Dommisse, 'Gelaagde berichtenuitwisseling in de strafrechtsketen', *Informatie* september 2007, p. 46-50; B. Dommisse, 'Elektronische berichtenuitwisseling in de strafrechtsketen', *<!ELEMENT* jaargang 12, nr. 1, p. 4-10; G.J. van Lochem, 'Ketenstandaarden: Berichten uit de Strafrechtsketen', *<!ELEMENT* jaargang 12, nr. 4, p. 16-22; Project Bouwstenen voor Berichtenuitwisseling tussen Overheden, *Handboek ePV* 2006; Justitiële informatiedienst, *Elektronisch Berichten Verkeer*, WWW <http://www.justid.nl/ebv> (geraadpleegd 16 april 2008).



Figuur 2 - Elektronische berichtenuitwisseling in de strafrechtsketen voorafgaand aan het ePV programma

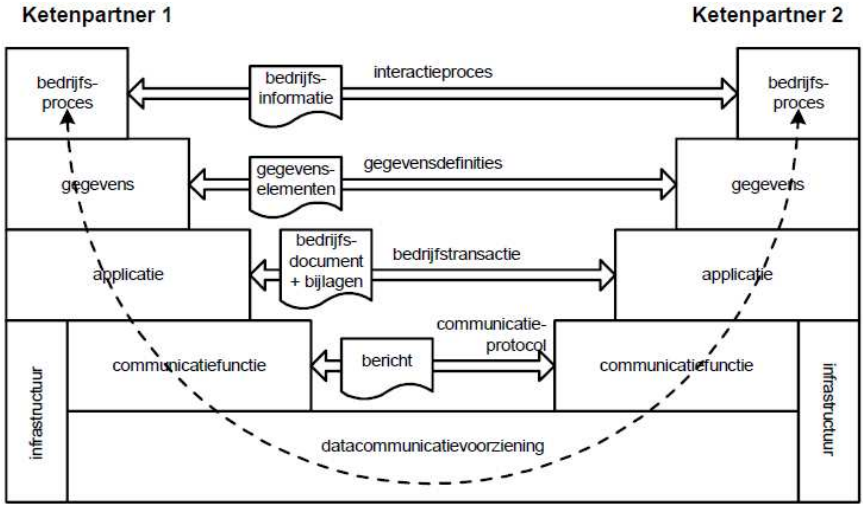
Het ePV-project is gericht op het realiseren van een goede interoperabiliteit. Hieronder wordt verstaan:

> 'De mate waarin twee of meer gelijksoortige, autonome entiteiten (i.e. organisaties, bedrijfsprocessen, applicaties, e.d.) met elkaar kunnen samenwerken op basis van vooraf bepaalde afspraken over o.a. gegevensuitwisseling, gegevensbetekenis en overkoepelende werkprocessen.'[318]

Het realiseren van een goede interoperabiliteit geschiedt middels het maken van afspraken. De totale set van generieke afspraken wordt aangeduid als het interoperabiliteitsraamwerk van ePV.[319]

Bij het inrichten van de elektronische gegevensuitwisseling in de strafrechtsketen zijn als eerste de relevante conceptuele modellen beschreven.[320] Hierbij is uitgegaan van de noodzaak om tot samenwerking te komen in de keten ten aanzien van de techniek, het proces en de inhoud. Er is ook meegenomen dat het van belang is een zekere gelaagdheid te onderkennen. Dit is weergegeven in het ePV *lagenmodel*, welke is ontleend aan het OSI-model.

[318] Project Bouwstenen voor Berichtenuitwisseling tussen Overheden, *Handboek ePV, Deel 2. Interoperabiliteitsraamwerk: Toelichting gebruikte standaarden*, 2006, p. 3.
[319] Idem.
[320] Zie Project Bouwstenen voor Berichtenuitwisseling tussen Overheden, *Handboek ePV, Deel 1. Conceptuele Modellen*, 2006.



Figuur 3 - ePV lagenmodel

Het lagenmodel laat zich als volgt toelichten.

- op het laagste niveau is er een *datacommunicatievoorziening* (netwerk) die zorgt voor de elementaire overdracht van 'bitstromen';
- de *ketenpartners* beschikken over eigen of gemeenschappelijke *communicatiefuncties* die de uitwisseling van *berichten* tussen hun applicaties mogelijk maken volgens een afgesproken *communicatieprotocol*. Een *communicatiefunctie* is te beschouwen als een elektronische postkamer, die verzend- en afleverdiensten biedt ongeacht de inhoud van de *berichten*. De *communicatiefuncties* en de *datacommunicatievoorziening* worden tezamen beschouwd als een generieke *infrastructuur;*
- de *applicaties* van de *ketenpartners* zijn dankzij de diensten van de onderliggende lagen in staat om *bedrijfstransacties* uit te voeren, waarbinnen *bedrijfsdocumenten* en hun *bijlagen* worden uitgewisseld;
- dankzij de *applicaties* vindt er feitelijk een overdracht plaats van *gegevenselementen* (gestructureerd en gegroepeerd in *bedrijfsdocumenten*), waarvan de betekenis en eigenschappen in *gegevensdefinities* zijn vastgelegd;
- de uitgewisselde *gegevenselementen* (in combinatie met de *bijlagen* bij de *bedrijfsdocumenten* die ongestructureerd zijn of waarvan de structuur niet primair relevant is voor de bedrijfstransactie) zijn de dragers van de *bedrijfsinformatie* die uiteindelijk op het niveau van de *bedrijfsprocessen* via afgesproken *interactieprocessen* wordt uitgewisseld.[321]

Ten aanzien van alle te onderscheiden lagen zijn afspraken gemaakt. De afspraken zijn op de volgende uitgangspunten gebaseerd:

- de gekozen standaard moet een open standaard zijn, dus niet leverancierspecifiek;
- er moeten COTS (Commercial Off the Shelf)-producten en open-sourceproducten zijn die de standaard ondersteunen;

[321] Idem, p. 7-8. Zie met betrekking tot semantische interoperabiliteit Bouwstenen voor Berichtenuitwisseling tussen Overheden, *Eindrapportage. Legal dictionaries in relatie tot het Gegevenswoordenboek Strafrechtsketen* 2007.

- de standaard volgt bij voorkeur uit Europese of Nederlandse e-Overheidsaanbevelingen;
- het geheel aan standaarden en voorzieningen moet in samenhang met elkaar samenwerken (raamwerk);
- in de toekomst moet de vervanging van onderdelen van het raamwerk mogelijk zijn. Daarom worden er bijvoorbeeld wel XML-schema's gegenereerd, maar niet onderhouden. Onderhoud vindt plaats op het functionele niveau (gegevenswoordenboek, bedrijfsdocumenten);
- de ketenpartners moeten autonoom kunnen blijven in de keuzes die ze maken voor de inrichting van hun eigen interne informatiehuishouding;
- de uitwisseling met andere domeinen waar andere afspraken gelden, moet ondersteund kunnen worden, liefst via algemene voorzieningen waarvan alle partijen gebruik kunnen maken als ze eenmaal zijn aangesloten.[322]

De gemaakte afspraken luiden als volgt. Ten eerste is *JAB* (Justitie Asynchrone Berichtenuitwisseling) als nieuwe berichtenverkeerstandaard geaccepteerd en geïmplementeerd. JAB is gebaseerd op de OASIS ebMS standaard. Ten tweede zijn voor het versturen van berichten behalve een standaard, ook voorzieningen nodig die het daadwerkelijk versturen van de berichten faciliteren: hiervoor is in 2006 de Justitie Berichten Service (JUBES) in het leven geroepen en in 2007 de Externe PolitieBroker (EPB). JUBES is een centraal knooppunt voor de uitwisseling van berichten tussen justitiepartijen onderling en voor de uitwisseling van berichten van die organisaties met externe partijen, zoals de politie. De EPB is een vergelijkbare voorziening als de JUBES, maar dan voor het politiedomein.

Interoperabiliteit van de gegevensuitwisseling
Uit bovenstaande beschrijving blijkt dat interoperabiliteit van begin af aan een centrale rol heeft gespeeld bij het ePV-project.

Het juridisch kader van het elektronisch proces-verbaal
In paragraaf 2.5 word het (toekomstig) juridisch kader inzake (onder meer) het elektronisch proces-verbaal geschetst. Deels recapitulerend houdt dit juridisch kader in dat op grond van de wet een PV:

> persoonlijk, gedagtekend en ondertekend wordt opgemaakt.
>
> En:
>
> met een ondertekend proces-verbaal wordt gelijkgesteld een proces-verbaal dat langs elektronische weg is opgemaakt en verzonden, mits dit voldoet aan de bij of krachtens algemene maatregel van bestuur (AMvB) gestelde eisen.

De tweede zinsnede is nog niet van kracht geworden. De AMvB die op grond van de tweede zinsnede vereist is, is nog niet vastgesteld. Uit de antwoorden van de respondenten blijkt dat aansluiting zal worden gezocht bij de Wet elektronische handtekeningen, met name bij de omschrijving van het 'veilig middel'.

Ervaren knelpunten en hiaten
De respondenten ervaren de wetgeving inzake de bescherming van persoonsgegevens (de Wet bescherming persoonsgegevens, de (oude) Wet politieregisters en de (nieuwe) Wet

[322] B. Dommisse, 'Gelaagde berichtenuitwisseling in de strafrechtsketen', *Informatie* september 2007, p. 49.

politiegegevens) als onduidelijk. Volgens één respondent, werkzaam bij een regiokorps, beschikt de politie niet altijd over een wettelijke basis voor het uitwisselen van gegevens. Veelal wordt dit opgelost middels een convenant[323] of een verklaring van betrokkenen: 'Zo tekenen de veelplegers een verklaring op basis waarvan informatie wordt uitgewisseld met OM, gemeenten, reclassering, DJI, bureau jeugdzorg, verslavingsinstellingen, GGZ, enz'. Vanuit juridisch oogpunt zijn er vraagtekens te zetten bij het laten tekenen van een verdachte of veroordeelde van een verklaring inhoudende de toestemming om diens persoonsgegevens te verwerken. De wet eist dat er sprake is van 'ondubbelzinnige toestemming'. Aangezien het de vraag is of in het bedoelde geval de verklaring uit vrije wil wordt ondertekend, is het onwaarschijnlijk dat dit een voldoende grondslag oplevert voor de verwerking van de betreffende gegevens. Voorts worden de volgende opmerkingen gemaakt, welke lijken te duiden op een behoefte aan meer regie, aansturing, dan wel voorlichting:

- 'organisaties zijn nog niet gewend om kwaliteitseisen te benoemen op basis waarvan standaard producten kunnen worden benoemd;
- er is nog geen sprake van 'zicht op zaken' in de gehele keten. Tussen partners begint [dit] vorm te krijgen, maar zicht op de hele keten is nog niet aanwezig;
- er worden regelmatig (al dan niet organisatorische) wijzigingen doorgevoerd die impact hebben op de hele keten, zonder dat dit [van] tevoren bekend wordt gemaakt;
- (geautomatiseerd) uitwisselen van gegevens vereist een gedegen gegevensbeheer en een goede registratie (bijvoorbeeld van de status van een gegeven);
- er is niet altijd het besef dat bij het uitwisselen van gegevens er sprake moet zijn van willen (intentie moet er zijn), mogen (het moet toegestaan zijn) en kunnen (de juiste gegevens moeten te genereren zijn).'

Conclusies

1. De wetgeving inzake de bescherming van persoonsgegevens wordt als onduidelijk ervaren. Dit moge ook blijken uit de praktijk om een veelpleger een verklaring te laten tekenen inhoudende de toestemming zijn persoonsgegevens te verwerken.
2. Er is behoefte aan meer regie, aansturen dan wel voorlichting inzake de inrichting van elektronisch berichtenverkeer, waaronder het elektronisch proces-verbaal.

3.4 De uitwisseling van geo-informatie

In deze 'case' wordt niet één toepassing of project onderzocht, maar wordt meer in het algemeen gekeken naar wat in het licht van interoperabiliteit de implicaties en met name knelpunten op terrein van de geo-informatie zijn. Alvorens daaraan toe te komen, zullen eerst een beschrijving van het veld en van de juridische setting worden gegeven. Vervolgens wordt ingegaan op de perceptie van interoperabiliteit ten aanzien van de geo-informatieuitwisseling en op de ontwikkeling van een nationale geo-informatie-basisvoorziening. Ten slotte zullen de op basis van het onderzoek geïdentificeerde knelpunten respectievelijk de conclusies worden weergegeven.

Beschrijving

De context waarin de uitwisseling van geo-informatie plaatsvindt, is om verschillende redenen complex. Er zijn verschillende soorten geo-informatie met uiteenlopende functies en mogelijkheden die onderling weer op uiteenlopende wijzen gerelateerd kunnen zijn (denk aan gebouwen in een bepaalde gemeente die onderdeel uitmaken van een of meer kadastrale

[323] Met het noemen van een convenant als instrument zou kunnen worden gedoeld op gegevensuitwisseling in het kader van de zogenaamde bestuurlijke aanpak.

percelen en waarin en -onder leidingen lopen).[324] De samenhang tussen de verschillende soorten geo-informatie is dan ook complex. Daar komt bij dat geo-informatie bijzonder waardevolle informatie is, zeker wanneer deze ook nog wordt gekoppeld aan andere informatie, zoals informatie uit de gezondheidszorg, financiële of verkeersinformatie. Bovendien zijn er veel verschillende partijen betrokken bij het gebruik van geo-informatie; verschillende overheden, maar ook allerlei semi-overheidsinstellingen. Voorts zijn de maatschappelijke en economische belangen in het geo-informatieveld groot. Vaak zijn er enorme investeringen in geo-informatie gedaan. Daarnaast is geo-informatie onmisbaar geworden in elektronische toepassingen op tal van overheidsterreinen (bijvoorbeeld ruimtelijke ordening, milieu, verkeer, veiligheid, landbouw, waterhuishouding), inclusief de elektronische basisvoorzieningen. Maar ook politiek-bestuurlijk is de uitwisseling van geo-informatie van grote betekenis. Mede vanwege de economische belangen bij innovatie, maar ook vanuit het oogpunt van, soms grensoverschrijdende, maatschappelijke problemen en ontwikkelingen (denk aan armoedebestrijding, klimaatverandering, duurzame ontwikkeling en veiligheid). Verder is het wettelijk kader voor geo-informatie (zie hierna voor een impressie) eveneens complex.[325]

Belangrijke coördinerende spelers op het terrein van uitwisseling van geo-informatie zijn het Ministerie van VROM, het Beraad voor de Geo-informatie (GI-beraad) en Geonovum. De Minister van *VROM* is coördinerend bewindspersoon als het gaat om de uitwisseling van geo-informatie. VROM is tevens penvoerder van het onderzoeksprogramma RGI (Ruimte voor Geo-Informatie). Daarnaast is VROM ook een belangrijke gebruiker van geo-informatie: de digitale ruimtelijke plannen, Omgevingsloket, Atlas Leefomgeving, etc. VROM voert de regie over het hierna te behandelen Gideon-programma dat gaat over de inrichting van een basisvoorziening voor geo-informatie. Het *GI-beraad* adviseert VROM op het terrein van geo-informatieuitwisseling en – dienstverlening en verzorgt de coördinatie van alle betrokken partijen. Het GI-raad stuurt tevens het Gideon-programma aan. Onder toezicht van VROM opereert de *stichting Geonovum* tussen beleid en uitvoering met als doelstelling het stimuleren van hergebruik door enerzijds het borgen van kennis met betrekking tot standaarden en infrastructuur en anderzijds betrokkenheid bij de inrichting van het procesmanagement van meerdere overheden ten aanzien van thema's waarover bestuurlijke consensus bestaat (bijv. op het terrein van veiligheid) door de omzetting naar daadwerkelijke voorzieningen te realiseren. Door Geonovum zijn inmiddels standaarden ontwikkeld in het kader van het Framework voor geo-standaarden[326] dat is goedgekeurd door de GI-Raad en het College Standaardisatie. Het ontwikkelen van dergelijke standaarden zit in de basisprogrammasubsidie die VROM aan Geonovum verstrekt. Voorts fungeert Geonovum als kenniscentrum, onder meer ook in het kader van het Gideon-programma.

Juridische setting
Vanuit verschillende perspectieven – te weten openbaarheid, toegankelijkheid en gegevensbescherming – werkt wetgeving in op de uitwisseling van geo-informatie. De meeste wetgeving is hiervoor reeds uitgebreid behandeld, maar ten behoeve van de inzichtelijkheid in

[324] Voorbeeld ontleend aan B. van Loenen e.a., 'Geo-informatie: wat is het en wat is de juridische context', in: L. van der Wees & S. Nouwt (red.), *Recht en locatie. Geo-informatie in een juridische context* (Nederlandse Vereniging voor Informatietechnologie en Recht), Den Haag: Reed Business BV 2008, p. 12.
[325] Zie alles: B. van Loenen e.a., *supra*, p. 11-34 ; GIDEON – Basisvoorziening geo-informatie Nederland, Visie en implementatiestrategie (2008-2011), Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu, April 2008.
[326] Framework van standaarden, Geonovum, 10 december 2007, versie 2.0 (definitief), WWW <http://www.geonovum.nl/framework-van-standaarden/> (geraadpleegd 18 juni 2008).

de juridische setting voor de geo-informatieuitwisseling wordt hier toch kort nog de wetgeving op een rij gezet en in het licht van de uitwisseling van geo-informatie toegelicht.

Wetgeving ziet ten eerste op de openbaarheid van geo-informatie. De Wet openbaarheid van bestuur is in dat verband natuurlijk relevant, maar meer in het bijzonder kunnen ook de Kadasterwet ten aanzien van de registers die in beheer van het Kadaster zijn en de Wet milieubeheer (hoofdstuk 19) ten aanzien van milieu-informatie van toepassing zijn. Het uitgangspunt is openbaarheid, maar in het kader van het hergebruik en intellectuele eigendomsrechten kunnen er wel nadere voorwaarden worden gesteld aan de verstrekking van geo-informatie.

Ten tweede speelt de in de Wob opgenomen hergebruikregeling een belangrijke rol met betrekking tot de toegankelijkheid van geo-informatie. De hergebruikregeling is ook van toepassing op informatie die geen bestuurlijke aangelegenheid betreft alsmede op informatie die onder een specifiek openbaarheidsregime valt, bijv. kadastrale informatie.

Binnen de overheid varieert het toegankelijkheidsbeleid alsmede de daaraan gekoppelde prijsstelling nogal. Op grond van de hergebruikregeling mogen de totale inkomsten uit het verstrekken en het verlenen van toestemming voor hergebruik, niet hoger zijn dan de kosten van verzameling, productie, vermenigvuldiging en verspreiding van de informatie. De totale inkomsten mogen wel worden aangevuld met een *redelijk rendement*.[327]

Een aantal overheden, waaronder provincies, waterschappen en Rijkswaterstaat, beoogt de realisatie van volledig vrije toegankelijkheid. In het kader van hergebruik is het ook belangrijk dat informatie zoveel mogelijk wordt vrijgegeven, want dan kan er worden gestandaardiseerd en, zo stelt één van de respondenten, 'wordt voorkomen dat iedereen iets anders gaat gebruiken'. Overigens is de doelstelling van het volledig vrijgeven van geo-informatie volgens diezelfde respondent soms lastig te bereiken, namelijk wanneer bepaalde geo-data sets een minder open toegankelijkheidsregime (in verband met bekostiging door een of meer andere partijen) kennen (bijvoorbeeld Actueel Hoogtebestand Nederland) of door de private sector worden gecreëerd en op de markt gebracht (denk aan het Nationaal Wegenbestand). Rijkswaterstaat wil bijvoorbeeld per 1 januari 2009 het Nationaal Wegen Bestand vrijgeven, maar Falkplan en Geobusiness hebben flink geïnvesteerd in de verkrijging van data daaruit voor de ontwikkeling van hun eigen producten. Het NWB is volgens deze respondent echter geen wettelijke taak voor Rijkswaterstaat.[328] Verder bestaat de intentie van volledig vrije toegankelijkheid bijvoorbeeld ook bij het KNMI, maar staat de Wet op het KNMI die een vergoeding vereist aan verwezenlijking van die doelstelling in de weg.[329]

Eveneens relevant in het kader van de toegankelijkheid is de INSPIRE richtlijn. Naar aanleiding van deze richtlijn zullen technische invoeringsregels worden vastgesteld. In mei 2008 is de eerste invoeringsregeling inzake meta-informatie vastgesteld. Op basis van INSPIRE worden dataleveranciers van geo-informatie gedwongen te standaardiseren en gegevens beschikbaar te stellen. Bij het vaststellen van de technische invoeringsregels is de

[327] Artikel 11h lid 1 Wob.
[328] Een duidelijke wettelijke taak met betrekking tot geo-informatie is bijvoorbeeld te vinden in de Kadasterwet (Wet van 3 mei 1989, laatst gewijzigd *Stb*. 2008, 197). Ook in de Wet bodembescherming (Wet van 3 juli 1986, houdende regelen inzake bescherming van de bodem, laatst gewijzigd Stb. 2007, 152) hebben overheidsorganen (bijvoorbeeld gemeenten) een rol in het verzamelen van geo-informatie (informatie over bodemkwaliteit).
[329] Zie meer in het bijzonder de Regeling beschikbaarheid algemeen weerbericht en KNMI-gegevens, prijs KNMI-gegevens en nadere regeling KNMI-taken en -raad (*Staatscourant*, 3 juli 2002).

Joint Research Center van de Europese Commissie betrokken ten aanzien van de technische standaarden.[330] Vanuit Nederland levert Geonovum technische experts voor de technische regelingen en beoordeelt het Ministerie van VROM de voorstellen van de Europese commissie. INSPIRE wordt door een van de respondenten beschouwd als een impuls om in ieder geval tussen de overheden een doorbraak met betrekking tot het hergebruik van geo-informatie te bewerkstelligen. Anderzijds wordt ook opgemerkt dat INSPIRE op detailniveau nog weinig duidelijkheid biedt en onvoldoende verantwoordelijkheden neerlegt bij de implementerende lidstaten, waardoor het nog maar de vraag is of het de gewenste stok achter deur is. Veel van het effect dat INSPIRE zal hebben op de uitwisseling van geo-informatie zal uiteindelijk afhangen van de invoeringsregels waarmee de Europese richtlijn wordt geïmplementeerd, zo het Plan van Aanpak voor INSPIRE van Geonovum. Hetzelfde rapport geeft echter ook aan dat het werkveld een overwegend positieve blik heeft op de impact van INSPIRE:

> 'Het werkveld is van mening dat de invoering van INSPIRE zal bijdragen aan nationale en organisatie-eigen ontwikkelingen en deze zelfs zal versnellen. INSPIRE zet Nederland ertoe aan zaken daadwerkelijk in de praktijk te brengen. INSPIRE stimuleert en sluit bijvoorbeeld aan bij:
> - efficiënte en transparante overheid en publieksgerichte dienstverlening van overheidsorganisaties (vraagsturing, klantgerichtheid);
> - publieke toegankelijkheid van geo-informatie van de overheid aan burgers en bedrijven, bijvoorbeeld door de ontwikkeling van gemeenschappelijke algemene voorwaarden;
> - verbetering van werkprocessen voor de inwin, verwerking en publicatie van geo-informatie en de toepassing van webservices;
> - informatie-uitwisseling, afstemming en samenwerking tussen overheidsorganisaties (bronhouders onderling en tussen bronhouders en gebruikers);
> - toepassing van standaarden voor geo-informatie;
> - ontwikkeling, profilering van en vergroting van bestuurlijk draagvlak voor geo-informatie en de geo-sector;
> - publiekprivate samenwerking.'[331]

De gegevensbescherming kan langs twee wegen worden benaderd, afhankelijk van de soort gegevens en de reden voor bescherming: intellectueel eigendomsrecht (met name auteursrecht en databankenrecht) en de bescherming van persoonsgegevens.
Op basis van het *intellectuele eigendomsrecht* kan de producent de (enorme) investeringen voor het creëren en onderhouden van geo-informatie bestanden eventueel terugverdienen. Overigens zullen overheden – zoals reeds vermeld – een uitdrukkelijk voorbehoud (bij wet of anderszins) moeten maken omdat er anders geen auteursrecht of databankenrecht op van overheidswege aan het publiek ter beschikking gestelde werken/databanken bestaat (artt. 15b, Aw, en 8, Databankenwet). Voorbeelden van voorbehouden zijn te vinden in VNG Modelverordeningen (auteursrecht) en artikel 7v, wetsontwerp nieuwe kadasterwet (databankenrecht).[332] Bovendien wordt aangenomen dat een weigering van toestemming voor hergebruik op grond van het auteurs- of databankenrecht alleen kan plaatsvinden in

[330] Het eerdergenoemde Framework voor standaarden sluit aan op de architectuur en standaarden] in het kader van INSPIRE (bron: WWW <www.geonovum.nl> (laatst bezocht: 18 juni 2008)).
[331] Plan van Aanpak, INSPIRE in Nederland, Geonovum, Ministerie van VROM, DG Milieu, 17 september 2007, versie 1.0 (definitief), p. 8.
[332] Wet basisregistraties kadaster en topografie, 5 maart 2007, *Stb*. 105, 5 maart 2007.

uitzonderingsgevallen (slechts als legitiem gebruik niet voor de hand ligt en voor misbruik mag worden gevreesd).[333]

Topografische kaarten genieten in de regel auteursrechtelijke bescherming. Dat geldt weer niet voor grootschalig kaartmateriaal, zoals de GBKN, omdat deze worden bepaald door feitelijke gegevens en door objectieve randvoorwaarden die afdoen aan de door het auteursrecht vereiste persoonlijke creativiteit ofwel originaliteit. Om dezelfde reden (objectivering) kan een toenemende standaardisatie eveneens een afname van de auteursrechtelijke bescherming betekenen.[334]
Voor databankenrechtelijke bescherming is een substantiële en risico-dragende investering vereist. Indien dat het geval is kan de producent (denk aan het Kadaster, het KNMI, en het CBS) bepalen dat toestemming vereist is of er aanvullende voorwaarden (bijv. betaling) worden gesteld aan het bevragen of hergebruiken van (een deel van) een databank. Door enkele rechterlijke uitspraken is er op zijn minst onduidelijkheid ontstaan ten aanzien van de mogelijkheden voor overheden om zich op het databankenrecht te beroepen. De juridische redenering van de rechter houdt hier in dat het databankenrecht alleen toekomt aan de producent van een databank. Om als producent te kunnen worden aangemerkt, dient er een investering te worden gedaan waarmee sprake is van een financieel risico. Aangezien overheden met publieke gelden databanken ontwikkelen, dragen zij geen financieel risico, en zullen zij dus niet als databankrechthebbende kunnen worden aangemerkt. Volgens Kabel betekent een uitspraak van het Europese Hof[335] dat overheidsinstellingen die de databank met publiek geld hebben gefinancierd en beheren ter uitoefening van hun publieke taak geen beroep op het databankenrecht zouden mogen doen.[336] Op basis van de uitspraak van de rechter in de Landmark-zaak wordt geconcludeerd dat investering uit publieke middelen niet wordt aangemerkt als een risico-dragende investering.[337] Dit zou betekenen dat overheden veelal geen databankenrechthebbenden zijn en dat een beroep op de hergebruikregeling van de Wob niet nodig is.[338]

Wettelijke gegevensbescherming speelt ook een rol in het kader van de bescherming van persoonsgegevens van individuele burgers. Relevante geo-informatieregistraties zijn in dit verband bijvoorbeeld de kadastrale registraties, grondgebonden belastingen (gemeenten, waterschappen) en aansluitingen bij nutsbedrijven. De Wet bescherming persoonsgegevens is medianeutraal dus het is irrelevant in welke vorm de geo-informatie wordt verwerkt. Denk bijvoorbeeld denk bijvoorbeeld aan foto's op Funda waarop persoonsgegevens, zoals straatnaam, huisnummer en kenteken, te zien waren. Overigens merkt een van de respondenten op dat het ondanks dat overheden hiervoor soms richtlijnen hebben, het niet

---

[333] H.W. Wefers Bettink, 'Intellectuele eigendomsrechten op geo-informatie', in: L. van der Wees & S. Nouwt (red.), *Recht en locatie. Geo-informatie in een juridische context* (Nederlandse Vereniging voor Informatietechnologie en Recht), Den Haag: Reed Business BV 2008, p. 73-90.
[334] B. van Loenen e.a., *supra,* p. 20-21. Zie ook H.F. Wefers Bettink, *supra*, p. 75-76.
[335] HvJEG, 9 november 2004, zaak C-203/02 (*The British Horseracing Board Ltd e.a. v. William Hill Organization Ltd.)*
[336] J.J.C. Kabel, Exclusiviteit en openbaarheid van ruimtelijke informatievoorziening, 2006, WWW <http://www.ivir.nl/publicaties/kabel/INSPIRE.pdf> (laatst bezocht op: 17 juni 2008). Zie ook H.W. Wefers Bettink, *supra*.
[337] Rechtbank Amsterdam, 21 februari 2007, AWB 07/786 WET (Landmark Nederland B.V./College van B&W Gemeente Amsterdam).
[338] *Kamerstukken II*, 2004/05, 30 188, nr. 3, p. 8: 'De hergebruikprocedure behoeft dus alleen te worden benut wanneer een overheidsorgaan informatie openbaar maakt en daarbij aangeeft dat zij op die informatie het auteursrecht, het databankenrecht of het naburig recht voorbehoudt.'

altijd duidelijk is voor hen wanneer iets wel of geen persoonsgegeven is. Overigens kunnen overheden ook bij het College Bescherming Persoonsgegevens te rade gaan.[339]
Volgens een van de respondenten speelt de discussie over geo-informatie en privacy – in tegenstelling tot België waar hierover kamervragen gesteld zouden zijn – in Nederland nog nauwelijks. Niettemin heeft het College bescherming persoonsgegevens volgens een andere respondent aangegeven dat informatie over vervuilde percelen die online wordt gezet voor het individu nadelige maatschappelijke consequenties kan hebben. Verder werd aangegeven door een respondent dat groeiend interesse vanuit de private sector (bijvoorbeeld marketingbedrijven) in geo-informatie resulteert in een toenemend spanningsveld tussen het hergebruik en de openbaarheid van geo-informatie en de bescherming persoonsgegevens. Ook in het kader van Location Based Services zouden context-afhankelijke locatiebepalingen kunnen leiden tot privacy-problemen. Het levert allerlei (nieuwe) gegevensrelaties op die een vrij indringend beeld kunnen geven van het doen en laten van een individu. Men moet daarbij wel voorzichtig zijn met het trekken van conclusies over dat individu, omdat uit de informatie geheel niet duidelijk hoeft te worden waarom iemand zich op een bepaalde locatie bevindt (iemand kan zich hebben verlopen en daarbij in de 'verkeerde' buurt zijn beland).

Interoperabiliteit
De wijze waarop interoperabiliteit door de respondenten wordt omschreven loopt enigszins uiteen. Een van de respondenten omschrijft interoperabiliteit als de 'aansluiting van of uitwisseling tussen systemen zonder menselijke tussenkomst'. Een ander geeft als definitie: 'het voorkomen van drempels in het opnieuw gebruiken van gegevens en tools' Daarbij is het volgens de betreffende persoon belangrijk voor ogen te houden dat leveranciers van tools in het algemeen onafhankelijk zijn en dat geo-informatie per definitie sectoroverschrijdend is, zodat geo-toepassingen altijd door meer dan een partij worden uitgevoerd.

De meesten erkennen dat interoperabiliteit in verschillende domeinen (technisch, economisch, juridisch, organisatorisch) relevant is. Drempels moeten bijvoorbeeld worden voorkomen op juridisch (afspraken maken), technisch en semantisch terrein. Daarnaast wordt echter ook wel aangegeven dat de knelpunten voornamelijk op het gebied van de samenwerking liggen. Taken en bevoegdheden die niet wettelijk zijn vastgelegd, worden niet of onvoldoende uitgevoerd waardoor de samenwerking stagneert. De organisatorisch-juridische setting voor samenwerking ten behoeve van de uitwisseling van geo-informatie kan ook nogal verschillen; soms is er een wettelijke basis, in andere gevallen gebeurt het op basis van afspraken (bijvoorbeeld informele mondelinge afspraken of licenties) of informele relaties (overleg, afstemming) tussen betrokken partijen.

Voor wat betreft de uitgangspunten voor interoperabiliteit wordt in de eerste plaats verwezen naar de INSPIRE richtlijn en de daarin neergelegde uitgangspunten (zie ook de bespreking van de richtlijn in paragraaf 2.16). Deze uitgangspunten worden op dit moment in uitvoeringswetgeving verder vormgegeven. Daarnaast wordt tevens gewezen op de verbinding met NORA.

GIDEON – Basisvoorziening voor geo-informatie
Met het oog op ketensamenwerking op het vlak van geo-informatie is relevant het onder VROM ressorterende Gideon-programma dat in 2011 moet resulteren in een basisvoorziening

[339] Zie ook de Handleiding voor verwerkers van persoonsgegevens van het Ministerie van Justitie, WWW <www.justitie.nl/images/Handleiding voor verwerkers persoonsgegevens_tcm34-3940.pdf> (geraadpleegd 17 juni 2008).

geo-informatie.[340] Ondanks de enorme kennis op terrein van geo-informatie en kwalitatief goed presterende leveranciers van geo-data en -diensten is geo-informatie nog teveel versnipperd met als gevolg slecht vindbare gegevens, hoge gebruikskosten en sterk uiteenlopende voorwaarden. Hierdoor komt ketensamenwerking op dit terrein onvoldoende van de grond.[341] Gideon beoogt daarin verandering te brengen.

De basisvoorziening geo-informatie beoogt meer in het bijzonder te voorzien in:

- locatie-onafhankelijke toegang tot geo-informatie voor burgers en bedrijven (bijvoorbeeld via mijnoverheid.nl en het bedrijvenloket);
- mogelijkheden voor economische waarde-toevoeging door bedrijven (harmonisatie van gebruiksvoorwaarden, nationale dataverstrekking en beleidslijn hergebruik geo-informatie);
- gebruik binnen de werkprocessen en dienstverlening van de overheid (ontwikkeling van standaarden, richtlijnen en algemene principes voor dataverstrekking, prijsbeleid en gebruiksvoorwaarden, en geïntegreerd beleid voor geo-informatie-uitwisseling);
- verdere ontwikkeling en innovatie door overheid, bedrijfsleven en kennisinstellingen.

Het uitgangspunt van de basisvoorziening geo-informatie is 'eenmalig vastleggen, meervoudig gebruiken'. Met de basisvoorziening geo-informatie wordt verder aangesloten bij principes zoals neergelegd in de INSPIRE-richtlijn en NORA en de standaarden op basis van het Framework van geo-standaarden van Geonovum. Voor wat betreft de randvoorwaardelijke context bestaat een brede kijk op interoperabiliteit (beleidsmatig, organisatorisch, juridisch en technisch). Interoperabiliteit wordt daarbij gedefinieerd als ‘het vermogen van een bepaald systeem (in brede zin) [om] effectief of correct te functioneren als deel van een ander systeem’, waarbij met name wordt gerefereerd aan de ontwikkeling van standaarden zoals in het kader van het Framework van geo-standaarden is gebeurd.[342] Dit laatste duidt weer vooral op een technische oriëntatie ten aanzien van het concept 'interoperabiliteit'.

Naar verwachting krijgen ook de (bestaande en toekomstige) geo-informatiebasisregistraties (adressen, gebouwen, Kadaster en topografie, GBKN, BRON) een plaats binnen het GIDEON-programma.

Knelpunten
In deze paragraaf wordt een overzicht gegeven van de knelpunten voor de uitwisseling van geo-informatie die in het kader van het onderzoek naar voren zijn gekomen.

Zoals hiervoor reeds werd aangegeven is de complexiteit binnen het geo-informatieveld om uiteenlopende redenen zeer groot. Zo is er een uiterst gevarieerd aanbod en een groot aantal betrokkenen met hun (soms aanzienlijke) belangen. Als mogelijke verbeteringen worden in dit verband gezien het concentreren van activiteiten en verkleinen van het aanbod. Er zijn te dien aanzien momenteel twee trends relevant. Ten eerste zie je dat marktpartijen op eigen initiatief en risico grote registraties starten en uiteindelijk de beste “wint” (bijvoorbeeld Navtec, Tele-atlas). Ten tweede ontstaan er zogeheten shared services (bijvoorbeeld bij de waterschappen, rijksdiensten en het Kadaster (laatstgenoemde ontsluit bepaalde informatie namens gemeenten die bronhouder zijn en blijven).

[340] GIDEON – Basisvoorziening geo-informatie Nederland, Visie en implementatiestrategie (2008-2011), Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu, April 2008.
[341] Ibid., p. 14.
[342] GIDEON, supra, p. 22.

Door het enorme aanbod is het overzicht zoek. Nederland heeft wat dat betreft een duidelijke achterstand ten opzichte van andere landen, zoals Zweden, Denemarken en Duitsland. Voor een deel wordt deze situatie geweten aan het ontbreken van regels. Wetgeving kan stimulerend werken door partijen te verplichten tot samenwerking of elektronische toegang tot informatie te realiseren (neem bijvoorbeeld de Wet ruimtelijke ordening die nu verplicht tot het digitaal beschikbaar stellen van bestemmingsplannen waardoor dit eindelijk van grond komt). In dat verband kan het ook van belang zijn dat de wet sancties stelt op het niet voldoen aan daarin neergelegde verplichtingen. Een van de respondenten merkte op: ‘zonder sanctie, geen actie’, ofschoon er ook door middel van goodwill en PR veel kan worden bereikt. Overigens wordt het als positief ervaren dat de bereidheid tot samenwerken op het terrein van de geo-informatie in Nederland erg groot is en er geen visieverschillen bestaan. Wel is er discussie met betrekking tot de nauwkeurigheid, actualiteit en het begrijpen van elkaars gegevens in interne gegevensbestanden.

Het inwinnen van geo-informatie is procesgebonden en wordt bepaald vanuit dat (interne) proces, terwijl in toenemende mate uitwisseling extern tot stand moet komen. Front offices zijn vaak echter nog niet toegerust voor die externe geo-informatieuitwisseling.

Gegevens worden vaak uit eigen business betaald en dat kan – naast diensten tegen verstrekkingskosten - ook leiden tot duurdere tariefgefinancierde diensten (voorbeeld Kadaster). De daaruit resulterende relatief hoge kosten kunnen een belemmering vormen voor kleinere overheden om hiervan gebruik te maken en aanleiding zijn om eigen registers aan te houden. Er is overigens binnen VROM wel een ontwikkeling om toe te werken naar een budgetfinancieringsmodel, waardoor het probleem zou kunnen worden verholpen.

Een van de respondenten beschouwt de beperkte beschikbaarheid van metadata en het feit dat deze niet is gekoppeld aan documenten als een groot probleem. De houder van de geo-informatie is verantwoordelijkheid voor de koppeling, maar dit ook meer centraal gefaciliteerd moeten worden. Ook in dit geval wordt aangegeven dat wet-en regelgeving kunnen bijdragen aan de oplossing voor het probleem door het als drukmiddel in te zetten. Ook zou met wet-en regelgeving ruimte worden geboden voor ondersteuning. Door regelgeving te ontwikkelen, geeft de centrale overheid er tevens blijk van dat het onderwerp belangrijk wordt gevonden.

Zoals hierover werd aangegeven worden de knelpunten in de samenwerking op het terrein van geo-informatie met name gevoeld op organisatorisch vlak. Niettemin zijn binnen het onderzoek ook knelpunten naar voren gekomen die nadrukkelijk in verband worden gebracht met wet- en regelgeving.

In het kader van de wetgeving voor basisregistraties vraagt een van de respondenten zich af of de consequenties voor hergebruik van geo-informatie voldoende zijn doordacht. De wetgeving is erg gericht op de achterkant van de e-overheid (voor alles één registratie) maar minder op de vraag hoe overheden die de gegevens in hun ‘business’ gebruiken er in de praktijk mee omgaan. De INSPIRE-richtlijn gaat in dit verband verder door zich niet alleen te richten op het ontwikkelen van standaarden en basisprincipes maar ook door het publiceren van gegevens te regelen. Overigens lopen de meningen over de mogelijke impact van INSPIRE uiteen. Enerzijds wordt de richtlijn beschouwt als een impuls om in ieder geval tussen de overheden een doorbraak met betrekking tot het hergebruik van geo-informatie te bewerkstelligen. Anderzijds wordt ook opgemerkt dat INSPIRE op detailniveau nog weinig duidelijkheid biedt en onvoldoende verantwoordelijkheden bij de implementerende lidstaten legt, waardoor het nog maar de vraag is of het de gewenste stok achter deur is. Veel van het effect dat INSPIRE zal hebben op de uitwisseling van geo-informatie zal uiteindelijk met name afhangen van de invoeringsregels waarmee de Europese richtlijn wordt geïmplementeerd.

Er bestaat volgens een respondent behoefte aan operationele uitspraken van de rechter over verstrekking van geo-informatie aan de markt. Bedrijven staan echter huiverig tegenover het aanspannen van procedures tegen de overheid, omdat ze ook afhankelijk zijn van samenwerking met diezelfde overheid. Bovendien zouden de Aanwijzingen Markt en Overheid[343] onvoldoende houvast bieden voor de afweging of de overheid zich met haar activiteiten al dan niet teveel richt op het terrein van de private sector. Al met al ontbreekt een heldere rolverdeling tussen markt en overheid.

Samenhangend met het voorgaande punt bestaat er volgens dezelfde respondent ook bij de overheid behoefte aan meer duidelijkheid omtrent aansprakelijkheid. De risico's worden momenteel als dusdanig onduidelijk ervaren dat dit aan de toegang tot geo-informatie in de weg staat. De overheid zou het er volgens een van de respondenten in de praktijk gewoon op aan moeten laten komen om te kijken wat er gebeurt. Een voorbeeld is de intentie bij sommige overheden om informatie vrij te geven (bijvoorbeeld het nationaal wegenbestand door Rijkswaterstaat) teneinde innovatie te stimuleren. De onduidelijkheid bestaat erin dat men moeilijk kan inschatten of dit tot claims zal leiden van bedrijven die eerder veel geld hebben betaald voor deze informatie.

De verschillen in wet- en regelgeving ten aanzien van informatiebeveiliging voor verschillende sectoren/overheden kunnen volgens een van de respondenten belemmerend werken in het realiseren van samenwerking of resulteren zelfs in een vijandelijke opstelling als het gaat om het uitwisselen van informatie. Een voorbeeld is de rampenbestrijding, waarin gemeenten, brandweer, politie en Rijkswaterstaat samen moeten werken, maar de uiteenlopende informatiebeveiligingsregels (verschillende standaarden en voorschriften per sector) problemen opleveren. Bovendien zijn dergelijke diensten autonoom en is er vaak alleen op hoog niveau beslissingsbevoegdheid (bijv. op het niveau van de Secretaris-Generaal) om samenwerking van de grond te krijgen. Toevallig is het domein van de veiligheid toch een succesverhaal geworden, omdat het goed te verkopen valt (anders vallen er (meer) doden). Een ander voorbeeld is de beoordeling van een subsidieaanvraag (bijvoorbeeld voor natuurvriendelijk boeren) waarbij gegevens van andere overheden noodzakelijk zijn. Het noodzakelijke real-time opvragen van dergelijke gegevens is in strijd met informatiebeveiligingsregels, zodat er alleen een jaarlijkse kopie van de database mag worden verstrekt met alle (kwaliteits)risico's van dien.

In tegenstelling tot andere landen wordt in Nederland, zo een van de respondenten, de regelgeving betreffende luchtkartering sinds ongeveer 5 jaar streng gehandhaafd. Zo zou Nederland als enige land verzocht hebben om het afschermen van militaire terreinen in Google Earth. Overigens geeft de Militaire Inlichtingen- en Veiligheidsdienst in de NRC aan dat dit soort maatregelen voor sommige objecten mogelijk achterhaald is en zou Google Earth, volgens datzelfde bericht, ook zelfcensuur toepassen.[344] Naar aanleiding van het bericht *Internet helpt terrorist* in het Algemeen Dagblad[345] hebben de VVD en PVDA in 2005 kamervragen gesteld aan Minister Donner over de zichtbaarheid van kerncentrales in Google Earth en de mogelijke veiligheidsrisico's in het licht van terroristische aanslagen. De Minister zag geen reden om maatregelen te nemen, aangezien deze informatie ook langs andere weg reeds publiekelijk beschikbaar is.[346]

---

[343] Vaststelling Aanwijzingen inzake verrichten marktactiviteiten door organisaties binnen de rijksdienst, *Stcrt*. 1998, nr. 95, p. 8.
[344] NRC, *Inlichtingendienst onderzoekt concurrent Google Earth*, 7 januari 2008.
[345] Bericht van 11 augustus 2005.
[346] Kamerstukken II, 2005-2006, 16 augustus 2005, Aanhangsel.

Conclusies
De knelpunten voor de uitwisseling van geo-informatie blijken op basis van dit onderzoek voornamelijk op het organisatorische vlak te liggen. Verschillende organisaties met uiteenlopende culturen moeten het vermogen en de bereidheid hebben om met elkaar samen te werken.

Wet- en regelgeving kunnen een stimulerende rol vervullen door de urgentie om tot samenwerking te komen te versterken bij partijen. Dit kan op basis van meer zachte factoren als goodwill en PR of op basis van onderlinge afspraken, maar in enkele specifieke gevallen en ook meer algemeen wordt aangegeven dat daar waar wetgeving noodzakelijk is deze niet al te vrijblijvend moet worden geformuleerd. Met andere woorden, wettelijke verplichtingen voorzien van sancties kunnen noodzakelijk zijn om de samenwerking op een professionele manier van de grond te krijgen. Nederland heeft wat dat betreft nog een weg te gaan op het terrein van de uitwisseling van geo-informatie. Mogelijk dat INSPIRE in dat verband een belangrijke rol zal vervullen, alhoewel de meningen daarover niet onverdeeld positief zijn. Veel zal afhangen van de wijze waarop de richtlijn zal worden geïmplementeerd in Nederland.

Overigens zijn er ook nog wel enkele aandachtspunten als het gaat om het juridisch kader voor de samenwerking in de uitwisseling van geo-informatie. Op dit moment bestaat er onduidelijkheid omtrent de aansprakelijkheid van de overheid ten aanzien van het vrij beschikbaar stellen van geo-informatie. Bovendien hebben de Europese en Amsterdamse rechter de databankenrechtelijke bescherming van met publieke gelden gefinancierde databanken onderuit gehaald. Voor overheden een letterlijke streep door rekening, maar tegelijkertijd zijn de uitspraken in lijn met de uitgangspunten van de Wob. Verder zal er natuurlijk steeds voldoende aandacht moeten zijn voor de privacy-aspecten en ook eventuele veiligheidsrisico's van geo-informatie die opvraagbaar wordt. Een reëel juridisch knelpunt voor samenwerking lijkt momenteel te bestaan op het punt van de onderling verschillende informatiebeveiligingsregelingen binnen de overheid.

4 Knelpunten en hiaten

4.1 Inleiding

In dit hoofdstuk worden de knelpunten en hiaten, zoals die naar voren zijn gekomen bij de analyse en de case studies, op een rij gezet. In paragraaf 4.2 worden de knelpunten en hiaten naar aanleiding van de analyse van de wet- en regelgeving weergegeven. Paragraaf 4.3 bevat de knelpunten en hiaten die uit de case studies naar voren zijn gekomen.

4.2 Knelpunten en hiaten uit de analyse van de wet- en regelgeving

In zijn algemeenheid kan worden geconcludeerd dat bestaande wet- en regelgeving als zodanig op het eerste gezicht geen daadwerkelijke knelpunten dan wel hiaten vertonen ten aanzien van het onderwerp van onderzoek. Dat neemt niet weg dat aansluitend in het case-study onderzoek nog wel enkele juridische knelpunten en hiaten naar voren zullen komen. Op deze plaats wordt echter wel reeds een tweetal juridische aandachtspunten vermeld.

Elektronisch bestuurlijk verkeer en de elektronische handtekening

Het juridisch kader met betrekking tot gebruik van elektronische handtekeningen bestaat in eerste instantie uit de norm van een betrouwbare en vertrouwelijke communicatie zoals vervat in de Wet elektronisch bestuurlijk verkeer (Webv). Een bestuursorgaan dient aan de hand van deze norm beleid vaststellen inzake de vraag op welke wijze zij langs elektronische weg communiceert. De wijze waarop wordt omgegaan met vormvereisten en elektronische handtekeningen kan in dat beleid worden omschreven. De gelijkstellingsbepaling van de Wet elektronische handtekeningen (Weh), en het op grond van de Weh geldende vermoeden van voldoende betrouwbaarheid, spelen een ondergeschikte rol ten opzichte van de norm van een betrouwbare en vertrouwelijke communicatie. Zij betreffen immers één methode (van de velen) waarop het bestuursorgaan de norm kan invullen. Toch lijkt de Weh een meer prominente rol te worden toegedicht dat vanuit juridisch perspectief gerechtvaardigd is. Bijvoorbeeld het gebruik van DigiD kan juridisch worden gezien als het elektronisch zetten van een handtekening, indien een bestuursorgaan daartoe besluit.. Het bestuursorgaan zou dan invulling geven aan de norm van een betrouwbare en vertrouwelijke communicatie en tegelijkertijd aangeven hoe op elektronische wijze aan een vormvereiste kan worden voldaan (bijvoorbeeld het vereiste van ondertekening bij de belastingaangifte). De Weh speelt hierbij nauwelijks of niet een rol.

PKIoverheid is een voorbeeld van een situatie waarin wordt aangesloten bij de eisen van de Weh. Juridisch gezien levert dit het voordeel op dat een elektronische handtekening automatisch wordt vermoed voldoende betrouwbaar te zijn om gelijkgesteld te kunnen worden met een handgeschreven handtekening. Een ander aan de Weh klevend knelpunt dat hier gesignaleerd kan worden, houdt in dat er wordt gesproken van ‘dezelfde rechtsgevolgen als de handgeschreven handtekening’, zonder dat duidelijk is op welke rechtsgevolgen wordt gedoeld. Dit heeft tot gevolg dat op de website van PKIoverheid wordt geclaimd dat met een PKIoverheid-certificaat een ‘rechtsgeldige’ elektronische handtekening kan worden gezet, zonder dat duidelijk is op wat voor ‘rechtsgeldigheid’ wordt gedoeld. De Weh lijkt hier dan ook eerder tot onduidelijkheid dan de beoogde rechtszekerheid te hebben geleid. Bovendien lijkt bij PKIoverheid de elektronische handtekening, die is gebaseerd op een *Public Key Infrastructure*, zoals beschreven in de Weh (en de onderliggende regelgeving), van een middel tot een doel op zich te zijn verworden. Er wordt immers aan alle vereisten voortvloeiend uit de Weh voldaan, toch is niet zonder meer duidelijk wat er ‘rechtsgeldig’ is aan een handtekening gezet met een PKIoverheid-certificaat.

Randvoorwaarden voor de beschikbaarheid van overheidsinformatie
Ten aanzien van de beschikbaarheid van overheidsinformatie, valt een aantal opmerkingen te maken. In de eerste plaats blijkt uit recente rechterlijke uitspraken dat de overheid op dit moment geen databankrechthebbende kan zijn. Op grond van de Databankenwet komt het databankenrecht toe aan de *producent*. De wet definieert de producent van een databank als *degene die het risico draagt van de voor de databank te maken investering*. Een overheidsorgaan zal in de regel met overheidsgelden een databank realiseren. Het is daarom de vraag of er een investeringsrisico wordt gedragen en een overheidsorgaan vervolgens kan worden aangemerkt als producent. Op basis van recente Europese en Nederlandse rechtspraak moet worden geconcludeerd dat op dit moment overheden in de regel geen databankrechthebbende zijn en dat voor de burger een beroep op de hergebruikregeling van de Wob derhalve niet nodig is om over de informatie te kunnen beschikken. Ofschoon dit in lijn zou zijn met de Wob, kan het voor overheden letterlijk een streep door de rekening zijn.

Ten tweede valt op dat de Wob twee regimes kent: het regime van de passieve en de actieve openbaarmaking en het regime is de hergebruikregeling. Volgens het eerste regime is de overheid niet verplicht de informatie op elektronische wijze openbaar te maken. Volgens het tweede regime worden document slechts ‘zoveel mogelijk’ langs elektronische weg beschikbaar gesteld.
Ten aanzien van de hergebruikregeling valt op zij niet van toepassing is op informatie waarop de overheid geen auteursrecht of databankenrecht kan doen gelden. In combinatie met de ontwikkeling dat de overheid niet als databankrechthebbende kan worden aangemerkt, leidt dit tot de vraag of informatie die door de overheid wordt geproduceerd en waarvan werd aangenomen dat de overheid er een databankenrecht op kon doen gelden, nu niet meer in het kader van de hergebruikregeling kan worden opgevraagd.

Een derde punt van aandacht is invloed van de INSPIRE-richtlijn op de vergoedingen die de overheid kan vragen voor het te beschikking stellen van ruimtelijke informatie. Op grond van de Wob kan de overheid in een ‘redelijk rendement’ voorzien. De INSPIRE-richtlijn schrijft voor dat het publiek kosteloos van de zoekdiensten en de raadpleegdiensten gebruik dient te kunnen maken. In afwijking hierop kan de overheid voor raadpleegdiensten vergoedingen in rekening brengen, indien de vergoedingen ervoor zorgen dat de verzamelingen ruimtelijke gegevens en de betreffende diensten in stand worden gehouden, met name ingeval van zeer grote hoeveelheden *real time*-gegevens. Ten aanzien van de uitwisseling van ruimtelijke informatie met andere overheidinstanties stelt de INSPIRE-richtlijn dat een vergunning en/of een vergoeding kan worden verlangd. Ingeval een vergoeding wordt gevraagd, dient deze beperkt te blijven tot het minimum dat nodig is om de noodzakelijke kwaliteit en beschikbaarheid van verzamelingen ruimtelijke informatie en de diensten te garanderen. Dit minimum mag worden vermeerder met een redelijk rendement op de investering, in voorkomend geval met inachtneming van de vereisten inzake zelffinanciering van de overheidsdiensten die verzamelingen ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens verstrekken. Er mag in geen geval betaling worden verlangd voor ruimtelijke informatie die overheidsinstanties nodig hebben ter vervulling van hun verplichtingen inzake verslaglegging op grond van EU-wetgeving inzake het milieu.

Verplicht gebruikt gesloten standaarden
In de behandelde regelgeving wordt af en toe het gebruik van gesloten standaarden verplicht gesteld. Het betreft de Regeling geordende en toegankelijke staat archiefbescheiden en de concept-regelgeving die eisen stelt aan de indiening van een aanvraag van een omgevingsvergunning.

Gevolgen INSPIRE-richtlijn voor financieringsstructuren ruimtelijke informatie

Het is op het moment nog niet duidelijk wat de gevolgen zullen zijn van de INSPIRE-richtlijn. De richtlijn schrijft voor dat de EU-lidstaten een infrastructuur moeten oprichten en exploiteren. Het netwerk dient te bestaan uit een aantal diensten met betrekking tot ruimtelijke informatie. Hiermee schrijft de richtlijn voor op welke wijze en onder welke voorwaarden ruimtelijke informatie beschikbaar dient te worden gesteld. De op te richten infrastructuur dient te bestaan uit een aantal diensten. Twee van deze diensten, de 'zoekdiensten' en de 'raadpleegdiensten', dienen kosteloos aan het publiek ter beschikking te worden gesteld. Ten aanzien van de overige diensten (onder meer de 'downloaddiensten' en de 'verwerkingsdiensten'), mag de overheid vergoedingen in rekening brengen, indien de vergoedingen ervoor zorgen dat de verzamelingen ruimtelijke informatie en de INSPIRE-diensten in stand worden gehouden, met namen ingeval van zeer grote hoeveelheden *real-time* informatie. De precieze gevolgen voor de wijze waarop in Nederland ruimtelijke informatie wordt gedeeld, zijn op dit moment nog niet duidelijk. Er worden in elk geval grenzen gesteld aan de vergoedingen die de overheid mag vragen voor het ter beschikking stellen van ruimtelijke informatie.

4.3 Knelpunten en hiaten uit de *case studies*

Omgang met persoonsgegevens

De omgang met persoonsgegevens wordt in de *case studies* als belemmerend ervaren. Er kunnen hier een vijftal onderwerpen worden aangewezen. Het gaat om:

- onduidelijk omtrent de betekenis van wettelijke voorschriften;
- het doelbindingsbeginsel;
- het transparantiebeginsel;
- het openbaarmaken van gegevens via het internet;
- de omgang met onjuiste gegevens; en
- de 'eigendom' van persoonsgegevens.

Onduidelijkheid betekenis voorschriften

Er is onduidelijkheid over de betekenis van de wettelijke voorschriften inzake persoonsgegevens, en over de wijze waarop zij dienen te worden toegepast. In een enkel geval (ePV) wordt gesteld dat de wet te weinig ruimte biedt voor het verwerker van persoonsgegevens (onder meer ten aanzien van veelplegers), waardoor men in de praktijk bijvoorbeeld met convenanten of verklaringen van betrokkenen moet werken. Ten aanzien van die laatste oplossing (de verklaring van betrokkene) is onduidelijk of dit een voldoende juridische grondslag oplevert om de verwerking mogelijk te maken.

Doelbinding

In de praktijk wordt het doelbindingsbeginsel van de Wbp als knelpunt ervaren. Dit beginsel brengt met zich mee dat de verantwoordelijke voor de gegevensverwerking de gerechtvaardigde doeleinden van de verwerking vaststelt en deze uitdrukkelijk omschrijft. Dat betekent dat organisatie ermee aan de slag moeten: en moet een gegronde reden worden opgegeven op persoonsgegevens te verwerken. Het is de vraag of dit knelpunt verholpen kan of dient te worden. De wetgeving inzake de bescherming van persoonsgegevens er juist toe om ongegronde verwerkingen tegen te gaan. Ketenpartijen moeten zich er van bewust worden dat gegevensuitwisseling geen doel op zich kan zijn. De overheid kan partijen wel een handje helpen door doelbindingsbepalingen vast te leggen in wetgeving, zoals dat ook is gedaan bij de Wet SUWI.

Transparantie

Het is noodzakelijk voor de partijen om zo transparant mogelijk te werken en processen van gegevensverwerking voor de burger inzichtelijk te maken. Alleen dan kan de burger namelijk actief zijn rechten op correctie, wijziging, verwijdering of verzet inroepen. Ook voorkomt een

transparant proces dat burgers niet weten bij welk 'loket' ze moeten zijn indien er problemen zijn. Het verdient dan ook aanbeveling om het organisatieproces zelf meer privacygericht in te richten. Dit oppert het CBP ook als het spreekt over 'privacy by design';[347] het incorporeren van privacyvraagstukken in de ontwikkelingen van (beleids)processen.

Openbaarmaking van persoonsgegevens via het internet
Gegevens over burgers kunnen niet zomaar via het internet openbaar gemaakt worden. Dit blijkt problematisch als het gaat om bijvoorbeeld bouwaanvragen en bouwbeschikkingen die ter inzage worden gelegd via het internet. Het is een knelpunt dat ontstaat tussen de Wob en de Wbp en wordt gevoed door openbaarmaking via het internet. Openbaarmaking via het internet houdt immers in dat de openbaarmaking op veel grotere schaal plaats vindt dan wanneer een stuk ter inzage op het gemeentehuis wordt gelegd. Overheidsinstanties worden in een dergelijk geval gedwongen om een afweging te maken tussen hun plicht tot actieve openbaarmaking en de Wbp. Het aanvragen van een bouwvergunning brengt immers persoonsgegevens mee die op grond van de Wob[348] niet openbaar gemaakt zouden mogen worden tenzij er geen sprake is van een kennelijke inbreuk. Het is echter van belang bij een bouwvergunning dat persoonsgegevens zoals een adres wel bekend zijn, teneinde bezwaar te kunnen maken tegen de bouwaanvraag of het de beschikking tot verlening van vergunning. Dergelijke openbaarmaking moet dan beschouwd worden als kennelijk niet inbreukmakend.

Het CBP geeft in de richtsnoeren 'Actieve openbaarmaking van persoonsgegevens'[349] een aantal handreikingen voor de overheid indien persoonsgegevens via internet openbaar gemaakt worden:

- bestuursorganen mogen in het algemeen persoonsgegevens niet via internet openbaar maken op grond van de Wet openbaarheid van bestuur;
- bestuursorganen moeten het belang van openbaarmaking via internet afwegen tegen de risico's waarmee dat gepaard gaat;
- bestuursorganen moeten burgers beter informeren en ze in de gelegenheid stellen om bezwaar te maken tegen openbaarmaking;
- bestuursorganen moeten openbaar gemaakte gegevens beveiligen, in het bijzonder door ze af te schermen voor zoekmachines;
- identificatienummers zoals het sofinummer of het burgerservicenummer vergemakkelijken de koppeling van verschillende bestanden en vormen dus een extra bedreiging. Bovendien mogen volgens artikel 24 Wbp wettelijk voorgeschreven nummers ter identificatie van personen alleen worden gebruikt voor de uitvoering van de betreffende wet of voor doeleinden die bij de wet zijn bepaald. In de praktijk betekent dit dat het niet is toegestaan om dergelijke nummers op internet te publiceren, ook niet met toestemming van de betrokkene.[350]

De verhouding tussen Wob en Wbp zou beter mogen worden gepositioneerd, teneinde het voor overheidsinstanties makkelijker te maken bij de beoordeling of openbaarmaking van persoonsgegevens kennelijk inbreukmakend is. De richtsnoeren 'Actieve openbaarmaking van

[347] WWW <http://www.cbpweb.nl/themadossiers/th_pbd_start.shtml>.
[348] Artikel 10 sub d Wob.
[349] CBP, *Actieve openbaarmaking van persoonsgegevens*, CBP richtsnoeren, maart 2008, beschikbaar via WWW <http://www.cbpweb.nl/downloads_rs/rs_conc_Actieve_openbaarmaking.pdf >. Zie ook: CBP, publicatie van persoonsgegevens op internet, CBP richtsnoeren, december 2007, beschikbaar via WWW <http://www.cbpweb.nl/downloads_rs/rs_20071211_persoons gegevens_op_internet_definitief.pdf >.
[350] WWW <http://www.cbpweb.nl/documenten/pb_20080402_conceptrichtsnoeren.shtml>, laatst geraadpleegd 20 juni 2008.

persoonsgegevens' dragen daar aan bij, maar het zijn "slechts" richtsnoeren en nog steeds moet de toch moeilijke afweging gemaakt worden door de openbaar makende instantie.

Onjuiste gegevens
De toepassingen van de e-Overheid maken het mogelijk dat steeds meer persoonsgegevens worden verzameld en verder verwerkt binnen de overheid. Het makkelijker beschikbaar worden van persoonsgegevens binnen de overheid, vergroot de kans dat onjuiste persoonsgegevens zich ongecorrigeerd snel verspreiden binnen de overheid.

Indien de Nederlandse burger het verwerken van onjuiste gegevens door de overheid wil tegengaan, dan is hij daartoe in beginsel aangewezen op zijn rechten op inzage, correctie en verzet, zoals vastgelegd in de Wbp of sectorale wetgeving zoals de Wet GBA. De burger zal hiermee echter achter de feiten aanlopen. Bovendien zal de burger vaak zelf moeten uitzoeken van welk onderdeel van de overheid de foutieve gegevens afkomstig zijn. Het huidige systeem om rechten van correctie, inzage en verzet te effectueren, zou hiermee niet meer toereikend kunnen zijn.

Als oplossing voor de problematiek wordt vaak aangedragen dat de burger zelf 'eigenaar' zou moeten zijn van de gegevens die op hem betrekking hebben. Vanuit juridisch perspectief verdient het aanbeveling om de term 'eigenaar' te vermijden, niet alleen omdat 'eigendom' al een vastomlijnde juridische betekenis[351] kent, maar ook omdat de precieze rolverdeling met betrekking tot de gegevens er niet duidelijk mee wordt omschreven. Er zou bedoeld kunnen worden dat de burger zelf zijn persoonsgegevens bijhoudt, en dat de overheid aan dat 'persoonlijke databankje' zou moeten toetsen of de door haar gebruikte gegeven kloppen. Dit legt echter wel een groot risico bij de burger neer: het zou namelijk kunnen betekenen dat hij zou moeten 'boeten' voor zijn eigen fouten. Een tweede punt van aandacht is of de burger zelf zou moeten kunnen bepalen of zijn persoonsgegevens überhaupt worden verwerkt. Die stelling dient te worden verworpen. De overheid moet de gegevens ook kunnen gebruiken als de burger dat niet wil.[352]
De verantwoordelijkheid bij de burger leggen is bovendien niet de enige mogelijkheid om het probleem op te lossen. Overheidsinstanties moeten immers instaan voor de kwaliteit van hun eigen datasets. Ontsluiting van gegevens moet alleen plaatsvinden op het moment dat gegevens van voldoende kwaliteit zijn. Ook moeten er afspraken zijn over de manier waarop moet worden omgegaan met ketenpartners die zich niet aan de kwaliteitsafspraken houden.

Open versus gesloten standaarden
De toepassing van gesloten standaarden zoals bijvoorbeeld in de Ministeriële regeling omgevingsrecht (MOR), is niet in lijn met de notitie 'Nederland in open verbinding' en met het algemene streven om meer met open standaarden te gaan werken. Indien open standaarden de norm moeten zijn, dan moeten ook wetgevingsinstrumenten, als Ministeriële regelingen, beleidsregels en algemene maatregelen van bestuur, daar rekening mee houden. Praktisch gezien wordt echter al wel aangesloten bij open standaarden (getuige de werkwijze van de Gemeente Tilburg, zie case study bouwloket / omgevingsloket) naast de wettelijk geregelde gesloten standaarden.

[351] 'Eigendom' is het meest omvattend recht dat een persoon op een zaak kan hebben, artikel 5:1 lid 1 BW. 'Zaken' zijn de voor menselijke beheersing vatbare stoffelijke objecten, artikel 3:3 lid 1 BW.
[352] Denk hierbij aan informatie betreffende bijvoorbeeld nationaliteit (artikel 1 sub a onder 4 Wet GBA) of curatele (artikel 1 sub a onder 1 Wet GBA).

Ontwikkelingstempo
Verschillende standaarden en modellen ontwikkelen zich in een eigen tempo. Dit heeft voor de betrokken organisaties tot gevolg dat interoperabiliteit, zelfs niet na de pilot-fase, vanzelfsprekend geacht kan worden. Het verdient aanbeveling om te zorgen voor helderheid rondom de uitwerking van standaarden voor e-overheidsapplicaties en de partijen te informeren over voorziene modellen en standaarden[353]. De onzekerheid dat er vertraging ontstaat in de beschikbaarheid van e-overheidsvoorzieningen kan hiermee niet worden weggenomen. Het verdient echter wel aanbeveling om pas landelijke implementatie van e-overheidsvoorzieningen toe te staan als de randvoorwaarden 'volwassen' genoeg zijn en de belangrijkste kinderziektes zijn verholpen. Dit staat wijzigingen die na landelijke uitrol plaatsvinden niet in de weg.

Auteursrecht
Het openbaar maken van gegevens via het internet, bijvoorbeeld door bouwtekeningen onbeperkt toegankelijk te maken via het bouwloket, kan een inbreuk op het auteursrecht opleveren. Er is immers geen sprake van het maken van een kopie voor privé-gebruik, wanneer een tekening volledig openbaar beschikbaar is.[354] Een dergelijke inbreuk kan dan de openbaar makende instantie worden aangerekend. Dergelijke grootschalige openbaarmaking van auteursrechtelijk beschermd materiaal vereist dan ook wettelijke verankering indien dit op deze wijze gewenst is. Indien dit niet gewenst is, dient er zorg te worden gedragen voor (technische) afscherming van grootschalige openbaarmaking.

Onderling uiteenlopende regelingen betreffende informatiebeveiliging
Een opvallend knelpunt in de geoinformatie-case zijn de uiteenlopende regelingen bij verschillende overheden op het terrein van informatiebeveiliging die de samenwerking belemmeren of op zijn minst vertragen.

Focus op back-office
Wetgeving voor basisregistraties is nu te veel gericht op de achterkant van de e-overheid (voor alles één registratie) en te weinig op de mogelijkheden in het licht van hergebruik van informatie. Dit in tegenstelling tot de INSPIRE-richtlijn die verder gaat door zich niet alleen te richten op het ontwikkelen van standaarden en basisprincipes maar ook door de publicatie van gegevens te regelen.

Onduidelijke rolverdeling tussen markt en overheid
In het kader van de uitwisseling van geo-informatie behoefte aan duidelijkheid over verstrekking van geo-informatie aan de markt. De Aanwijzing Markt en Overheid biedt onvoldoende houvast voor de afweging of de overheid zich met haar activiteiten al dan niet teveel richt op het terrein van de private sector. Al met al ontbreekt een heldere rolverdeling tussen markt en overheid.

Onduidelijkheid over aansprakelijkheid
Eveneens in het kader van de uitwisseling van geo-informatie bestaat behoefte aan meer duidelijkheid omtrent aansprakelijkheid wanneer de informatie voor vrijgegeven om innovatie te stimuleren. De vrees bestaat dat dit zal leiden tot claims door bedrijven die eerder veel geld hebben betaald voor deze informatie. De risico's worden momenteel als dusdanig onduidelijk ervaren dat dit aan de toegang tot geo-informatie in de weg staat.

[353] Onder meer op grond van een helder versiebeleid.
[354] Artikelen 10 en 12 juncto artikelen 16b en 16c Auteurswet.

5 Eisen en randvoorwaarden

Interoperabiliteit en wet-en regelgeving
Uit de beschrijving van de wet- en regelgeving blijkt dat interoperabiliteit als zodanig niet door de wetgever wordt geadresseerd. De behandelde wet- en regelgeving bevat wel eisen en randvoorwaarden ten aanzien van interoperabiliteit en de e-Overheid. Vaak betreft het open normen die nader dienen te worden ingevuld of beginselen waarvan moet worden uitgegaan, en daarmee ruimte bieden voor beleid waarin interoperabiliteit wel een zelfstandige rol toekomt. De Wet elektronisch bestuurlijk verkeer (Webv) kan hierbij als voorbeeld dienen. De Webv bevat de hoofdregels met betrekking tot de elektronische communicatie met de overheid. Wanneer een bestuursorgaan de e-Overheidsdiensten wil verlenen, heeft het meteen te maken met nevenschikking, kenbaarmaking en de norm van een voldoende betrouwbare en vertrouwelijke communicatie. De Webv biedt geen kant-en-klare voorschriften, maar geeft een kader dat bestuursorganen verder dienen in te vullen. Bestuursorganen dienen zich met name af te vragen:

- op welke wijze de openstelling van de elektronische weg kenbaar dient te worden gemaakt;
- op welke wijze de norm van een voldoende betrouwbare en vertrouwelijke communicatie in dient te worden gevuld. Hierbij dient het bestuursorgaan uit te gaan van de hierboven beschreven 'voldoende mate van betrouwbaarheid en vertrouwelijkheid'. Dit betekent dat elektronisch verkeer even betrouwbaar en vertrouwelijk dient te zijn als 'conventioneel verkeer'. Het bestuursorgaan kan de norm van een betrouwbare en vertrouwelijke communicatie invullen aan de hand van de beginselen van behoorlijk IT-gebruik.

Wet- en regelgeving: lappendeken
Eén en ander wordt bemoeilijkt door het feit dat het landschap van wet- en regelgeving eruit ziet als een lappendeken. De overheid zal zich daarom steeds weer moeten afvragen welke onderdelen, welke wetten en/of regelingen, in een bepaalde geval van toepassing zijn. Aan de hand van (een deel van) de behandelde wet- en regelgeving kan bijvoorbeeld het volgende schema worden opgesteld waarin de belangrijkste open normen, in de vorm van eisen en randvoorwaarden worden weergegeven. Binnen deze eisen en randvoorwaarden kan beleid inzake interoperabiliteit worden vormgegevens. Wel zal steeds moeten worden bepaald of een wet of regeling van toepassing is.

Voor zover er concrete eisen en randvoorwaarden uit de wet- en regelgeving zijn af te leiden, worden deze in onderstaande tabel weergegeven.

Wet of regeling	Eisen en randvoorwaarden

Wet elektronisch bestuurlijk verkeer (Webv)	• Nevenschikking
	• Voldoende betrouwbare en vertrouwelijke communicatie
	  ○ Deze norm moet met een beleidsregel worden ingevuld.
	  ○ Elektronisch verkeer moet even betrouwbaar en vertrouwelijk zijn als conventioneel verkeer.
	  ○ Algemene beginselen van behoorlijk IT-gebruik:
	  ▪ authenticiteit;
	  ▪ integriteit;
	  ▪ onweerlegbaarheid;
	  ▪ transparantie;
	  ▪ beschikbaarheid;
	  ▪ flexibiliteit;

	▪ vertrouwelijkheid. ○ De gelijkstellingsregel inzake de elektronische handtekening (artikel 2:16 Awb) is slechts een methode om de open norm van een betrouwbare en vertrouwelijke communicatie in te vullen. ○ Ga na welke rechtsgevolgen worden beoogd bij het gebruik van een elektronische handtekening.
Wet bescherming persoonsgegevens (Wbp)	• Stel de doeleinden voor de verwerking van persoonsgegevens vast en omschrijf deze uitdrukkelijk. • Verwerk alleen persoonsgegevens voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn. • Tref maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn. • Draag zorg voor voldoende inzichtelijkheid tegenover de betrokkene(n).
Wet algemene bepalingen burgerservicenummer (Wabb)	• Als overheidsorgaan: maak alleen gebruik van het BSN bij het verwerken van persoonsgegevens in het kader van de uitvoering van de taak. • Als niet-overheidsorgaan: maak alleen gebruik van het BSN indien dit bij of krachtens wet is voorgeschreven. • Gebruik alleen het BSN als persoonsnummer bij het uitwisselen van persoonsgegevens met een andere gebruiker in de zin van de Wabb. • Voldoe aan de vergewisplicht: vergewis je ervan dat het betreffende BSN daadwerkelijk betrekking heeft op de persoon wiens persoonsgegevens je verwerkt. • Verplicht degene aan wie een BSN is toegekend niet tot het verstrekken van een ander persoonsnummer dan het BSN. • Stel de verificatievragen indien dat nodig is ter uitvoering van de vergewisplicht of indien je daartoe bij of krachtens wet bent verplicht.
Wetgeving inzake basisregistraties	• Verplicht gebruik authentieke gegevens. • Een ingeschrevene mag weigeren een gegeven te verstrekken, indien die afnemer in het kader van het verplicht gebruik dit gegeven uit de betreffende basisregistratie dient te betrekken. De ingeschrevene kan zich hier niet op beroepen voor zover het gegeven noodzakelijk wordt geacht voor een deugdelijke vaststelling van de identiteit. • Voldoe aan de terugmeldplicht.

Wet als drukmiddel
In het licht van het realiseren van interoperabiliteit kan de wet als zodanig (dus los van de her en der neergelegde afzonderlijke eisen en randvoorwaarden) een belangrijke functie hebben door als drukmiddel voor het bewerkstelligen van samenwerking tussen de verschillende partijen in de keten te worden ingezet. Bij het DKD is bijvoorbeeld duidelijk te zien dat door het bestaan van een wettelijke verplichting nagenoeg alle partijen op tijd klaar zijn voor de landelijke uitrol van het DKD. Maar ook in de andere cases word gerefereerd aan het belang van wetgeving als drukmiddel.

In regelgeving kunnen bovendien stimuleringsregelingen en sancties worden opgenomen om de verwezenlijking van het samenwerkingsdoel kracht bij te zetten.

Voorts zou een minder vrijblijvende opstelling ten opzichte van e-overheidsmodules (zie case study bouwloket / omgevingsloket omtrent de ‘dossiermodule’) kunnen bijdragen aan verbeterde interoperabiliteit binnen de elektronische overheid. De huidige situatie laat vaak

nog veel ruimte aan overheden om eigen applicaties te ontwikkelen die wellicht niet goed aansluiten bij het interoperabiliteitsraamwerk. In het kader van unifomiteit in de dienstverlening richting de burger is het aan te bevelen zoveel mogelijk algemene producten te ontwikkelen die dan zo nodig verplicht worden gebruikt.

Wetgeving zou met het oog op rechtszekerheid en ter stimulering van de samenwerking overigens wel in een (zo) vroegtijdig stadium moet worden gerealiseerd. Partijen kunnen namelijk een afwachtende houding aannemen, wanneer wettelijke regels (inclusief procedures en handreikingen) nog niet bekend zijn, waardoor veel tijd verloren gaat.

6 Conclusies en aanbevelingen

6.1 Inleiding

In dit rapport zijn de juridische randvoorwaarden geschetst ten aanzien van de e-Overheid en een interoperabiliteitsraamwerk. Het is duidelijk dat interoperabiliteit als zodanig (nog) niet direct door de wetgever wordt geadresseerd. In het voorgaande is een overzicht gegeven van de meest in het oog springende wetgeving die randvoorwaardelijk is voor een interoperabiliteitsraamwerk. Daarnaast kan er, afhankelijk van het specifieke domein, nadere wet- en regelgeving relevant zijn, zoals bijvoorbeeld de WABO (digitaal omgevingsloket) en de Wet SUWI (digitaal klantdossier). Voor zover relevant in het kader van de onderzochte cases is de wet- en regelgeving in het overzicht meegenomen. Over het geheel beschouwd bevat deze wet- en regelgeving belangrijke eisen en randvoorwaarden voor het inrichten van de elektronische overheid en meer in het bijzonder interoperabiliteit in e-overheidprocessen tussen verschillende organisaties. Zo moet de gegevensuitwisseling voldoen aan de beginselen van de Wbp (o.a. transparantie, doelbinding, dataminimalisatie). Zo is het transparantiebeginsel goed terug te zien bij de landkaart e-Overheid en komt de discussie over doelbinding bij ontwikkeling van nieuwe e-Overheidsproducten steeds weer op gang (zie bijvoorbeeld de case study DKD).

In deze studie is tevens onderzocht in hoeverre het voornoemde wettelijk kader knelpunten en hiaten oplevert voor interoperabiliteit e-overheidprocessen tussen de verschillende organisaties. In zijn algemeenheid kan worden geconcludeerd dat het wettelijk kader als zodanig slechts in enkele uitzonderingsgevallen knelpunten dan wel hiaten vertoont ten aanzien van het onderwerp van onderzoek. De knelpunten en hiaten worden in de volgende paragraaf besproken Daarnaast zijn er enkele aandachtspunten op basis van het wettelijk kader die vermelding verdienen. Enerzijds zijn dit aandachtspunten die rechtstreeks voortkomen uit het wettelijk kader; anderzijds laat het onderzoek aandachtspunten zien die vooral de uitvoeringspraktijk betreffen maar voldoende verband houden met de behandelde wet- en regelgeving om ze hier te noemen. Na een beknopte behandeling van de knelpunten/hiaten en de aandachtspunten, wordt afgesloten met een lijst met aanbevelingen die uit het onderzoek resulteren.

6.2 Juridische knelpunten en hiaten

Omgang met persoonsgegevens

Een knelpunt ten aanzien van de omgang met persoonsgegevens kan zich voordoen ten aanzien van de verwerking van onjuiste gegevens. De toepassingen van de e-Overheid maken het mogelijk dat steeds meer persoonsgegevens worden verzameld en verder verwerkt binnen de overheid en dit vergroot de kans op de verspreiding van onjuiste persoonsgegevens binnen de overheid. Met de rechten op inzage, correctie en verzet die de Wbp biedt, loopt de burger echter achter de feiten aan. Bovendien zal de burger vaak zelf moeten uitzoeken van welk overheidsonderdeel de foutieve gegevens afkomstig zijn. Het huidige systeem zoals neergelegd in de Wbp is met het oog op de bescherming van de burger, zou in de nabije toekomst onvoldoende toereikend kunnen zijn.

Databankenwet

De Databankenwet definieert de producent van een databank als degene die het risico draagt van de voor de databank te maken investering. Een overheidsorgaan zal in de regel met overheidsgelden een databank realiseren. Het is daarom de vraag of er een investeringsrisico wordt gedragen en een overheidsorgaan vervolgens kan worden aangemerkt als producent. Ofschoon deze benadering in lijn is met de Wob, zullen overheidsorganen het ‘wegvallen’ van

het databankenrecht als probleem ervaren. Zij zullen immers minder te zeggen hebben over 'hun' informatie.

Auteurswet
Het openbaar maken van gegevens van derden via het internet, bijvoorbeeld door bouwtekeningen onbeperkt toegankelijk te maken via het bouwloket, kan een inbreuk op het auteursrecht opleveren. Er is immers geen sprake van het maken van een kopie voor privé-gebruik, wanneer een tekening volledig openbaar beschikbaar is.[355] Een dergelijke inbreuk kan dan de openbaar makende instantie aangerekend worden. Dergelijke grootschalige openbaarmaking van auteursrechtelijk beschermd materiaal vereist dan ook wettelijke verankering indien dit op deze wijze gewenst is. Indien dit niet gewenst is dient er zorg gedragen te worden voor (technische) afscherming van grootschalige openbaarmaking.

Onduidelijkheid over aansprakelijkheid
In het kader van de uitwisseling van geo-informatie bestaat behoefte aan meer duidelijkheid omtrent aansprakelijkheid wanneer de informatie wordt vrijgegeven om innovatie te stimuleren. De vrees bestaat dat dit zal leiden tot claims door bedrijven die eerder veel geld hebben betaald voor deze informatie. De risico's worden momenteel als dusdanig onduidelijk ervaren dat dit aan de toegang tot geo-informatie in de weg staat. Het gaat in het kader van deze studie te ver om een inschatting te geven van de mogelijke risico's in dit verband en uiteindelijk biedt alleen een rechterlijke uitspraak pas daadwerkelijke duidelijkheid. In het onderzoek is geopperd dat overheden in het er in het maatschappelijk belang maar op aan moeten laten komen en niettemin informatie zoveel mogelijk dienen vrij te geven.

Focus op back-office
Eveneens in het kader van de uitwisseling van geo-informatie werd aangegeven dat wetgeving voor basisregistraties te veel gericht is op de achterkant van de e-overheid (voor alles één registratie) en te weinig op de mogelijkheden in het licht van het hergebruik van informatie. Dit in tegenstelling tot de INSPIRE-richtlijn die verder gaat door zich niet alleen te richten op het ontwikkelen van standaarden en basisprincipes maar ook door de publicatie van gegevens te regelen.

Onduidelijke rolverdeling tussen markt en overheid
In het kader van de uitwisseling van geo-informatie bestaat behoefte aan duidelijkheid over verstrekking van geo-informatie aan de markt. De Aanwijzing Markt en Overheid[356] biedt onvoldoende houvast voor de afweging of de overheid zich met haar activiteiten al dan niet teveel richt op het terrein van de private sector. Al met al ontbreekt een heldere rolverdeling tussen markt en overheid.

Onderling uiteenlopende regelingen betreffende informatiebeveiliging
Een opvallend knelpunt in de geo-informatie-case bestaat erin dat de diverse instanties uiteenlopende regelingen op het terrein van informatiebeveiliging hanteren. Dit kan de samenwerking belemmeren of op zijn minst vertragen.

6.3 Juridische aandachtspunten

Elektronische handtekeningen
Ten aanzien van de elektronische handtekening verdient het aanbeveling om de norm van een betrouwbare en vertrouwelijke communicatie voorop te stellen. Bestuursorganen kunnen met

[355] Artikelen 10 en 12 juncto artikelen 16b en 16c Auteurswet.
[356] Vaststelling aanwijzingen inzake verrichten marktactiviteiten door organisaties binnen de rijksdienst, Staatscourant 1998, nr. 95, p. 8.

behulp van deze norm zelf invulling geven aan de wijze waarop zij de elektronische weg openstellen. Dat betreft ook het gebruik van elektronische handtekeningen en de wijze waarop het bestuursorgaan wenst om te gaan met wettelijke vormvereisten. De bepaling uit de Webv inzake de elektronische handtekening, bevattende een gelijkstellingsbepaling met een betrouwbaarheidscriterium, kan worden gezien als een *methode* waarop invulling kan worden gegeven aan de open norm van een betrouwbare en vertrouwelijke communicatie.

Het is van belang dat overheidspartijen bij het inrichten van elektronisch bestuurlijk verkeer zich van deze verhouding tussen de open norm en de gelijkstellingsbepaling bewust zijn. Zij dienen zich daarbij af te vragen wat de redenen zijn om al dan niet het gebruik van een bepaalde elektronische handtekening voor te schrijven. Die redenen kunnen gelegen zijn in:

- het waarborgen van veilige elektronische communicatie. Het is dan de vraag of het nodig is om aan te sluiten bij de Weh;
- er wordt juist wel een rechtsgevolg beoogd. Er wordt bijvoorbeeld beoogd om op elektronische wijze aan een vormvereiste te voldoen (neem bijvoorbeeld de belastingaangifte of de aanvraag).

Een overweging die ook een rol kan spelen (bijvoorbeeld bij het ePV), is dat er wordt beoogd op den duur met andere EU-lidstaten gegevens uit te wisselen, waarbij men gebruik wenst te maken van een elektronische handtekening. Nu de Europese Richtlijn inzake een gemeenschappelijk kader voor de elektronische handtekening het recht van de lidstaten voor een groot deel heeft geharmoniseerd, ligt het voor de hand in dat geval aan te sluiten bij de Weh.
Voor de praktijk is het van belang voor ogen te houden dat een elektronische handtekening op zichzelf niet een duidelijke juridische betekenis heeft. De juridische betekenis hangt af van de context waarin de elektronische handtekening wordt gebruikt (bijvoorbeeld de belastingaangifte, de elektronische factuur of bewijsaspecten).

Omgang met persoonsgegevens
De omgang met persoonsgegevens wordt in de uitvoeringspraktijk om verschillende redenen als problematisch ervaren. Er is onduidelijkheid over de betekenis van de wettelijke voorschriften inzake persoonsgegevens, en over de wijze waarop zij dienen te worden toegepast. Verder worden het doelbindings- en transparantiebeginsel als belemmerend ervaren. Het is de vraag of deze knelpunten verholpen kunnen worden. De wetgeving inzake de bescherming van persoonsgegevens dient er juist toe om ongegronde verwerkingen tegen te gaan. Ketenpartijen moeten zich er van bewust worden dat gegevensuitwisseling geen doel op zich kan zijn en voor burgers zoveel mogelijk transparant dient te gebeuren.

Een ander aandachtspunt in dit verband is het publiceren van persoonsgegevens op Internet, bijvoorbeeld het online ter inzage aanbieden van bouwaanvragen en bouwbeschikkingen Openbaarmaking via het internet houdt immers in dat de openbaarmaking op veel grotere schaal plaats vindt dan wanneer een stuk ter inzage op het gemeentehuis wordt gelegd. Overheidsinstanties worden in een dergelijk geval gedwongen om een afweging te maken tussen hun plicht tot actieve openbaarmaking en de Wbp.

Open versus gesloten standaarden
De toepassing van gesloten standaarden zoals bijvoorbeeld in de Ministeriële regeling omgevingsrecht (MOR), is niet in lijn met de notitie ‘Nederland in open verbinding’ en met het algemene streven om meer met open standaarden te gaan werken. Indien open standaarden de norm moeten zijn, dan moeten ook wetgevingsinstrumenten als Ministeriële regelingen, beleidsregels en algemene maatregelen van bestuur daar rekening mee houden. Praktisch gezien wordt echter al wel aangesloten bij open standaarden (getuige de werkwijze van de

Gemeente Tilburg zie case study bouwloket / omgevingsloket) naast de wettelijk geregelde gesloten standaarden die in ieder geval open moeten staan voor de burger.

6.4 Aanbevelingen

Uitgangspunten voor de omgang met persoonsgegevens

- Overheden actief wijzen op handreikingen en richtsnoeren van het CBP (bijvoorbeeld 'Actieve openbaarmaking van persoonsgegevens') en het Ministerie van Justitie ter verduidelijking van het wettelijk kader voor de omgang met persoonsgegevens.
- Het opnemen van richtinggevende bepalingen in sectorale wetgeving overwegen, zoals in de Wet SUWI is gebeurd ten aanzien van doelbinding.
- Overheden voorlichten over en tools bieden voor het privacy-gericht vormgeven van organisatieprocessen.

Uitgangspunten voor het elektronisch bestuurlijk verkeer

- De norm van een betrouwbare en vertrouwelijke communicatie, ook ten aanzien van de elektronische handtekening, vooropstellen in het elektronisch bestuurlijk verkeer.
- Indien de op de Weh gebaseerde elektronische handtekening met zoveel woorden wordt voorgeschreven in e-overheidsprocessen aangeven met welk doel dat gebeurt (bijvoorbeeld het voldoen aan een wettelijk vormvoorschrift of het realiseren van interoperabiliteit met andere EU lidstaten).

Aandacht voor intellectuele eigendomsrechten

- Een herbezinning op het 'wegvallen' van vermeende databankrechten op met publieke gelden gefinancierde overheidsdatabanken in het licht van de rechtspraak.
- Onderzoek naar de noodzakelijkheid van maatregelen (bijvoorbeeld wettelijke verankering of technische afscherming) in verband met mogelijke auteursrechtinbreuken ten aanzien van gegevens (bijvoorbeeld bouwtekeningen) die via Internet openbaar worden gemaakt.

Meer helderheid ten aanzien van aansprakelijkheid

- Nader onderzoek naar de risico's van het volledig vrijgeven van geo-informatie die steeds voor veel geld aan de markt is verkocht, en de aansprakelijkheid die daardoor zou kunnen bestaan jegens bedrijven die reeds aanzienlijk hebben geïnvesteerd in verkrijging van de informatie onder het 'oude' (betaal)regime.

Zorgen voor faciliterende wet- en regelgeving

- In een vroegtijdig stadium (met het oog op rechtszekerheid en een voortvarende aanpak) overwegen om wetgeving als drukmiddel voor het totstandbrengen van samenwerking in te zetten.
- Ook hier relevant: het opnemen van richtinggevende bepalingen in sectorale wetgeving overwegen, zoals in de Wet SUWI is gebeurd ten aanzien van doelbinding.
- Verplicht gebruik, althans een minder vrijblijvende opstelling ten aanzien, van generieke e-overheidsmodules overwegen in het licht van uniformiteit in de dienstverlening richting de burger en grotere interoperabiliteit tussen e-overheidsprocessen.
- Regelgeving afstemmen op het gebruik van open standaarden.
- Onderzoeken of wetgeving (bijvoorbeeld inzake de basisregistraties) betere afstemming op hergebruik van (geo-)informatie behoeft en, zo ja, hoe dat die kan worden gerealiseerd.
- Onderzoeken of, en zo ja, op welke wijze wetgeving kan bijdragen aan een helderder rolverdeling tussen markt en overheid.

- In een vroegtijdig stadium aandacht voor het afstemmen van interne overheidsregelingen, bijvoorbeeld in het kader van beveiligingseisen voor informatie(processen).

Bijlage 1 – Indicatief overzicht van wet- en regelgeving

1 De Europese Unie

- Richtlijn 2007/2/EG tot oprichting van een infrastructuur voor ruimtelijke informatie in de Gemeenschap (Inspire).[1]

- Richtlijn 2006/123/EG betreffende diensten op de interne markt (Dienstenrichtlijn).[2]

- Verordening 1367/2006 betreffende de toepassing van de bepalingen van het Verdrag van Aarhus betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden op de communautaire instellingen en organen.[3]

- Verordening 638/2004 betreffende de communautaire statistieken van het goederenverkeer tussen de lidstaten en houdende intrekking van Verordening 3330/91 (Intrastatverordening).[4]

- Besluit 2004/387/EG betreffende de interoperabele levering van pan-Europese e-overheidsdiensten aan overheidsdiensten, ondernemingen en burgers (vaststelling IDABC-programma).[5]

- Richtlijn 2003/98/EG van 17 november 2003 inzake het hergebruik van overheidsinformatie.[6]

- Verordening 1049/2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie.[7]

- Richtlijn 1999/93/EG betreffende een gemeenschappelijk kader voor elektronische handtekeningen.[8]

    - Beschikking 2000/709/EG betreffende de minimumcriteria die de lidstaten in acht moeten nemen bij de aanwijzing van instanties overeenkomstig artikel 3, lid 4, van Richtlijn 1999/93/EG betreffende een gemeenschappelijk kader voor elektronische handtekeningen.[9]

    - Beschikking 2003/511/EG inzake de bekendmaking van referentienummers van algemeen erkende normen voor producten voor elektronische handtekeningen overeenkomstig Richtlijn 1999/93/EG.[10]

- Richtlijn 98/34/EG betreffende een informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende de diensten van de informatiemaatschappij.[11]

---

[1] *PbEG* 2007 L 108/1.
[2] *PbEG* 2006 L 376/36.
[3] *PbEG* 2006 L 264/13.
[4] *PbEG* 2004 L 102/1.
[5] *PbEG* 2004 L 181/25.
[6] *PbEG* 2003 L 345/90.
[7] *PbEG* 2001 L 145/43.
[8] *PbEG* 2000 L 13/12.
[9] *PbEG* 2000 L 289/42.
[10] *PbEG* 2003 L 175/45.

Deze richtlijn is later gewijzigd door:

- Richtlijn 98/48/EG tot wijziging van Richtlijn 98/34/EG betreffende een informatieprocedure op het gebied van normen en technische voorschriften;[12] en
- Richtlijn 2006/96/EG tot aanpassing van een aantal richtlijnen op het gebied van vrij verkeer van goederen in verband met de toetreding van Bulgarije en Roemenië.[13]

- Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.[14]

2 Nederland

2.1 Generieke wet- en regelgeving

- Algemene wet bestuursrecht (bevattende de Wet elektronisch bestuurlijk verkeer)
- Archiefwet 1995
  - Archiefbesluit 1995
- Auteurswet
- Besluit beheer DigiD
  - Organisatiebesluit directoriat-generaal Bestuur (Organisatiebesluit DGB)
  - Beleidsregel tot vaststelling niveau DigiD voor inzage in GBA persoonsgegevens via MijnOverheid.nl
- Databankenwet
- Wet algemene bepalingen burgerservicenummer
  - Regeling burgerservicenummer
- Wet bescherming persoonsgegevens
- Wet elektronische handtekening
- Wet openbaarheid van bestuur
- Organisatiebesluit directoraat-generaal Bestuur (Organisatiebesluit DGB)
- Telecommunicatiewet

---

[11] *PbEG* 1998 L 204/37.
[12] *PbEG* 1998 L 217/18.
[13] *PbEG* 2006 L 363/81.
[14] *PbEG* 1995 L 281/31.

  - Wet bewaarplicht telecommunicatiegegevens (wetsvoorstel)
- Tijdelijk besluit nummergebruik overheidstoegangsvoorziening

2.2 Sectorale wet- en regelgeving

- Algemene wet inzake rijksbelastingen
  - Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994
- Burgerlijk Wetboek, boek 2, titel 9 inzake de jaarrekening
  - Besluit tot vaststelling van modelschema's voor de inrichting van jaarrekeningen (Modellenbesluit)
- Handelsregisterwet
- Kadasterwet
- Regeling gegevenslevering onderwijsnummer VO
- Regels inzake het gebruik van het burgerservicenummer in de zorg (Wet gebruik burgerservicenummer in de zorg)
- Wet algemene bepalingen omgevingsrecht (wetsvoorstel)
- Wet basisregistraties adressen en gebouwen (wetsvoorstel)
- Wet basisregistraties kadaster en topografie
- Wet justitiële en strafvorderlijke gegevens
  - Besluit justitiële gegevens
  - Regeling verwijdering justitiële gegevens
- Wet kenbaarheid publiekrechtelijke beperkingen
- Wet op de expertisecentra
- Wet op de identificatieplicht
- Wet op de gemeentelijke basisadministratie persoonsgegevens
  - Besluit gemeentelijke basisadministratie persoonsgegevens
  - Regeling gemeentelijke basisadministratie persoonsgegevens
  - Regeling bewaring GBA-bescheiden

    - Vaststelling autorisatie-aanvraagformulieren
- Wet op de geneeskundige behandelingsovereenkomst
- Wet op de ruimtelijke ordening
- Wet op het centraal bureau voor de statistiek
    - Besluit gegevensverwerving CBS
    - Regeling statistieken goederenverkeer
    - Regeling verstrekking gegevens doodsoorzaken CBS
- Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW)
- Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI-wet)
- Wet verzelfstandiging informatiseringsbank (WVI)
- Wet werk en bijstand
- Wijzigingswet van enkele onderwijswetten in verband met de invoering van persoonsgebonden nummers in het onderwijs
- Wet Maatschappelijke Ondersteuning (WMO)

Bijlage 2 - Rapporten, (deel)studies en beleidsstukken

1 Nederland

1.1 Rapporten en (deel)studies

Towards a Dutch Interoperability Framework – Recommendations to the Forum Standaardisatie (2008)
Rapport van Rand in opdracht van het Forum Standaardisatie waarin de beleidskeuzes uiteen worden gezet ten aanzien van het ontwikkelen van een interoperabiliteitsframework. De auteurs stellen onder meer dat een interoperabiliteitsframework drie niveaus dient te adresseren: *Governance*, *System* en *Implementation*. De drie niveaus worden in het rapport nader uitgewerkt en er wordt een stappenplan geformuleerd om tot een interoperabiliteitsframework te komen.

Eerste fase evaluatie Wet bescherming persoonsgegevens (2007)
Er is geïnventariseerd wat de doelstellingen waren bij de invoering van de Wbp. Daarnaast is nagegaan wat de bedoelingen van de gemeenschapswetgever daarbij waren (doelstellingeninventarisatie). Vervolgens is onderzocht welke knelpunten er in de literatuur en rechtspraak zijn gesignaleerd bij de uitvoering en toepassing van de wet (knelpuntenanalyse). Het doel van dit onderzoek is het doen van aanbevelingen met betrekking tot het nader articuleren van de onderzoeksvragen voor de tweede fase van de evaluatie (vraagarticulatie).

Het uur van de waarheid (2007)
Advies van de commissie Postma/Wallage inzake onder meer de financiering van en de sturing van de invoering van de e-Overheid. De commissie pleit onder meer voor een Nationaal Urgentie Programma (NUP) dat door de Ministerraad dient te worden vastgesteld, waarna de samenstelling en uitvoering van het programma in handen komen van een ministeriële commissie onder leiding van de minister-president, dan wel één van de vice premiers. Het NUP dient een verplichtend karakter te hebben.

Kink in de Keten (2007)
Rapport uitgevoerd door de Universiteit Twente, ter inventarisatie van bevorderende / belemmerende factoren bij samenwerking in e-overheid ketens.

OECD e-Government Studies – Netherlands (2007)
Dit is één van de landenstudies van de OECD, dit keer uitgevoerd ten aanzien van de Nederlandse e-Overheid. Het bevat een uitgebreid overzicht en van diverse aspecten van de e-Overheid en van de verschillende e-Overheidsinitiatieven.

Open standaarden en open source – Onderzoek ter ondersteuning van gewenste beleidsintensivering (2007)
Dit is een internationaal onderzoek inzake de beleidsopties ten aanzien van open standaarden en open source, uitgevoerd door Verdonck, Klooster & Associates, op verzoek van het Forum Standaardisatie.

Verkenning authenticatie (2007)
Dit is een verkenning naar authenticatie, uitgevoerd door KPMG, op verzoek van het Forum Standaardisatie. Het rapport stelt onder meer dat er verbetering kan plaatsvinden op het gebied van authenticatie door een aantal zaken te standaardiseren, te weten:

1. de gebruikte terminologie;
2. de kwaliteitsklassen voor authenticatiemiddelen.

Open toegankelijkheidsbeleid voor geo-informatie vergeleken: het gras leek groener dan het was (2007)
In dit onderzoek van de universiteit Delft, uitgevoerd in opdracht van het ministerie van Binnenlandse Zaken, is een internationale verkenning uitgevoerd van de mogelijkheden om op een efficiënte manier uniformering van gebruiksvoorwaarden en tariefstelling bij wet te regelen. Er staan drie onderzoeksvragen centraal:

1. Welk nationaal en lokaal beleid ligt ten grondslag aan de beschikbaarstelling van geo-informatie? Welke wet- en regelgeving is hiervoor ontwikkeld en op welke wijze is de overheid georganiseerd?
2. Wat zijn de effecten van dit beleid voor de overheid en het bedrijfsleven?
3. Welke elementen uit het beleid van andere lidstaten zou Nederland kunnen gebruiken om vrij hergebruik van geo-informatie te bevorderen?

Naar aanleiding van het onderzoek komen de auteurs tot acht aanbevelingen, welke deels ook door de INSPIRE-richtlijn worden vereist:

1. De uitgangspunten van het huidige algemene toegankelijkheidsbeleid (maximaal marginale verstrekkingskosten en geen voorwaarden die het hergebruik beperken) zouden ook als beleid voor de publieke geo-informatie moeten gelden. Slechts bepaalde categorieën van uitzonderingen zouden van dit beleid kunnen afwijken.
2. Stimuleer de transparantie van gebruiksvoorwaarden.
3. Stimuleer de documentatie van metadata.
4. Schrijf het gratis inzien van overheids(geo-)informatie voor.
5. Streef naar gratis beschikbaarheid van geo-informatie tussen overheden, waar nodig door “bovenlangs” via de begroting financiële stromen aan te passen.
6. Beleg one-stop shop (één loket waar een overzicht van alle bij de overheid beschikbare geo-informatie kan worden verkregen) * bij een neutrale partij, die zelf niet in de markt zit.
7. Stimuleer de ontwikkeling van private value-added services door in de Algemene wet overheidsinformatie een experimenteerbepaling op te nemen.
8. Grens helder af wat de (semi-) publieke sector zelf aan value-added activiteiten mag ontplooien en wat aan het bedrijfsleven moet worden overgelaten.

Beschikbaar stellen van geoinformatie bij Rijkswaterstaat. Analyse van de (on)mogelijkheden van het op korte termijn vrij beschikbaar stellen van vier geo-data sets (2006)
Dit onderzoek is uitgevoerd door de universiteit Delft in opdracht van Rijkswaterstaat. Het onderzoek bevat een analyse van de juridische en economische randvoorwaarden van een voornemen om alle beschikbare geografische datasets binnen de Adviesdienst Geo-informatie en ICT van Rijkswaterstaat (RWS-AGI). Het rapport behandelt vier vragen:

1. Wat zijn geschikte gebruiksvoorwaarden voor vrije verstrekking?
2. Kan RWS-AGI het zich permitteren om alleen actief via internet haar gegevens beschikbaar te stellen?
3. Kan RWS-AGI het zich permitteren om geen vragen van klanten te beantwoorden?
4. In hoeverre werpt het kader voor markt en overheid belemmeringen op voor het vrij verstrekken van geo-data en in hoeverre mag RWS-AGI (web-)services aanbieden?

Interoperabiliteit in de publieke sector: Een IT-probleem of een bestuurlijke uitdaging? (2006)
Rapport uitgevoerd door het Nolan Norton Institute, op verzoek van Microsoft B.V., inzake interoperabiliteit in de publieke sector. Het rapport stelt onder meer dat om zo goed mogelijk gebruik te maken van het concept van interoperabiliteit, open standaarden verplicht moeten worden gesteld en de naleving daarvan dient te worden gecontroleerd.

Tussen het kastje en de muur, Project 'Kwaliteit van de publieke dienstverlening', (2006)
Een studie van M. van Dam, A. Timmer (PVDA) over voorwaarden voor het verbeteren van de uitvoeringspraktijk binnen de overheid door middel van ICT-innovaties.

Impactanalyse Europese ontwikkelingen, 'Eens gegeven, blijft een gegeven' (2005)
In opdracht van ICTU door HEC en TILT (Universiteit van Tilburg) uitgevoerd onderzoek naar de gevolgen van Europese ontwikkelingen (waaronder de Richtlijn hergebruik, de INSPIRE- en de dienstenrichtlijn) voor het programma Stroomlijning Basisgegevens.

FIDIS rapportage D4.2: Set of requirements for interoperability of Identity Management Systems (2005)
Het FIDIS-project[371] onderzoek identiteit in de informatiemaatschappij. In dit rapport worden, uitgaande van het conceptuele raamwerk van *technical*, *formal* en *informal dimensions* 23 experts ondervraagd inzake interoperabiliteit van Identity Management Systems.

FIDIS rapportage D4.1: Structured account of approaches on interoperability (2005)
In dit rapport, eveneens afkomstig van het FIDIS-project, wordt onderzoek gedaan naar interoperabiliteit in verband met identificatie/authenticatie.

PRIME-rapport Legal Requirements (2004)
Het PRIME-project (Privacy and Identity Management for Europe)[372] beoogt een werkend prototype van een privacy-enhancing Identity Management System te ontwikkelen. Dit rapport beschrijft vanuit voornamelijk privacyregelgeving een aantal scenario's.

Naar een ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie (2002)
In dit rapport wordt onderzocht wat de inhoud zou kunnen zijn van een 'Wet gebruiksrechten overheidsinformatie'. Hiertoe is een rechtsvergelijkend onderzoek gedaan naar een vijftal landen en is nagegaan voor welke informatie de regeling zou kunnen of moeten gelden.

Elektronische overheid en privacy, Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid (2002)
Versmissen en de Heij deden een verkennende studie voor het College Bescherming Persoonsgegevens naar de bescherming van persoonsgegevens binnen de informatie-infrastructuur van de overheid.

Wob & ICT (2000)
In dit rapport wordt de Wet openbaarheid van bestuur (Wob) geëvalueerd. Er wordt ingegaan op de vraag in hoeverre ICT van invloed is op de werking van de Wob en of er om die reden aanleiding is de Wob en aanverwante regelgeving te wijzigen. Er wordt hierbij een onderscheid gemaakt tussen het verstrekken van informatie op verzoek (passieve verstrekking) en het verstrekken van informatie uit eigen beweging (actieve verstrekking).

---

[371] http://www.fidis.net/
[372] https://www.prime-project.eu/

1.2 Beleidsstukken

ICT-Agenda 2008-2011. De gebruiker centraal in de digitale dienstenmaatschappij (2008)
In de ICT-Agenda 2008-2011 zet het kabinet haar ambitie en voorgenomen acties uiteen ten aanzien van ICT. De uitwerking van de ambitie van het kabinet is in de ICT-Agenda verdeeld in een vijftal prioriteiten en enkele randvoorwaarden. De prioriteiten zijn:

1. eVaardigheden;
2. elektronische dienstverlening door de overheid;
3. interoperabiliteit en standaardisatie;
4. maatschappelijke domeinen en ICT;
5. diensteninnovatie en ICT.

De randvoorwaarden vormen de ICT-basis. De ICT-basis bestaat uit drie lagen:

1. fundament van infrastructuur en ICT-onderzoek;
2. diensten van en aan MKB en prosumenten; en
3. betrouwbaarheid van ICT en werking van de markt.

GIDEON – Basisvoorziening geo-informatie Nederland – Visie en implementatiestrategie (2008)
GIDEON is de te realiseren basisvoorziening geo-informatie Nederland. Bij de realisatie van GIDEON worden de volgende uitgangspunten gehanteerd:

- als organisatorisch principe wordt ‘eenmalig vastleggen, meervoudig gebruik’ toegepast;
- de ontwikkeling van GIDEON vindt plaats binnen de context van de INSPIRE-richtlijn en sluit aan op de NORA. Er wordt op toegezien dat er wordt afgestemd en samengewerkt met relevante projecten en programma’s die in het kader van de e-Overheid worden uitgevoerd;
- kwaliteit en duurzaamheid: GIDEON-gegevens en diensten worden gecertificeerd en GIDEON zal voldoen aan Europese regels voor metadata en harmonisatie, zoals vastgelegd in de INSPIRE-richtlijn, en aan de voorwaarden voor informatieverstrekking uit de Wet openbaarheid van bestuur.

Actieve openbaarmaking van persoonsgegevens (2008)
Dit is consultatiedocument van het College bescherming persoonsgegevens (CBP) betreffende de actieve openbaarmaking van gegevensbestanden, dat wil zeggen de informatieverschaffing door overheidsorganen uit eigener beweging. De actieve openbaarmaking kan met zich meebrengen dat een overheidsorgaan persoonsgegevens openbaar maakt. Omdat de wet grenzen stelt aan de verwerking van persoonsgegevens, kan zij ook grenzen stellen aan de actieve openbaarmaking.

Publicatie van persoonsgegevens op internet (2007)
Dit consultatiedocument van het College Bescherming Persoonsgegevens (CBP) richt zich op de randvoorwaarden voor publicatie van persoonsgegevens via het internet. Hoewel dit richtsnoer zich in eerste instantie niet specifiek richt op de elektronische overheid, is het toch ook voor hen een handreiking. Het stuk bevat een aantal interessante e-Overheid gerelateerde voorbeelden.

Nederland Open in Verbinding – Een Actieplan voor het gebruik van Open Standaarden en Open Source Software bij de (semi-)publieke sector (2007)
Dit is een actieplan van het Nederlandse kabinet waarin wordt gekozen voor de volgende beleidsaccenten:

1. brede toepassing van open standaarden door het ‘comply-or-explain and commit’ principe in te voeren bij opdrachten van Rijksdiensten vanaf april 2008 en voor de overige overheden en instellingen vanaf december 2008. Om hen daarbij te ondersteunen wordt een basislijst open standaarden (januari 2008) en een raamwerk voor interoperabiliteit opgesteld (basisversie in juni 2008) met richtinggevende keuzes voor de ontwikkeling en het gebruik van standaarden;

2. implementatiestrategieën voor de aanbesteding, inkoop en het gebruik van open source software te realiseren door alle ministeries (januari 2009) en door medeoverheden en instellingen in semi-publieke sectoren (onderwijs, zorg, sociale zekerheid) in januari 2010;
3. stapsgewijze invoering van de open standaard ODF (Open Document Format) voor het lezen, schrijven, uitwisselen, publiceren en ontvangen van documenten (uiterlijk januari 2009 door alle ministeries en mede-overheden ondersteund) op weg naar grootschalig gebruik van open document formaten voor overheidstoepassingen.

Op weg naar de elektronische overheid (2004)
Beleidsstuk van het kabinet waarin onder meer het voornemen wordt uitgesproken dat de overheid voor haar communicatie, zowel intern als met de buitenwereld, open standaarden gaat gebruiken. Inclusief Voortgangsrapportage elektronische overheid (2005).

De Rijksbrede ICT-agenda – Beter presteren met ICT (2004)
Het kabinet kondigt in dit document zes speerpunten aan:

- Burgers en bedrijven hoeven bepaalde gegevens nog maar één keer aan te leveren bij de overheid. Om dit te realiseren wordt er onder meer een stelsel van basisregistraties gerealiseerd dat het mogelijk moet maken dat van burgers, bedrijven en onderwijs- en zorginstellingen bepaalde gegevens niet meer (mogen) worden gevraagd als die al beschikbaar zijn binnen de overheid.
- Er komt een elektronisch systeem waarmee burgers en bedrijven zich eenduidig bekend kunnen maken bij de overheid. Om dit te realiseren wordt er een burger servicenummer ingevoerd en wordt er naar gestreefd om nog in deze kabinetsperiode een elektronische identiteitskaart te introduceren.
- Voor haar communicatie, zowel intern als met de buitenwereld, gaat de overheid open standaarden gebruiken, waardoor de leveranciersafhankelijkheid wordt verminderd. Het in 2003 gestarte programma Open Standaarden en Open Source Software wordt dan ook met kracht doorgezet.
- Burgers en bedrijven kunnen tegen vergelijkbare kosten een substantieel snellere aansluiting krijgen op internet en daarover geleverde diensten dan thans het geval is. Hiertoe wordt het Actieprogramma Breedband uitgevoerd en zal het kabinet op korte termijn een aanscherping van dit actieprogramma uitbrengen.
- Veiligheid en betrouwbaarheid van en vertrouwen in het gebruik van ICT-voorzieningen en internet nemen sterk toe. Om deze doelstelling te bereiken worden onder meer acties ondernomen om het gevoel van onveiligheid dat bij sommigen is ontstaan door zaken als spam en cybercrime, te verminderen.
- Er komt een Regie-orgaan ICT-Onderzoek en -Innovatie om het ICT-onderzoek te versterken en sterker aan te sturen over het gehele traject van fundamenteel onderzoek tot toepassing. Het dient er voor te zorgen dat het onderzoek zich internationaal met erkende sterktes profileert en meer bijdraagt aan verhoging van de arbeidsproductiviteit en vermindering van maatschappelijk gevoelde knelpunten.

In 2005 is er een vervolg op de ICT-agenda vastgesteld, resulterende in de volgende zeven speerpunten:

- Eenmalige aanlevering van gegevens. Burgers en bedrijven hoeven gegevens nog maar één keer aan te leveren bij de overheid.
- Elektronische identificatie. Burgers en bedrijven kunnen zich elektronisch eenduidig bekend maken bij de overheid.
- Sneller op internet. Burgers, bedrijven en instellingen kunnen tegen vergelijkbare kosten een substantieel snellere aansluiting krijgen op internet en daarover geleverde diensten dan nu het geval is.
- Veiligheid en betrouwbaarheid. Veiligheid en betrouwbaarheid van en vertrouwen in ICT-voorzieningen en internet nemen sterk toe.

- Standaardisatie. Gegevensuitwisseling van en met de overheid wordt gemakkelijker door standaardisatie.
- Consumentenbeleid. De ICT-consument beschikt over optimale keuzevrijheid; voldoende kennis; vereenvoudigde klachtenafhandeling en bescherming tegen inbreuk op rechten.
- ICT in het (semi)publieke domein. De mogelijkheden van ICT worden beter gebruikt en ICT wordt ingezet voor het oplossen van grote maatschappelijke knelpunten.

Actieprogramma 'Andere overheid' (2003)
Dit Actieprogramma geeft het kabinetsvoornemen weer, inhoudende dat de overheid terughoudender moet zijn in wat zij regelt en vooral *hoe* zij regelt. Ook moet er een groter beroep worden gedaan op maatschappelijke krachten. Ter uitvoering van dit voornemen, wenst het kabinet meer elektronische dienstverlening te realiseren. Om te zorgen voor een probleemloze elektronische gegevens-uitwisseling met en tussen overheidsorganisaties, zou een beperkte set (open) standaarden moeten worden vastgesteld.

Architectuur elektronische overheid, samenhang en samenwerking (2002)
In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Directie Informatiebeleid Openbare Sector (DIOS), uitgevoerd door Verdonck, Klooster & Associates. Dit rapport geeft de noodzakelijk randvoorwaarden weer teneinde de overheid efficiënter en kwalitatief beter te laten werken. Op basis van een aantal interoperabiliteitskenmerken wordt een voorstel gedaan tot verbetering van de architectuur.

Naar optimale beschikbaarheid van overheidsinformatie (2000)
In deze beleidslijn wordt een kader geschetst ten aanzien van de toegankelijkheid en het gebruik van overheidsinformatie en de daarop betrekking hebbende wetgeving. De beleidslijn maakt een onderscheid tussen 'basisinformatie van de democratische rechtsstaat', Wob-informatie en 'overige informatie'.

Contract met de toekomst. Een visie op de elektronische relatie overheid-burger (2000)
Nota van het ministerie van BZK. Kernthema's voor deze nota en de discussie zijn:

- 'vrijheid in verbondenheid', een visie op de elektronische relatie overheid-burger;
- `de aanspreekbare overheid', over bereikbaarheid, keuzevrijheid, geloofwaardigheid en participatie; de mogelijk verregaande consequenties voor een aantal aspecten van overheidshandelen;
- 'de overheid in beweging', acties die nu al worden ondernomen of ondernomen kunnen gaan worden; hiermee versterkt de overheid haar rol in de informatiemaatschappij en geeft zij haar voorbeeldpositie verder vorm.

1.3 EU

eID Interoperability for Pan-European eGovernment Services. Analysis and Assessment of Similarities and Differences – Impact on eID interoperability (2007)
Het project *eID Interoperability for Pan-European eGovernment Services* poogt oplossingen aan te dragen voor de juridische, technische en organisatorische onderwerpen, gerelateerd aan het opstellen van een interoperabele pan-Europese *identity management*-infrastructuur. Door middel van het bereiken van interoperabiliteit, wordt gepoogd uiteindelijk een generieke architectuur voor te stellen die, rekening houdend met het bestaan van verschillende modellen, in staat is om te gaan met deze verschillende modellen. Eén van de fases van het project houdt in dat rapporten dienen te worden opgesteld ten aanzien van de verschillende deelnemende landen. In het kader van deze fase wordt in dit rapport een overzicht gegeven van de overeenkomsten en de verschillen van de *identity management*-systemen die in de verschillende landen worden gebruikt. Naast het overzicht van

overeenkomst en verschillen, bevat het rapport ook een impact analyse ten aanzien van de gevolgen voor interoperabiliteit.

Het rapport concludeert onder meer dat geen van de 32 onderzochte landen beschikt over een juridisch raamwerk ten aanzien van de identificatie van entiteiten.[373]

Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications (2007)
In dit rapport wordt een overzicht gegeven van eOverheidstoepassingen van verschillende deelnemende landen, waarmee gebruik wordt gemaakt van elektronische handtekeningen. Doel van het onderzoek is om overeenkomsten en verschillen tussen de verschillende toepassingen te signaleren en om knelpunten ten aanzien van interoperabiliteit te signaleren. Aan de hand van een impactanalyse wordt vervolgens een aantal aanbevelingen gedaan.

Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (2006)[374]
In dit rapport wordt richtlijn 1999/93/EG betreffende een gemeenschappelijk kader voor elektronische handtekeningen geëvalueerd.

Creating a European Identity Management Architecture for eGovernment (2005)
In het kader van het zesde kader programma van de EU deed het consortium GUIDE een onderzoek naar de mogelijkheid tot het creëren van een interoperabele open architectuur van identiteitsmanagement binnen de e-overheid in Europa.

1.4 Sectorale interoperabiliteitsraamwerken

Legal dictionaries in relatie tot het Gegevenswoordenboek Strafrechtsketen (2007)
Rapportage in het kader van het project Bouwstenen voor Berichtenuitwisseling inzake de semantische interoperabiliteit in de strafrechtsketen.

[373] Deze conclusie strookt overigens niet geheel met het bij het rapport behorende overzicht van wetgeving van de verschillende landen, waarin het *E-Government-Gesetz* van Oostenrijk wordt genoemd als een voorbeeld waarin de identificatie van entiteiten juist wel wordt geregeld.
[374] COM(2006) 120 final.