Bij twijfel niet gebruiken?

Een verkenning naar oplossingen voor belemmeringen bij het gebruik van persoonsgegevens uit basisregistraties

iNUP, Programma Stelsel van Basisregistraties, cluster STOUT

Koen Versmissen

Versie 1.1, maart 2013

Inhoudsopgave

Managementsamenvatting

Deze verkenning inventariseert privacy-issues die in de weg staan aan effectief gebruik van basisregistraties. Aanleiding voor de verkenning was het toenemende aantal meldingen dat cluster STOUT in de loop van 2012 ontving over belemmeringen bij het gebruik van persoonsgegevens uit verschillende basisregistraties. De verkenning is gebaseerd op een aantal gesprekken met direct betrokkenen – zowel leveranciers als afnemers van persoonsgegevens uit basisregistraties – aangevuld met een beperkte literatuurstudie.

Het beeld dat uit de verkenning naar voren komt, is dat het ten aanzien van persoonsgegevens meestal niet gaat om op zichzelf staande issues. Het is eerder zo dat de noodzaak voor betrokken partijen om zich rekenschap te geven van de regels en normen voor de omgang met persoonsgegevens allerlei zaken een stuk complexer maakt. Vaak echter wel op zo'n manier, dat daardoor ook daadwerkelijk nieuwe problematiek ontstaat.

In de verkenning worden de volgende zeven typen issues onderscheiden.

1) *Overzicht.* Afnemers hebben te weinig overzicht als gevolg van een gebrek aan goede informatie en een overdaad aan complexiteit. Informatie is vaak wel beschikbaar, en wordt ook wel gevonden; afnemers hebben echter moeite om uit de complexe brei aan informatie een concreet kader voor onderlinge afspraken en concrete handvatten voor de eigen uitvoeringspraktijk af te leiden. Dit leidt soms tot onnodige terughoudendheid in ketens van verstrekkingen.

2) *Wet- en regelgeving.* De verkenning had niet ten doel bestaande regelgeving fundamenteel ter discussie te stellen. Wel blijkt er op dit terrein sprake van diverse onbedoelde blokkeringen: gesloten verstrekkingenregimes schieten tekort bij nieuwe maatschappelijke ontwikkelingen die nieuwe gegevensuitwisselingen wenselijk maken; sommige regelgeving is te techniekafhankelijk geformuleerd, waardoor nieuwe technische mogelijkheden onbenut blijven; en er zijn soms te weinig mogelijkheden voor het bedrijven van statistiek op basis van persoonsgegevens. Ook interpretatieverschillen tussen (met name) juristen kunnen belemmerend werken.

3) *Verantwoordelijkheid.* Er blijkt vaak veel onduidelijkheid te zijn over wie precies waarvoor verantwoordelijk is. In twee soorten gevallen (bij het gebruik van kopiebestanden en voor knooppunten) zijn verantwoordelijkheden mogelijk verkeerd belegd. Verstrekkers van persoonsgegevens hebben een grote behoefte aan controle van het handelen van de ontvanger, en dat kan verstrekkingen flink ingewikkeld maken – zeker in ketens.

4) *Regels voor hergebruik.* Bij afnemers van persoonsgegevens bestaat veel onduidelijkheid over wat ze wel en niet met die gegevens mogen. Daardoor worden soms persoonsgegevens verwerkt in situaties waar dat niet is toegestaan, maar het omgekeerde komt net zo goed voor. Extra ingewikkeld ligt het bij de GBA, die een apart

wettelijk regime kent: waar ligt de overgang van de Wet GBA naar de Wet Bescherming Persoonsgegevens?

5) *Bruikbaarheid en kwaliteit.* Zelfs bij basisregistraties is er discrepantie tussen administratie en werkelijkheid. Er blijken hardnekkige beelden te bestaan over gebrekkige kwaliteit van basisregistraties. Vaak blijken die niet te kloppen, of is de kwaliteit van de gegevens voor de afnemer niettemin adequaat. Overigens zijn er verschillende situaties waarin de burger of de bronhouder van de basisregistratie bewust kiest voor het opnemen van onjuiste gegevens in de registratie.

6) *Techniek en informatiebeveiliging.* Diverse succesvolle knooppunten vormen het bewijs dat techniek en informatiebeveiliging rondom persoonsgegevens geen intrinsiek probleem vormen. Met name kleinere afnemers lukt het in de praktijk echter vaak onvoldoende om grip te krijgen hierop. Vooral de complexe autorisaties die nodig zijn om ongeoorloofde raadpleging van persoonsgegevens te voorkomen maken het ingewikkeld.

7) *Rekenschap.* Dit in het WRR-rapport over de i-Overheid uitvoerig behandelde onderwerp speelt hier op verschillende manieren. Rekenschap jegens de individuele burger blijkt vaak onvoldoende ingevuld: burgers kunnen er veel last van hebben als gegevens over ze in basisregistraties niet kloppen. Vooral omdat zulke fouten zich als een olievlek over overheidsregistraties verspreiden en voor een individuele burger vrijwel niet te corrigeren zijn. Een ander issue is rekenschap bij incidentele verwerking: wat wordt er allemaal buiten de officiële kanalen uitgewisseld over telefoon en e-mail?

Complexiteit en een gebrek aan overzicht bepalen in belangrijke mate de problematiek. Het scheppen van eenvoud, orde en duidelijkheid is hiervoor een goede oplossing. In sommige gevallen kan dat bereikt worden door eenvoudig gerichter en pragmatischer te informeren, zodat hardnekkige onjuiste beeldvorming wordt gecorrigeerd. In andere gevallen is er meer nodig, zoals: goede afspraken maken met elkaar, juridische duidelijkheid scheppen, grijze gebieden vanuit het beleid pro-actief inkleuren en taken en verantwoordelijkheden daar neerleggen waar ze ook daadwerkelijk gerealiseerd kunnen worden. Om rekenschap jegens de individuele burger waar te kunnen maken, zullen mechanismen gecreëerd moeten worden die over bestuurlijke, beleidsmatige, juridische en operationele barrières heen effectief zijn.

1. Inleiding

Het stelsel van basisregistraties is door de overheid opgezet met het oog op breed gebruik van de daarin beschikbare gegevens – in ieder geval binnen de overheid, en waar mogelijk ook daarbuiten. Bij het gebruiken van gegevens uit basisregistraties doen zich in de praktijk allerlei en veelsoortige problemen voor. Een aantal belemmeringen doet zich voor als het specifiek om *persoons*gegevens gaat. Regels en normen voor de bescherming van privacy en persoonsgegevens werpen in de praktijk dan extra barrières op – daadwerkelijke zowel als gepercipieerde.

Het doel van dit document is drieledig:

1) Het presenteren van een overzicht van belemmeringen die betrokken partijen zien of in de praktijk ervaren als het gaat om het gebruik van persoonsgegevens uit basisregistraties.

2) Het analyseren van die ervaren belemmeringen:

    a) Is er daadwerkelijk sprake van een belemmering?

    b) Zo ja:

        i) Om wat voor soort belemmering gaat het?

        ii) Hoe belangrijk en hoe urgent is die?

3) Het aandragen van oplossingsrichtingen voor het wegnemen van belemmeringen.

De focus ligt hier specifiek op persoonsgegevens. In de praktijk ervaren betrokken partijen echter vooral problemen met het gebruik van gegevens in algemene zin, zonder daarbij altijd een duidelijk beeld te hebben in hoeverre deze problemen terug te voeren zijn op het feit dat het gaat om *persoons*gegevens. Ook in de analyse blijkt het lastig om dit onderscheid te maken. Dat heeft ermee te maken dat het meestal niet gaat om op zichzelf staande issues. Het is eerder zo dat de noodzaak voor betrokken partijen om zich rekenschap te geven van de regels en normen voor de omgang met persoonsgegevens allerlei zaken een stuk complexer maakt. Vaak op zo'n manier, dat daardoor ook echt nieuwe problematiek ontstaat.[1]

De term 'privacy' leidt vaak tot verwarring, en is hierboven daarom zoveel mogelijk vermeden. In het rapport wordt wel veelvuldig de term 'privacywet- en -regelgeving' gebezigd. Die is bedoeld in brede zin, dat wil zeggen: alle wettelijke regels en normen over de omgang met persoonsgegevens, dus ook bijvoorbeeld over wie er onder welke voor-

[1] Overigens zal in veel gevallen iets vergelijkbaars gelden voor gegevens over bedrijven, aangezien ook die vaak vertrouwelijk van aard zijn. Ze vallen echter buiten het bestek van deze verkenning.

waarden recht heeft op welke gegevens (of zelfs van bepaalde gegevens verplicht gebruik moet maken) en hoe dat in de praktijk is vormgegeven en ingekaderd.

Voor alles geldt dat de huidige en voorgenomen wet- en regelgeving als uitgangspunt wordt genomen. Oplossingen die erop neer komen dat de wet dan maar moet worden aangepast vallen daarmee buiten de reikwijdte van deze analyse.

Dit rapport is als volgt opgebouwd. Hoofdstuk 2 bevat een probleemanalyse, in de vorm van een geordend overzicht van de issues die uit de gevoerde gesprekken en de geraadpleegde literatuur naar voren zijn gekomen. Hoofdstuk 3 verkent mogelijke oplossingen. Hoofdstuk 4 geeft een beknopte conclusie. Hoofdstuk 5 bevat een aantal aanbevelingen.

Diverse bijlagen completeren het geheel. De eerste daarvan bevat een overzicht op hoofdlijnen van de persoonsgegevens die in de verschillende basisregistraties beschikbaar zijn, en de belangrijkste regels die gelden voor het gebruik van die gegevens.

De tekst is doorspekt met kaders. Die zijn er in drie soorten, die hieronder worden geïntroduceerd.

Voorbeeld
Een concreet voorbeeld ter illustratie van de hoofdtekst.

Citaat
Een illustratieve of ondersteunende passage uit een van de geraadpleegde bronnen.

Dilemma
Een korte beschouwing die de te maken afwegingen in een breder kader plaatst.

2. Probleemanalyse

Uit de gevoerde gesprekken en de geraadpleegde literatuur blijkt een grote diversiteit aan issues die gerelateerd zijn aan de vraagstelling.

Deze issues vallen in te delen in de volgende categorieën (die in de praktijk uiteraard vaak door elkaar lopen):

1. Overzicht
2. Wet- en regelgeving
3. Verantwoordelijkheid
4. Regels voor hergebruik
5. Bruikbaarheid en kwaliteit
6. Techniek en informatiebeveiliging
7. Rekenschap

Zie overigens de inleiding van paragraaf 2.2 voor een nadere toelichting op het begrip ‘persoonsgegeven’.

2.1. Overzicht

Een belangrijke belemmering die afnemers ervaren bij het gebruik van persoonsgegevens uit basisregistraties is dat zij te weinig overzicht hebben als gevolg van een gebrek aan goede informatie en een overdaad aan complexiteit.

Op beleidsniveau zijn afnemers over het algemeen wel bekend met de toepasselijke wet- en regelgeving en de relevante beleidskaders. Bij elkaar vormen die vaak echter een zo omvangrijk en complex geheel dat het moeilijk blijkt om daarover effectief overzicht te krijgen en te houden.

De informatie is op zich dus wel beschikbaar en wordt ook wel gevonden. Het probleem zit hem er vooral in dat het moeilijk is om uit de complexe brei aan informatie een concreet kader voor onderlinge afspraken en concrete handvatten voor de eigen uitvoeringspraktijk af te leiden.

Voorbeeld
Enkele jaren geleden zijn de Regionale Informatie en Expertise Centra (RIECs) opgericht. De RIECs zijn informatieknooppunten en expertisecentra op het gebied van de (bestuurlijke) aanpak van de georganiseerde criminaliteit. Verschillende overheidsinstanties werken in een RIEC samen.
Het Landelijk Informatie en Expertise Centrum (LIEC) is het overkoepelende orgaan voor de RIECs. Het LIEC is in kaart aan het brengen wat de wettelijke mogelijkheden en verplichtingen zijn om binnen RIECs persoonsgegevens uit te wisselen. Dat blijkt nog niet mee te vallen. Er is veel en complexe wetgeving, de verschillende regels zijn niet altijd op elkaar afgestemd, en geregeld verschillen deskundigen over de interpretatie ervan.

Het gaat in dit soort gevallen dus niet om 'harde', op zichzelf staande belemmeringen. Eerder is sprake van een versterkende negatieve factor die in meerdere of mindere mate een rol speelt bij alle overige issues hieronder.

Voorbeeld
Een provincie kan ontheffingen verlenen voor bepaalde gevaarlijke transporten. Daarvoor moet een route worden uitgestippeld met zo min mogelijk gevaar voor aanwonenden. Om die risico's goed in te kunnen schatten, heeft de provincie een zo compleet en actueel mogelijk beeld nodig van de bewoning en het gebruik van panden. Nu is de provincie daarvoor nog aangewezen op onder meer bevolkingsdichtheidsgetallen en CBS-cijfers. De provincie wil aanvankelijk uit een koppeling tussen de BAG[2] en de GBA betere informatie (geen persoonsgegevens) halen. De wet GBA voorziet echter niet in een dergelijke verstrekking. In een workshop kijken medewerkers van de provincie nog eens goed naar de geldende wet- en regelgeving en naar hun eigen behoefte. Als ze zo alle relevante informatie op een rijtje hebben, komen ze tot de conclusie dat ze anders dan ze dachten met de al beschikbare informatie uit de voeten kunnen.

Een gebrek aan overzicht is een tweesnijdend zwaard. Aan de ene kant kan het ertoe leiden dat soms voor de pragmatische benadering wordt gekozen: "Laten we het maar doen, want de burger moet geholpen worden" c.q. "… de boef moet opgespoord worden". Aan de andere kant neemt men soms juist ook het zekere voor het onzekere, met onnodige terughoudendheid als gevolg. Zeker bij ketens van verstrekkingen en andere complexe samenwerkingen kan onduidelijkheid op deze manier snel uit de hand lopen. Daar is uiteindelijk niemand bij gebaat.

"De inspectie heeft uit de interviews met gemeenten het beeld gekregen dat respondenten beperkingen ervaren in de dienstverlening als gevolg van de ervaren complexiteit van de privacywetgeving. Het kan zijn dat gemeenten (te) snel denken de Wbp en materiewetgeving te overtreden."

Bron: Inspectie SZW, "Informatie-uitwisseling van de SUWI-keten met andere partijen", augustus 2012

[2] Basisregistraties Adressen en Gebouwen.

2.2. Wet- en regelgeving

Het is van belang om te beseffen dat 'persoonsgegeven' een breed begrip is. Het verwijst niet alleen naar 'persoonsidentificerende gegevens' zoals NAW-gegevens, BSN[3], geboorteplaats en -datum, paspoortnummer of DigiD-inlogcode. Zo zijn bijvoorbeeld ook klantprofielen, medische dossiers, strafdossiers, gegevens over verzonden en ontvangen e-mail of bezochte website, opnames van telefoongesprekken en beelden van bewakingscamera's meestal persoonsgegevens. Daarnaast zijn er diverse gegevens die in sommige contexten wel maar in andere geen persoonsgegevens zijn, zoals adressen, kenteken en gegevens over eenmanszaken.

Aan de grondrechten op bescherming van de persoonlijke levenssfeer en bescherming van persoonsgegevens is invulling gegeven in een behoorlijk aantal wetten en lagere regelgeving. Hieronder volgt een beknopt overzicht.

De overkoepelende privacywet is de Wet bescherming persoonsgegevens (WBP).

Voor enkele overheidssectoren is in plaats van de WBP 'eigen' wetgeving van toepassing, onder meer:

- bevolkingsadministratie (Wet gemeentelijke basisadministratie persoonsgegevens)
- politiegegevens (Wet politiegegevens)
- justitiële gegevens (Wet justitiële en strafvorderlijke gegevens)
- gegevensverwerkingen door inlichtingen- en veiligheidsdiensten (Wet op de inlichtingen en veiligheidsdiensten).

Voor een aantal basisregistraties zijn de algemene regels uit de WBP nader uitgewerkt, zoals:

- het Kentekenregister c.q. de BRV[4] (Wegenverkeerswet 1994)
- het Handelsregister c.q. het NHR[5] (Handelsregisterwet)
- het Kadaster c.q. de BRK[6] (Kadasterwet)

Voor de meeste overheidssectoren zijn de algemene regels uit de WBP nader uitgewerkt in sectorale wet- en regelgeving, zoals:

- de Algemene Wet Rijksbelastingen (AWR)

[3] Burgerservicenummer.
[4] Basisregistratie Voertuigen.
[5] Handelsregister.
[6] Basisregistratie Kadaster.

- de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (Wet SUWI)

- de Wet Maatschappelijke Ondersteuning (WMO)

Tot slot gelden er voor de overheid nog diverse andere wetten die invloed hebben op de verwerking van persoonsgegevens. Het gaat dan om zowel specifiek op dat onderwerp gerichte wetten (zoals de Wet Algemene Bepalingen Burgerservicenummer) als andere (zoals de Algemene Wet Bestuursrecht).

Uiteraard hangt onder veel van deze wetten nog een omvangrijk complex aan lagere regelgeving. Er is dus sprake van een veelvoud aan regels, waarvoor verschillende ministeries verantwoordelijk zijn. Het waar nodig op elkaar afstemmen van die regels vergt dan ook samenwerking over de departementale grenzen heen.

Problemen veroorzaakt door het complexe geheel aan privacywet- en -regelgeving vallen onder te verdelen in twee soorten:

- daadwerkelijk blokkerende wet- en regelgeving

- wet- en regelgeving over de interpretatie waarvan discussie bestaat

2.2.1. Daadwerkelijk blokkerende wet- en regelgeving

Hier gaat het over wet- en regelgeving waarvan algemeen erkend wordt dat deze bepaalde verwerkingen niet toestaat, terwijl die in ieder geval door sommige partijen wel als gewenst gezien worden. Zulke blokkeringen kunnen bedoeld of onbedoeld zijn.

Bedoelde blokkeringen

Het kan zijn dat een door een of meerdere partijen gewenste verwerking duidelijk en bewust niet toegestaan is op basis van de bestaande regels. In feite wordt daarmee de overweging die gemaakt is ten tijde van het tot stand komen van de betreffende regels ter discussie gesteld, bijvoorbeeld op grond van gewijzigde maatschappelijke omstandigheden. Mocht dit leiden tot de conclusie dat de blokkering opgeheven dient te worden, dan moet de betreffende wetgeving aangepast worden.[7]

In hoofdstuk 1 is aangegeven dat de huidige en voorgenomen wet- en regelgeving hier als uitgangspunt geldt. Bedoelde blokkeringen vallen daarmee buiten de reikwijdte van de huidige analyse en worden daarom niet nader beschouwd. Wél worden in de volgende paragraaf een aantal gevallen besproken waar sprake is van blokkeringen die door de wetgever zonder opzet lijken te zijn gecreëerd.

[7] Zulke aanpassingen zijn overigens alleen mogelijk binnen de kaders van de (nationale en Europese) privacyregels.

Voorbeeld
Een aantal gemeenten betoogt dat de scheiding tussen publieke en niet-publieke taken administratief onhandig is en geld en tijd kost.
Juridisch gezien is het nu zo dat in de meeste gevallen gegevens uit de GBA en de RNI[8] alleen voor publieke taken gebruikt mogen worden. Anders dan niet-overheidsorganisaties moeten gemeenten (en andere overheidsorganisaties) daardoor een soort 'dubbele' boekhouding bijhouden. Dat kan efficiënter en klantvriendelijker door gemeenten de voor publieke taken beschikbare gegevens ook te laten gebruiken voor de eigen medewerkerregistratie en voor de niet-publieke taken die ze uitvoeren.
Het gaat om een beperkte gegevensset (zoals NAW-gegevens) die alleen binnen de eigen administratieve organisatie gebruikt mag worden. En de gemeente heeft die (soort) gegevens voor de taken in kwestie sowieso nodig en moet ze dus in ieder geval ergens vandaan halen.
Diverse gemeenten betogen dat binnen deze grenzen een 'enkele' boekhouding toch mogelijk zou moeten zijn.

Een geval apart vormt hier nog de positie van knooppunten zoals het Inlichtingenbureau, BKWI, RINIS en SNG. Waar het gaat om het ontsluiten van basisregistraties wordt er in toenemende mate gekeken naar zulke knooppunten als mogelijke probleemoplossers. Voor BKWI is dat echter problematisch vanwege zijn specifieke taken en verantwoordelijkheden in de socialezekerheidsector, die ook vastliggen in de Wet SUWI. En SNG moet zich statutair beperken tot dienstverlening aan deurwaarders.

Onbedoelde blokkeringen

In een aantal gevallen werpt de huidige wet- en regelgeving blokkeringen op, terwijl het duidelijk lijkt dat dat niet zo bedoeld is. Dit probleem uit zich voornamelijk in drie vormen: gesloten verstrekkingenregimes, techniekafhankelijkheid en het gebrek aan mogelijkheden om statistische gegevens te verwerken.

Gesloten verstrekkingenregimes

Wet- en regelgeving loopt bijna per definitie achter op maatschappelijke ontwikkelingen. Dat is een probleem voor wetgeving waarbij sprake is van gesloten verstrekkingenregimes. Dat wil zeggen dat de betreffende wet- en regelgeving een limitatieve opsomming bevat van de mogelijke verstrekkingen van persoonsgegevens uit een registratie. Maatschappelijke ontwikkelingen kunnen nieuwe of andere uitwisselingen, mogelijk ook met nieuwe of andere partijen, noodzakelijk of wenselijk maken. De wet- en regelgeving moet daarvoor dan aangepast worden.

[8] Basisregistratie Niet Ingezetenen.

Voorbeeld
Voor het uitvoeren van de jeugdgezondheidszorg heeft de GGD gegevens nodig over welke kinderen er op de scholen in zijn regio zitten. De GGD zou deze graag van DUO krijgen, maar de wettelijke regels voorzien daar niet in. Toen die werden opgesteld was deze casus überhaupt nog niet in beeld. Daardoor moet de GGD de scholen om dezelfde gegevens vragen die ze ook al aan DUO geleverd hebben.

Techniekafhankelijkheid

Een bijzondere vorm van onvoorziene ontwikkelingen vormen technologische vernieuwingen. Het komt geregeld voor dat regels zijn toegeschreven naar een specifieke technische inrichting van de verwerking. Soms is zonder succes geprobeerd om wet- en regelgeving techniekonafhankelijk te formuleren, in andere gevallen is men daar niet eens aan toegekomen. Hoe dan ook kan dit ertoe leiden dat de regels nieuwe oplossingen onmogelijk maken, hoewel de gegevensverwerking in kwestie op zich niet op bezwaren lijkt te stuiten.

Voorbeeld
Nogal wat gerechtsdeurwaarders verrichten ook diensten als gemeentelijke deurwaarder. Als gerechtsdeurwaarder zijn zij geautoriseerd voor het ontvangen van gegevens uit de GBA. Daarvoor maken ze gebruik van een aansluiting op het netwerk van SNG[9]. Als gemeentelijke deurwaarder mogen zij gebruik maken van de gemeentelijke toegang tot de GBA. Daarvoor kunnen ze echter niet het SNG-netwerk gebruiken. Het autorisatiebesluit voor SNG staat dat namelijk niet toe. Terwijl de deurwaarder dus met één druk op de knop bij de benodigde gegevens zou kunnen komen, waar hij ook recht op heeft, moet hij in plaats daarvan naar het gemeentehuis gaan om ze daar op te halen. Aanvullende regelgeving (een tweede autorisatiebesluit) is daarom onontkoombaar om dit te regelen. Een eerder verzoek daartoe is op juridische gronden afgewezen.

Gebrek aan mogelijkheden om statistische gegevens te verwerken

In sommige gevallen bestaat er bij afnemers een informatiebehoefte waarin voorzien kan worden door het verstrekken van statistische of geaggregeerde informatie gebaseerd op persoonsgegevens. De afnemer heeft dan dus geen belang bij de persoonsgegevens zelf. Maar hij heeft wel statistische of geaggregeerde informatie nodig die alleen kan worden geproduceerd op basis van persoonsgegevens. Hoewel de afnemer dus geen persoonsgegevens verstrekt krijgt, is het om in zijn informatiebehoefte te kunnen voorzien wel nodig om persoonsgegevens te verwerken.

Op grond van de algemene privacyregels uit de WBP is het – binnen zekere grenzen – toegestaan om persoonsgegevens te verwerken om daaruit statistische of geaggregeer-

[9] Stichting Netwerk Gerechtsdeurwaarders.

de informatie te halen. In de gesloten verstrekkingenregimes van bepaalde basisregistraties is met zo'n mogelijkheid echter geen rekening gehouden. Het is dan voor een bronhouder niet toegestaan om statistische informatie te verstrekken die gebaseerd is op persoonsgegevens uit zo'n registratie.

Overigens is de scheiding niet helemaal duidelijk met de volgende categorie: wet- en regelgeving over de interpretatie waarvan discussie bestaat. Sommige juristen zien namelijk mogelijkheden om ook binnen de huidige kaders statistische gegevens gebaseerd op persoonsgegevens te verstrekken, zelfs wanneer daarvoor een expliciete wettelijke basis ontbreekt.

Voorbeeld
DICA is een stelsel van registraties in de zorg gericht op kwaliteitsverhoging en kostenbesparing. Om de effectiviteit van behandelingen zo goed mogelijk in kaart te kunnen brengen hebben zij behoefte aan mortaliteitscijfers (op individueel niveau). Gegevens over overledenen worden niet beschouwd als persoonsgegevens. Niettemin lukt het DICA vooralsnog niet om deze gegevens uit de GBA geleverd te krijgen.

Voorbeeld
Politiekorpsen in de grensstreek werken nauw samen met de collega-korpsen uit België en Duitsland. In het kader daarvan willen zij graag statistische gegevens uitwisselen gebaseerd op onder meer de verschillende persoonsgegevens in hun bestanden; daar zitten ook persoonsgegevens bij die uit basisregistraties afkomstig zijn. De wet politiegegevens biedt daarvoor echter geen grondslag, hoewel het niet waarschijnlijk is dat tegen zo'n verstrekking inhoudelijke bezwaren bestaan.

2.2.2. Wet- en regelgeving over de interpretatie waarvan discussie bestaat

Privacywet- en -regelgeving blinkt uit door vage normen en grijze gebieden, aangevuld met een bont geheel aan formele en informele jurisprudentie. Verschillende partijen kunnen soms dan ook flink van mening verschillen over de interpretatie daarvan. Wat mag er wel en wat niet? En wat zijn de randvoorwaarden? Als we kijken naar het gebruik van persoonsgegevens uit basisregistraties, dan kunnen leveranciers en afnemers het oneens zijn met elkaar of met toezichthouders zoals het CBP. Het kan zowel gaan om de fundamentele vraag of een partij een grondslag heeft voor het verkrijgen van bepaalde gegevens als over 'flankerende' vragen over bijvoorbeeld gegevensbeveiliging en verantwoordelijkheid. Die laatste komen overigens in latere paragrafen nog aan de orde.

Voorbeeld
SNG heeft een app ontwikkeld waarmee geautoriseerde afnemers op hun tablet toegang kunnen krijgen tot GBA-informatie. Naar aanleiding van een bericht daarover vraagt een gemeente zich af in hoeverre dat is toegestaan. BPR antwoordt dat toegang tot de GBA buiten de kantoormuren van de afnemer niet is toegestaan omdat het onmogelijk is om een voldoende niveau van beveiliging van de gegevens te garanderen. Vrijwel tegelijkertijd echter constateert een andere gemeente dat de informatiebeveiliging voldoende gegarandeerd kan worden wanneer haar ambtenaren via tablets of smartphones toegang tot de GBA krijgen.

2.3. Ketenverantwoordelijkheid

Bij het gebruiken van persoonsgegevens uit basisregistraties zijn ten minste twee partijen betrokken: de leverancier van de gegevens en de afnemer ervan.[10] Dat roept onmiddellijk de vraag op wie er op welke aspecten van de gegevensverstrekking kan worden aangesproken.

De belangrijkste issues zijn hier:

1. Verantwoordelijkheden zijn niet of onduidelijk belegd

2. Verantwoordelijkheden zijn (mogelijk) verkeerd belegd

3. Verantwoordelijkheid verstrekker voor handelen ontvanger

Op deze punten wordt hieronder nader ingegaan.

Terzijde zij nog opgemerkt dat de nieuwe EU-privacyverordening nog nergens echt op het netvlies lijkt te staan. Weliswaar wordt deze verordening naar verwachting pas eind 2013 of begin 2014 van kracht, en geldt daarna nog een overgangs- en implementatietermijn van twee jaar, maar er gaat ook wel het nodige veranderen en dat zal behoorlijke impact hebben. Dit issue is echter niet specifiek voor (gebruikers van gegevens uit) basisregistraties, maar speelt overheids- en zelfs maatschappijbreed.

2.3.1 Verantwoordelijkheden zijn niet of onduidelijk belegd

Wanneer verschillende partijen betrokken zijn bij een verwerking van persoonsgegevens, dan moeten ze met elkaar duidelijke afspraken maken over ieders rol, taken, be-

[10] De leverancier is meestal de bronhouder van de basisregistratie, maar soms ook een ontvanger die de gegevens op zijn beurt weer aan een derde partij doorlevert. Dat laatste is meteen een voorbeeld waarbij drie partijen betrokken zijn (basisregistratie, 'doorleverancier' en de uiteindelijke afnemer); een ander voorbeeld daarvan is het afnemen van gegevens uit een basisregistratie via een knooppunt.

voegdheden en verantwoordelijkheden. De privacywetgeving onderscheidt hiervoor de rollen “verantwoordelijke” en “bewerker”.[11]

De verantwoordelijke is degene die doel en middelen van de verwerking bepaalt en primair op de verwerking kan worden aangesproken.

Het kan zijn dat een verantwoordelijke andere partijen inhuurt om namens hem persoonsgegevens te verwerken. Dat zijn bewerkers. Een bewerker verwerkt gegevens in opdracht van de verantwoordelijke, en legt dan ook primair aan die laatste verantwoording af.

“**Ben ik bewerker?**
Uw dienstverlening moet gericht zijn op het uitvoeren van een bepaalde verwerking van persoonsgegevens ten behoeve van de opdrachtgever. U voert bijvoorbeeld in opdracht van een bedrijf de salarisadministratie van dat bedrijf uit: u bent bewerker. Is uw dienstverlening op iets anders gericht en verwerkt u daarbinnen zelfstandig persoonsgegevens van uw opdrachtgever, dan bent u geen bewerker, maar verantwoordelijke. Als u bijvoorbeeld als pensioen-verzekeraar een flexibele collectieve pensioenregeling aan een bedrijf hebt aangeboden en dat bedrijf verstrekt u ter uitvoering van die regeling de gegevens van de deelnemende werknemers, dan bent u zelf verantwoordelijk voor het vervolgens verwerken van die gegevens. Als bewerker hebt u geen zeggenschap over de gegevens.”

Bron: Handleiding voor verwerkers van persoonsgegevens. Ministerie van Justitie, april 2002.

De WBP stelt randvoorwaarden aan het inschakelen van een bewerker. Zo moeten er schriftelijke vastgelegde, juridisch bindende afspraken gemaakt over de werkzaamheden die de bewerker voor de verantwoordelijke gaat verrichten.

In samenwerkingsrelaties is vaak geen sprake van bewerkerschap, maar zijn twee of meer betrokken partijen alle te beschouwen als verantwoordelijke voor de verwerking. Dat is een figuur die de wet toelaat. Vereist is dan wel dat de verantwoordelijken goede afspraken maken over wie voor welke delen van de verwerking verantwoordelijk is. Doen ze dat niet, dan kan iedere verantwoordelijke worden aangesproken op de gehele verwerking.

[11] De begrippen “verantwoordelijke” en “bewerker” komen uit de WBP. In wetten over gegevensverwerkingen waarop de WBP niet van toepassing is (zoals de Wet GBA en de Wet Politiegegevens) worden ze op dezelfde manier gebruikt.

"**Voorbeeld: Portalen voor eOverheid**
Portalen voor eOverheid fungeren als schakel tussen de burger en overheidsdiensten: het portaal zendt verzoeken van burgers door en plaatst de documenten van de overheidsdienst zodat zij door de burger kunnen worden opgevraagd. Elke overheidsdienst blijft verantwoordelijk voor de verwerking van degegevens voor de eigen doeleinden. Toch kan ook het portaal zelf als voor de verwerking verantwoordelijk worden beschouwd. Het verwerkt namelijk zowel aanvragen van burgers (deze worden verzameld en doorgestuurd naar de bevoegde dienst) als overheidsdocumenten (deze worden op het portaal geplaatst en ontsloten, bijvoorbeeld voor burgers die ze kunnen downloaden) voor andere doeleinden (bevorderen van eOverheidsdiensten) dan waarvoor de gegevens oorspronkelijk door elke overheidsdienst werden verwerkt.
Deze voor de verwerking verantwoordelijken moeten onder meer waarborgen dat persoonsgegevens van de gebruiker veilig naar het systeem van de overheidsdienst worden verzonden, omdat deze overdracht op macroniveau een wezenlijk onderdeel is van het geheel van verwerkingen dat via het portaal plaatsvindt."
Bron: Art. 29 Werkgroep. Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker". *WP 169.*

In de praktijk blijkt vaak dat partijen die op een of andere manier met elkaar samenwerken geen duidelijke afspraken maken met elkaar over ieders verantwoordelijkheid of bewerkerschap ten aanzien van de persoonsgegevens die verwerkt worden. Dit leidt vroeg of laat onherroepelijk tot problemen, ook waar het het gebruik van persoonsgegevens uit basisregistraties aangaat. Op een gegeven moment is eenvoudig niet meer helder wat er juridisch wel en niet is toegestaan, omdat niet duidelijk is welke rol de verschillende partijen spelen. En ook loopt de burger die geconfronteerd wordt met een zich door een keten verspreidende fout in zijn gegevens dan een grote kans dat hij van het kastje naar de muur wordt gestuurd.

Maken partijen wél duidelijke afspraken, dan realiseren ze zich daarbij soms onvoldoende wat daarvan de consequenties zijn ten aanzien van de verwerking van persoonsgegevens.

Voorbeeld
Een gemeentelijke bibliotheek wordt verzelfstandigd in een stichtingsvorm. Dat heeft onvermoede gevolgen voor de ledenadministratie. Omdat de bibliotheek door de verzelfstandiging geen onderdeel (meer) is van de gemeente, mag zij namelijk geen GBA-gegevens meer verstrekt krijgen als binnengemeentelijke afnemer.[12]

2.3.2 Verantwoordelijkheden zijn (mogelijk) verkeerd belegd

Twee issues die in de gevoerde gesprekken niet expliciet naar voren zijn gekomen, maar die niettemin serieuze aandacht verdienen, zijn de status van kopiebestanden en de rol

[12] In dit geval bleek gelukkig nog een oplossing voorhanden: de bibliotheek kon de gegevens alsnog ontvangen als "bijzondere derde". Daarvoor was dan wel per gemeente waarin leners woonachtig waren een gemeentelijke verordening nodig om de verstrekking van leners uit die gemeente te regelen.

van knooppunten. Hieraan wordt momenteel gewerkt door het project Oplossingen (cluster STOUT) in samenwerking met de stelselarchitect.

Kopiebestanden

Veel afnemers bevragen basisregistraties niet voortdurend *real-time*, maar maken daarentegen (of in aanvulling daarop) gebruik van kopiebestanden. De afnemer heeft dan dus een eigen bestand dat is gevuld met uit de basisregistratie verkregen gegevens. Denk bijvoorbeeld aan een uitvoeringsorganisatie die een aantal GBA-gegevens van burgers in haar eigen cliëntsysteem bijhoudt. Dat leidt tot vragen rondom onder meer de kwaliteit, actualiteit en integriteit van die gegevens (zie daarvoor paragraaf 2.5).

Er kan echter ook een fundamentelere vraag spelen, te weten naar de verantwoordelijkheden van verstrekker en ontvanger. De WBP bepaalt namelijk dat een bestuursorgaan niet meer gegevens mag verwerken dan noodzakelijk is voor de goede vervulling van zijn publiekrechtelijke taken. Of een kopiebestand aan dat criterium voldoet is sterk afhankelijk van de wijze waarop het is ingericht. Het kan voorkomen dat een kopiebestand meer gegevens bevat, van meer burgers, dan op een gegeven moment nodig zijn voor de taken van het bestuursorgaan. Bijvoorbeeld doordat de kopie nog gegevens bevat van een burger die inmiddels geen cliënt meer is. Een andere mogelijkheid dat de kopie, om bruikbaar te zijn, gegevens uit een bepaalde basisregistratie moet bevatten van alle burgers waarmee een overheidsorgaan te maken kan krijgen (bijvoorbeeld bij een gemeente: van alle inwoners).

Staan er in een kopiebestand meer persoonsgegevens dan de afnemer nodig heeft voor zijn taken, dan kan die daarvoor juridisch gezien niet (alleen) de verantwoordelijke zijn. Het lijkt dan onvermijdelijk dat de leverancier van de gegevens ook verantwoordelijk is voor de kopie bij de afnemer. De afnemer zelf is dan mede-verantwoordelijke of bewerker. In beide gevallen moeten de consequenties daarvan goed doordacht worden, en zullen partijen afspraken met elkaar moeten maken.

Verantwoordelijkheid knooppunten

Wanneer er verschillende partijen betrokken zijn bij een verwerking van persoonsgegevens, dan hebben zij een zekere mate van vrijheid om onderling afspraken te maken over wie er verantwoordelijk is voor (welk deel van) de verwerking, en over eventueel bewerkerschap. Die vrijheid is echter verre van onbeperkt. Dat blijkt bijvoorbeeld uit het advies waarin de Artikel 29 Werkgroep, het samenwerkingsverband van Europese privacytoezichthouders, deze materie adresseert (zie kader).[13]

[13] Artikel 29 Werkgroep. *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker".* WP 169.

"De Groep erkent dat het moeilijk is om de definities van de richtlijn toe te passen in een complexe omgeving, waarin vele scenario's mogelijk zijn met voor de verwerking verantwoordelijken en verwerkers, alleen of gezamenlijk, met verschillende mates van autonomie en verantwoordelijkheid.
In zijn analyse heeft de groep benadrukt dat verantwoordelijkheden zodanig moeten worden belegd dat de naleving van de regelgeving met betrekking tot gegevensbescherming in de praktijk voldoende is gewaarborgd."

Bron: Art. 29 Werkgroep. Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker". *WP 169.*

Waar dit op neerkomt, is dat taken, rollen, verantwoordelijkheden en bevoegdheden in de praktijk vaak op zo'n manier zijn ingericht dat betrokken partijen niet ontkomen aan een bepaalde rol – meestal die van (mede)verantwoordelijke.

Knooppunten zoals het Inlichtingenbureau, BKWI, SNG en (in mindere mate) RINIS hebben op dit punt mogelijk een probleem zonder dat zij zich daarvan bewust zijn. Om dat te introduceren wordt in de volgende alinea's eerst kort de SWIFT-affaire besproken.

Medio 2006 komt SWIFT in het nieuws. SWIFT is het belangrijkste internationale elektronische netwerk waarover banken betalingen tussen hun klanten regelen. Alle grote Europese banken maken er gebruik van. De organisatie is gevestigd in België, en haar systemen bevinden zich in een EU-lidstaat. Echter: een backup van de systemen van SWIFT bevindt zich in de Verenigde Staten. De Amerikaanse overheid kan daardoor financiële gegevens over EU-burgers van SWIFT vorderen, en doet dat ook.

Naar aanleiding van de onstane commotie stelt de Artikel 29 Werkgroep – waarin de nationale EU-privacytoezichthouders samenwerken – een onderzoek in. SWIFT stelt zich op het standpunt dat zij slechts bewerker is, en dat de banken die van het systeem gebruik maken de verantwoordelijken zijn voor de verwerking. Deze redenering wordt door de gezamenlijke toezichthouders van de hand gewezen: SWIFT is vanwege de grote mate van vrijheid die zij heeft bij de invulling van haar rol wel degelijk ook een verantwoordelijke. (Zie ook het kader hieronder.)

Mogelijk moeten ook sommige knooppunten binnen de overheid om vergelijkbare redenen als medeverantwoordelijke beschouwd worden voor de gegevensuitwisselingen die over hun netwerk plaatsvinden. Weliswaar beschikken zij naar het zich laat aanzien over minder vrijheid van handelen dan SWIFT, maar de vraag is of het verschil groot genoeg is om ze niettemin puur als bewerkers te kunnen beschouwen.

2.3.3. Verantwoordelijkheid verstrekker voor handelen ontvanger

In de vorige paragraaf ging het over de soms gebrekkige rolverdeling tussen verschillende partijen: wie is of zijn de verantwoordelijke(n), wie de bewerker(s)? Maar ook als die rollen op zichzelf duidelijk zijn, bestaat er vaak nog veel onduidelijkheid over de precieze verantwoordelijkheden die dat meebrengt voor de betrokken partijen.

Hierboven is al aangegeven dat de verantwoordelijke degene is die kan worden aangesproken op een verwerking van persoonsgegevens. Formeel juridisch zijn de verantwoordelijkheden bij een verstrekking van gegevens in het algemeen dan ook vrij helder: de verstrekkende partij dient voldoende zorgvuldigheid te betrachten bij het nemen van een besluit om gegevens door te verstrekken; de ontvangende partij is verantwoordelijk vanaf het moment dat de gegevens zijn ontvangen.

In de praktijk ligt het vaak ingewikkelder. Dat heeft ermee te maken dat lang niet altijd duidelijk is hoe de verstrekkende partij de eis van zorgvuldigheid concreet moet invullen. Is het voldoende als de verstrekking wettelijk is voorgeschreven? Zijn er concrete extra eisen gesteld in de wet- en regelgeving voor de betreffende basisregistratie? Gelden er strengere voorwaarden in het geval van omvangrijke of structurele verstrekkingen? Hoe pro-actief moet de verstrekker in dezen optreden? En mocht er iets mis gaan aan de kant van de ontvanger, heeft de verstrekker dan in de praktijk ook mogelijkheden om handhavend op te treden? “De stekker eruit” is vaak geen reële optie…

Voorbeeld
Naar verluidt zijn bij sommige gemeenten de autorisaties zodanig dat bijvoorbeeld parkeerwachters toegang hebben tot gegevens van de sociale dienst. De leveranciers van sommige van die gegevens zien geen goede mogelijkheden om hier wat aan te doen.

“[In de Memorie van Toelichting bij het wetsvoorstel tot Wijziging van de Wegenverkeerswet 1994] is het belang onderstreept van controle op de doelbinding. Ten aanzien van het toezicht op ontvangers van persoonsgegevens is aangegeven dat tijdens de looptijd van de gegevensverstrekking de ontvangers door middel van periodieke steekproeven worden gecontroleerd. Voorts wordt aangegeven dat bij misbruik allereerst een interne controle plaatsvindt op de betrokken gegevens. Vervolgens worden de afnemers schriftelijk om opheldering gevraagd en zo nodig gehoord. Dit kan leiden tot een waarschuwing of het tijdelijk of blijvend achterwege laten van de gegevensverstrekking.”

Bron: CBP. Onderzoek naar de controle door de Dienst Wegverkeer op de online verstrekking van persoonsgegevens uit het kentekenregister aan beroepsbeoefenaren. Rapport definitieve bevindingen. Juni 2012

“Bescherming van de privacy en doelbinding zijn weliswaar verankerende beginselen, maar voor de overheidsinstanties dienen zij het verder gelegen doel van het waarborgen van de betrouwbaarheid van de overheid en daarmee de effectiviteit en de efficiency van het overheidsoptreden. De bescherming van de belangen van de burger wordt daarbij ook als het belang van de eigen organisatie gezien, omdat daarmee de informatiestroom open wordt gehouden. [...] De vertegenwoordigers van burgers en bedrijven [hechten] zeer aan de bescherming van de positie van hun cliënt. Bescherming van de privacy, doelbinding en geheimhouding zijn hier de sleutelbegrippen ter omschrijving van deze belangen. Overheidsorganisaties zullen dus om hun informatiepositie te behouden en om hun imago als betrouwbare overheid te beschermen noodzakelijkerwijs een goede bescherming van deze belangen moeten bieden.
Dit blijkt ook uit de positie van de ontvangers van gegevens. Daar ontbreekt de directe relatie tot het subject en leven de noties geheimhouding, bescherming van de privacy en

doelbinding minder sterk bij de verwerking van gegevens. Voor de ontvanger nemen juist de resultaten die met de verkregen gegevens kunnen worden gerealiseerd een prominente plaats in."
[Conclusie expertmeeting:] "Voor gegevensuitwisseling is communicatie het eerste vereiste. Niemand verstrekt graag gegevens als niet duidelijk is wat ermee gebeurt, aldus de experts. Zicht op het hele proces is nodig, zowel inhoudelijk als bijvoorbeeld in het tijdsverloop. De originele bronhouder wil weten of en, zo ja, welke actie plaatsvindt op grond van de ontvangen gegevens. Wat gebeurt er bijvoorbeeld met gegevens nadat de actie in het kader waarvan de gegevens zijn verkregen is afgelopen?"

Bron: Universiteit van Amsterdam, Rapport Gegevensuitwisseling door Toezichthouders, *in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (Justitie).*

2.4. Regels voor hergebruik

Uit de gesprekken en de geraadpleegde literatuur komt herhaaldelijk naar voren dat het voor partijen vaak onduidelijk is welke privacyregels er gelden voor hergebruikte gegevens. Daarmee bedoelen we hier alle gebruik van basisregistraties anders dan door de beheerder van de registratie voor eigen doeleinden. Een veel voorkomende vorm van hergebruik is doorverstrekking: de afnemer van gegevens uit een basisregistratie die op zijn beurt de gegevens aan een derde partij verstrekt (zie de laatste alinea van deze paragraaf).

De onduidelijkheid die daarvan het gevolg is, heeft de gevolgen die in de paragraaf "Informatie" al genoemd werden. Aan de ene kant kan het ertoe leiden dat soms voor de pragmatische benadering wordt gekozen: "Laten we het maar doen, want de burger moet geholpen worden" c.q. "… de boef moet opgespoord worden". Aan de andere kant neemt men soms juist ook het zekere voor het onzekere, met onnodige terughoudendheid als gevolg. Zeker bij ketens van verstrekkingen en andere complexe samenwerking kan onduidelijkheid op deze manier snel uit de hand lopen.

Hoewel het gaat om regels die veelal de mogelijkheden beperken om persoonsgegevens te gebruiken en uit te wisselen, vormt de onduidelijkheid erover niettemin vaak een belemmering voor gebruik. Daarom wordt dit issue hieronder nader uitgewerkt.

In een aantal gevallen legt de wet- en regelgeving voor een bepaalde basisregistratie beperkingen op aan het gebruik van de verstrekte gegevens door (alle of bepaalde) afnemers.

Voorbeeld
De verstrekking van gegevens uit het Kentekenregister c.q. de Basisregistratie Voertuigen is geregeld in de Wegenverkeerswet 1994 en nader uitgewerkt in artikel 9 van het Kentekenreglement. Art. 9 lid 3 Kentekenreglement bepaalt:
"Bij ministeriële regeling kunnen regels worden gesteld omtrent het gebruik van de aan de in het eerste lid genoemde personen en instanties verstrekte gegevens. Daarbij kun-

nen beperkingen aan het gebruik worden gesteld alsmede voorschriften ten aanzien van de beveiliging van de verstrekte gegevens en voorschriften voor het verlenen van medewerking aan het toezicht door de [RDW]".
Van die bevoegdheid heeft de minister gebruik gemaakt. De Regeling gegevensverstrekking kentekenregister 2008 bevat uitgebreide bepalingen over wie welke gegevens uit het Kentekenregister waarvoor mag gebruiken, hoe de gegevens beveiligd moeten worden en hoe de afnemers verantwoording moeten afleggen over het naleven van die bepalingen.

Het andere geval komt echter ook voor: De wet- en regelgeving voor een basisregistratie schept wel mogelijkheden om gegevens te verstrekken, maar kadert het gebruik ervan door afnemers niet nader in.

Voorbeeld
De verstrekking van gegevens uit het Handelsregister (NHR) is geregeld in de Handelsregisterwet en nader uitgewerkt in Hoofdstuk 8 van het Handelsregisterbesluit 2008. De Handelsregisterwet bevat in artikel 28 een opsomming van publieke organisaties die voor bepaalde doeleinden het Handelsregister mogen doorzoeken met de persoonsnaam van een functionaris van een onderneming als zoekingang. Nieuwe manieren van ontsluiting van het Handelsregister (als machine-machine koppeling en kopieën) maken het betrekkelijk eenvoudig dat de ontvangende partij persoonsbestanden kan opbouwen en zo artikel 28 kan omzeilen. Dit schept onduidelijkheid en onzekerheid. De wet schept in artikel 23 ook de mogelijkheid om beperkingen op te nemen in het Handelsregisterbesluit. Van die bevoegdheid heeft de wetgever echter geen gebruik gemaakt.

Extra ingewikkeld vindt men het soms als het over de GBA gaat. Die kent immers een apart wettelijk regime: de WBP is er niet op van toepassing. Dat roept de vraag op wanneer gegevens vallen onder de reikwijdte van de Wet GBA, en wanneer onder de reikwijdte van de WBP.

Voorbeeld
Een afnemer van GBA-gegevens wil weten in hoeverre hij de gegevens op zijn beurt aan andere overheidspartijen mag verstrekken, gelet op de autorisaties die gelden voor het gebruik van de GBA. Concreet heeft hij de volgende vragen:
- Mag een afnemer überhaupt doorverstrekken?
- Zo ja, mag hij dan bepalen waarvoor de afnemer van de gegevens volgens het GBA-regime geautoriseerd is?
- Zodra gegevens zijn afgenomen door de afnemer, in hoeverre zijn het dan nog GBA-gegevens?

Kort gezegd zit het als volgt. Op de GBA is alleen de Wet GBA van toepassing.14 Zodra gegevens uit de GBA verstrekt zijn, is alleen de WBP van toepassing. Wel is het dan zo dat de algemene privacyregels uit Hoofdstuk 2 paragraaf 1 WBP ervoor zorgen dat de regels voor de GBA in behoorlijke mate “doorwerken” op het gebruik van de gegevens door afnemers. Met de bepalingen uit de Wet GBA moeten die dus niettemin nadrukkelijk rekening houden. Voor de andere basisregistraties geldt hetzelfde, met als verschil dat daarop de WBP wél van toepassing is.

In het bijzonder geldt dit voor het principe van doelbinding. Dat zegt dat persoonsgegevens alleen gebruikt mogen worden voor vooraf vastgestelde doeleinden. Omdat de wetgever ook wel inzag dat het in die absolute vorm te strikt was, heeft hij het principe van doelbinding afgezwakt. Daartoe is het begrip ‘verenigbaarheid’ geïntroduceerd. Persoonsgegevens mogen gebruikt worden voor andere doeleinden dan waarvoor ze oorspronkelijk verzameld zijn, mits het nieuwe gebruik daarmee wel *verenigbaar* is. Art. 9 WBP geeft de belangrijkste criteria die gebruikt moeten worden om te bepalen wanneer er sprake is van verenigbaar gebruik.

Voorbeeld
Begin 2005 besluit de minister van Vreemdelingenzaken om informatie uit individuele dossiers van asielzoekers in de openbaarheid te brengen als reactie op in haar ogen onjuist berichtgeving in de media.
Het CBP neemt deze verstrekking onder de loep, en concludeert: “Publicatie van gegevens uit dergelijke dossiers in de media ter verdediging van het gevoerde beleid is als uitgangspunt niet verenigbaar met het doel waarvoor de gegevens worden verwerkt: de beoordeling van de individuele zaak.”

In een aantal gevallen valt verenigbaarheid af te leiden uit de wettelijke regels. Zo geldt voor authentieke gegevens een gebruiksplicht, waarmee de wetgever feitelijk aangeeft dat verenigbaarheid verondersteld mag worden. Hetzelfde geldt wanneer wet- en regelgeving toestaat dat gegevens uit een basisregistratie voor een specifiek doel aan een bepaalde afnemer verstrekt mogen worden.

In de overige gevallen dient dan een afweging te worden gemaakt of gewenst gebruik van gegevens uit een basisregistratie verenigbaar is met het doel waarvoor de gegevens oorspronkelijk verzameld zijn. Die beoordeling is primair aan de afnemer van de gegevens: die is immers de verantwoordelijke voor de verwerking zodra hij de gegevens uit de basisregistratie verkregen heeft. Vanwege het zorgvuldigheidsbeginsel dient de verstrekker (de bronhouder van de basisregistratie) echter – bij gebreke van een wettelijke plicht om te verstrekken – ten minste een marginale toets te doen of het voorgenomen gebruik door de ontvanger verenigbaar is.

[14] Met dien verstande dat ook de Wet GBA blijft binnen het kader dat is gesteld door de EU-privacyrichtlijn, waarvan de WBP een uitwerking is.

Voorbeeld
Artikel 14.8 van het “Convenant Ketensamenwerking Mensenhandel” bepaalt dat de convenantpartner zich onthoudt van instemming voor derdenverstrekking indien verdere verwerking niet verenigbaar is met het doel waarvoor de oorspronkelijke gegevens zijn verzameld.[15]

Een speciaal geval vormen nog openbare registers. Verenigbaarheid geldt onverkort voor de persoonsgegevens daarin. Van de beheerder van het register kan echter moeilijk een controle daarop verwacht worden. Wel stelt de wet met het oog op het tegengaan van niet verenigbaar gebruik soms beperkingen aan de manier waarop de gegevens openbaar gemaakt worden.

Voorbeeld
Artikel 107c Kadasterwet beperkt de verstrekking door het Kadaster van verzamelingen persoonsgegevens “in een zodanige vorm dat daarop rechtstreeks een geautomatiseerde verwerking mogelijk is ten aanzien van een op voorhand onbepaalde groep van personen” tot een aantal specifiek omschreven gevallen.

Tot slot is nog van belang dat doelbinding kan leiden tot praktische problemen op de werkvloer wanneer medewerkers verschillende taken hebben. Zie paragraaf 2.60.

Dilemma: Meer = beter?
Hoe meer je weet van een burger, hoe minder je hem hoeft lastig te vallen, hoe gemakkelijker je met hem kan communiceren, hoe beter je hem kunt helpen, hoe zorgvuldiger je over hem kunt besluiten en hoe moeilijker hij kan frauderen.
Maar klopt dat wel? Is meer ook altijd beter? Betekent meer informatie ook meer kennis? Want hoe meer informatie, hoe groter de kans dat er fouten in zitten. En hoe moeilijker het is om te bepalen wat er van al die informatie in een concreet geval relevant is. Moet je als overheid daarom bepaalde informatie misschien helemaal niet wíllen hebben?
Maar hoe zit het dan met de zorgvuldigheid en de eisen die burgers stellen aan het niveau van dienstverlening?

De hierboven gesignaleerde issues worden navenant ingewikkelder als er sprake is van een keten van verstrekkingen. Een afnemer van gegevens uit een basisregistratie verstrekt dan op zijn beurt de gegevens door aan een derde. In een aantal gevallen is zo’n arrangement voor de derde praktischer dan het rechtstreeks van de bron afnemen van de gegevens, bijvoorbeeld omdat bij de “tussenpartij” al gegevens uit verschillende basisregistraties bij elkaar gebracht zijn, mogelijk nog verrijkt met gegevens van de tussenpartij zelf.

[15] Toetsing verenigbaarheidvereiste van art. 9 Wbp.

2.5. Bruikbaarheid en kwaliteit

Het idee van basisregistraties – en zeker van authentieke gegevens – is dat er bepaalde gegevens zijn die breed gebruikt (kunnen) worden binnen de overheid, en dat die centraal beschikbaar worden gesteld. Dat voorkomt dat overheidspartijen onafhankelijk van elkaar dezelfde gegevens gaan verzamelen, met alle verspilling van belastinggeld en administratieve lasten van dien.

De praktijk is echter weerbarstiger. Geen enkele registratie is te allen tijde een perfecte administratieve weergave van de complexe werkelijkheid – ook basisregistraties niet, zelfs niet waar het de authentieke gegevens betreft. En ook als een gegeven wel klopt, dan kan de juiste interpretatie ervan nog altijd afhankelijk zijn van de context waarin het is verzameld. Daardoor is het dan niet of minder bruikbaar voor afnemers.

Zoals bij wel meer issues rondom het gebruik van persoonsgegevens geldt dit voor *alle* gegevens uit basisregistraties. Vanwege de eisen die de privacyregels stellen aan bijvoorbeeld actualiteit en juistheid is dit issue waar het persoonsgegevens aangaat toch van een apart kaliber.

In essentie kunnen gegevens uit basisregistraties zoals gezegd om twee redenen niet of slecht bruikbaar zijn:

1. De kwaliteit (mate van juistheid, actualiteit e.d.) van de gegevens is voor de afnemer onvoldoende.

2. De definitie van het gegeven in de basisregistratie past niet precies bij het gebruik dat de afnemer ervan wil maken.

2.5.1. Kwaliteit onvoldoende

In het ideale geval vormen de gegevens in een basisregistratie een precieze administratieve weergave van de werkelijkheid die er volgens de gegevensdefinitie aan ten grondslag ligt. In de praktijk is dat echter niet haalbaar.

De mate van discrepantie tussen administratie en werkelijkheid hangt onder meer af van het belang dat de bronhouder heeft bij het zo klein mogelijk houden daarvan, de vluchtigheid van de in het gegeven vastgelegde omstandigheid, het belang dat de goedwillende burger erbij heeft om het gegeven juist te houden en het belang dat de kwaadwillende burger heeft bij onjuiste gegevens.

De meest gehoorde klacht is dat de eisen of wensen van de afnemer niet matchen met het kwaliteitsniveau dat de basisregistratie redelijkerwijs kan leveren. Dit dient echter wel in perspectief te worden gezien. Uiteraard willen afnemers het liefst 100% betrouwbaarheid, maar de vraag is welk kwaliteitsniveau zij echt nódig hebben. Ook blijkt in de praktijk de kwaliteit van gegevens in basisregistraties vaak beter dan afnemers denken, doordat verhalen over slechte gegevenskwaliteit gemakkelijk gaan rondzingen.

Wat ook voorkomt is dat de bronhouder bewust onjuiste gegevens opneemt in de basisregistratie omdat (naar het oordeel van de daarvoor verantwoordelijke ambtenaar) het opnemen van de juiste gegevens ernstige ongewenste gevolgen zou hebben voor de burger in kwestie.

Voorbeeld
Medewerkers van Artsen zonder Grenzen verblijven soms langere tijd in het buitenland. Zij zijn dan wettelijk verplicht om zich uit te schrijven uit het GBA. Dat heeft voor hen echter allerlei vervelende consequenties, bijvoorbeeld dat zij (tijdelijk) geen recht meer hebben op bepaalde uitkeringen, aanspraken en verzekeringen. Om die reden kiezen sommige ambtenaren burgerzaken ervoor om deze personen ingeschreven te laten, in afwijking van de wettelijke regels.

Natuurlijk kan de burger ook zelf – al dan niet bewust – de hand lichten met de regels door een verkeerde verblijfplaats op te geven.

Voorbeeld
Er zijn verschillende departementale ambtenaren die ver van Den Haag wonen en (tijdelijk) gebruik maken van een pied-à-terre in de hofstad waar zij doordeweeks verblijven. Wettelijk gezien moeten zij zich dan in Den Haag inschrijven in de GBA. Gevoelsmatig wonen zij vaak echter in de plaats waar ook hun gezin verblijft. Al dan niet bewust laten zij daarom na om hun verblijfplaats formeel te wijzigen. Zoals blijkt uit de recente affaire rondom staatssecretaris Co Verdaas een issue dat meer dan louter formele betekenis heeft.

En soms heeft de bronhouder eigen overwegingen om zaken onjuist te registreren.

Voorbeeld
In een gemeente wordt een pand gesplitst in meerdere zelfstandige wooneenheden. De gemeente besluit echter om huisnummer 40 formeel niet te wijzigen in huisnummers 40a, 40b enz. Aan het aantal adressen is namelijk een parkeerquotum gekoppeld. Door deze wijziging door te voeren zou de gemeente in de straat nieuwe parkeerplaatsen moeten aanleggen.

Ten slotte kan het ook op dit punt nog extra ingewikkeld worden als er sprake is van doorverstrekkingen. Weet de uiteindelijke ontvanger bijvoorbeeld wel zeker of de gegevens afkomstig zijn uit de basisregistratie, en zo ja, of ze onderweg niet veranderd zijn?

“Een bewuste iOverheid benadert de eigen informatiehuishouding voortdurend vanuit een kritische houding. Deze houding kenmerkt zich door een realistisch wantrouwen ten opzichte van de kwaliteit van zowel informatie als informatieprocessen, waarbij beide constant op waarde worden geschat en waar nodig verbeteringen worden doorgevoerd.”

Bron: WRR-rapport iOverheid

2.5.2. Gegevensdefinitie past niet

Een ander probleem is het als de gegevensdefinitie die de basisregistratie hanteert niet matcht met de definitie waarmee de afnemer werkt. De afnemer zou dan onzorgvuldig handelen als hij de gegevens uit de basisregistratie klakkeloos zou hanteren alsof ze juist waren gegeven zijn eigen definitie. Dat betekent echter dat hij extra moeite moet doen om de gegevens aan te passen aan zijn eigen definitie. Dit vermindert de meerwaarde van het gebruik van basisregistraties.

> "Als afnemer kiezen we [bij wijze van voorbeeld] de Douane, met haar normale verblijfplaats als adresbegrip. Dit adresbegrip wordt gebruikt in het proces voor verlening van vrijstellingen: maatregelen die beogen goederen vrij te stellen van rechten bij invoer en belastingen. De vraag die we onszelf stellen is of en in hoeverre voor de normale verblijfplaats hergebruik gemaakt kan worden van het woonadres van de GBA. [...]
> Gegeven de besproken definities van normale verblijfplaats en GBA-woonadres is hergebruik mogelijk voor zover de aanwezige een GBA-ingeschrevene is. In dat geval is het GBA-woonadres een aanwijzing voor het mogelijke feit dat de normale verblijfplaats Nederland is. Dat betekent dat er voor een volledige bepaling van normale verblijfplaats (veel) meer informatie nodig is, die uit andere, al dan niet elektronische, bronnen zou moeten worden betrokken. Voor niet-ingeschrevenen moet zelfs al die informatie van elders komen."
>
> *J. Kielema & P. Oude Luttighuis.* Adresinformatie en het Stelsel van Basisregistraties.Semantiek als sleutel voor hergebruik. *Essence, mei 2012.*

Dilemma: "Context is king"
Voordeel van basisregistraties is dat je gegevens die in de ene context verzameld zijn, kunt gebruiken in andere contexten. Maar dan moeten de hergebruikers zich wel bewust zijn van die veranderde context, en zich realiseren dat ze niet blindelings op de gegevens kunnen vertrouwen. Maar is dat reëel? Want dat is toch juist het idee (zeker van authentieke gegevens)?

2.6. Techniek en informatiebeveiliging

Techniek kan een belemmerende factor zijn bij het gebruik van gegevens uit basisregistraties. Het kenmerkende technische aspect bij het gebruik van *persoons*gegevens vormen de hoge eisen die worden gesteld aan de beveiliging van die informatie. De complexiteit van het geheel blijkt in de praktijk het grootste obstakel te vormen.

Het lijkt erop dat techniek en informatiebeveiliging geen intrinsiek probleem vormen. Wie zijn oor te luister legt bij knooppunten als het Inlichtingenbureau, BKWI, RINIS en SNG krijgt te horen dat technisch alles geregeld kan worden, en vaak ook zonder veel problemen geregeld wordt. We hebben het dan echter wel over partijen waarvan de technische aspecten van gegevensverkeer de *core business* vormen. Deze partijen constateren tegelijkertijd echter dat (met name kleinere) afnemers en (in mindere mate) verstrek-

kers van gegevens vaak moeite hebben om de technische en informatiebeveiligingsaspecten te behappen. En dat geldt zelfs ook voor hun softwareleveranciers.

Voorbeeld
Met slechts zeventien medewerkers zorgde RINIS er in 2012 voor dat zo'n 800 miljoen elektronische berichten foutloos werden verstuurd voor organisaties als DUO, UWV, SVB, LBIO, CBS en Zorgverzekeraars Nederland.

Zoals gezegd zitten de belangrijkste technische problemen op het gebied van informatiebeveiliging. Voor persoonsgegevens geldt een strikt 'need to know'-principe. Daarom zijn vaak complexe autorisaties nodig om ongeoorloofde raadpleging te voorkomen. Als het gaat om gegevens van één leverancier is dat misschien nog wel te doen. De modale gemeente die persoonsgegevens verkrijgt uit een divers aantal bronnen groeit dit echter gemakkelijk boven het hoofd, aangezien elke gegevensleverancier met eigen auditing- en verantwoordingsregimes werkt.

Voorbeeld
Binnen de keten Werk en Inkomen vindt veel gegevensuitwisseling plaats. Een groot deel van deze gegevensuitwisseling wordt geregeld door bepalingen op grond van de wet Suwi. Wanneer een niet-Suwi organisatie gebruik wil maken van gegevens, dan moet er voldaan worden aan extra voorwaarden ten aanzien van privacy en beveiliging. Hiervoor moeten dan aanvullende specifieke contracten voor gegevensleveringen worden opgesteld. De inhoud van deze contracten is sterk wisselend naar gelang de voorwaarden die door de gegevensleverancier worden gesteld. Dit belemmert een efficiënte gegevensdistributie.

Daarnaast kan het principe van doelbinding (zie paragraaf 2.3.3) leiden tot praktische problemen op de werkvloer wanneer medewerkers verschillende taken hebben. Het kan voorkomen dat zij voor de ene taak bepaalde gegevens over een burger niet mogen gebruiken waar zij uit hoofde van de andere taak wel toegang toe hebben. Het is moeilijk om in dergelijke gevallen het niet toegstane 'nevengebruik' te voorkomen.

Overigens kan het ook voor de gegevensverstrekkers, vaak toch grote partijen, moeilijk zijn om overzicht te verkrijgen. Soms hebben ze als gevolg van de technische inrichting van systemen en netwerken al moeite om na te gaan door wat voor partij bepaalde bevragingen eigenlijk gedaan worden. Laat staan dat ze eenvoudig zicht kunnen houden op wat er verderop in de keten met 'hun' persoonsgegevens gebeurt – een wens die bij veel gegevensleveranciers lijkt te leven, al dan niet ingegeven door bepalingen in wet- en regelgeving (vgl. paragraaf 2.3.3).

2.7. Rekenschap

Het laatste grote issue dat in de gesprekken, en met name ook in de geraadpleegde literatuur, naar voren is gekomen, duiden we hier aan met de term "rekenschap". Het valt als volgt onder te verdelen:

1. Rekenschap jegens de maatschappij.

2. Rekenschap jegens de individuele burger.

3. Rekenschap bij incidentele verwerking.

2.7.1. Rekenschap jegens de maatschappij

Waar het in paragraaf 2.3 met name gaat over de onderlinge relaties van de betrokken overheidspartijen, staat hier het geheel van registraties en informatiestromen, als het ware “van buitenaf bekeken”, ter discussie.

Hoe kan geborgd worden dat niet alleen individuele gegevensstromen voldoen aan de daaraan gestelde eisen, maar dat ook het stelsel als geheel en het gebruik dat gemaakt wordt van de daarin beschikbare informatie voldoet aan eisen van behoorlijk bestuur en zorgvuldige verwerking van persoonsgegevens? En als zelfs de direct betrokken partijen soms maar nauwelijks weten waar ze mee bezig zijn, hoe valt dat dan ooit aan de burger en de maatschappij uit te leggen?

Discussies over dit soort fundamentele vragen zijn niet direct relevant voor de uitvoeringspraktijk. Maar ze kunnen op lange termijn wel de legitimiteit van het stelsel ondergraven en tot een tegenbeweging leiden. In de volgende twee paragrafen laten we bovendien zien dat een gebrek aan rekenschap heel concrete problematiek tot gevolg kan hebben.

Dilemma: Wie snapt het nog?
Er worden binnen de overheid steeds meer persoonsgegevens uitgewisseld en doorgeleverd. Kan en mag alles ook wat er gebeurt? En heeft er überhaupt nog iemand een beeld van wat er allemaal gebeurt? Binnen de overheid waarschijnlijk al niet, laat staan de burger. De transparantie, en daarmee uiteindelijk ook de rechtsstaat, is in het geding. Maar je kunt toch moeilijk nuttige dingen met persoonsgegevens niet meer doen, alleen omdat het dan te ingewikkeld zou worden!

“De iOverheid moet investeren in procedures om transparantie (ter ondersteuning van de burger als citoyen) en accountability (ter ondersteuning van de individuele burger als rechtzoekende) te verbeteren. Verantwoordelijkheid en verantwoordingsprocedures binnen de iOverheid zijn momenteel ontoereikend en onvoldoende effectief, en dienen daarom omvattender, explicieter en helderder te worden benoemd en belegd.”.

Bron: WRR-rapport iOverheid

Er zit overigens ook een keerzijde aan de medaille. Privacy wordt vaak ook gebruikt als smoes om bestuurlijke onwil te maskeren. Aandacht voor rekenschap ten aanzien van de omgang met persoonsgegevens zal er ook aan bijdragen dat het moeilijker wordt voor partijen om de wet- en regelgeving ter zake ten onrechte op te voeren als belemmering.

2.7.2. Rekenschap jegens de individuele burger

De overwegingen uit de vorige paragraaf dienen zoals gezegd toegespitst te worden op de relatie van beheerders en gebruikers van basisregistraties met individuele burgers. Die burgers hebben volgens de WBP recht op inzage in hun persoonsgegevens. Mocht daarbij blijken dat er iets niet klopt aan de verwerking, dan hebben ze bovendien het recht om te verzoeken om verbetering, aanvulling, afscherming of verwijdering van de gegevens. Naarmate overheidsinstanties meer gebruik maken van uit andere bronnen verkregen gegevens, zal het moeilijker voor ze zijn om burgers die deze rechten willen uitoefenen te faciliteren. Als ze daartoe al bereid zijn... Zodra het herstellen van fouten en gevolgen buiten de eigen afdeling of organisatie komt, haken de betrokken ambtenaren vaak af. Het probleem wordt dan te groot en valt buiten hun werk en/of bevoegdheden. Ook worden werknemers door hun baas niet positief beoordeeld op inspanningen die buiten hun directe werkterrein (en targets) liggen.

Waar het het recht op inzage betreft, moet deze problematiek niet overschat worden. In de praktijk van de meeste verwerkingen van persoonsgegevens door overheidsinstanties komen inzageverzoeken namelijk zelden of nooit voor. Bovendien hebben burgers dankzij portals zoals mijnoverheid.nl steeds meer mogelijkheden op inzage in hun gegevens zonder dat ze zich daarvoor expliciet tot het betreffende overheidsorgaan hoeven te richten. Daarbij moet wel aangetekend worden dat portals meestal alleen “standaard” gegevens bevatten. Wat er niet in staat zijn de dossiers die organisaties over mensen aanleggen. Het gaat hier dus over het topje van de ijsberg aan informatie. Ook wordt de informatie in portal soms onvoldoende begrijpelijk gemaakt voor de burger.

De positie van de burger kan echter wél ernstig in het gedrang komen als er aan overheidszijde fouten gemaakt zijn. Hoe ingewikkelder de achterliggende gegevensstromen die daarbij een rol hebben gespeeld, des te groter het risico op “kafkaëske toestanden”. Denk bijvoorbeeld aan het combineren van gegevens uit verschillende registraties en het daaraan ook nog eens verbinden van eigen conclusies. Bestuursorganen behoren daarvoor volledige verantwoordelijkheid te nemen, maar verwijzen in de praktijk (te) vaak naar de bron van de gegevens. Zij gaan er meestal vanuit dat wat ze van anderen aangeleverd hebben gekregen correct is. De burger moet dan maar aantonen dat dat niet zo is. Dat komt er vaak op neer dat hij moet aantonen dat hij iets níet heeft gedaan (ergens niet gewerkt, geen strafbaar feit gepleegd, niet met zijn auto op een bepaald tijdstip ergens geweest), wat meestal onmogelijk is. Een recente uitspraak[16] van de Afdeling Bestuursrecht van de Raad van State maakt dit issue nog pregnanter. De Afdeling heeft daarin bepaald dat om gegevens in een basisregistratie te corrigeren of zelfs maar van een aantekening te voorzien onomstotelijk vast moet staan dat de gegevens onjuist zijn.

[16] ABRvS 19 september 2012, LJN: BX7701. Zie noot van Prof.mr. G. Overkleeft-Verburg op haar website (http://www.overkleeft-verburg.nl/PDFs/ABRvS%2019-09-2012%20201202583-1-A2%20en%20201202584-1-A2%20LJN%20BX7701%20k.pdf).

Wat de zaak vaak nog erger maakt, is dat als informatie niet klopt, mensen daar pas achter komen als ze met de gevolgen ervan worden geconfronteerd. Dat is vaak als een (hen onbekend) besluit wordt gehandhaafd. Dan resteren – in het beste geval – alleen nog bezwaar en beroep. Echter, deze instrumenten zijn gericht op besluiten, niet op foute gegevens. Het besluit kan goed zijn, maar gebaseerd op foutieve informatie.

Dilemma: "Computer says no"
(Vrijwel) vaste gegevens in overheidsregistraties betekenen voor burgers duidelijkheid, vertrouwen en minder administratieve lasten. Zo lang alles klopt, tenminste. Maar o wee als er daar wat fout gaat, dan moet de kleine burger de machtige overheid van haar administratieve ongelijk zien te overtuigen. En dat valt niet altijd mee – vraag maar aan Ron Kowsoleea en Steven Romet! (Zie de voorbeelden hieronder)

"**Voorbeeld: De zaak Kowsoleea**
In Nederland is het bekendste geval van identiteitsfraude de zaak van Ron Kowsoleea. Zijn naam werd in de periode 1994 tot en met 2002 stelselmatig misbruikt door Imro C., een crimineel die een oude bekende van hem was. Bij iedere aanhouding gaf Imro C. zich uit voor Kowsoleea. Nadat Imro C. in 2002 in de gevangenis terecht kwam heeft Kowsoleea hier nog tot 2009 problemen door ondervonden. Hij is in die periode bijvoorbeeld herhaaldelijk aangehouden, als ongewenst vreemdeling gearresteerd en in 2003 had hij te maken met een inval door de fiscale inlichtingen en opsporingsdienst (FIOD). Ondanks dat de identiteitsfraude reeds bij de eerste rechtszaak in 1994 duidelijk was, werden zijn strafdossiers niet opgeschoond waardoor misverstanden bleven ontstaan. Door de strafrechtelijke onderzoeken verloor hij steeds meer zakenpartners en kwamen zijn bedrijven in surseance van betaling."

Bron: Wikipedia

Meneer B. werd 20 jaar lang regelmatig opgepakt voor strafbare feiten die hij niet had gepleegd. Ook kon hij onterecht boetes betalen op Schiphol, ontving hij dagvaardingen en hebben hij en zijn gezin eenmaal 's nachts een gewapende politie-inval in zijn woning gehad. Door identiteitsfraude én door fouten in de strafrecht- en vreemdelingenketen als gevolg van één interpretatiefoutje bij de controle van een geboortedatum, bleken B en de echte dader versmolten tot één persoon in overheidsregistraties. Vermoedelijk was dit bekend in beide ketens, maar men deed er niets aan. Het gezinsleven van B is verwoest omdat uiteindelijk zijn vrouw en kinderen hem niet meer geloofden. Na escalatie door het Meldpunt Identiteitsfraude kwam vaart in deze zaak en zijn grote inspanningen gepleegd door JustID, het Parket Rotterdam en uiteindelijk door het Ministerie van Veiligheid en Justitie zelf. Meneer B. heeft namens de (gehele) overheid excuses en een schadevergoeding gekregen. Maar het belangrijkste is het feit dat hij verlost is van 51 strafdossiers en in de betrokken dossiers zijn alle mogelijke waarschuwingen opgenomen om toekomstige persoonsverwisselingen te voorkomen.

Bron: Meldpunt Identiteitsfraude

"**Voorbeeld: Vermist rijbewijs met grote gevolgen**
Steven Romet deed op 3 november 1995 aangifte van vermissing van zijn rijbewijs en vroeg een nieuw. Het duurde tot 14 maart 1997 voordat dit er kwam. In de tussentijd accepteerde het Kentekenregister ondanks zijn protesten 1.737 auto's op zijn naam, werd hij ten onrechte vervolgd wegens ongevallen, het niet betalen van belasting et cetera. Romet verloor een uitkering omdat de sociale dienst vond dat hij te veel auto's op zijn naam had staan. De treuzelende overheid beriep zich op 'de zuiverheid van het kentekenregister' die zich zou verzetten tegen opschoning. Het Europese Hof veegde dit van tafel en veroordeelde Nederland wegens een ongerechtvaardigde inbreuk op de persoonlijke levenssfeer van Romet."

Bron: Column "Privacywetgeving in beweging" van Frank Kuitenbrouwer op InGovernment.nl (http://www.ingovernment.nl/artikelingovernment/privacywetgeving-beweging)

"[Er] is een veel grotere mate van openheid en transparantie richting burgers noodzakelijk om hen inzicht te bieden in de informatie die over hen is vergaard en hen tevens te faciliteren de informatie waar nodig te corrigeren. Burgers staan nu vrijwel machteloos als zij persoonlijk worden geconfronteerd met fouten in de uitgestrekte informatienetwerken van de iOverheid die soms grote gevolgen hebben."

Bron: WRR-rapport iOverheid

Meneer G. moet zich melden bij het CBR voor een verplichte cursus over alcohol en verkeer. Ook moet hij binnen drie weken voor de cursus betalen. Bezwaar levert niets op: hij is immers tweemaal betrapt met teveel alcohol op achter het stuur. De heer G. bestrijdt dit, maar het CBR verwijst naar de informatie in hun bestanden. De heer G. schakelt het Meldpunt Identiteitsfraude in. Dat verneemt via de RDW van het CBR dat het de informatie van de politie in Amsterdam heeft gekregen. De politie heeft inderdaad meneer G. aangehouden en heeft zijn voorletter, achternaam en geboortedatum aan het CBR doorgegeven. Maar in de GBA staan twee personen G. met dezelfde voorletter, achternaam en geboortedatum. Het CBR blijkt (achteraf) op de verkeerde persoon te hebben "geklikt". Op het nippertje hoeft meneer G. de cursus niet te doen en ook niet te betalen. Zijn dossier bij CBR wordt geschoond. De politie had gelukkig wél de juiste G. geregistreerd. Zonder tussenkomst van het Meldpunt Identiteitsfraude had de heer G. dit niet kunnen oplossen.

Bron: Meldpunt Identiteitsfraude

Het probleem ligt overigens niet altijd bij de overheid. Burgers kunnen ook elkaar in moeilijkheden brengen.

Voorbeeld
Wanneer iemand zichzelf in de GBA ten onrechte ingeschreven laat staan op een adres waar hij niet meer woont, dan kan dat nadelige gevolgen hebben voor de personen die daadwerkelijk op het adres (blijven of gaan) wonen. Zij kunnen bijvoorbeeld hun recht op huursubsidie kwijt raken..

2.7.3. Rekenschap bij incidentele verwerking

De term “stelsel van basisregistraties” roept al snel een beeld op van massale gegevensstromen, en die zijn er natuurlijk ook volop binnen het stelsel. Door de begrijpelijke nadruk op grootschalige uitwisselingen is er wellicht te weinig aandacht voor incidentele verwerkingen van persoonsgegevens buiten de gangbare kanalen om. Van wat er op dat niveau gebeurt, blijft veel onder water.

Illustratief zijn in dit opzicht enkele passages uit het rapport van de Inspectie SZW over informatie-uitwisseling in de SUWI-keten met andere partijen. Elders in het rapport stelt de Inspectie vast dat er wat structurele uitwisselingen betreft weinig reden tot zorg is. Daarna vraagt zij aandacht voor uitwisseling op gevalsniveau; daarop komen twee reacties uit gemeenteland.

- “Uit de onderzoeken die de inspectie heeft uitgevoerd, komt het beeld naar voren dat de informatie-uitwisseling tussen individuele professionals uit verschillende domeinen niet gestandaardiseerd plaatsvindt. De uitwisseling verloopt vooral telefonisch, per mail of in casusoverleg. Dit heeft de voorkeur van professionals, maar de bescherming van persoonsgegevens is hierdoor minder gewaarborgd, omdat deze professionals bij maatwerk niet altijd bekend zijn met wat wel en niet mogelijk is binnen de (privacy-)wetgeving vanwege de complexiteit van de toepassing van deze wetgeving.
  Het proces van informele informatie-uitwisseling op gevalsniveau is niet transparant. Het gaat daarbij om informatie-uitwisseling, die in de meeste gevallen niet (standaard) geregistreerd wordt, niet geprotocolleerd is en waarbij er geen enkel zicht is op waarborgen rondom privacy en beveiliging van persoonsgegevens.”
- “VNG hecht een groot belang aan zorgvuldig gebruik van gegevens, maar benadrukt daarbij tegelijk de handelingsvrijheid van de gemeentelijke behandelaars. Vanuit zijn professionele integriteit moet de behandelaar voldoende ruimte hebben om effectief zijn werk te doen.”
- “Divosa bevestigt in haar reactie dat gemeenten soms te voorzichtig omgaan met privacykwesties, maar dat in een enkel geval nood wet breekt en gemeenten er voor kiezen om een goede dienstverlening voorop te plaatsen. Medewerkers van sociale diensten moeten dagelijks laveren tussen belangen die soms ook strijdig kunnen zijn en komen daarbij dilemma’s tegen.”

Bron: Inspectie SZW, “Informatie-uitwisseling van de SUWI-keten met andere partijen”, augustus 2012

3. Oplossingen

Dit hoofdstuk inventariseert een aantal mogelijke typen interventies en neemt die als vertrekpunt voor een verkenning van mogelijke oplossingen voor de in het vorige hoofdstuk geïnventariseerde issues die het gebruik van persoonsgegevens uit basisregistraties belemmeren.

3.1. Typen interventies

In hoofdstuk 2 is een divers scala aan belemmeringen de revue gepasseerd. Het spreekt voor zich dat niet één type interventie geschikt is om die allemaal te adresseren. De volgende geschikte soorten acties worden in deze paragraaf nader uitgewerkt:

1. Goede informatie verschaffen
2. Juridische duidelijkheid creëren
3. Verbinden
4. Privacy by design
5. Nader onderzoek doen
6. Beleid maken
7. Wet- en regelgeving aanpassen

3.1.1. Goede informatie verschaffen

In paragraaf 2.1 is aangegeven dat betrokken partijen en hun medewerkers op vrijwel alle hier besproken vlakken kampen met een gebrek aan overzicht. De benodigde informatie is meestal wel beschikbaar, maar niet op zo'n manier dat die effectief gebruikt kan worden. Een aantal belemmeringen kunnen beperkt, en misschien zelfs opgeheven worden eenvoudig door aan de juiste doelgroepen op het juiste moment de juiste informatie ter beschikking te stellen. En daar waar er sprake is van daadwerkelijke (en dan met name bedoelde) blokkeringen, kan goede informatie over wat er dan wél kan en hoe dat geregeld kan worden, bijdragen aan positieve beeldvorming over het stelsel.

Een interessante optie kan in enkele gevallen het bouwen van een 'privacy wizard' zijn. Denk daarbij aan een tool die gebruikers door een beslisboom stuurt en ze waar relevant ook de mogelijkheid geeft om gemaakte afwegingen vast te leggen. In plaats van met een beslisboom kan het ook interessant zijn om een regelgebaseerde benadering te kiezen, die de professional op het gebied van zijn competentie meer vrijheid laat.

3.1.2. Juridische duidelijkheid creëren

Een typerend kenmerk van privacywet- en -regelgeving zijn de vele open normen. Die zorgen in de praktijk voor veel onduidelijkheid en onzekerheid. In zekere mate zijn die te ondervangen door pro-actief handelen. Een organisatie die op duidelijke en transparante wijze aangeeft hoe zij de open normen uit de privacyregels vertaalt naar concrete eisen aan haar beleids- en handelingspraktijk heeft op zijn minst een voorsprong in een eventuele discussie met bijvoorbeeld een toezichthouder. Vanzelfsprekend hoeft een dergelijke stellingname niet tot één organisatie beperkt te blijven, verschillende partijen kunnen daarover ook samen afspraken maken. Het draagvlak voor dergelijke afspraken zal groter zijn naarmate alle stakeholders beter betrokken worden bij het tot stand komen ervan.

3.1.3. Verbinden

Complexiteit, gebrek aan goede informatie en overzicht, en juridische onduidelijkheid, leiden gemakkelijk tot spanning in de relaties tussen verschillende betrokken partijen. In sommige gevallen kan de oplossing van een belemmering gelegen zijn in het tot stand brengen of herstellen van de juiste relaties. Daarbij is het wel zaak de valkuil van vrijblijvendheid te vermijden.

3.1.4. Privacy by design

Privacybelemmeringen zijn er soms op terug te voeren dat een partij iets wil wat gewoon echt niet mag (vgl. paragraaf 2.2.1). Veel vaker echter zit het probleem hem vooral in de manier waarop een verwerking is ingericht. Verantwoordelijken voor de gegevensbescherming zijn nogal eens geneigd om “Het mag niet van de privacy” te horen, waar de boodschap in feite luidt: “Het mag niet zó van de privacy – maar het is heel goed mogelijk dat het op een andere manier wel kan!”.

Met andere woorden: het beeld kan ontstaan dat een bepaalde behoefte aan persoonsgegevens niet te vervullen is binnen de bestaande kaders, terwijl het in feite vaak een kwestie is van goed nadenken over hoe je de verwerking zo in kunt richten dat je binnen die kaders blijft. Hoewel de term meestal in wat engere zin gebruikt wordt, zou je dat laatste kunnen aanduiden met: ‘privacy by design’.

3.1.5. Nader onderzoek doen

Zoals in de inleiding al is aangegeven, betreft het onderhavige rapport slechts een eerste verkenning. Het is gebaseerd op een beperkt aantal gesprekken en een handvol relevante publicaties. In een aantal gevallen zal de meest gerede stap dan ook zijn het doen van nader on-

derzoek naar de feitelijke aard en omvang van de gesignaleerde belemmering, de negatieve gevolgen die betrokken partijen daarvan ondervinden en de mogelijke oplossingsrichtingen.

3.1.6. Beleid maken

Bepaalde belemmeringen kunnen zo serieus zijn dat het nodig is er nieuw of aangepast beleid voor te ontwikkelen. De overige hier genoemde interventies kunnen van dat beleid uiteraard onderdeel uitmaken. Gelet op het geconstateerde in paragraaf 2.1 zou bij het opstellen van dat beleid het reduceren van de algehele complexiteit en het verbeteren van het overzicht bij de betrokken partijen een belangrijke randvoorwaarde moeten zijn.

3.1.7. Wet- en regelgeving aanpassen

Tot slot kan het in sommige gevallen nodig blijken de wet- en regelgeving ter zake aan te passen. Zoals in de Inleiding aangeven vallen aanpassingen aan de geldende regels ter bescherming van persoonsgegevens buiten de reikwijdte van deze verkenning.

3.2. Concrete oplossingen

Hieronder komen alle belemmeringen uit hoofdstuk 2. aan de orde en worden concrete oplossingsrichtingen geopperd, waarbij geput wordt uit het overzicht in de vorige paragraaf.

3.2.1. Overzicht

Betrokken partijen en hun medewerkers kampen met een gebrek aan overzicht. De benodigde informatie is meestal wel beschikbaar, maar niet op zo’n manier dat die effectief gebruikt kan worden.

Zoals in paragraaf 2.1 is aangegeven, gaat het bij dit thema niet om op zichzelf staande belemmeringen, maar gaat het om een versterkende negatieve factor bij elk van de overige issues. Het ligt dan ook niet voor de hand geïsoleerd op dit issue zwaar in te zetten. Niet voor niets is het verschaffen van betere informatie in de vorige paragraaf opgenomen als mogelijk type interventie.

Niettemin kan het zinvol zijn om – voor zover nog niet beschikbaar – per sector of werkveld een geconsolideerd overzicht te maken van de belangrijkste elementen uit de toepasselijke wet- en regelgeving en gemaakte afspraken. Zijn er voldoende zulke overzichten van voldoende kwaliteit, dan heeft ook een overkoepelend overzicht met doorverwijzingen daarnaar duidelijke meerwaarde.

Een bescheiden aanzet tot een overzicht van welke persoonsgegevens er in de diverse basisregistraties staan en de daarvoor geldende regels is overigens te vinden in de bijlage.

3.2.2. Wet- en regelgeving

Bedoelde blokkeringen uit wet- en regelgeving vallen buiten de reikwijdte van deze verkenning. Hetzelfde geldt voor de gesloten verstrekkingenregimes.

Bij de onbedoelde blokkeringen zijn daarnaast onderscheiden: techniekafhankelijkheid en statistische gegevens.

Techniekafhankelijkheid

Het beperken van techniekafhankelijkheid van wet- en regelgeving is altijd lastig, aangezien het een vooruitziende blik vereist. Niettemin lijken er hier en daar binnen het stelsel zaken onhandig geregeld te zijn terwijl dat eenvoudig te voorkomen was geweest. Aangewezen lijkt hier dan ook een beperkte actie om te komen tot een beknopte richtsnoer die specifiek voor basisregistraties aangeeft hoe de belangrijkste valkuilen ten aanzien van techniekafhankelijkheid kunnen worden voorkomen. Deze richtsnoer zou bijvoorbeeld een plek kunnen krijgen in de aanwijzingen voor de regelgeving.

In aanvulling hierop kan geprobeerd worden concrete gesignaleerde problemen op te lossen. Zo zijn ten aanzien van het aangehaalde voorbeeld van de gemeentelijke deurwaarders SNG en het Agentschap BPR momenteel een manier aan het zoeken om de gewenste werkwijze toch mogelijk te maken.

Geaggregeerde gegevens

Ten aanzien van de wens tot het gebruik van geaggregeerde gegevens gebaseerd op persoonsgegevens uit basisregistraties zijn verschillende overwegingen relevant. In de eerste plaats is niet duidelijk hoe sterk de behoefte aan dit soort gegevens nu eigenlijk is. Ten tweede is de vraag of in die behoefte niet kan worden voorzien met bestaande middelen, in het bijzonder de producten en diensten van het CBS.

Mocht het toch nodig blijken om basisregistraties structureel rechtstreek voor statistische doeleinden te ontsluiten, dan zijn er twee samenhangende vragen: wat zijn nu precies de juridische mogelijkheden en onmogelijkheden, en in hoeverre kan privacy by design een oplossing bieden?

Waar het de GBA betreft wordt de verstrekking van geaggregeerde gegevens (bij besluit van de minister van BZK) overigens mogelijk gemaakt in artikel 3.14 van het wetsvoorstel BRP.

3.2.3. Verantwoordelijkheid

Hieronder komen achtereenvolgens de drie in paragraaf 2.3 benoemde issues aan de orde.

Verantwoordelijkheden zijn niet of onduidelijk belegd

Het gaat hier om de verwerkingen waarbij meer partijen betrokken zijn. Het geconstateerde probleem is dat er soms onduidelijkheid bestaat over welke partij welke rol heeft: wie is of zijnde verantwoordelijke(n), en wie de bewerker(s)? Het is primair aan de betrokken partijen bij een specifieke verwerking om hierover duidelijke afspraken te maken. Daarmee is echter de burger nog niet geholpen die geen of te weinig gehoor krijgt als hij fouten in de verwerking van zijn gegevens aan de orde stelt, zeker wanneer die zich door een keten verspreid hebben. Voor hen zou een laagdrempelig loket beschikbaar moeten komen waartoe zij zich dan kunnen wenden.

Verantwoordelijkheden zijn (mogelijk) verkeerd belegd

Het gaat hier om twee issues die te maken hebben met de interpretatie van de privacywet- en -regelgeving: de verantwoordelijkheid voor kopiebestanden en de formele rol van knooppunten. Blijkt hier inderdaad een serieus issue te liggen, dan zal ten aanzien van kopiebestanden een stellingname nodig zijn over de juridische mogelijkheden en beperkingen, gekoppeld met privacy by design. Ten aanzien van de verantwoordelijkheid van knooppunten zal dan voor elk knooppunt dat het aangaat een forse juridische en beleidsinspanning noodzakelijk zijn, waarbij het ze grote voordelen kan bieden om samen op te trekken.

Verantwoordelijkheid verstrekker voor handelen ontvanger

Hier gaat het erom dat verstrekkers van persoonsgegevens graag zicht willen hebben op wat de afnemer doet met die gegevens, en soms zelfs een zekere mate van controle daarover. Dit complexe issue kent vele facetten. Zo zijn er enerzijds de juridische vereisten voor sommige basisregistraties, maar spelen anderzijds ook vertrouwen, informatiepositie en behoorlijk bestuur een rol.

In eerste aanleg kan het verschaffen van op dit aspect toegesneden informatie enige uitkomst bieden. Op langere termijn lijkt een beleidsinitiatief op dit gebied echter onontkoombaar.

Technische voorzieningen kunnen een deel van de oplossing vormen. BKWI beproeft momenteel een tool die het voor verstrekkers van gegevens mogelijk maakt om de gang van het gegeven nadat het verstrekt is te monitoren. Als deze proef slaagt, dan kan de bezien worden of de ontwikkelde tool breder ingezet kan worden.

3.2.4. Regels voor hergebruik

Ten aanzien van hergebruik zijn in het vorige hoofdstuk twee issues benoemd. Het eerste betreft de algemene vraag welke privacyregels er gelden voor uit basisregistraties verkregen persoonsgegevens. Een geval apart vormt daarbij de GBA, waarop de WBP niet van toepassing is. Het tweede issue is de specifieke vraag hoe het zit met doelbinding en verenigbaarheid bij gebruik van persoonsgegevens uit basisregistraties. Een geval apart vormen daarbij openbare gegevens.

Het beantwoorden van de algemene vraag welke regels er gelden voor het verwerken van uit basisregistraties verkregen persoonsgegevens is in hoofdzaak een kwestie van het verschaffen van goede informatie, al kan in sommige gevallen een pro-actieve juridische stellingname gewenst zijn. Ten aanzien van doelbinding (inclusief het gebruik van openbare gegevens) geldt precies het omgekeerde: daar zal de nadruk moeten liggen op pro-actief juridisch stelling nemen, waar nodig in combinatie met het verschaffen van goede informatie.

3.2.5. Bruikbaarheid en kwaliteit

Hier gaat het om een bijzonder complex issue, dat talrijke facetten kent. Aangezien kwaliteit van basisregistraties een beleidsprioriteit is, worden veel van die facetten al op een of andere manier geadresseerd. Denk bijvoorbeeld aan het inrichten van terugmeldvoorzieningen en het vergroten van de juistheid van adresinformatie in de GBA. Op basis van deze beknopte verkenning is niet te zeggen of met dit alles deze problematiek voldoende aandacht krijgt.

3.2.6. Techniek en informatiebeveiliging

Het belangrijkste issue hier vormen de verschillende auditing- en verantwoordingsregimes per basisregistratie. Afnemers die persoonsgegevens betrekken uit meerdere basisregistraties hebben daar last van, aangezien het leidt tot onnodige overhead en complexiteit. Aangewezen is hier een beleidsmatige interventie met als doel het zoveel mogelijk uniformeren van de op dit vlak door basisregistraties gestelde eisen.

Knooppunten nemen momenteel in de praktijk hun klanten al een aantal zorgen op dit gebied uit handen. BKWI heeft interesse in deelname aan een project op dit vlak, en participeert momenteel zelf ook in een experiment waarbij UWV beziet of verstrekkingen aan afdelingen burgerzaken van gemeenten te regelen zijn met één (of zelfs nul?) contracten per gemeente, in plaats van de zes of zeven die momenteel gangbaar zijn.

Een mogelijke oplossing, voorgesteld door SNG, is het vormen van een samenwerkingsverband van basisregistraties dat afnemers op dit vlak ondersteunt. Als de afnemer het zelf kan en wil doen, prima, en anders kan hij (betaald) ondersteuning krijgen vanuit het samenwerkingsverband.

3.2.7. Rekenschap

Dit issue is uitvoerig aan de orde gesteld door de Wetenschappelijke Raad voor het Regeringsbeleid in zijn rapport over de iOverheid. Als het gaat om belemmeringen voor het gebruik van persoonsgegevens uit basisregistraties, dan komt vooral rekenschap jegens de individuele burger naar voren. Onvoldoende aandacht nu daarvoor kan op termijn leiden tot politiek-bestuurlijke terughoudendheid bij het ontsluiten van persoonsgegevens uit basisregistraties.

Basisregistraties, maar meer nog afnemers van gegevens uit basisregistraties, kunnen stappen zetten ten aanzien van het pro-actief, laagdrempelig en met duidelijke toelichting geven van inzage aan burgers in de persoonsgegevens die ze over hen verwerken. Hét grote probleem is hier echter het ontbreken van een enkel loket waar de burger zich toe kan wenden in het geval hij in de knel komt als gevolg van foutieve gegevens in basisregistraties. Weliswaar kan hij aankloppen bij onder meer het College Bescherming Persoonsgegevens, het Meldpunt Identiteitsfraude en de Nationale Ombudsman, maar geen van deze instanties lijkt te beschikken over de juiste combinatie van kennis, middelen en doorzettingsmacht om het verschil te kunnen maken. Met name die doorzettingsmacht is cruciaal: aan een loket dat uiteindelijk ook niets weet te bereiken heeft de burger weinig.

Enigerlei vorm van samenwerking tussen de genoemde en wellicht nog andere instanties zou een oplossing kunnen vormen, mits zo'n samenwerkingsverband voldoende budget tot haar beschikking zou krijgen.

4. Conclusie

Vertrekpunt voor deze verkenning was de gedachte dat verschillende knelpunten bij het gebruik van gegevens uit basisregistraties terug te voeren zijn op het feit dat het in de gevallen in kwestie om *persoons*gegevens gaat. Doel was om deze gedachte te toetsen en uit te werken, en om vast te stellen in hoeverre daadwerkelijk sprake is van knelpunten.

Geconcludeerd kan worden dat het verwerken van *persoons*gegevens uit basisregistraties inderdaad een aantal specifieke aandachtspunten kent. Relevant is daarbij dat het niet zozeer om een geheel andere problematiek gaat dan bij het verwerken van gegevens in het algemeen. Door de grote hoeveelheid aan regels voor het verwerken van persoonsgegevens kunnen op zich bekende uitdagingen in essentie tot knelpunten leiden. Zeker in complexe omgevingen zoals het stelsel van basisregistraties.

Wat opvalt, is dat de beschikbaarheid van goede informatie op alle vlakken een belangrijke rol speelt. Eigenlijk geldt voor alle geconstateerde issues dat zij voor een groter of kleiner deel zijn terug te voeren op het feit dat de betrokken partijen de grootst mogelijke moeite hebben om de complexiteit het hoofd te bieden. Goede, gerichte, effectieve en tijdige informatie kan dan wonderen doen.

De overige problematiek is divers van karakter: juridisch, bestuurlijk, organisatorisch, informatiekundig, technisch en maatschappelijk. Belangrijke kenmerken zijn het brede wetgevingskader – het gaat over veel meer dan alleen de WBP en de GBA – en de complicaties die ketens van verwerkingen met zich meebrengen. Het lijkt duidelijk dat er alles bij elkaar genomen sprake is van serieuze problematiek. Er liggen hier dus kansen!

5. Aanbevelingen

In hoofdstuk 2. is een aantal issues benoemd, in hoofdstuk 3. zijn mogelijke oplossingen daarvoor verkend. Voor de meeste voorgestelde oplossingen is het niet aan het cluster STOUT om daaruit keuzes te maken of de uitvoering ervan op zich te nemen. Evenmin ligt het op de weg van het cluster om anderen aan te wijzen om zaken ter hand te nemen. Niettemin volgen hieronder enkele voorzichtige aanbevelingen ten aanzien van mogelijke nadere uitwerking van een aantal oplossingen uit hoofdstuk 3. . In een aantal gevallen is daarbij ook aangegeven welke partijen binnen de overheid daarbij een rol zouden kunnen spelen.[17]

[17] Zie voor een overzicht van de meest direct bij het stelsel betrokken partijen de bijlage.

§	Issue	Mogelijke oplossing	Door wie?
3.2.1	Geen overzicht *N.B. 'verzwarende' factor, dus bij voorkeur niet geïsoleerd inzetten.*	• Geconsolideerd overzicht belangrijkste regels per sector of werkveld maken Overkoepelend overzicht met doorverwijzingen opstellen	• Beheerders basisregistraties, 'brancheorganisaties' afnemers • Sectoraal overzicht: het ministerie dat het aangaat • STIP
3.2.2	Techniekafhankelijkheid	• Richtsnoer techniekonafhankelijkheid voor regelgeving over basisregistraties • SNG heeft voorgesteld om een denktank van technici en juristen bij elkaar te brengen die samen discussiëren over hoe wetgeving zo techniekonafhankelijk mogelijk in te richten is.	• BZK, V&J • BZK, V&J
	Geaggregeerde gegevens	• Informeren over bestaande mogelijkheden • Duiden juridische mogelijkheden in combinatie met privacy-by-design	• CBS • Programma Stelsel van Basisregistraties samen met 'vragende' partijen
3.2.3	Verantwoordelijkheden niet of onduidelijk belegd	Geen actie op stelselniveau	• Individuele partijen die het aangaat
	Kopiebestanden	• Wordt meegenomen in project Oplossingen	• STOUT
	Rol knooppunten	• Meenemen in de bredere discussie die nu loopt over de rol van knooppunten in het stelsel	• STOUT

§	Issue	Mogelijke oplossing	Door wie?
	Verantwoordelijkheid verstrekker voor handelen ontvanger	• Gericht over informeren, zowel algemeen als per basisregistratie	• Algemeen: STIP • Per basisregistratie: bronhouder
3.2.4	Hergebruik	• Gericht over informeren, in combinatie met pro-actieve juridische stellingname	• STIP • Voor GBA ook: Agentschap BPR
	Doelbinding	• Pro-actief juridisch stellingnemen, in combinatie met gericht over informeren	• BZK, zo mogelijk samen met Justitie, CBP
3.2.5	Bruikbaarheid en kwaliteit	• Wordt meegenomen in lopende trajecten rondom gegevensdefinities en kwaliteit	
3.2.6	Audit- en verantwoordingseisen	• Zoveel mogelijk uniformiteit aanbrengen	beleidsvraagstuk
3.2.7	Rekenschap	• Eén loket met doorzettingsmacht creëren	• Samenwerking CBP, Meldpunt Identiteitsfraude, Nationale Ombudsman

Bijlage: Gevoerde gesprekken en bijgewoonde overleggen

In het kader van deze verkenning zijn gesprekken gevoerd met de volgende personen:

» Dhr. T. Bos (Ministerie van BZK)

» Mw. M. Crasborn (Ministerie van BZK)

» Mw. E. ’t Hoen (Ministerie van BZK)

» Dhr. P. Jansz en dhr. J.P. Bergfeld (Inlichtingenbureau)

» Dhr. E. Jonker (Ministerie van BZK)

» Mw. S. Laaper (LIEC)

» Dhr. J. Klapwijk (BKWI)

» Dhr. R. Siegerist (UWV)

» Dhr. R. Verweij (RINIS)

» Dhr. M. Windemuller (SNG)

Daarnaast zijn de volgende overleggen bijgewoond:

» Overleg clusterleider STOUT met dhr. F. Jacob en mw. C. Olivers (Agentschap BPR)

» Overleg clusterleider STOUT met dhr. A. Reuijl (CIP: Centrum voor Informatiebeveiliging en Privacy)

» Werkgroep Kwaliteit GBA (9 okt. 2012 en 20 nov. 2012)

» ‘Tantalusbijeenkomst’ georganiseerd door cluster STOUT (13 nov. 2012)

Ook is over deze materie geput uit en van gedachten gewisseld op diverse LinkedIn-groepen gewijd aan het stelsel van basisregistraties en gemeentelijke dienstverlening.

Bijlage: Geraadpleegde literatuur

» Art. 29 Werkgroep. *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker".* WP 169.

» College Bescherming Persoonsgegevens. "Onderzoek naar de controle door de Dienst Wegverkeer op de online verstrekking van persoonsgegevens uit het kentekenregister aan beroepsbeoefenaren. Rapport definitieve bevindingen." Juni 2012.

» Inspectie VGZ. "Informatie-uitwisseling van de SUWI-keten met andere partijen." Augustus 2012.

» Prof. G. Overkleeft-Verburg. "Basisregistraties en rechtsbescherming. Over de dualisering van de bestuursrechtelijke rechtsbetrekking". Nederlands Tijdschrift voor Bestuursrecht 2009-4.

» Prof.dr. A.J.C. de Moor-Van Vugt e.a. "Gegevensuitwisseling door Toezichthouders". Onderzoek uitgevoerd in opdracht van het WODC. Universiteit van Amsterdam, juni 2012.

» Wetenschappelijke Raad voor het Regeringsbeleid. "Rapport iOverheid". Maart 2011.

Bijlage: Gebruikte afkortingen

BAG	Basisregistraties Adressen en Gebouwen
BKWI	Bureau Keteninformatisering Werk en Inkomen
BPR	(Agentschap) Basisadministratie Persoonsgegevens en Reisdocumenten
BRI	Basisregistratie Inkomen
BRK	Basisregistratie Kadaster
BRP	Basisregistratie Personen
BRV	Basisregistratie Voertuigen (= Kentekenregister)
BSN	Burgerservicenummer
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBP	College Bescherming Persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
DICA	Dutch Institute for Clinical Auditing
DUO	Dienst Uitvoering Onderwijs
GBA	Gemeentelijke Basisadministratie Persoonsgegevens
GGD	Gemeentelijke Gezondheidsdienst
LBIO	Landelijk Bureau Inning Onderhoudsbijdragen
LIEC	Landelijk Informatie en Expertise Centrum
NAW	Naam-Adres-Woonplaats
NHR	Handelsregister
RDW	Dienst Wegverkeer
RIEC	Regionaal Informatie en Expertise Centrum
RINIS	Routeringsinstituut (inter)Nationale Gegevensstromen
RNI	Basisregistratie Niet Ingezetenen
SNG	Stichting Netwerk Gerechtsdeurwaarders
SVB	Sociale Verzekeringsbank
STIP	Stelselinformatiepunt
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen
SWIFT	Society for Worldwide Interbank Financial Transactions
UWV	Uitvoeringsinstituut Werknemersverzekeringen
WBP	Wet Bescherming Persoonsgegevens
WGBA	Wet Gemeentelijke Basisadministratie
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Bijlage:
Persoonsgegevens in basisregistraties en de regels daarvoor

Op de volgende bladzijden is voor de zes in dit verband meest relevante basisregistraties een overzicht op hoofdlijnen te vinden van de persoonsgegevens die ze bevatten en de regels die gelden voor het gebruik van die persoonsgegevens. Het betreft een beknopt overzicht waarin niet alle juridische finesses zijn verwerkt. Aanvullende informatie is te vinden op onder meer de websites van de basisregistraties in kwestie.

Achtereenvolgens komen aan de orde:

» Gemeentelijke Basisadministratie Persoonsgegevens

» Basisregistratie Inkomen

» Handelsregister

» Kadaster

» Basisregistratie WOZ

» Kentekenregister (Basisregistratie Voertuigen)

GBA (Gemeentelijke basisadministratie persoonsgegevens)

De GBA bevat een aantal fundamentele persoonsgegevens over Nederlanders. Over enkele jaren wordt de GBA opgevolgd door de Basisregistratie Persoonsgegevens (BRP). Een wetsvoorstel voor de BRP ligt op het moment van opstellen van dit stuk bij de Tweede Kamer. Daarbij gaan een aantal zaken flink veranderen. Het onderstaande beschrijft de huidige situatie.

Welke wetten en regels gelden er?

» Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA)
» Besluit gemeentelijke basisadministratie persoonsgegevens (Besluit GBA)
» Regeling vaststelling systeembeschrijving GBA

Waarvoor worden de gegevens verzameld?

De GBA heeft als doeleinden:
» primair: bestuursorganen te voorzien van de algemene en bijzondere gegevens[18] waarover zij moeten beschikken voor het vervullen van hun taken;[19]
» secundair:
  - gegevens te verstrekken aan de organisaties die een taak uitvoeren met een publiek of bijzonder maatschappelijk belang waarvoor bij de uitoefening daarvan de gegevens uit de GBA noodzakelijk zijn;[20]
  - een ingeschrevene te voorzien van de hem betreffende algemene gegevens.[21]

Welke gegevens mogen waarvoor aan wie verstrekt worden?

De GBA - regelgeving hanteert haar eigen terminologie voor ontvangers van gegevens:[22]
» Afnemer = bestuursorgaan
  - Binnengemeentelijke afnemer = ieder orgaan van de gemeente die de betreffende gemeentelijke basisadministratie bijhoudt
  - Buitengemeentelijke afnemer = iedere andere afnemer

[18] Zie voor een toelichting op de verschillende categorieën het overzicht van persoonsgegevens achteraan.
[19] Art. 3 lid 1 en 2 Wet GBA.
[20] Vgl. art. 3 lid 3 Wet GBA.
[21] Art. 3 lid 4 Wet GBA.
[22] Art. 1 Wet GBA. Het begrip “bijzondere derde” komt uit het Besluit GBA; de term “vrije derde” komt niet voor in de regelgeving, maar is eveneens algemeen gangbaar.

» Derde = elke andere gebruiker die niet als bestuursorgaan kan worden aangeduid[23]
  - Bijzondere derden = een aantal specifieke derden met een taak met een publiek of bijzonder maatschappelijk belang die systematisch gegevens uit de GBA verstrekt kunnen krijgen
  - Verplichte derden = een aantal specifieke derden die systematisch gegevens uit de GBA verstrekt kunnen krijgen[24]
  - Vrije derden = alle andere derden, bijvoorbeeld derden die op grond van een gemeentelijke verordening gegevens verstrekt krijgen

Afnemers ontvangen op verzoek algemene en verwijsgegevens, alsook de daarop betrekking hebbende administratieve gegevens; in beide gevallen alleen voor zover die noodzakelijk zijn voor het vervullen van hun taken.[25]

Verplichte derden ontvangen op verzoek een gewaarmerkt afschrift van algemene en verwijsgegevens, voorzover die verstrekking is voorgeschreven is in een algemeen verbindend voorschrift of – waar het gaat om gerechtelijke werkzaamheden – noodzakelijk is om een algemeen verbindend voorschrift uit te voeren.[26]

De wet onderscheidt de onderstaande categorieën **bijzondere derden** en doeleinden waarvoor die voor een autorisatiebesluit in aanmerking komen.[27]

Bijzondere derde	doeleinde
Financiële instellingen, meerbepaald:	
▪ Pensioenfondsen, pensioenverzekeraars, premiepensioeninstellingen e.d.	Uitvoeren van een pensioenregeling, spaarfonds of VUT-regeling
▪ Banken, effecteninstellingen, verzekeraars en beleggingsinstellingen	Honoreren van aanspraken van gerechtigden op (al dan niet op termijn) opvorderbare gelden, effecten of goederen
▪ Zorgverzekeraars	Aanbieden en uitvoeren zorgverzekering
De Stichting Interkerkelijke Ledenadministratie	Het verwerken van persoonsgegevens van de tot de genootschappen behorende leden
Instellingen en voorzieningen voor onderwijs, gezondheidszorg en maatschappelijke dienstverlening	Voor zover noodzakelijk voor de vervulling van hun taak
Het Centraal Bureau voor de Genealogie	De bijhouding van een registratie van overleden personen
BKR[28] en het Landelijk Informatiesysteem Schulden	Identiteitscontrole betrokkene bij aangaan van nieuwe financiële verplichtingen of een traject van schuldhulpverlening

Een *beperkte set gegevens*[29] kan bij gemeentelijke verordening verstrekt worden aan de onderstaande **vrije derden**.[30]

[23] En niet de ingeschrevene zelf; art. 1 Wet GBA.
[24] Zie art. 98 Wet GBA.
[25] Art. 88 lid 1 en 3 Wet GBA.
[26] Art. 98 Wet GBA.
[27] Art. 99 Wet GBA en Hst. 3 §2a Besluit GBA.
[28] Bureau Krediet Registratie.
[29] Art. 100 lid 2 Wet GBA.
[30] Art. 100 lid 1 Wet GBA.

Vrije derde	doeleinde	beperking
Rechtspersonen zonder winstoogmerk	Bescherming van de betrokkene of van de rechten en vrijheden van anderen	▪ gerechtvaardigd door een dringende maatschappelijke behoefte ▪ staat in een juiste verhouding tot het doel waarvoor de gegevens worden gevraagd ▪ dit doel kan niet op minder ingrijpende wijze worden bereikt
Natuurlijke personen	Een persoonlijk, niet-commercieel belang	Voorafgaande schriftelijke toestemming van de ingeschrevene van wie gegevens worden verstrekt

Bijzondere gegevens worden aan een beperkt aantal ontvangers verstrekt.

Bijzondere gegevens	ontvanger
Gegevens noodzakelijk i.v.m. uitvoering van de Paspoortwet	▪ afnemers die betrokken zijn bij de uitvoering van de Paspoortwet; ▪ afnemers die belast zijn met de opsporing of vervolging van strafbare feiten; ▪ de directie van het Landelijk Bureau Inning Onderhoudsbijdragen
Gegevens noodzakelijk i.v.m. uitvoering van de Kieswet	Afnemers betrokken bij de uitvoering van de Kieswet of van andere bij of krachtens wet gegeven regelingen betreffende verkiezingen

Ook de **geregistreerde zelf** heeft recht om te weten welke gegevens er over hem in de GBA staan,[31] en aan wie die gegevens het voorgaande jaar verstrekt zijn.[32] Hij kan inzage krijgen in de gegevens en een, desgewenst gewaarmerkt, afschrift van die gegevens ontvangen. Daarbij zitten ook gegevens over gerelateerden, zoals de ouders en eventuele echtgenoot, geregistreerd partner en/of kinderen. Dat betekent omgekeerd dat **gerelateerden** in sommige gevallen gegevens over een geregistreerde verstrekt kunnen krijgen.

Welke voorwaarden gelden daarbij?

Alleen binnengemeentelijke afnemers kunnen rechtstreeks toegang tot de (gemeentelijke) GBA krijgen.

Systematische verstrekking – zoals verstrekking op gestructureerde wijze – van gegevens uit de GBA aan buitengemeentelijke afnemers en bijzondere derden is alleen mogelijk op basis van een autorisatiebesluit van de minister van BZK.[33] Systematische verstrekking aan vrije derden is niet mogelijk. Systematische verstrekking is in beginsel beperkt tot enkele specifieke verstrekkingsvormen.[34] Deze zijn nader uitgewerkt in de systeembeschrijving.
De voorwaarden voor het verstrekken van gegevens voor historische, statistische of

[31] Art. 79 Wet GBA.
[32] Art. 103 Wet GBA.
[33] Art. 91 resp. art. 99 Wet GBA.
[34] Art. 64 lid 1 en art. 68e Besluit GBA.

wetenschappelijke doeleinden zijn uitgewerkt in art. 67 Besluit GBA.
Geregistreerden kunnen bezwaar maken tegen verstrekking van hun gegevens aan de Stichting Interkerkelijke Ledenadministratie en aan vrije derden.[35] Hetzelfde geldt voor incidentele verstrekkingen aan derden, maar zo'n verzoek wordt alleen gehonoreerd als zijn persoonlijke levenssfeer door de verstrekking onevenredig geschaad zou worden.[36]

Overzicht persoonsgegevens

In beginsel zijn alle gegevens in de GBA persoonsgegevens. In art. 34 Wet GBA staat welke gegevens er over een ingeschrevene geregistreerd staan. Dit is nader uitgewerkt in de bijlagen I en II bij de wet. De onderstaande *algemene gegevens* over geregistreerden staan in de GBA.[37]

Gegeven(s)	Toelichting
1) Burgerlijke staat	NAW, geboorte, geslacht, ouders, huwelijk en echtegenoot c.q. geregistreerd partner(schap)[38], kinderen, overlijden, datums rechtsgeldigheid
2) Curatele	
3) Gezag over minderjarige	
4) Nationaliteit	
5) Verblijfsrecht vreemdeling	
6) Verblijfsgegevens	Gemeente van inschrijving, adres, verblijf in Nederland, vertrek uit Nederland
7) Administratienummers	Van geregistreerde zelf en diverse gerelateerden
8) en 9) Burgerservicenummers	Van geregistreerde zelf en diverse gerelateerden
10) Gebruik geslachtsnaam	

Daarnaast bevat de GBA ook enkele *bijzondere gegevens* over geregistreerden. Het gaat dan om gegevens die nodig zijn in verband met de uitvoering van de Paspoortwet en de Kieswet.[39]
Tot slot bevat de GBA ook nog diverse administratieve gegevens.[40]

[35] Art. 102 lid 1 Wet GBA.
[36] Art. 102 lid 1 en lid 2 Wet GBA.
[37] Art. 34 lid 1 onder a Wet GBA.
[38] Ook historisch.
[39] Art. 34 lid 1 onder b Wet GBA.
[40] Art. 34 lid 1 onder c Wet GBA.

Basisregistratie Inkomen (BRI)

De BRI is een basisregistratie.[41]
De Belastingdienst is de beheerder van en de verantwoordelijke voor de BRI.[42]
Informatie over de BRI is te vinden op de website van de Belastingdienst.[43]

Welke wetten en regels gelden er?

» Algemene wet inzake rijksbelastingen 1964 (AWR)

Waarvoor worden de gegevens verzameld?

De basisregistratie inkomen heeft tot doel om inkomensgegevens (verzamelinkomen of belastbaar jaarloon) van burgers te verstrekken aan bestuursorganen die deze gegevens op grond van een wettelijk voorschrift mogen gebruiken.[44]

Welke gegevens mogen waarvoor aan wie verstrekt worden?

Gegevens uit de BRI worden uitsluitend vertrekt aan bestuursorganen die die gegevens op grond van een wettelijk voorschrift mogen gebruiken.[45] De Belastingdienst noemt op zijn website als voorbeelden SVB, UWV, CAK, DUO en de Raden voor de Rechtsbijstand.

Welke voorwaarden gelden daarbij?

Bestuursorganen mogen inkomensgegevens alleen gebruiken als zij daartoe een expliciete wettelijke bevoegdheid hebben. De gegevens mogen slechts verder bekend gemaakt worden voor zover dat noodzakelijk is voor het uitoefenen van die bevoegdheid.[46]

[41] Art. 21a lid 1 AWR.
[42] Art. 21b lid 2 en 3 AWR.
[43] http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/werk_en_inkomen/basisregistratie_inkomen/.
[44] Art. 21b lid 1 jo. art. 21 AWR.
[45] Art. 21b lid 1 jo. art. 21 AWR.
[46] Art. 21f lid 1 en 2 AWR.

Overige opmerkingen

Een burger mag weigeren een bestuursorgaan gegevens te vertrekken over inkomen als het die uit de BRI verstrekt kan krijgen.[47]

Overzicht persoonsgegevens

Het inkomensgegeven is het enige authentieke gegeven eigen aan de basisregistratie Inkomen.[48] Bevoegde bestuursorganen zijn verplicht gebruik te maken van de inkomensgegevens in het register[49]. Zij hebben een terugmeldverplichting voor alle authentieke gegevens in het register.[50]

Gegeven(s)	Pgg?[51]	Toelichting
Inkomensgegevens	ja	
BSN	ja	

[47] Art. 21i lid 2 AWR.
[48] Art. 21a lid 1 AWR.
[49] Art. 21g AWR.
[50] Art. 21h AWR. Bij AMvB kunnen authentieke gegevens uit andere registraties aangewezen worden die in de Basisregistratie Inkomen opgenomen worden (art. 21a lid 2 AWR). Op het moment van schrijven is zo'n AMvB er echter (nog) niet.
[51] Gaat het hier om persoonsgegevens?

Handelsregister

Het Handelsregister is een basisregistratie.[52] De Kamers van Koophandel zijn houder van, en verantwoordelijke (in de zin van de WBP) voor het Handelsregister.[53]
Informatie over het Handelsregister is te vinden op de website van de Kamers van Koophandel.[54]

Welke wetten en regels gelden er?

» Handelsregisterwet 2007
» Handelsregisterbesluit 2008

Waarvoor worden de gegevens verzameld?

Het handelsregister heeft de onderstaande doeleinden.[55]
» bevorderen van de rechtszekerheid in het economisch verkeer
» verstrekken van algemene gegevens over ondernemingen en rechtspersonen ter bevordering van de economie
» bijdragen aan het efficiënt functioneren van de overheid

Welke gegevens mogen waarvoor aan wie verstrekt worden?

Het Handelsregister is een openbaar register. In beginsel kunnen dus alle gegevens uit het register aan iedereen verstrekt worden, ook de persoonsgegevens. Uitzonderingen zijn het BSN, geslacht, de geboorteplaats en het geboorteland;[56] deze kunnen echter wel verstrekt worden aan bestuursorganen.[57] Privé-adressen van bepaalde categorieën functionarissen, zoals bestuurders en commissarissen, zijn echter afgeschermd.[58] Anderen kunnen onder strikte voorwaarden hun privé-adres eveneens afgeschermd krijgen.[59]
Bij verstrekking van gegevens uit het Handelsregister worden die gegevens niet gerangschikt naar

[52] De Handelsregisterwet 2007 hanteert de term “basisregister”. Opmerkelijk genoeg bepaalt de wet nergens expliciet dat het Handelsregister een basisregistratie is. Dat valt er echter wel uit op te maken, onder meer uit de volledige naam van de wet (Wet houdende regels omtrent een basisregister van ondernemingen en rechtspersonen) en uit het feit dat in art. 17 lid 2 wordt gesproken over “gegevens overgenomen uit een ander basisregister”.
[53] Art. 3 Handelsregisterwet 2007.
[54] http://www.kvk.nl/over-de-kvk/over-het-handelsregister/.
[55] Art. 2 Handelsregisterwet 2007.
[56] Art. 21 lid 1 Handelsregisterwet 2007.
[57] Art. 28 lid 1 Handelsregisterwet 2007.
[58] Art. 51 lid 1 Handelsregisterbesluit 2008.
[59] Art. 51 lid 3 Handelsregisterbesluit 2008.

natuurlijke personen, met uitzondering van de hieronder opgesomde bestuursorganen voor de vermelde doeleinden.

bestuursorgaan	doeleinde
Minister van Veiligheid en Justitie	controle op misbruik van rechtspersonen
Officier van Justitie	opsporing van strafbare feiten
Belastingdienst	uitvoering taken
UWV, SVB, Minister van SZW	uitvoering SUWI-taken
Burgemeesters en wethouders	uitvoering diverse sociale wetten
Bureau BIBOB	afgeven integriteitsbeoordeling
NMA, AFM, OPTA, Consumentenautoriteit	uitvoering taken

Welke voorwaarden gelden daarbij?

Op het gebruik van persoonsgegevens uit het Handelsregister is de WBP van toepassing. Dat het gaat om openbare gegevens wil dus niet zeggen dat er onbeperkt gebruik van mag worden gemaakt. In ieder geval dient het gebruik van de persoonsgegevens verenigbaar te zijn met een van de doelen waarvoor ze in het register zijn opgenomen.

Overzicht persoonsgegevens

Het Handelsregister bevat gegevens over bedrijven en rechtspersonen.[60] Op twee manieren kan daarbij sprake zijn van persoonsgegevens. In de eerste plaats bevat het register informatie over bij de onderneming of rechtspersoon betrokken natuurlijke personen, zoals eigenaren of bestuurders.[61] Daarnaast zal informatie over bijvoorbeeld een eenmanszaak of maatschap vaak ook iets zeggen over de eigenaar of maten. Ook dan is dus sprake van persoonsgegevens.
Het begrip ‘persoonlijke gegevens’ uit het Handelsregisterbesluit 2008 beschrijft een heel andere soort gegevens, en moet dus niet met het begrip ‘persoonsgegevens’ verward worden.
Met uitzondering van administratieve gegevens zijn alle gegevens in het Handelsregister authentieke gegevens.[62] De Handelsregisterwet bevat verplichtingen voor bevoegde bestuursorganen om in beginsel verplicht gebruik te maken van de authentieke gegevens in het register[63] en om fouten terug te melden.[64] Deze bepalingen zijn echter nog niet in werking getreden.
Omdat veel gegevens in het Handelsregister geen persoonsgegevens zijn, is onderstaand overzicht beperkt tot de hoofdlijnen. Een gedetailleerd overzicht van de gegevens in het Handelsregister is te vinden in Hoofdstuk 4 van het Handelsregisterbesluit 2008.

[60] Art. 5 en 6 Handelsregisterwet 2007.
[61] O.a. art. 9 onder d, art. 10 lid 2 en 3 en art. 17 Handelsregisterwet 2007.
[62] Art. 15 Handelsregisterwet 2007.
[63] Art. 30 Handelsregisterwet 2007.
[64] Art. 31 Handelsregisterwet 2007.

Gegeven(s)	Pgg?[65]	Toelichting
Naam en adres[66]	context	Wel bij bijv. eenmanszaken
Contactgegevens[15]	context	Wel bij bijv. eenmanszaken
Gegevens vestigingen	nee	
Functionarissen en tekenbevoegdheden	ja	
De curator (bij een failissement)	ja	Over de curator
Aantal medewerkers	Ja	Wel bij bijv. eenmanszaken

[65] Gaat het hier om persoonsgegevens? “Context” wil zeggen dat het antwoord op die vraag afhangt van de context waarin de gegevens gebruikt worden.
[66] Van de onderneming c.q. de rechtspersoon zelf.

BRK (Basisregistratie Kadaster)

De BRK is een basisregistratie.[67]
Het Kadaster is de verantwoordelijke voor de BRK.[68]
Informatie over de BRK is te vinden op STIP[69], op de website van het Kadaster[70] en de algemene website van de overheid.[71]
Onderstaande beschrijving beperkt zich zoveel mogelijk tot verstrekkingen aan overheidsinstanties. Zij is gebaseerd op bovengenoemde informatie, alsook op de wet- en regelgeving zoals die te vinden is op wetten.overheid.nl en officielebekendmakingen.nl.

Welke wetten en regels gelden er?

» Burgerlijk Wetboek (boek 3 en 5)
» Kadasterwet[72]
» Kadasterregeling 1994
» Kadasterbesluit
» Uitvoeringsregeling Kadasterwet 1994

Waarvoor worden de gegevens verzameld?

Het Kadaster heeft onder meer tot taak het houden van openbare registers en het houden en bijwerken van de basisregistratie kadaster. Het doel waarvoor onder andere de (persoons)gegevens in de BRK verwerkt worden, is vastgelegd in art 2a van de Kadasterwet. Kortweg: het bevorderen van rechtszekerheid ten aanzien van registergoederen, het bevorderen van een doelmatige geo-informatie-infrastructuur, doelmatige informatievoorziening van de overheid en ondersteuning en bevordering van economische activiteiten.

Welke gegevens mogen waarvoor aan wie verstrekt worden?

Het Kadaster verstrekt op verzoek afschriften, uittreksels, getuigschriften en verklaringen van c.q. over gegevens in de BRK.[73]
Uit de BRK worden geen verzamelingen van persoonsgegevens verstrekt in een zodanige vorm dat daarop rechtstreeks een geautomatiseerde verwerking mogelijk is ten aanzien van een op voorhand

[67] Art. 1a lid 1 Kadasterwet.
[68] Art. 3 lid 1 onder b Kadasterwet en art. 3b Kadasterwet.
[69] http://www.e-overheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties/1487-basisregistratie-kadaster-brk
[70] http://www.kadaster..nl/web/Themas/Registraties/BRK.htm.
[71] http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2007/12/24/basisregistratie-kadaster-en-topografie.html
[72] Zoals gewijzigd door de Wet basisregistraties kadaster en topografie.
[73] Artt. 99-103 Kadasterwet.

onbepaalde groep van personen.[74]
Art. 107b Kadasterwet bepaalt dat bij AMvB beperkingen kunnen worden gesteld aan zulke verstrekkingen met het oog op bescherming van de persoonlijke levenssfeer van geregistreerden. Van deze mogelijkheid heeft de wetgever vooralsnog echter geen gebruik gemaakt.[75]

Welke voorwaarden gelden daarbij?

Voor verstrekkingen uit de BRK is doorgaans een vergoeding verschuldigd.[76]

Overzicht persoonsgegevens

In de BRK worden authentieke en niet-authentieke gegevens onderscheiden.[77]
Authentieke gegevens zijn, kort gezegd:
» kadastrale aanduiding
» NAW+ gegevens van eigenaren en andere rechthebbenden
» informatie over beperkte rechten en beslagen
» perceelsgrenzen en –grootte
» rijks-, provincie- en gemeentegrenzen

Overheidsorganen zijn (waar van toepassing, en behoudens enkele uitzonderingen) verplicht gebruik te maken van de authentieke gegevens in het register.[78] Ze hebben een terugmeldverplichting voor authentieke gegevens.[79]
Een beschrijving van de gegevens in de BRK is te vinden in Hoofdstuk 3 Titel 1 Kadasterwet.
Een uitgebreide technische beschrijving van de gegevens in de BRK is te vinden in de Basis Registratie Catalogus: Kadaster.[80]

[74] Art. 107c Kadasterwet bepaalt dat dat alleen is toegestaan als het geregeld is in een AMvB, maar zo'n AMvB is er niet.
[75] Onderhanden is een toevoeging aan artikel 37 Kadasterbesluit (artikel 37a en 37b) waarin beperkingen worden gesteld aan verstrekkingen met het oog op bescherming van de persoonlijke levenssfeer van geregistreerden. Verwachting is dat deze maatregel medio 2013 in werking treedt.
[76] Art. 108 Kadasterwet.
[77] Art. 7f lid 1 Kadasterwet.
[78] Art. 7k Kadasterwet.
[79] Hoofdstuk 1A Titel 3 Kadasterwet.
[80] https://catalogus.stelselcatalogus.nl/StelselCatalogus/WAStelselcatalogus/basisregistratiecatalogi_algemene_specificaties/basisregistratie_catalogi/Kadaster.

Gegeven(s)	Pgg?[81]	Toelichting
kadastrale aanduiding	nee	
NAW+ gegevens	ja	
beperkte rechten en beslagen	ja	
kadastrale perceelsgrootte	nee	
gegevens over onderliggende stukken	context	Primair ervan afhankelijk of in de documenten (natuurlijke) personen genoemd staan. Dat zal vaak wel het geval zijn.
hypotheekinformatie	context	Indien te linken aan de hypotheekgever
aanvullende feitelijke gegevens	context	Als het gegeven dat wordt aangevuld een persoonsgegeven is, of als wordt aangevuld met een persoonsgegeven
aandeel van een eigenaar	ja	
perceelsgrenzen	nee	
rijks-, provincie- en gemeentegrenzen	nee	
voorstelling van de omtrek van een (hoofd)gebouw	nee	

[81] Gaat het hier om persoonsgegevens? “Context” wil zeggen dat het antwoord op die vraag afhangt van de context waarin de gegevens gebruikt worden.

Basisregistratie WOZ

De basisregistratie WOZ is ingesteld op grond van art. 37a van de Wet WOZ.
Dit overzicht is beperkt tot verstrekkingen aan overheidsinstanties.

Welke wetten en regels gelden er?

» Wet waardering onroerende zaken (Wet WOZ)
» Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet WOZ

Waarvoor worden de gegevens verzameld?

De Basisregistratie WOZ heeft tot doel om gegevens over de vastgestelde waarde van onroerende zaken te verstrekken aan bestuursorganen die op grond van een wettelijk voorschrift bevoegd zijn om die gegevens te gebruiken.[82]

Welke gegevens mogen waarvoor aan wie verstrekt worden?

Waardegegevens worden primair verstrekt aan bestuursorganen die die gegevens gebruiken voor het heffen van belastingen.[83]
Ze worden daarnaast verstrekt aan onderstaande bestuursorganen voor de aangegeven doeleinden.[84]

Bestuursorgaan	doeleinde
Notaris	bestrijding vastgoedcriminaliteit: vergelijken met taxatie-, aankoop- of verkoopwaarde
CBS	vaststellen belastingcapaciteit voor verdeling gemeentefonds; statistische doeleinden
Bureau Ontnemingswetgeving OM	zicht krijgen op waarde in beslag genomen onroerende zaken
Minister van BZK	verlenen van vergunningen aan woningbouwverenigingen voor verkoop sociale huurwoningen
Staatsbosbeheer	waardevaststelling van in erfpacht gegeven onroerende zaken bij herziening canon
Huurcommissie	vaststellen van het aantal schaarstepunten van een woning

[82] Art. 37a lid 3 jo. art. 2 Wet WOZ.
[83] Art. 37b Wet WOZ.
[84] Art. 37h Wet WOZ jo. art. 10 Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet WOZ.

Waardegegevens van woningen kunnen worden verstrekt aan onderstaande derden voor de aangegeven doeleinden.[85]

Derde	doeleinde
Verzekeraar	vergelijken met de veronderstelde waarde van een aan een financieringsaanvraag ten grondslag liggend waardeobject
Hypotheekaanbieders	*idem*

Gegevens worden ten slotte verstrekt aan eigenaren en gebruikers van onroerende zaken in verband met de beoordeling van de juistheid van een voor deze eigenaar of gebruiker genomen WOZ-beschikking.[86]

Welke voorwaarden gelden daarbij?

Bestuursorganen mogen waardegegevens alleen gebruiken als zij daartoe een expliciete wettelijke bevoegdheid hebben. De gegevens mogen slechts verder bekend gemaakt worden voor zover dat noodzakelijk is voor het uitoefenen van die bevoegdheid.[87]
Derden mogen waardegegevens alleen gebruiken voor het aangegeven[88] doeleinde. De gegevens mogen slechts verder bekend gemaakt worden voor zover dat voor dat doeleinde noodzakelijk is.[89]

Overzicht persoonsgegevens

Het waardegegeven van onroerende zaken is het enige authentieke gegeven eigen aan de basisregistratie WOZ.[90] Het gaat vergezeld van temporele en meta-kenmerken. Deze worden altijd met het waardegegeven meegeleverd.[91]
Bevoegde bestuursorganen zijn verplicht gebruik te maken van de waardegegevens in het register[92]. Zij hebben een terugmeldverplichting voor alle authentieke gegevens in het register.[93]
Aan het waardegegeven worden ook andere gegevens gekoppeld, zoals over adres, eigenaars en gebruikers van een object. Een deel daarvan betreft authentieke gegevens uit andere basisregistraties.[94]
De persoonsgegevens die aan andere afnemers verstrekt worden staan gegroepeerd in de bijlage bij het ‘Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet waardering onroerende zaken’.

[85] Art. 40a Wet WOZ jo. art. 11 Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet WOZ.
[86] Artikel 40 Wet WOZ.
[87] Art. 37c Wet WOZ.
[88] In art. 11 Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet WOZ.
[89] Art. 40a lid 3 Wet WOZ.
[90] Art. 37a Wet WOZ.
[91] Art. 37b lid 1 Wet WOZ.
[92] Art. 37d lid 1 Wet WOZ.
[93] Art. 37f Wet WOZ.
[94] Art. 37a lid 2 Wet WOZ en art. 7 lid 2 Uitvoeringsbesluit kostenverrekening en gegevensuitwisseling Wet WOZ.

Op site van de Waarderingskamer[95] staat[96]: 'Omdat de Belastingdienst, het Centraal Bureau voor de Statistiek (CBS) en de waterschappen voor het gebruik van de WOZ-waarden meer gegevens nodig hebben dan in de Basisregistratie WOZ worden opgenomen, ontvangen deze partijen in de toekomst enkele extra gegevens via de Landelijke Voorziening WOZ.'
Niet verder is onderzocht welke gegevens het hier betreft.

Gegeven(s)	Pgg?[97]	Toelichting
Personalia en adres van eigenaar/gebruiker (natuurlijk persoon) van een WOZ-object.	ja	BSN en A-nummer (GBA) zijn onderdeel van de gegevensset
b) Naam, adres en KvK-nr. eigenaar/gebruiker (rechtspersoon)	context	gegevens over o.a. eenmanszaken zijn persoonsgegevens als ze iets relevants zeggen over de persoon of personen achter het bedrijf
c) Waardegegeven WOZ-object	ja	waardegegeven kan door een ieder eenvoudig in verband gebracht worden met de eigenaar die in de BRK (Kadaster) opgezocht kan worden
d) Geboortedatum van de eigenaar/gebruiker (natuurlijk persoon)	ja	
e) Postadres van de eigenaar/gebruiker	ja	mits het gaat om een natuurlijk persoon

[95] Toezichthouder op de uitvoering van de Wet WOZ door gemeenten.
[96] http://www.waarderingskamer.nl/default.aspx?sec=content&id=800.
[97] Gaat het hier om persoonsgegevens? "Context" wil zeggen dat het antwoord op die vraag afhangt van de context waarin de gegevens gebruikt worden.

Kentekenregister (BRV: Basisregistratie Voertuigen)

Het Kentekenregister is een basisregistratie.[98]
De RDW is de houder van en de verantwoordelijke voor het Kentekenregister.[99]
Onderstaande beschrijving beperkt zich zoveel mogelijk tot verstrekkingen aan overheidsinstanties. Zij is gebaseerd op de wet- en regelgeving zoals die te vinden is op wetten.overheid.nl en officielebekendmakingen.nl.

Welke wetten en regels gelden er?

» Wegenverkeerswet 1994
» Kentekenreglement
» Regeling gegevensverstrekking kentekenregister 2008
» Reglement verwerking gegevens Kentekenreglement
» Verstrekkingsvoorwaarden inzake het Kentekenregister van de Dienst Wegverkeer 2008

Waarvoor worden de gegevens verzameld?

De gegevens in het Kentekenregister kennen de drie onderstaande verzameldoeleinden:[100]
1. goede uitvoering WVW'94 en daaronder hangende regelgeving;
2. goede uitvoering van een aantal wettelijke regelingen t.a.v. motorrijtuigen (waarvan er een aantal expliciet vermeld worden);
3. overheidsorganen voorzien van gegevens uit het register voor zover zij aangeven die nodig te hebben voor een goede uitoefening van hun publiekrechtelijke taak.

Welke gegevens mogen waarvoor aan wie verstrekt worden?

De RDW verstrekt gegevens uit het Kentekenregister verstrekt aan overheidsorganen voor zover ze die nodig hebben voor een goede uitoefening van hun publiekrechtelijke taak.[101]
Naast bestuursorganen worden ook een aantal andere personen en organisaties als overheidsorganen aangewezen in de context van bepaalde taken die zij uitoefenen.[102]

[98] Art. 42 lid 1 WVW'94.
[99] Art. 42 lid 2 WVW'94.
[100] Art. 42 lid 4 WVW'94.
[101] Art. 43 lid 1 WVW'94.
[102] Art. 1 Regeling gegevensverstrekking kentekenreglement.

ontvanger	doeleinde
Uitvoeringsinstanties sociale regelingen	vermogenstoets
Curatoren	beheer en vereffening failliete boedel
Bewindvoerders	schuldsanering
Auto Recycling Nederland BV	uitvoeren Besluit beheer autowrakken
Waarborgfonds Motorverkeer	afwikkelen en verhalen schade
Stichting Nationale en Internationale Wegvervoer Organisatie	afgifte van en controle op vergunningen
Nederlands Bureau Motorrijtuigverzekeraars	afwikkelen en verhalen schade in het buitenland verzekerde voertuigen
Onderzoeks- en onderwijsinstellingen	wetenschappelijk onderzoek in opdracht van de overheid

Welke voorwaarden gelden daarbij?

De aanvrager moet de reden voor zijn aanvraag opgeven en zich identificeren.[103]
Voor de verstrekking is een tarief verschuldigd.[104]
Voor overheidsorganen gelden geen aanvullende verplichtingen uit hoofde van de hierboven genoemde wet- en regelgeving. De RDW houdt ten aanzien van de verstrekkingen van persoonsgegevens aan overheidsorganen passief toezicht. [105] De RDW wijst bij een verstrekking een overheidsorgaan op de eigen verantwoordelijkheid en verklaart middels meelevering van de Verstrekkingsvoorwaarden Kentekenregister 2008 deze voorwaarden van toepassing op overheidsorganen.

Overzicht persoonsgegevens

In het Kentekenregister worden authentieke en niet-authentieke gegevens onderscheiden.[106]
Authentieke gegevens zijn:

» gegevens die op grond van EU-regelgeving verplicht op het kentekenbewijs staan, en die niet al elders als authentiek gegeven zijn aangewezen[107]
» de voertuigcategorieën[108]
» de tenaamstelling
» bij afgifte van een kentekenbewijs:[109]
    ▪ de overlegde legitimatie

[103] Art. 10 lid 2 Kentekenreglement.
[104] Art. 43 lid 6 en 7 WVW'94.
[105] Zie ook de Memorie van Toelichting Wijziging Wegenverkeerswet 1994, Kamerstukken II, 31219 nr. 3, blz. 19.
[106] Art. 42a lid 1 onder a WVW'94.
[107] Art. 42a lid 2 WVW'94.
[108] Vgl. art. 21 lid 1 WVW'94.
[109] Art. 42a lid 3 WVW'94 jo. art. 7 Kentekenbesluit.

- een indicatie van niet betaalde belastingen of boetes
- erkenning bedrijfsvoorraad[110]

Overheidsorganen zijn (waar van toepassing, en behoudens enkele uitzonderingen) verplicht gebruik te maken van de authentieke gegevens in het register.[111] Ze hebben een terugmeldverplichting voor authentieke gegevens[112] én een algemene meldplicht van feiten die relevant kunnen zijn ten aanzien van de gegevens in het register.[113]
In het Kentekenregister worden eveneens gevoelige en niet-gevoelige gegevens onderscheiden.[114] Tot de gevoelige gegevens horen onder meer alle persoonsgegevens. Dit onderscheid is voor overheidsorganen echter niet direct relevant.
De RDW verwerkt strafrechtelijke persoonsgegevens en persoonsgegevens ter vaststelling van mogelijk strafbaar gedrag voor zover dit verband houdt met de uitvoering van de WVW'94 en een aantal andere wettelijke regelingen t.a.v. motorrijtuigen.[115]
Onderstaand overzicht is gebaseeerd op art. 6 Kentekenregister. Een volledig overzicht van de gegevens in de BRV is te vinden in de Gegevenscatalogus BRV[116].

Gegeven(s)	Pgg?[117]	Toelichting
a) Personalia en adres kentekenhouder (natuurlijk persoon)	ja	
b) Adres en KvK-nr. kentekenhouder (rechtspersoon)	context	Gegevens over o.a. eenmanszaken zijn persoonsgegevens als ze iets relevants zeggen over de persoon of personen achter het bedrijf
c) Personalia en adres gemachtigde	ja	
d) NAW invoerder of producent van (nog) kentekenloos voertuig	ja	Mits het gaat om een natuurlijk persoon
e) NAW- en legitimatiegegevens exporteur voertuig	ja	
f) Legitimatiegegevens aanvrager kentekenbewijs	ja	
g) Gegevens over afgifte, invorderen en ongeldig verklaren kentekenbewijs	context	Hangt ervan af of de kentekenbewijsdata in verband te brengen zijn met de kentekenhouder
h) Gegevens erkenning bedrijfsvoorraad	context	Gegevens over o.a. eenmanszaken zijn persoonsgegevens als ze iets relevants zeggen over de persoon of personen achter het bedrijf

[110] Vgl. art. 62 WVW'94.
[111] Art. 43b WVW'94.
[112] Art. 43c WVW'94.
[113] Art. 43f WVW'94.
[114] Art. 42a lid 1 onder b WVW'94.
[115] Art. 42 lid 5 WVW'94.
[116] http://www.rdw.nl/SiteCollectionDocuments/Over%20RDW/Catalogus%20Basisregistratie%20Voertuigen%20%283_B_0909c%29.pdf.
[117] Gaat het hier om persoonsgegevens? "Context" wil zeggen dat het antwoord op die vraag afhangt van de context waarin de gegevens gebruikt worden.

i) Gegevens over schorsing kentekenbewijs	context	Hangt ervan af of de kentekenbewijsdata in verband te brengen zijn met de kentekenhouder
j) Gegevens over de APK-keuring	context	Hangt ervan af of het kenteken in verband te brengen is met de kentekenhouder en of de gegevens iets over de kentekenhouder zeggen
k) Gegevens t.b.v. motorrijtuigen-belasting en bpm	context	Hangt ervan af of het kenteken in verband te brengen is met de kentekenhouder en of de gegevens iets over de kentekenhouder zeggen
l) Voertuiggegevens	context	Hangt ervan af of het kenteken in verband te brengen is met de kentekenhouder en of de gegevens iets over de kentekenhouder zeggen
m) Andere wetstechnische gegevens	context	Hangt ervan af of het kenteken in verband te brengen is met de kentekenhouder en of de gegevens iets over de kentekenhouder zeggen
n) Gegevens over in buitenland geregistreerde voertuigen	?	Hangt af van het soort gegeven
o) Gegevens over typegoedkeuringen	nee	
p) Gegevens over verwerken en gebruiken van gegevens uit het register	ja	
q) Administratieve gegevens over de tenaamstelling	context	Hangt ervan af of de gegevens iets zeggen over de kentekenhouder
r) Gegevens over vermissing en diefstal	context	Hangt ervan af of het kenteken in verband te brengen is met de kentekenhouder en of de gegevens iets over de kentekenhouder zeggen
s) BSN, A-nummer, RDW-nummer	ja	
t) Overlijden kentekenhouder	nee	Gegevens over overledenen worden niet beschouwd als persoonsgegevens
u) Gegevens over achterstallige boetes en belastingen	context	Hangt ervan af of het kenteken in verband te brengen is met de kentekenhouder