
Samenvatting

Dit onderzoek is gericht op het beantwoorden van de vraag met welke belangen rekening moet worden gehouden bij de verstrekking van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het Openbaar Ministerie, de politie en de buitengewoon opsporingsambtenaren anderzijds. Daarnaast wordt de vraag onderzocht in hoeverre het gewenst en juridisch mogelijk is om voor het verstrekken van toezichtgegevens tussen genoemde partijen een algemene regeling in de Algemene wet bestuursrecht en/of eventuele andere wetten op te nemen.

Betrokken belangen en juridische erkenning ervan

Om de belangen die spelen rond gegevensuitwisseling tussen toezichthouders en de weging ervan te inventariseren is gekozen voor een aanpak door middel van bestudering van de relevante stukken, een quickscan, casus, gesprekken met ervaringsdeskundigen, een expert-meeting en een internetenquête onder ervaringsdeskundigen op de werkvloer ten behoeve van een Multicriteria-analyse. In paragraaf 1.3 en 3.1 zijn de onderzoeksmethoden nader toegelicht.

Uit het onderzoek blijkt dat gaat het om een uiteenlopend palet van belangen. In de eerste plaats zijn dat de belangen van de in deelvraag 1 genoemde inspectie- en opsporingsdiensten, de toezichthoudende functionarissen en opsporingsambtenaren. In de tweede plaats zijn dat de belangen van de in deelvraag 2 bedoelde andere belanghebbenden, te weten onder toezicht gestelde burgers en bedrijven en hun vertegenwoordigers. Deze belanghebbenden hebben ieder vanuit hun eigen positie belang bij de uitwisseling van gegevens. In paragraaf 3.2, 3.3 en 3.4, alsmede in bijlage 7.2 zijn de gedetailleerde resultaten te vinden van de

inventarisatie van belangen. Het antwoord op de vraag welke belangen een rol spelen hangt af van de soort gegevens die zullen worden uitgewisseld. Zoals in hoofdstuk 2 is uiteengezet, kunnen toezichtgegevens worden onderverdeeld in persoonsgegevens, bedrijfs- of fabricagegegevens en overige gegevens. Voor laatstgenoemde categorie bestaan geen belemmeringen voor de uitwisseling: veelal wordt aangenomen dat uitwisseling bijdraagt aan de efficiency en de effectiviteit van het overheidsoptreden, terwijl er geen belangen zijn die pleiten tegen uitwisseling.

Voor de eerste twee categorieën geldt dat het belang bij privacy c.q. bescherming van bedrijfsgegevens wettelijk wordt gewaarborgd. De aard van de uit te wisselen gegevens en het gewicht van de betrokken belangen hangen aldus sterk samen.

Private belangen die hierbij een rol kunnen spelen zijn de vertrouwelijke behandeling van gegevens (geheimhouding), de bescherming van bedrijfs- en fabricagegegevens en de bescherming van persoonsgegevens (ook van derden), de transparantie ten aanzien van de uitwisseling van gegevens, de mogelijke baten doordat administratieve lasten verminderen, en het belang bij zorgvuldige gegevensverzameling en verwerking met het oog op beroepsaansprakelijkheid.

Overheidsbelangen zijn de efficiency en de effectiviteit van het overheidsoptreden, het openhouden van de informatiestroom (geheimhouding en organisatiebelang), de betrouwbaarheid van de overheid bij het beschermen van privacy en andere vertrouwelijke gegevens (privacy, imago en organisatiebelang), het zicht op gegevens bij doorverstrekking in verband met de eigen verantwoordelijkheid en het vertrouwen van de burger (doelbinding), de resultaten die met de verkregen gegevens kunnen worden gerealiseerd (eigen baten), de nadelen voor de eigen informatiepositie bij verstrekking van de gegevens, het belang van de juistheid/goede kwaliteit van de gegevens en het risico van het niet of niet correct ontvangen van de toezichtgegevens.

Een aantal van deze belangen is juridisch te labelen onder de categorieën bescherming van persoonsgegevens, bescherming van bedrijfs- en fabricagegegevens en geheimhoudingsplichten. De niet juridisch erkende belangen zijn terug te voeren op organisatorische, praktische, en ICT-gerelateerde omstandigheden.

Waardering van belangen

Uit de MCA en de expertmeeting blijkt dat juist bij de uitwisseling van toezichtgegevens het belang van de bescherming van persoonsgegevens, de eis van doelbinding en de geheimhouding van grote waarde worden geacht. De stuwende en procesmatige beginselen in de sfeer van baten voor de organisatie en kosten van de gegevensuitwisseling scoren lager. Kosten scoren zelfs uitgesproken laag. Hieruit zou kunnen worden afgeleid dat de zogenoemde verankerende beginselen ook werkelijk goed verankerd zijn in onze handhavingorganisaties. Een aandachtspunt is dat de procesmatige beginselen zoals transparantie en accountability niet expliciet lijken te leven. Denkbaar is dat deze principes intrinsiek

worden meegewogen bij de besluitvorming over het al of niet vragen of verstrekken van gegevens, maar de uitkomsten van ons onderzoek geven daarvoor geen basis. Eerder moet worden geconcludeerd dat deze beginselen geen rol spelen.

Als een rangorde van de hoogst gewaardeerde belangen moet worden aangegeven dan valt op dat doelbinding de hoogste score haalt, daarna volgen geheimhouding en privacy, en bij de overheid baten voor de ontvangende of leverende organisatie. De reden voor deze eenduidige keuze zou kunnen worden gezocht in de diepe worteling van de grondrechten in de overheidsorganisatie. Deze beginselen bieden immers tegenwicht aan de voortdurende roep om veiligheid, effectief optreden en efficiency van de overheidsdiensten.

Deze observatie behoeft echter nuancering. 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. Zoals uit de MCA blijkt, hechten de vertegenwoordigers van burgers en bedrijven 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.

Organisatiebelang en transparante afwegingsprocessen

Convenanten zijn bedoeld om een structureel samenwerkingsverband tot stand te brengen, waarbinnen op grond van de Wbp of de Wpg gegevens mogen worden uitgewisseld. Bij het onderzoek naar de inhoud van convenanten viel op dat deze convenanten over het algemeen meer intentieverklaringen zijn en weinig verheldering bieden over de verschillende posities en bevoegdheden. Zij dienen vooral ter legitimatie van de gegevensuitwisseling. Een convenant kan echter geen bevoegdheidsgrondslag bieden: deze moet worden ontleend aan de wet. Een convenant is wel de plaats om vast te leggen hoe deze bevoegdheden in procedurele zin zullen worden uitgeoefend. Zo zou een convenant moeten bepalen voor welke doeleinden de samenwerking dient, welke gegevens of gegevenssets daarvoor zullen worden aangemaakt of aangeleverd, wie bewaakt dat wordt voldaan aan de Wbp (melding aan het CBP), via welke media zal worden uitgewisseld (databank, cloud) en hoe de veiligheid van deze media wordt bewaakt.

In het onderzoek is veel aandacht uitgegaan naar de bescherming van persoonsgegevens. Dat is een kernpunt bij de afweging of tot uitwisseling kan worden overgegaan. In paragraaf 2.3.2

wordt het EU kader voor privacybescherming besproken, dat is uitgewerkt in artikel 7, 8 en 9 Wbp (paragraaf 2.4). Dit kader biedt ruime mogelijkheden om gegevens uit te wisselen, als maar is voldaan aan de randvoorwaarde dat duidelijk vaststaat waarvoor gegevens worden verzameld en verwerkt. Wanneer bestuurlijke toezichthouders en uitvoeringsorganisaties onderling willen uitwisselen, kan dat ook op grond van de Wbp. Het Europese recht, noch de Wbp staan daaraan in de weg. De problematiek van de doelbinding, die in het onderzoek in paragraaf 2.4.3 en 4.6 werd besproken, is niet onoverkomelijk.

Op de strafrechtelijke persoonsgegevens is de Wbp niet van toepassing. De Wpg en de Wjsg geven hier een kader voor de uitwisseling met benoemde partijen c.q. in een samenwerkingsverband. Beide wetten kennen daarnaast de bevoegdheid om in incidentele gevallen gegevens te verstrekken aan niet benoemde partijen, als dat een zwaarwegend belang dient (artikel 19 Wpg en 39f Wjsg). De wet biedt aldus ruimte voor afweging, zij het dat de normconditie ‘zwaarwegend belang’ tot terughoudendheid noopt. Uit ons onderzoek blijkt dat vragende partijen de politie en het OM soms te terughoudend vinden bij het maken van die afweging (zie paragraaf 3.2.1.4 en 3.2.3.7). Het eigen belang van de organisatie, het krijgen en behouden van de eigen informatiepositie, weegt daarbij volgens de vragende partijen regelmatig zwaarder dan het belang van de goede werking van de overheid in den brede. Bij concrete afwegingen zouden OM en de opsporingsinstanties daarom meer aandacht moeten besteden aan de belangen van andere overheidsorganisaties. Niet zelden wordt bovendien de doelbinding, die ook in de Wpg en de Wjsg beperkingen stelt, als argument naar voren gebracht om verstrekking te weigeren.

Ook het belang bij geheimhouding heeft in het onderzoek nadere aandacht gekregen. Geheimhoudingsplichten strekken zich niet alleen uit over de hiervoor besproken vertrouwelijke gegevens (persoonsgegevens en bedrijfs- en fabricagegegevens) maar over alle soorten toezichtgegevens. Zoals in paragraaf 2.6 is aangegeven heeft de wetgever geheimhoudingsplichten in het leven geroepen ter bevordering van de goede werking van het openbaar bestuur, daaronder begrepen de belangen bij toezicht, controle en opsporing. Geheimhouding, zeker zoals het op de werkvloer wordt geïnterpreteerd, is daarmee vooral ook een organisatiebelang: het openhouden van de inkomende informatiestroom en het niet weggeven van de informatiepositie in een onderzoek. In paragraaf 5.3.1.3 is ingegaan op het strategische belang van de geheimhoudingsplicht. De geheimhoudingsplicht biedt de mogelijkheid om zich in gevallen van twijfel over de wenselijkheid of toelaatbaarheid van de gegevensverstrekking daarachter te verschuilen.

Om de acceptatie van de uitkomst bij vragende instanties te vergroten, verdient het aanbeveling de afwegingsprocessen beter inzichtelijk en toetsbaar te maken. Dit kan voorkomen dat overheidsinstanties uitgaan van tegengestelde belangen en daarmee hun eigen organisatiebelang als belangrijkste ijkpunt zien. Het kan ook voorkomen dat overregulering ontstaat, waarbij de lijst van instanties waaraan bepaalde gegevens moeten worden verstrekt steeds langer wordt. Een andere oplossing kan zijn dat een verplichting tot het verstrekken van gegevens wordt opgenomen (bij twijfel wel inhalen) met de mogelijkheid tot het maken van een uitzondering, waarvoor dan wel een zware motiveringsplicht geldt. Deze laatste optie

is door respondenten in het onderzoek als wenselijk naar voren gebracht (zie paragraaf 3.2.3.7 en hierna ook paragraaf 5.5.2).

(G)een algemene regeling

De behoefte aan een algemene regeling is gepeild via de oriënterende gesprekken over de drie casus en de expertmeeting. Uit deze gesprekken is geen eenduidig beeld gekomen. Op de werkvloer, waar daadwerkelijk beslissingen over doorverstrekking c.q. verzoeken om gegevens worden genomen, bestaat wel behoefte aan een algemene regeling, met name in de verwachting dat meer duidelijkheid zou ontstaan over de juridische basis bij het uitwisselen van gegevens. Op managementniveau blijkt die behoefte echter niet.

Omdat hieruit geen eenduidige conclusies zijn te trekken, hebben de onderzoekers zich gebogen over de vraag hoe een wettelijke regeling, zo die er moest komen, eruit zou kunnen zien. In de eerste plaats is onderzocht of een regeling voor uitwisseling van toezichtgegevens een plaats zou kunnen krijgen in de Awb. De Awb is om verschillende redenen die in paragraaf 4.2 uiteen zijn gezet een minder geschikte plek. Vervolgens is onderzocht of een kaderwet een geschikt medium zou kunnen zijn. Een kaderwet heeft het voordeel dat daarin de zaken geregeld kunnen worden die momenteel als belemmerend worden gezien voor de gegevensuitwisseling in het algemeen, zoals een duidelijke regeling inzake de bevoegdheid om gegevens uit te wisselen en verduidelijking van de wijze waarop verschillende verstrekingsregimes met elkaar te verenigen zijn. Tegelijkertijd laat een kaderwet ruimte om onderwerpen die specifiek voor een bepaald beleidsterrein gelden, in bijzondere wetgeving en daarop gebaseerde (lagere) regelingen te regelen. Een kaderwet heeft als nadeel dat het naast elkaar bestaan van een kaderwet en de Wbp weer nieuwe vragen kan oproepen. De Wbp kan echter als uitgangspunt dienen en worden omgebouwd tot een brede wet inzake de gegevensverstrekking. Daarbij moet dan ook de verhouding tot de Wpg en de Wjsg worden geregeld. Denkbaar is dat ook de uitwisseling van strafrechtelijke persoonsgegevens in een brede kaderwet wordt geregeld.

De eis van doelbinding zorgt voor veel vragen. Dit leidt er toe dat veel partijen die over persoonsgegevens beschikken bij twijfel over de toelaatbaarheid van uitwisseling er dan maar van afzien. In Hoofdstuk 4 zijn drie oplossingen voor dit probleem aangedragen. De eerste mogelijkheid zou zijn het criterium van artikel 9 Wbp (voldoende verwantschap) helderder en concreter te formuleren, zodat een maatstaf bestaat die voor de praktijk beter hanteerbaar is. De tweede mogelijkheid is het laten vallen van de eis van de dubbele doelbinding zoals die nu in de wet geformuleerd is. De derde mogelijkheid is in een nadere regeling specifiek voor een bepaald beleidsterrein op te sommen welke gegevens aan welke toezichthouders verstrekt mogen worden.

Al met al concluderen wij dat een algemene wettelijke regeling weliswaar mogelijk is, maar slechts voor een beperkt aantal van de in dit rapport gesignaleerde problemen een oplossing biedt.

Aanbevelingen

1. Het verdient aanbeveling de bepalingen uit de Wbp over de voor gegevensverwerking vereiste doelbinding - die nu een belemmering vormen bij de gegevensuitwisseling - te verduidelijken in een kaderwet, eventueel met nadere uitwerking in sectorale wetgeving. Deze bepalingen zouden samen met de bepalingen die thans in de Wbp zijn opgenomen, tot een brede kaderwet omgevormd kunnen worden.
2. Met betrekking tot de eis van doelbinding bij doorverstreking is het aan te bevelen het criterium van voldoende verwantschap te schrappen. De vraag of twee doelen onverenigbaar zijn, is in de meeste gevallen makkelijker te beantwoorden dan de vraag of er tussen twee doelen voldoende verwantschap bestaat. Als het in artikel 9, tweede lid, Wbp genoemde element van verwantschap van doelen voor toezicht-houders zou komen te vervallen, zou dat de eisen die de Wbp op dit punt stelt, voor de praktijk beter hanteerbaar maken.
3. Convenanten zouden niet opgesteld moeten worden met als primair doel te regelen welke gegevens uitgewisseld kunnen worden en tussen welke partijen dat kan. Het centrale probleem bij de gegevensuitwisseling is dat de wettelijke normen die momenteel vaak onduidelijkheid veroorzaken, eerst verduidelijkt moeten worden. Als het al mogelijk zou zijn deze normen in convenanten zodanig te concretiseren dat ermee gewerkt kan worden, is nog niet duidelijk of ze in overeenstemming zijn met de wettelijke normen. Wel kunnen convenanten worden afgesloten ter nadere uitvoering van de wettelijke normen uit een kaderwet of sectorale wetgeving, die al wel concreet genoeg zijn. Het verdient aanbeveling om in een convenant louter praktische en procedurele afspraken te maken tussen de gegevensverstrekker en ontvanger.
4. In het geval dat onwil een factor is bij het uitwisselen van gegevens, zou een wettelijke verplichting tot gegevensuitwisseling overwogen kunnen worden. Een algemene verplichting in een kaderwet lijkt echter niet doelmatig en schiet wellicht over het doel heen. Voldoende is dat in een kaderwet wordt opgenomen dat 'bij of krachtens de wet' een verplichting in het leven kan worden geroepen. Deze verplichting zou uitzondering moeten kunnen lijden om zwaarwegende redenen, die worden geëxpliciteerd in de motivering van de weigeringsbeslissing.
5. In die gevallen waarin niet wordt gekozen voor het invoeren van een wettelijke verplichting tot gegevensverstrekking als in Aanbeveling 4 genoemd, verdient het aanbeveling de afwegingsprocessen die leiden tot weigering van gegevensverstrekking beter inzichtelijk en toetsbaar te maken. Dit kan voorkomen dat overheidsinstanties uitgaan van tegengestelde belangen en daarmee hun eigen organisatiebelang als belangrijkste ijkpunt zien. Verder kan het leiden tot een betere acceptatie van een weigering bij de vragende partij.
6. Aanpassing van wettelijke regels kan helpen bij het oplossen van de hier besproken problemen. Los daarvan verdient het aanbeveling om voor degenen die moeten beslissen over gegevensverstrekking praktische handvatten te ontwikkelen op basis waarvan zij verantwoorde en transparante beslissingen kunnen nemen.