Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

31 051 Evaluatie Wet bescherming persoonsgegevens

Nr. 5

BRIEF VAN DE MINISTERS VAN JUSTITIE, EN VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 november 2009

Hierbij bieden wij u, mede namens de Staatssecretaris van Economische Zaken, het kabinetsstandpunt aan ten aanzien van de bevindingen van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf) alsmede de evaluatierapporten van de Wet bescherming persoonsgegevens.

Samenvatting

De verwerking en de bescherming van persoonsgegevens zijn van vitaal belang voor het functioneren van de hedendaagse samenleving. De burger mag erop vertrouwen dat zorgvuldig met zijn persoonsgegevens wordt omgegaan. En hij mag er op rekenen dat informatie tussen overheidsinstanties wordt gedeeld als dat voor de bescherming van zijn veiligheid noodzakelijk is.

Het kabinet kiest voor het stimuleren van een optimale gegevensbescherming en -verwerking. Instanties die persoonsgegevens gaan gebruiken, moeten vooraf bepalen welke gegevens zij nodig hebben en met welk doel, en moeten dit ook duidelijk maken aan de burger. Het toezicht op de naleving van de wet wordt aangescherpt. Het delen van reeds beschikbare gegevens tussen overheidsinstanties wordt verder gestimuleerd ten behoeve van de veiligheid en de hulpverlening. Het kabinet werkt deze voornemens uit aan de hand van een viertal kernthema's.

Kernthema 1: «Gewoon doen»: meer waarborgen bij de omgang met persoonsgegevens

Allereerst wil het kabinet meer aandacht voor de wijze waarop met persoonsgegevens wordt omgegaan en de waarborgen die daarbij moeten worden vervuld. Dat begint met een zorgvuldige toets in de vorm van een risicoanalyse voorafgaand aan het verzamelen van gegevens. De overheid ontwikkelt hiervoor een instrument zoals dit in het Verenigd

KST136762
0910tkkst31051-5
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2009

Koninkrijk wordt gebruikt (*Privacy Impact Assessments*). Risico's die zijn geïdentificeerd hoeven echter niet altijd tot gevolg te hebben dat afgezien moet worden van een verwerking. Door goede waarborgen kan het mogelijk zijn om privacyrisico's weg te nemen, waardoor gegevens op een correcte manier kunnen worden verwerkt.

De Adviescommissie Veiligheid en persoonlijke levenssfeer sluit hierbij aan met de presentatie van een richtinggevend kader voor het veiligheidsdomein. Het kabinet onderschrijft de daarin opgenomen criteria. Deze zijn met name dienstig voor de uitvoeringorganisaties en instellingen die dagelijks te maken hebben met afwegingen die raken aan de persoonlijke levenssfeer van burgers.

Voor *professionals* binnen de overheid wordt een helpdesk ingericht, die hen kan helpen bij het nemen van besluiten over wanneer en op welke wijze persoonsgegevens uitgewisseld kunnen worden. Deze helpdesk voorziet daarmee in de maatschappelijke adviestaak die op dit moment door het College bescherming persoonsgegevens (Cbp) wordt behartigd.

Met de grondslag «indien noodzakelijk voor de veiligheid moet je delen» geeft de commissie een duidelijk signaal naar de praktijk. Als duidelijk is dat de veiligheid van individuen concreet wordt bedreigd en het delen van persoonsgegevens dat risico kan wegnemen, móeten persoonsgegevens uitgewisseld worden tussen verschillende organisaties.

Het kabinet onderschrijft in die zin de door de commissie Brouwer-Korf bepleite explicitering van art. 9 van de Wbp via voorlichting, facilitering en het bieden van handelingsperspectief. Tevens zal het kabinet onderzoeken op welke wijze de uitwisseling van gegevens tussen toezichthouders, politie en Openbaar Ministerie kan worden vergemakkelijkt.
De positieve resultaten in de *pilots* geven aanleiding om de verdere ontwikkeling van *Automatic Number Plate Recognition* (ANPR) voortvarend ter hand te nemen. De huidige wetgeving biedt daarvoor onvoldoende ruimte. Thans wordt een wettelijk kader voorbereid dat de inzet van de verschillende toepassingsmogelijkheden van ANPR reguleert.

Kernthema 2: Robuuster extern toezicht

Het kabinet heeft de versterking van het externe toezicht als tweede thema aangemerkt. Voor de burger is het van belang dat hij zich gesteund weet door een toezichthouder wanneer op een onjuiste manier met zijn gegevens zou worden omgegaan. Onafhankelijk toezicht en onafhankelijke handhaving zijn daarbij kernwaarden.

Een sterke toezichthouder draagt via zijn bevindingen en uitspraken bij aan een betere rechtsontwikkeling. Uit de evaluatierapporten over de werking van de Wet bescherming persoonsgegevens (Wbp) blijkt een nalevingstekort. Het kabinet meent dat daarom de handhaving versterkt moet worden. Het kabinet zal de handhaving van de materiële normen van de Wbp door middel van het opleggen van bestuurlijke boetes wettelijk mogelijk maken.

Het Cbp vervult daarnaast een rol als wetgevingsadviseur. De EU-privacyrichtlijn (nr. 95/46/EG) legt aan de lidstaten de verplichting op de toezichthouder om advies te vragen voorafgaand aan de vaststelling van wettelijke voorschriften die geheel of grotendeels de bescherming van persoonsgegevens betreffen. Het kabinet is niet voornemens ten aanzien van deze rol van het Cbp veranderingen voor te stellen.

Kernthema 3: Minder nadruk op procedures en controle vooraf

Onder deze noemer wil het kabinet bereiken dat administratieve lasten van burgers en bedrijven zoveel als mogelijk worden teruggedrongen. Bedrijven die een kwalitatief goed beleid voeren op het gebied van bescherming van persoonsgegevens kunnen worden bevrijd van bestaande administratieve lasten.

Bestuursrechtelijke verplichtingen zullen waar mogelijk worden vervangen door andere methoden waarmee kan worden voorzien in voorafgaande noodzakelijkheidstoetsen. Het kabinet is uiteraard gehouden aan de EU-privacyrichtlijn, maar neemt wel een voorschot op de Nederlandse inbreng in de discussie over de actualisatie van de privacyrichtlijn.

Er zal een ruimhartiger vrijstellingsbeleid ten aanzien van meldingsplichten worden gevoerd. De eerste stappen zijn daartoe gezet in de vorm van een inmiddels in consultatie gezonden aanpassing van het Vrijstellingsbesluit Wbp. Dit besluit zal in de loop van 2010 in werking kunnen treden. In overleg met het Cbp en het georganiseerd bedrijfsleven wordt bezien hoe de lasten die verbonden zijn aan het Voorbereidend Onderzoek kunnen worden verminderd. Dat kan door het aantal gevallen waarin een VO vereist is verder te beperken en door de procedure aanmerkelijk te verkorten.

Kernthema 4: Het burgerperspectief

Om de positie van de burger beter te beschermen moet de burger door overheidsinstellingen en bedrijven die zijn gegevens verwerken, beter worden geïnformeerd over die verwerkingen.
Initiatieven die een bijdrage leveren aan de positie van de burger bij de verwerking van zijn persoonsgegevens worden versterkt. Op de website www.burgerservicenummer.nl kan iedereen nagaan welke organisatie welke gegevens uitwisselt met behulp van het burgerservicenummer (BSN). Op de website www.mijnoverheid.nl kunnen burgers inzien welke informatie bij overheidsorganisaties over hen bekend is.

Verder staan de burger privaatrechtelijke en bestuursrechtelijke mogelijkheden ter beschikking bij een onrechtmatige verzameling, verwerking of gebruik van gegevens. In aanvulling is het van groot belang het inzagerecht te ondersteunen door het ontwerpen van klachtregelingen die per sector op maat zijn gesneden.
Verplichtingen van overheidsinstellingen en bedrijven om persoonsgegevens te beveiligen zullen worden aangescherpt.

1. Inleiding

De verwerking en de bescherming van persoonsgegevens zijn van vitaal belang voor het functioneren van de hedendaagse samenleving. De burger mag erop vertrouwen dat zorgvuldig met zijn persoonsgegevens wordt omgegaan. En hij mag er op rekenen dat informatie tussen overheidsinstanties wordt gedeeld als dat voor de bescherming van zijn veiligheid noodzakelijk is.
De grote aandacht die voor dit onderwerp bestaat is naar de mening van het kabinet dan ook terecht. Vooral de ontwikkeling van de technologie, die in hoog tempo plaatsvindt, heeft invloed op de manier waarop burgers en overheid met persoonsgegevens omgaan.

Hierbij wordt met name gedacht aan het feit dat persoonsgegevens gemakkelijker kunnen worden verspreid en gedeeld, maar ook dat in toenemende mate gegevens over burgers worden vastgelegd, zowel in de

publieke als in de private sector. Breder gebruik stelt hogere eisen aan de kwaliteit en aan de beveiliging van gegevens, om fouten en misbruik te voorkomen. Deze ontwikkelingen stellen het kabinet voor een aantal belangrijke vraagstukken op het terrein van de bescherming van de persoonlijke levenssfeer.

Enkele van deze vraagstukken hebben betrekking op het veiligheidsdomein, waar blijkt dat *professionals* in de praktijk niet altijd in staat zijn tot het maken van een goede afweging tussen privacy- en veiligheidsbelangen. Om deze reden heeft het kabinet de Adviescommissie Veiligheid en persoonlijke levenssfeer (hierna te noemen: de commissie) verzocht om te onderzoeken wat de belemmeringen voor de *professionals* zijn bij het maken van dergelijke afwegingen en hoe deze belemmeringen op een afgewogen manier kunnen worden weggenomen. Tevens heeft de vaste commissie voor Justitie van de Eerste Kamer op 20 maart 2008 een expertbijeenkomst over gegevensbescherming gehouden.

De uitkomsten van de expertbijeenkomst vertonen qua strekking overeenkomsten met de conclusies van het rapport van bovengenoemde commissie. In beide gevallen bestaat de roep om een kader dat kan worden gebruikt om een deugdelijke afweging te maken tussen privacy en veiligheid en worden daartoe voorstellen gedaan.

In de door het kabinet in deze brief verwoorde benadering van gegevensbescherming zijn zowel de aanbevelingen van de commissie als de aanbevelingen uit de expertbijeenkomst gebruikt, conform de toezegging van de minister-president aan de Eerste Kamer[1]. Dit komt met name naar voren in de keuze van het kabinet om veel aandacht te besteden aan de waarborgen rondom de verwerking van persoonsgegevens in het veiligheidsdomein en de totstandkoming van regelgeving die daartoe strekt, zoals zowel in het rapport van de commissie als in de conclusies van de expertbijeenkomst is benadrukt. Het richtinggevend kader van de commissie is daarbij een nuttige handreiking, die wordt aangevuld met andere voorstellen van het kabinet.

De verwerking van persoonsgegevens vindt echter voor het grootste gedeelte plaats op tal van terreinen buiten het veiligheidsdomein. Ook hier bestaan de nodige vraagstukken over de bescherming van de persoonlijke levenssfeer van burgers. De verwerking van persoonsgegevens wordt geregeld in de Wet bescherming persoonsgegevens (Wbp). In de afgelopen jaren is de werking van deze wet geëvalueerd.

De evaluatie van de Wbp vloeit voort uit een wettelijke opdracht (art. 80 Wbp). Als zodanig heeft de evaluatie van de Wbp een zelfstandige betekenis, en valt deze te onderscheiden van de rapportage van de commissie. Immers, de evaluatie van de Wbp gaat primair over de doeltreffendheid en de effecten van één specifieke wet in algemene zin en betreft niet zozeer de veiligheid of de rechtshandhaving als algemeen verschijnsel.

Het advies van de commissie en de uitkomsten van de evaluatie van de Wbp zijn door hun strekking complementair ten opzichte van elkaar. Vandaar dat de beleidsconsequenties die aan het rapport van de commissie en de uitkomst van de evaluatie worden verbonden in één brief worden behandeld. Deze voornemens zijn voorts ter consultatie voorgelegd aan: het College bescherming persoonsgegevens, VNO-NCW, de Consumentenbond, Google Nederland en het Nederlands Genootschap van Functionarissen voor Gegevensbescherming. Het kabinet wil de voornemens in deze brief in overleg met de daarvoor relevante partijen verder vormgeven.

[1] EK 31 700, nr. 6.

In deze brief wordt ingegaan op de zienswijze van het kabinet op de manier waarop gegevensbescherming en -verwerking optimaal kan worden vormgegeven. In zijn benadering stelt het kabinet de belangen van de burger centraal. Het kabinet beseft dat de keuzes die burgers maken over de verwerking van persoonsgegevens afhankelijk zijn van de rol die zij daarin spelen. Afwegingen over hun persoonlijke levenssfeer vallen daarom anders uit wanneer zij handelen als burger, klant, patiënt, werknemer of mogelijk slachtoffer.

Het rapport «Niets te verbergen en toch bang»[1], uitgevoerd in opdracht van het Cbp, geeft een interessant inzicht in de opvattingen van burgers over privacy en meer in het bijzonder de bescherming van persoonsgegevens. De uitkomsten van het rapport hebben bijgedragen aan de totstandkoming van deze brief.

Het kabinet herkent zich met name in de verwachting van burgers dat transparant is wat er met hun gegevens gebeurt en dat zij tegen eventueel misbruik beschermd zijn. Het kabinet vindt de conclusie, dat burgers onvoldoende op de hoogte zijn van mogelijke risico's die zijn verbonden aan het delen en verwerken van persoonsgegevens, echter zorgelijk. De onderwerpen transparantie en privacybewustzijn van burgers worden verder in deze brief behandeld.

De verschillende rollen van de burger geven – net als de abstracte wet- en regelgeving – weinig houvast voor de professional om in de praktijk correcte afwegingen te maken. Deze *professional* kan daarbij, zoals ook de commissie benadrukt voor wat betreft het veiligheidsdomein, beschouwd worden als een sleutelfiguur bij het beschermen van de rechten van de burger.

De «professional» waar het kabinet zich in deze brief tot richt, dient te worden onderscheiden van de «verantwoordelijke» ex art. 1d Wbp. Het is de *professional* die in de praktijk geacht wordt deugdelijke afwegingen in concrete gevallen te maken. Het kabinet wil echter nadrukkelijk geen afbreuk doen aan de verantwoordelijkheden die in de wet aan de «verantwoordelijke» zijn toebedeeld.

Het kabinet kiest voor een nieuwe benadering voor de verwerking van persoonsgegevens, gebaseerd op een viertal kernthema's. Het kabinet wil meer aandacht voor de wijze waarop op een behoorlijke manier met persoonsgegevens wordt omgegaan en welke rol goede waarborgen daarbij kunnen spelen. Deze benadering doet meer recht aan de wens van de burger om zoveel mogelijk vrijheid te hebben om zelf te beslissen over de verwerking van zijn persoonsgegevens. Waar die vrijheid beperkt is, zoals het geval is in het veiligheidsdomein en enkele andere gevallen, moet de positie van de burger ter compensatie versterkt worden door andere waarborgen.

De verwerking van persoonsgegevens in het *veiligheidsdomein* heeft mede daarom binnen de benadering van het kabinet een bijzondere positie. De rol van de burger is in dit domein wezenlijk anders dan het geval is binnen de andere terreinen. Dit komt naar voren in de beperkte keuzevrijheid van de burger om zelf te kiezen of zijn persoonsgegevens worden verwerkt, maar ook in de af te wegen belangen: de overheid heeft tot taak de bescherming van de veiligheid van zijn burgers.

Voor een goede uitoefening van deze taak is het soms nodig om een inbreuk te maken op de persoonlijke levenssfeer. Het is van belang dat deze afwegingen proportioneel en correct plaatsvinden. Het kabinet is daarbij van mening dat bij het beoordelen van de proportionaliteit van

[1] «Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving». Regioplan, januari 2009.

maatregelen en verwerkingen ook in dit domein meer aandacht dient te bestaan voor de waarborgen rondom de verwerking van persoonsgegevens. Bij internationale gegevensuitwisseling met andere lidstaten in de Europese Unie en met landen buiten de EU, is daarop ook sterk de aandacht gericht.

De burger heeft echter altijd en binnen alle domeinen het recht op een correcte omgang met zijn gegevens als zijn persoonsgegevens worden verwerkt. Dit uitgangspunt van een correcte omgang met persoonsgegevens valt samen met het belang van de *professional*. Het kabinet wil dan ook meer aandacht voor de vraag *hoe* persoonsgegevens worden verwerkt en wie bijvoorbeeld onder welke omstandigheden toegang heeft tot deze gegevens. Technologie maakt niet alleen meer inbreuken mogelijk op de persoonlijke levenssfeer maar kan ook worden ingezet ter bescherming ervan. De bescherming van de verschillende belangen van de burger wordt volgens het kabinet tekort gedaan wanneer de aandacht bij de verwerking en bescherming van persoonsgegevens zich uitsluitend richt op de vraag *of* zijn gegevens wel verwerkt mogen worden.

Meer aandacht voor materiële normen van de Wet bescherming persoonsgegevens en de waarborgen waaronder gegevens worden verwerkt, houdt in dat nog steeds kritisch nagedacht moet worden over de risico's die verbonden zijn aan het aanleggen van een gegevensverzameling. Het benoemen van risico's bij de gegevensopslag en -verwerking moet echter in het teken staan van het zoeken naar oplossingen.

De brief is als volgt ingedeeld. In paragraaf twee zal eerst aandacht worden besteed aan de vier kernthema's binnen de nieuwe benadering die het kabinet kiest bij de bescherming van persoonsgegevens. Het kabinet is zich er daarbij van bewust dat de vier thema's vanwege de veelvormigheid van de voorkomende situaties per domein een afzonderlijke vertaling behoeven. In paragraaf drie zal aandacht worden besteed aan de verwerking van persoonsgegevens binnen het veiligheidsdomein en de voornemens van het kabinet op dit terrein. Daarbij gaat het kabinet in op de aanbevelingen die de commissie heeft gedaan in haar rapport «Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer»[1].

Het kabinet wil de kernthema's ook binnen andere domeinen uitwerken. Gezien het grote aantal verschillende belanghebbenden en het aantal sterk uiteenlopende situaties, kiest het kabinet voor een invulling van de thema's per domein. Tevens is het kabinet bij een verdere uitwerking van de nieuwe benadering gebonden aan de ruimte die de EU-privacyrichtlijn hiervoor biedt.

De door het kabinet gekozen benadering zal daarom inzet worden bij de herziening van de richtlijn, waarvoor de Europese Commissie voorzieningen zal nemen. De voornemens die het kabinet heeft voor de korte termijn, zijn daarom gebonden aan de huidige wetgeving en richten zich met name op het realiseren van verbeteringen van het huidige juridisch kader. Daarbij heeft het kabinet zich laten leiden door de uitkomsten van de evaluatie van de Wet bescherming persoonsgegevens[2]. Dit zal worden uiteengezet in paragraaf vier.

In de bijlage treft u een overzicht aan van de in deze brief voorgestelde kabinetsvoornemens, de beoogde resultaten en de termijnen die daaraan zijn verbonden.

[1] Het rapport van de commissie is bij onze brief van 10 februari 2009 aan de Tweede Kamer aangeboden (Kamerstukken II, 2008/09, 28 684, nr. 199).

[2] Over de in twee fasen uitgevoerde evaluatie van de werking van de Wet bescherming persoonsgegevens is de Tweede Kamer, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, geïnformeerd bij brieven van de Minister van Justitie van 15 mei 2007, respectievelijk van 16 februari 2009 (Kamerstukken II 2006/07, 31 051, nr. 1 en Kamerstukken II 2008/09, 31 051, nr. 4).

2. Een nieuwe benadering van persoonsgegevens

Er bestaan grote verschillen in de manier waarop met persoonsgegevens wordt omgegaan in de diverse domeinen. Toch zijn er wel degelijk de nodige overeenkomsten. Zo constateert het kabinet dat de open normen in de privacywet- en regelgeving zorgen voor moeilijkheden in de praktijk omdat zij weinig duidelijkheid verschaffen over de manier waarop in concrete gevallen door de *professional* gehandeld zou moeten worden. Dit beeld komt ook naar voren in het advies van de commissie en de evaluatie van de Wbp. De uitgangspunten die de basis vormen van het huidige stelstel van gegevensbescherming leunen daarbij sterk op zaken als preventie en controle vooraf. Voorafgaande controles op gegevensverwerking lijken de noodzakelijke gegevensverwerking eerder te hinderen dan te bevorderen. Dit is noch in het belang van de burger, noch in het belang van de professional.

Het kabinet kiest voor een andere benadering van gegevensbescherming en baseert deze op een viertal kernthema's. Bij de keuze voor deze thema's ziet het kabinet zich gesteund door de uitkomsten van de genoemde rapporten.

De vier kernthema's van het kabinet zijn:

1. «Gewoon doen»: meer aandacht voor waarborgen bij de omgang met persoonsgegevens
2. Robuuster extern toezicht
3. Minder nadruk op procedures en controle vooraf
4. Het burgerperspectief

2.1. Kernthema 1: «Gewoon doen»: meer waarborgen bij de omgang met persoonsgegevens

Het is op tal van terreinen in de maatschappij belangrijk dat persoonsgegevens kunnen worden verwerkt. Het is uiteraard van belang dat dit op een correcte manier gebeurt. Uit beide rapporten komt naar voren dat *professionals* grote moeite hebben om aan de hand van het bestaande juridisch kader afwegingen en keuzes te maken, maar zich naar hun beleving wel geconfronteerd zien met omslachtige procedures en meldingen vooraf.

Daarom wil het kabinet dat juist de materiële normen die zijn verbonden aan de bescherming van persoonsgegevens verder worden ontwikkeld. De achterliggende gedachte is dat juist hier de sleutel ligt tot een wijze van gegevensbescherming die recht doet aan de keuzevrijheid die de burger heeft bij het verwerken van zijn gegevens, maar waarbij ook de *professional* beter in staat wordt gesteld om «gewoon» zijn werk te doen.

Meer aandacht voor materiële normen betekent dat voorafgaand aan de verwerking allereerst dat het uitgangspunt van doelbinding bij de verwerking van persoonsgegevens blijft bestaan. Een verantwoordelijke behoort voorafgaand aan de verwerking doel en middelen voor de verwerking vast te stellen. Doel en middelen behoren gerechtvaardigd te zijn. Wanneer de wetgever het doel van gegevensverwerking vaststelt, behoort deze keuze te zijn gebaseerd op een draagkrachtige motivering, waarbij uitdrukkelijk aandacht wordt gegeven aan noodzaak, proportionaliteit en subsidiariteit.

Deze vraag is in ieder domein belangrijk, of het nu gaat om de relatie burger-overheid, of om de verhouding klant-dienstverlener. Het kabinet vindt het belangrijk dat bij deze afweging ook voldoende aandacht wordt besteed aan de mogelijke waarborgen rondom de verwerking.

Dit betekent in de praktijk dat naast vragen over of en zo ja, welke gegevens worden opgeslagen, vragen over onder andere toegang tot en beveiliging van gegevens moeten worden beantwoord. Juist voor wat betreft de omgang met persoonsgegevens bestaan steeds meer mogelijkheden – onder meer in de techniek – om privacybeschermende waarborgen te organiseren. Deze waarborgen kunnen een belangrijke rol spelen bij het terugbrengen van de risico's die mogelijk zijn verbonden aan de verwerking van persoonsgegevens en de invloed daarvan op de persoonlijke levenssfeer.

Een manier om risico's tegen te gaan is het toepassen van *privacy-by-design:* bescherming door ontwerp. Hieronder verstaan wij dat privacyaspecten zo vroeg mogelijk, in de ontwerpfase, in systemen én organisatorische praktijken worden ingebouwd, zodat al in die fase rekening wordt gehouden met risico's die verbonden zijn aan het werken met persoonsgegevens. De architectuur van het systeem moet bijdragen aan het wegnemen van geïdentificeerde risico's en aan de zorgvuldigheid van de feitelijke omgang van persoonsgegevens. Op deze wijze kan het effect dat een gegevensverwerking heeft op de persoonlijke levenssfeer van een betrokkene zoveel mogelijk worden ingedamd.

2.2. Kernthema 2: Robuuster extern toezicht

Het kabinet benadrukt de verantwoordelijkheid van de *professionals* om op een behoorlijke wijze met persoonsgegevens om te gaan. Vooral deze *professional* staat dan ook aan de spreekwoordelijke «lat» om in de dagelijkse praktijk de juiste afwegingen te maken. Het kabinet vertrouwt op de *professional*, aangezien het vaak ook in zijn eigen belang is om op een correcte manier met de gegevens van personen om te gaan, of het nu burgers, klanten of patiënten zijn. Daarbij dient het de *professional* wel makkelijker gemaakt te worden om in de dagelijkse praktijk de juiste afwegingen te maken.

Daarnaast onderstreept het kabinet het belang van robuust, extern toezicht. Op dit belang wordt ook in beide rapporten gewezen. Als één van de criteria uit het kader van de expertbijeenkomst in de Eerste Kamer wordt het belang van goede, onafhankelijke controlemogelijkheden ook genoemd. Voor de burger is het van belang dat hij niet in de kou staat wanneer op een onjuiste manier met zijn gegevens wordt omgegaan. Onafhankelijk toezicht en onafhankelijke handhaving zijn daarbij kernwaarden. Daarbij kan van een sterke toezichthouder een prikkel uitgaan om op een zorgvuldige manier om te gaan met persoonsgegevens.

Een andere, belangrijke overweging is dat een sterkere toezichthouder door middel van zijn bevindingen kan bijdragen aan een betere rechtsontwikkeling. Zoals uit de evaluatie van de Wbp naar voren komt, is een trage rechtsontwikkeling één van de oorzaken van het feit dat de open normen uit het huidige wettelijk kader nog onvoldoende zijn ingevuld.

2.3. Kernthema 3: Minder nadruk op procedures en controle vooraf

Uit de evaluatie van de Wbp blijkt dat procedurele verplichtingen zoals de meldplicht of het voorafgaand onderzoek weinig bijdragen aan de daadwerkelijke bescherming van persoonsgegevens. Het kabinet wil daarnaast de administratieve lasten zoveel mogelijk terugdringen.

Beide uitgangspunten houden echter niet in, dat iedere toets of afweging voorafgaand aan een verwerking moet worden afgeschaft. Bestuursrechtelijke verplichtingen zullen, waar dat mogelijk is, moeten worden

vervangen door andere methoden waarmee kan worden voorzien in voorafgaande noodzakelijkheidstoetsen.

In de praktijk betekent dit dat kritische afwegingen, risicoanalyses en inrichtingsvraagstukken juist belangrijker worden. Zo zullen op het terrein van veiligheid en ook op het domein van private verhoudingen afwegingen over proportionaliteit en subsidiariteit van groot belang blijven. Volgens het kabinet blijven deze voorvragen juist noodzakelijke voorwaarden om effectieve waarborgen te kunnen organiseren.

Bij de wens om de administratieve lasten terug te brengen, is het kabinet gebonden aan de ruimte die de EU-privacyrichtlijn (nr. 95/46/EG) daarvoor biedt. Deze ruimte is echter niet groot. Met het oog op de lange termijn wil het kabinet met dit kernthema alvast een voorschot nemen op de Nederlandse inbreng in de discussie over de actualisatie van de privacyrichtlijn. In paragraaf vier wordt daartoe een aantal maatregelen voorgesteld. Een verdere uitwerking van de genoemde beleidsvoornemens zal plaatsvinden in samenspraak met het College bescherming persoonsgegevens en het bedrijfsleven.

2.4. Kernthema 4: Het burgerperspectief

Is bescherming van persoonsgegevens een zaak van alleen de overheid of van andere instanties die gegevens verzamelen, zoals bedrijven en instellingen? Naar het oordeel van het kabinet kan een effectief beleid niet worden vormgegeven zonder aandacht te schenken aan de positie en het handelen van degenen over wie, en soms ook ten behoeve van wie, gegevens worden verzameld: de burger zelf. Het gaat daarbij om twee zaken: het effectueren van de rechten die krachtens de wet aan hem zijn toegekend en het bewust omgaan met vrijwillige gegevensverstrekking.

Allereerst de bescherming van de positie van de burger. Deze is primair geregeld in de bestaande wettelijke voorzieningen, waaronder de Wbp, de Wpg en de Wjsg. Het kabinet blijft hechten aan belangrijke algemene beginselen die in deze wetten zijn vastgelegd. Het is echter wel zo dat de manier waarop de principes worden toegepast binnen het veiligheidsdomein anders is dan daarbuiten. Een voorbeeld hiervan is transparantie.

De burger kan zijn rechten pas laten gelden als hij daadwerkelijk weet dat zijn gegevens worden verwerkt. Het kabinet wil de bestaande verplichtingen tot informatie versterken, zie paragraaf 4.3. Verder staan de burger privaatrechtelijke en bestuursrechtelijke (sanctie-)mogelijkheden ter beschikking bij een onrechtmatige verzameling, verwerking of gebruik van gegevens.

In aanvulling hierop acht het kabinet het wenselijk het inzagerecht te ondersteunen door het ontwerpen van klachtregelingen die per sector op maat zijn gesneden. Dit is nader uitgewerkt in paragraaf 4.3.1. Wanneer het gaat om het veiligheidsdomein ligt transparantie naar de burger toe niet altijd in de rede. Opsporingsbelangen zouden immers door een te grote mate van transparantie kunnen worden geschaad. Het gebrek aan transparantie wordt echter wel gecompenseerd door andere middelen, waaronder sterker toezicht en door middel van toetsing door de rechter achteraf.

Ten tweede het verhogen van de privacybewustwording. Veel gegevens worden verzameld omdat de burger die vrijwillig ter beschikking stelt, bijvoorbeeld bij aankopen op het Internet. Uit het rapport van Regioplan blijkt dat burgers zich niet altijd bewust zijn van privacyrisico's, maar ook dat zij hun handelen slechts mondjesmaat aanpassen wanneer zij daar

wel bewust van zijn. Het is echter van groot belang dat burgers zich van de mogelijke effecten van hun gedrag bewust worden en daar ook naar handelen. Om dit te bevorderen is de overheid een campagne «Veilig internetten. Heb je zelf in de hand» gestart om dit te bevorderen.

Hieronder wordt het eerste kernthema: ««Gewoon doen»: meer aandacht voor waarborgen bij de omgang met persoonsgegevens» nader uitgewerkt voor het veiligheidsdomein. Robuuster extern toezicht, waar ook de commissie voor pleit, wordt in paragraaf vier behandeld. Daarin komen ook de voorstellen aan de orde die invulling geven aan de andere kernthema's buiten het veiligheidsdomein.

3. Veiligheid en persoonsgegevens

Het kabinet hecht aan een vrije en veilige samenleving. Er zijn verschillende redenen voor een aparte behandeling van de verwerking van persoonsgegevens in het veiligheidsdomein. Allereerst moet worden vastgesteld dat het verzamelen en gebruiken van persoonsgegevens in het veiligheidsdomein deels leidt tot andere uitkomsten dan in de andere domeinen. Om die reden heeft het kabinet advies gevraagd aan de Adviescommissie Veiligheid en persoonlijke levenssfeer. In de volgende paragrafen zal uiteen worden gezet hoe het advies van de commissie het kabinet behulpzaam is bij het vormgeven van toekomstig beleid op het terrein van gegevensverwerking in het veiligheidsdomein.

3.1. Het richtinggevend kader van de Adviescommissie Veiligheid en persoonlijke levenssfeer

Het kabinet heeft de commissie gevraagd een advies uit te brengen over het zorgvuldig omgaan met persoonsgegevens op een manier dat de veiligheid van mensen daarmee is gediend. Een belangrijke aanleiding om de commissie deze opdracht te geven is gelegen in het Beleidsprogramma «Samen werken, samen leven», waarin onder pijler V (Veiligheid, stabiliteit en respect) is opgenomen dat bij de aanpak van agressie, geweld en criminaliteit «het kabinet privacybelemmeringen voor betrokken beroepsgroepen aanpakt». De hoofdconclusie van de commissie is dat de huidige wet- en regelgeving deze verwerking en met name de uitwisseling van informatie niet in de weg hoeft te staan, maar dat de *professional* handvatten nodig heeft om de bestaande wettelijke kaders te kunnen toepassen in de praktijk.

Als handreiking naar de praktijk heeft de commissie een richtinggevend kader ontwikkeld. Een belangrijk uitgangspunt van de commissie bij het opstellen van dit kader is de gedachte om het terrein waar de bescherming van de persoonlijke levenssfeer en veiligheid elkaar raken te zien als een normaal beleidsterrein. De commissie presenteert een risicoanalyse als eerste stap en kern van het richtinggevend kader. De afweging of een inbreuk op de persoonlijke levenssfeer nodig is, start met de vraag welke kansen het vergaren en verwerken van persoonsgegevens kan bieden bij het wegnemen of beheersen van een veiligheidsrisico.

Daarna moet worden beoordeeld welke gegevens daarvoor nodig zijn en welk risico is verbonden aan het afzien van deze verwerking. Voor het maken van verdere afwegingen over de vragen of en op welke wijze persoonsgegevens vervolgens verwerkt mogen worden, biedt het door de commissie opgestelde kader een leidraad.

Op basis van zes grondslagen kunnen de relevante privacywaarborgen beter worden geïdentificeerd en kunnen de daaraan verbonden risico's worden beheerst. Het gaat hier bijvoorbeeld concreet om zaken als: de

beveiliging van gegevens en de toegang daartoe, maar zeker ook om de kwaliteit en integriteit van de gegevens. De grondslagen van de commissie zijn:

1. «Transparantie, tenzij».
2. «Selecteer voordat je verzamelt en houd het sober»
3. «Indien noodzakelijk voor de veiligheid, moet je delen»
4. «Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers»
5. «Zorg voor voorlichting en facilitering»
6. «Zorg voor naleving en intern toezicht»

Zowel in het rapport van de commissie als in expertbijeenkomst in de Eerste Kamer zijn daarbij genoeg aandachtspunten voor het voetlicht gebracht waarbij is aangegeven hoe verstrekkend de gevolgen voor burgers kunnen zijn, wanneer het onverhoopt misgaat.

Daarbij merkt het kabinet op dat het kader van de commissie zonder verdere uitwerking zowel krachtig als kwetsbaar is. De grondslagen zijn weliswaar breed toepasbaar, maar bieden zonder nadere sectorale uitwerking nog geen garantie voor zorgvuldige afwegingen door *professionals.* Zo komen vraagstukken rond veiligheid en persoonlijke levenssfeer voor op tal van beleidsterreinen, van de jeugdzorg en individuele hulpverlening tot voortijdig schoolverlaten, overlast, kleine criminaliteit, de strijd tegen radicalisering en tot aan de aanpak van (internationale) georganiseerde criminaliteit en terrorisme.

De commissie heeft beoogd aan te tonen dat het soort afwegingen dat hulpverleners en rechtshandhavers moeten maken in wezen steeds dezelfde is, ongeacht het beleidsterrein. De af te wegen belangen, maar ook het gewicht dat daaraan verbonden wordt, verschillen in de praktijk echter per werkterrein en vaak ook van geval tot geval. Het kader van de commissie dient voor hen als vertrekpunt, maar de verantwoordelijkheid voor de afweging in een concreet geval ligt bij de *professionals* zelf. Met de commissie zijn wij van mening dat de *professionals* hierbij geholpen dienen te worden in het maken van de juiste afwegingen over proportionaliteit.

3.2. Evenwicht tussen bescherming van persoonsgegevens en veiligheid: een tweevoudige bescherming

In een maatschappij waarin de activiteiten van burgers zich steeds meer begeven op het digitale terrein, is het van belang dat de overheid ook daar zorg draagt voor de veiligheid. Daarnaast zijn digitale activiteiten en de fysieke wereld onlosmakelijk met elkaar verbonden, ook wanneer het gaat om criminele activiteiten. Informatie, ook gedigitaliseerde, speelt een steeds belangrijkere rol op alle terreinen in onze samenleving en wordt daarmee steeds waardevoller. Zo ook voor het streven naar veiligheid. Het gebruik van nieuwe technologie is dan ook geen doel op zich, maar heeft een ondersteunend karakter ten behoeve van de processen van opsporings-, inlichtingen- en veiligheidsdiensten.

Wanneer sprake is van een aanzienlijke verschuiving van activiteiten van burgers naar het digitale vlak, is het noodzakelijk dat de overheid deze beweging volgt. De ontwikkelingen van de laatste jaren hebben gezorgd voor een toename in zowel mobiliteit als anonimiteit van de burger. Het kabinet is van mening dat deze ontwikkelingen positief zijn, tenzij zij worden gebruikt om het plegen van criminele activiteiten te vergemakkelijken.

De meest in het oog springende voorbeelden zijn bijvoorbeeld het gebruik maken van de anonimiteit die wordt geboden door het internet en het bestaan van «mobiel banditisme» waarbij door criminelen activiteiten worden ondernomen in andere regio's of landen. Tevens maakt een onzorgvuldige omgang met gegevens de burger ook kwetsbaar. Een voorbeeld hiervan is identiteitsdiefstal, een ander belangrijk aandachtspunt voor dit kabinet.

Uiteraard biedt het bestaan van informatie in bepaalde gevallen ook nieuwe mogelijkheden voor gerichte opsporing, detectie en preventie van criminaliteit. Door middel van informatiegestuurde opsporing en preventie kunnen delicten worden opgelost die anders onopgelost (en daarmee onbestraft) zouden blijven of kunnen zij wellicht zelfs worden voorkomen. Voorbeelden van nieuwe technieken op het terrein van informatiegestuurde opsporing zijn: automatische kentekenherkenning (ANPR) en mogelijkheden die bestaan op het terrein van intelligente verwerking van gegevens, zoals *profiling*.

In een rechtsstaat is het noodzakelijk dat de personen die een inbreuk maken op de rechten van anderen, daarvoor ter verantwoording kunnen worden geroepen. Soms is het daarvoor bijvoorbeeld nodig dat de bestaande anonimiteit van een burger kan worden opgeheven en dat nader onderzoek kan worden verricht naar zijn activiteiten. Op deze manier kunnen inbreuken op de rechten van burgers soms ook worden voorkomen. Van belang is hier het besef dat sprake moet zijn van een tweevoudige bescherming: zowel van de veiligheid van de burger *door* de overheid als van de persoonlijke levenssfeer van de burger tegen onzorgvuldig handelen *van* dezelfde overheid.

In dit kader kan ook de registratie van bijzondere persoonsgegevens, zoals etniciteit en levensovertuiging, worden bezien. Hieraan heeft de commissie op verzoek van het kabinet specifieke aandacht besteed.

Voor wat betreft de registratie van herkomstgegevens verwijzen wij naar de brief van de Minister voor Wonen, Wijken en Integratie aan de Tweede Kamer van 19 december 2008 (TK 2008–2009, 26 283, nr. 49). In die brief wordt het belang van die registratie op zichzelf onderschreven. Het gaat daarbij niet alleen om registratie van herkomstgegevens ten behoeve van individuele hulpverlening, maar ook om het genereren van beleidsinformatie als stap naar een beleid gericht op het oplossen van problemen die zich voordoen binnen specifieke groepen. Zoals in eerder genoemde brief van de Minister voor WWI is aangegeven, zal het kabinet nog met een nadere brief over dit onderwerp komen. Daarin zal een reactie op dit onderdeel van het advies van de commissie worden meegenomen.
De Minister van Binnenlandse Zaken en Koninkrijksrelaties is in overleg met de grote steden over interventiestrategieën in de strijd tegen radicalisering. Een aantal burgemeesters heeft daarbij voorgesteld onderzoek te doen naar nut en noodzaak van registratie van levensovertuiging.

Het kabinet onderschrijft de grondslagen van het richtinggevend kader die de commissie heeft ontworpen. In de volgende paragrafen wordt aangegeven op welke wijze het kabinet deze wil toepassen. Het zesde criterium «zorg voor naleving en intern toezicht» wordt in paragraaf vier behandeld.

3.3. Selecteer voor je verzamelt

Het uitgangspunt is dat niet meer gegevens verzameld of gegenereerd dienen te worden dan noodzakelijk zijn voor het bereiken van het te verwezenlijken doel. Als belangrijk aspect van deze grondslag noemt de commissie dat alleen persoonsgegevens worden verzameld met een

rechtmatig doel, daarbij rekenschap gevend aan de belangen van proportionaliteit en subsidiariteit. Met andere woorden: kies het lichtste middel om het doel te bereiken en zorg ervoor dat dit middel in een passende relatie tot het doel staat. Het duidelijk formuleren van de doelstelling waarvoor gegevens worden verwerkt is hiervoor zoals aangegeven een noodzakelijk vertrekpunt.

Het kabinet is het met de commissie eens dat «selecteer voor je verzamelt» soms kan betekenen dat met het oog op een bepaald doel juist álle beschikbare gegevens moeten worden verzameld. Ook kunnen bijzondere omstandigheden waarbij ernstige misdrijven en vitale belangen van de staat in het geding zijn soms rechtvaardigen dat gegevens worden verzameld, voordat selectie plaatsvindt. Er dient naar gestreefd te worden om het selectiemoment plaats te laten vinden zo kort mogelijk nadat de gegevens zijn verzameld. Het in het kader van – zoals de commissie formuleert – *«nice to know»* verzamelen en verwerken van gegevens moet worden voorkomen, de overheid beperkt zich tot het verzamelen en verwerken van gegevens die noodzakelijk zijn voor de te bereiken doelen.

Terecht stelt de commissie ook dat wanneer gegevens niet meer worden gebruikt, het met het oog op de integriteit van gegevens de aanbeveling verdient deze te vernietigen. Hoe minder gegevens worden bewaard, hoe minder de kans aanwezig is dat gegevens op een onjuiste wijze gaan worden gebruikt.

3.4. Transparantie

De commissie benadrukt de noodzaak tot transparantie over de verwerking van persoonsgegevens. Uit het rapport van Regioplan komt daarbij naar voren dat transparantie en controle van invloed zijn op het privacybewustzijn en de privacyattitude van burgers. Het kabinet onderschrijft het belang van transparantie. Voor wat betreft de wijze waarop die transparantie wordt vormgegeven, wijkt het veiligheidsdomein echter af van de andere domeinen.

Zo is het niet altijd in het belang van de veiligheid om volledige transparantie te bieden. Hierbij kan bijvoorbeeld worden gedacht aan voorgenomen controles, de gegevensverwerking bij opsporingsonderzoeken of een te grote transparantie over de werkwijzen van opsporings- en inlichtingen- en veiligheidsdiensten. Transparantie wordt dan ook op het terrein van veiligheid op een andere manier ingevuld dan daarbuiten.

Wanneer het gaat om het veiligheidsdomein, kan transparantie van gegevensverwerking immers niet altijd worden geboden. Waar dit niet mogelijk is, behoort dit gemis in het belang van de burger te worden gecompenseerd met andere middelen zoals toezicht door één, of soms meer instanties en door middel van toetsing door de rechter achteraf. Veelal is hierin door middel van wetgeving ook voorzien, zoals het geval is in de Wet politiegegevens en het Wetboek van Strafvordering.

Een ander voorbeeld van effectief toezicht op een terrein waarbinnen al te veel externe transparantie schadelijk zou zijn, is de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD). Deze commissie toetst zowel het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) als de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) aan de juridische kaders die er voor deze diensten bestaan. Voor het handelen van de overheid betekent dit dan niet altijd vooraf aan burgers openheid gegeven kan worden, maar dat de rechtmatigheid en zorgvuldigheid van overheidshandelen altijd moeten kunnen worden getoetst.

3.5. Integriteit van systemen: privacybescherming door ontwerp

Het kabinet ziet hier dat nieuwe technologische ontwikkelingen kansen bieden voor de bescherming van de persoonlijke levenssfeer, doordat het steeds beter mogelijk wordt om waarborgen voor een correct gebruik van persoonsgegevens vorm te geven bij de inrichting van systemen. Voorbeelden hiervan zijn: de toepassing van authenticatiemogelijkheden voor het regelen van toegang, de beveiliging en – indien gewenst – aggregatie van gegevens door middel van versleuteling en het automatisch opschonen van gegevens.

Om optimaal vorm te geven aan noodzakelijke waarborgen onderstrepen wij in navolging van de commissie het belang van *privacy-by-design:* bescherming door ontwerp. Het kabinet is zich ervan bewust dat de keuze voor *privacy-by-design* een keuze is voor een meer gedegen benadering van beleid en systeemontwerp, maar nog geen kant en klare oplossingen voor problemen biedt. Om met succes gebruik te maken van een privacybewuste manier van beleids- en systeemontwerp, is inzet en ervaring nodig. Het kabinet maakt op dit moment al op verschillende manieren werk van de ontwikkeling van *privacy-by-design*. Hieronder wordt ingegaan op de ontwikkeling van *Privacy Impact Assessments (PIA)* en op de casus kentekenherkenning met camera's (ANPR).

3.5.1. Privacy Impact Assessments

Het uitvoeren van *Privacy Impact Assessments* is een concrete mogelijkheid om privacyrisico's effectief te kunnen identificeren bij het ontwikkelen nieuw beleid, wetgeving, of bij de introductie van nieuwe ICT-systemen die een grote potentiële impact op de gegevenshuishouding hebben. Hierop is bijvoorbeeld ook gewezen tijdens de expertbijeenkomst in de Eerste Kamer. Met een PIA, een protocol, kan op een meer gestructureerde wijze een zorgvuldig beeld geschetst worden van de privacyaandachtspunten verbonden aan de implementatie van nieuwe systemen. Bij het inrichten van systemen kunnen deze risico's zoveel mogelijk worden weggenomen. Ook afwegingen over toegang en mogelijkheden tot het delen van informatie, waaronder die in EU- en internationaal verband, kunnen worden meegenomen.

Daarnaast kan een informatiesysteem met behulp van «*privacy enhancing technologies*» persoonsgegevens waarover anderen niet behoeven te beschikken, afschermen. Het uitvoeren van een PIA zou bijvoorbeeld kunnen inhouden dat, wanneer het afbreukrisico verbonden aan een verwerking van persoonsgegevens te groot wordt geacht, wordt afgezien van het verwerken van persoonsgegevens, of dat gekozen wordt voor een beperktere variant. Het kabinet vindt de ontwikkeling van PIA's belangrijk, ook voor gebruik buiten het veiligheidsdomein. De ministeries van EZ, Justitie en BZK , het MKB, de VNG, het Cbp, het HEC en in voorkomende gevallen VNO/NCW zijn in overleg over een Nederlandse versie van het in het Verenigd Koninkrijk ontwikkelde model van een PIA. Het streven is erop gericht dit binnen een jaar te realiseren.

3.5.2. Kentekenherkenning met camera's (ANPR)

Het kabinet heeft de Adviescommissie Veiligheid en persoonlijke levenssfeer gevraagd in haar advies bijzondere aandacht te geven aan automatische kentekenherkenning. *Automatic Number Plate Recognition* (ANPR) is een instrument waarbij camera's worden gebruikt om kentekens vast te leggen. Het vastleggen van deze kentekens gebeurt met het doel deze te vergelijken met een verzameling kentekens die onderzoek behoeven. Vanwege de verschillende toepassingsmogelijkheden van dit middel is de

commissie gevraagd een toekomstbestendig kader voor de inzet van ANPR te ontwikkelen.

De commissie heeft aan dit verzoek gevolg gegeven door het door haar ontworpen richtinggevend kader toe te passen op de huidige praktijk en daar een aantal conclusies aan te verbinden. Een van de kanttekeningen die de commissie daarbij maakt is het gegeven dat ANPR door de politie regionaal, incidenteel en zonder daadwerkelijke samenhang wordt ingezet, waardoor in onvoldoende mate kennis en ervaring worden uitgewisseld en de impact van de ANPR-systemen op de persoonlijke levenssfeer onderbelicht blijft.

Vooral binnen de politie en de Koninklijke Marechaussee wordt geëxperimenteerd met ANPR. Toepassingen liggen op de terreinen van controle, opsporing en (administratief) toezicht. Eerder is de Kamer hierover geïnformeerd bij de beantwoording van Kamervragen van de leden Azough (2080909990, ingezonden 16 januari 2009) en van Haersma Buma (2080910140, ingezonden 19 januari 2009).

Uit de *pilots* die plaatsvinden bij de politie komt naar voren dat ANPR een aanzienlijke toegevoegde waarde heeft bij het uitvoeren van de politietaak. Ook bij toezichtactiviteiten van inspecties (VROM, IVW) en de Belastingdienst blijkt ANPR een waardevol hulpmiddel te zijn. Als de politie samen met deze toezichthouders acties houdt waarbij meerdere hitlijsten aan de camera-apparatuur worden gekoppeld, kan de hitratio oplopen tot 1 op 25. Dat betekent dat er bij 4% van de passerende voertuigen aanleiding bestaat tot een controle.

Verder lukt het de politie steeds meer om met behulp van ANPR ernstig strafbare feiten op te lossen, zoals doodslag, beroving en fraude. Daarbij worden de meeste resultaten geboekt als de politie enige tijd terug kan kijken in de historie van het gegevensbestand. Dat is verklaarbaar uit het feit dat de meeste criminaliteit zich pas achteraf openbaart. Zo worden bijvoorbeeld gegevens in de regel pas relevant wanneer er sprake is van een aangifte, of wanneer uit een opsporingsonderzoek blijkt dat deze gegevens nodig zijn. Dan is het belangrijk dat er een recente verzameling van kentekengegevens is waarin kan worden gezocht.

Met een totaal van 10 miljoen kentekens in Nederland is duidelijk dat ANPR kan uitgroeien tot een belangrijk handhavingsinstrument voor de overheid en bij kan dragen aan een veiliger samenleving in het bijzonder. Daarbij worden de financiële opbrengsten van deze handhavingsactiviteiten hoog ingeschat. De belastingdienst schat de opbrengsten van controle van zakelijke rijders bijvoorbeeld op enkele tientallen miljoenen euro's per jaar.

Het is dan ook de ambitie van het kabinet om de verdere ontwikkeling van ANPR mogelijk te maken. Het kabinet is van mening dat de huidige wetgeving onvoldoende ruimte biedt voor een verdere ontwikkeling van ANPR. Wij zullen ons daarom inzetten voor de totstandkoming van een specifiek wettelijk kader dat de inzet van de verschillende toepassingsmogelijkheden van het middel ANPR op een eenduidige wijze reguleert, mede met het oog op de bestaande ambities voor inzet van het instrument in de toekomst.

De overwegingen en het kader van de commissie worden hierbij gebruikt. De afwegingen uit het richtinggevend kader zijn van invloed op een aantal belangrijke keuzes bij het vormgeven van een nieuwe wettelijke voorziening. Het beoogde resultaat is een juridisch kader dat transparant is en

met voldoende waarborgen omkleed, waarmee tevens geen afbreuk wordt gedaan aan de effectiviteit van het instrument in de praktijk.

Het kabinet neemt de opvatting van de commissie dat ANPR op dit moment zonder veel onderlinge samenhang wordt toegepast serieus en onderschrijft de onwenselijkheid van deze situatie. Om deze reden is het ANPR-platform in het leven geroepen. Hierin zijn op dit moment, naast de Ministeries van BZK en Justitie, ook de politie, de Koninklijke Marechaussee, de Belastingdienst, het Openbaar Ministerie, de Inspecties VROM en Verkeer en Waterstaat, het Centraal Justitieel Incasso Bureau en de RDW vertegenwoordigd.

Een belangrijk doel van het Platform is om te komen tot een meer uniforme toepassing van ANPR. Daarvoor zal, zoals hierboven aangegeven, nieuwe, specifieke wetgeving worden ontworpen. Voor de tussenliggende periode wordt op dit moment in samenspraak met het Platform een beleidskader ANPR ontwikkeld. Het beleidskader is een voorschot op de uitgangspunten die het kabinet zal hanteren bij de inzet van ANPR en zal daarom grotendeels in lijn zijn met de toekomstige wetgeving. Het spreekt voor zich dat aandachtspunten zoals voldoende transparantie, waarborgen en toezicht een grote rol zullen spelen bij de toepassing van ANPR. Het richtinggevend kader van de commissie zal daarmee een belangrijke pijler vormen voor het beleidskader, dat thans in ontwikkeling is.

3.6. Gegevensuitwisseling en veiligheid: een kwestie van belang

Het rapport van de commissie laat zien dat in de praktijk over de verhouding tussen privacy en veiligheid verschillende misverstanden bestaan. *Professionals* denken nogal eens dat de privacywetgeving hen belemmert om criminaliteit effectief aan te pakken en onderling gegevens uit te wisselen. Het rapport van de commissie laat zien dat dit een wijdverbreid misverstand is. De ruimte om gegevens uit te wisselen wanneer dit in het belang van de veiligheid van personen is, is immers groter dan verondersteld. Als goed voorbeeld noemt de commissie de afspraken die worden gemaakt over uitwisseling van informatie bij vermoedens van kindermishandeling.

Het kabinet benadrukt dat privacyregelgeving niet bedoeld is om gegevensbescherming in alle gevallen te laten prevaleren boven andere belangen, zeker niet wanneer in concrete gevallen de veiligheid van burgers in het geding is. Zoals de commissie terecht stelt is de systematiek omtrent de bescherming van de persoonlijke levenssfeer, zoals ook volgt uit art. 8 EVRM, op een dusdanige wijze vormgegeven dat uitzonderingen mogelijk zijn, bijvoorbeeld wanneer de veiligheid daarom vraagt. In de regel zal hier sprake zijn van een concrete afweging per geval.

Inbreuken dienen voorts wel op een proportionele en correcte wijze plaats te vinden. Zo moet kritisch worden gekeken welke gegevens aan wie worden verstrekt en of dit daadwerkelijk in het belang is van de burger, wiens veiligheid in het geding is. De doelstelling van de *professional* aan wie wordt verstrekt, speelt daarbij een belangrijke rol. Het kabinet vindt het van belang dat gegevens worden uitgewisseld wanneer dit noodzakelijk is voor de veiligheid.

Met de grondslag «indien noodzakelijk voor de veiligheid moet je delen» geeft de commissie een duidelijk signaal naar de praktijk. Als duidelijk is dat de veiligheid van individuen concreet wordt bedreigd en het delen van persoonsgegevens dat risico kan wegnemen, móeten persoonsgegevens uitgewisseld worden tussen verschillende organisaties. Het kabinet onder-

schrijft in die zin de door de commissie Brouwer-Korf bepleite explicitering van art. 9 van de Wbp via voorlichting, facilitering en het bieden van handelingsperspectief.

Hieronder wordt een aantal initiatieven opgesomd die illustreren hoe slimmer en effectiever omgegaan kan worden met (al beschikbare) gegevens en tegelijkertijd hoe de mogelijkheden om informatie uit te wisselen tussen overheidsorganisaties worden verruimd.

3.6.1. Verbetering informatie-uitwisseling bij multidisciplinaire samenwerking

De aanpak van complexe vormen van criminaliteit zoals georganiseerde misdaad, fraude en financieel-economische criminaliteit vergt een geïntegreerde, gezamenlijke aanpak door Openbaar Ministerie, politie, Bijzondere Opsporingsdiensten, toezichthouders, lokaal bestuur en soms ook van private partijen. Een essentiële randvoorwaarde voor het succesvol opereren van samenwerkingsverbanden die daartoe worden ingericht, is dat relevante informatie doelgericht wordt uitgewisseld tussen de deelnemende partners. Het bevorderen van samenwerking en informatie-uitwisseling is daarom een continu aandachtspunt in de Task Forces die de afgelopen periode onder voorzitterschap van het Openbaar Ministerie zijn ingericht op de thema's mensenhandel, georganiseerde hennepteelt en vastgoedcriminaliteit.

De brief aan de Tweede Kamer van 11 maart 2009[1] bevat een uitvoerig overzicht van de bestaande wettelijke mogelijkheden en beperkingen voor informatie-uitwisseling tussen overheidsdiensten bij de bestrijding van georganiseerde misdaad en financieel-economische criminaliteit. Mede op basis van deze brief verricht de parlementaire werkgroep «verwevenheid van de bovenwereld met de onderwereld» thans een vervolgonderzoek naar mogelijk resterende knelpunten bij informatie-uitwisseling op dit vlak. Op basis van de uitkomsten van dit onderzoek, maar ook op basis van eventuele signalen over knelpunten die uit de bovenvermelde Task Forces komen, zal het kabinet bezien of nadere maatregelen noodzakelijk zijn.

Zoals aangekondigd in voornoemde brief van 11 maart 2009 zijn de volgende maatregelen al in gang gezet dan wel in voorbereiding, met het oog op het wegnemen van knelpunten bij het uitwisselen van informatie:

– *Verruiming van de mogelijkheid tot het opvragen van de WOZ-waarde voor bestuursorganen (gerealiseerd met ingang van 1 januari 2009).*
– *Introductie van een wettelijke plicht voor de notaris om de fiscus en het Openbaar Ministerie te informeren over transacties via de derdengeldrekening van de notaris (voorstel tot wijziging van de wet op het Notarisambt is in consultatie).*
– *Aanvulling en verbetering van de wet BIBOB is in voorbereiding (uitbreiding werkingssfeer tot vastgoedtransacties waarbij de overheid als partij optreedt; creëren wettelijke grondslag voor een landelijk register van BIBOB-adviezen).*
– *Mogelijkheid van verstrekking justitiële gegevens aan bestuursorganen is in voorbereiding (wijziging Besluit justitiële gegevens).*
– *Het op 24 september 2008 afgesloten bestuurlijk akkoord tussen de ministers van BZK, Justitie, Financiën, SZW en Defensie, de voorzitter van het College van procureurs-generaal van het Openbaar Ministerie en de voorzitter van de VNG (zie ook hieronder).*
– *De onder regie van de Minister van BZK ingerichte 11 Regionale Informatie- en Expertise Centra (RIECs) voor versterking van de bestuurlijke aanpak van georganiseerde misdaad. Het verbeteren van*

[1] Kamerstukken II, 2008/09, 29 911, nr. 23.

informatie-uitwisseling en het signaleren en helpen oplossen van eventuele knelpunten daarbij vormt een belangrijk onderdeel van de werkzaamheden van deze centra[1].

Voorts is een wetsvoorstel tot wijziging van onder meer Boek 2 BW en de Wet documentatie vennootschappen (31 948) aanhangig bij de Tweede Kamer waarvan onderdeel uitmaakt de verruiming en de verbetering van de gegevensuitwisseling in het kader van de voorkoming en bestrijding van misbruik van rechtspersonen. Kern van dit voorstel is dat gegevens over rechtspersonen uit diverse openbare en gesloten bronnen worden opgenomen in een registratie en dat gedurende de levensloop van een rechtspersoon voortdurend een automatische risicogestuurde analyse van die gegevens plaatsvindt. Dit maakt het mogelijk om in een vroeg stadium een verhoogd risico op misbruik van of door rechtspersonen te signaleren. Die signalering kan worden neergelegd in een risicomelding, die door de dienst Justis van het ministerie van Justitie doorverstrekt kan worden aan een selecte groep van handhavers.

In Europees verband streeft het kabinet naar optimalisering van de voorwaarden voor informatie-uitwisseling, waarvoor aanpassingen in wet- en regelgeving (onder andere de genoemde aanpassing van de EU-privacyrichtlijn) en verbetering van processen en ICT-systemen nodig zijn, zoals ook verwoord in het kabinetsstandpunt inzake het JBZ-meerjarenbeleidskader 2010–2014, het Stockholm Programma[2].

Het kabinet ondersteunt in dit kader de ontwikkeling van de Informatie Management Strategie (IMS). Deze strategie maakt deel uit van de Nederlandse inzet voor het Stockholm Programma en wordt momenteel onder leiding van het Zweeds voorzitterschap ontwikkeld. De IMS is gericht op een planmatige aanpak in het streven naar optimalisatie van informatie-uitwisseling, om een wildgroei van juridische instrumenten en nieuwe processen en ICT-systemen tegen te gaan. De strategie kiest voor een integrale benadering en heeft daarmee betrekking op informatie-uitwisseling op diverse terreinen.

Conform de hierboven uiteengezette lijnen, kiest het kabinet ook in dit kader voor de benadering van een tweevoudige bescherming. Zowel de veiligheid van burgers als hun persoonlijke levenssfeer dient te worden beschermd. De bescherming van persoonsgegevens is dan ook een essentieel onderdeel van de IMS.

3.6.2. Vergemakkelijken uitwisseling toezichtgegevens tussen toezichthouders, politie en OM

Mede naar aanleiding van de aandacht die daaraan is besteed in de evaluatie wordt hieronder ingegaan op het delen van informatie tussen toezichthoudende organen die structureel samenwerken in ketens of domeinen. Dit punt is aan de orde gesteld in het rapport Herijking toezichtswetgeving (31 700-VI, nr. 70) en besproken in het algemeen overleg dat de Minister van Justitie met de Vaste Commissie voor Justitie op 25 maart 2009 heeft gevoerd (31 700-VI, nr. 118).

Bij die gelegenheid heeft de Minister van Justitie toegezegd nader terug te zullen komen op de mogelijkheid om op een nader te bepalen plaats in de wetgeving een algemene bepaling op te nemen op grond waarvan het mogelijk wordt dat toezichtgegevens gemakkelijker kunnen worden uitgewisseld tussen toezichthouders, politie en OM onderling. Indien een dergelijke bepaling zou worden opgesteld, zou deze in elk geval een aanvullend karakter moeten hebben. Dat aanvullend karakter komt op verschillende wijzen tot uiting.

[1] Brief Minister van Justitie en Minister van BZK van 21–04–200, Kamerstukken II, 2008/09, 29 911, nr. 27.

[2] Kabinetsstandpunt inzake de Nederlandse visie op een toekomstig JBZ-meerjarenbeleidskader 2010–2014 (Stockholm Programma), kamerstukken II, 2008/09, 23 490, nr. 552.

Er is naar het oordeel van het kabinet geen reden om bestaande én voorgenomen bijzondere wettelijke regelingen met betrekking tot specifieke toezichtgegevens – zoals die bijvoorbeeld voorkomen in de sociale zekerheidswetgeving – te herzien. De bijzondere wetgever is vaak beter in staat goed in kaart te brengen waar de specifieke behoefte aan specifieke toezichtinformatie bestaat. Die regelingen moeten naar het oordeel van het kabinet blijven bestaan en de wetgever zou dit maatwerk, waar nodig, mogelijk moeten blijven maken.

Dat neemt op zichzelf niet weg dat verder kan worden nagedacht over aanvulling van de bepalingen met betrekking tot het toezicht op de naleving van de Algemene wet bestuursrecht (Awb) met een algemene regeling – een zogeheten vangnetbepaling – die van toepassing is als de wetgever geen specifieke regeling heeft getroffen. Regeling in de Awb verdient voorkeur boven regeling in de Wbp, omdat toezichtgegevens een meer omvattende categorie is dan persoonsgegevens.

Er moet verder worden nagedacht over de precieze formulering van een dergelijke bepaling, omdat er nadere vragen rijzen. Zo moet de vraag naar de reikwijdte nader worden beantwoord: wordt beoogd elke toezichthouder onder de reikwijdte te laten vallen, of moet deze beperkter zijn? Verder mag een dergelijke bepaling geen nadeel toebrengen aan de werking van maatschappelijk zeer belangrijke geheimhoudingsverplichtingen, zoals het fiscale geheim van art. 67 Algemene wet inzake rijksbelastingen. Daarnaast zijn sommige samenwerkings- én geheimhoudingsbepalingen ontleend aan Europese richtlijnen, zoals bijvoorbeeld op het gebied van het financieel toezicht. Daaraan mag geen afbreuk worden gedaan.

De vraag is ook of betrekking van de positie van politie en OM in deze informatiebetrekkingen moet leiden tot volledige symmetrie in de uitwisseling van informatie tussen bestuur enerzijds en politie en justitie anderzijds, of dat er juist aanleiding bestaat dat niet te doen. Tenslotte moet het grensoverschrijdende aspect – waaronder het beschikbaarheidsbeginsel bij de overdracht van politiële en justitiële informatie – ook aandacht krijgen. Het kabinet heeft behoefte aan nadere advisering over deze vraagstukken. Een dergelijk advies, zou bij voorbeeld in wetenschappelijke kring kunnen worden gevraagd.

3.7. Organiseren van facilitering, voorlichting en educatie

Ondersteuning van de *professional* (ook buiten het veiligheidsdomein) is nodig en – zo blijkt uit het rapport van de commissie en uit de evaluatie van de Wet bescherming persoonsgegevens – de wet zelf biedt deze ondersteuning niet, vanwege de daarin vervatte abstracte normen. Rechtsontwikkeling heeft onvoldoende plaatsgevonden. Dit betekent dat de open normen uit de wet in de praktijk slechts beperkt zijn ingevuld.

Daarnaast zijn nog andere ontwikkelingen in de praktijk te zien. Zo heeft het College bescherming persoonsgegevens het zwaartepunt van haar activiteiten belegd bij haar rol als handhaver en toezichthouder en minder bij de maatschappelijke adviesrol die zij tot voor kort ook uitoefende. Tevens is het Cbp terughoudender geworden in het behandelen van klachten van individuele burgers. Ook blijkt dat het in de praktijk voor organisaties niet eenvoudig is om kennis met betrekking tot de bescherming van persoonsgegevens te bundelen en te behouden.

Ervaring binnen de overheid leert dat een actieve ondersteuning van het veld uitermate effectief is. Een voorbeeld hiervan de Helpdesk Privacy Jeugd en gezin, die sinds 2004 actief is. Deze helpdesk beantwoordt

vragen van professionals op het terrein van de jeugdzorg en helpt hen tevens met bestaande belemmeringen om te gaan. Ook heeft de helpdesk een voorlichtingsfunctie, waarbij producten worden ontworpen zoals modelconvenanten en handleidingen. Voorbeelden van dergelijke producten zijn het eerder genoemde modelconvenant Veiligheidshuizen en het modelconvenant Verwijsindex risicojongeren. De helpdesk ontwikkelt tevens elektronische beslissingsondersteunende systemen. Ten behoeve van de jeugdzorg heeft de helpdesk twee wegwijzers ontwikkeld die via www.privacywegwijzer.nl te benaderen zijn. Met behulp van deze eenvoudige en gebruiksvriendelijke webapplicaties kunnen hulpverleners inzicht krijgen in welke persoonsgebonden informatie zij met wie mogen delen.

Een ander voorbeeld is het hierboven genoemde bestuurlijk akkoord inzake de geïntegreerde decentrale aanpak van de georganiseerde misdaad. Dit akkoord bevat een model van een regionaal convenant over de informatie-uitwisseling tussen de decentrale convenantpartners. Uitdrukkelijk wordt aandacht besteed aan de spelregels waarbinnen de informatie-uitwisseling in de regionale samenwerkingsverbanden vorm kan krijgen. In een juridisch kader worden de minimumrandvoorwaarden van de werkwijze transparant gemaakt. Er worden handvatten gegeven om op decentraal niveau concreet invulling te geven aan de waarborgen, noodzakelijk voor de rechtsbescherming van de burgers die het betreft.

Ten behoeve van de ondersteuning van de *professional* binnen de overheid zal een helpdesk worden ingericht. Deze helpdesk zal taken krijgen op de terreinen voorlichting, educatie en advisering met betrekking tot vraagstukken rondom de bescherming van de persoonlijke levenssfeer, met name voor wat betreft het realiseren van voldoende waarborgen bij de omgang met persoonsgegevens.
De beperktere invulling die het Cbp geeft aan zijn maatschappelijke adviesrol heeft ook gevolgen voor *professionals* buiten de overheid. Het kabinet zal met de relevante partijen, waaronder het bedrijfsleven en het Cbp, in overleg treden om te onderzoeken op welke wijze de facilitering van ook deze *professionals* het beste kan worden vormgegeven.

Het kabinet wil bereiken dat de nu op diverse plekken georganiseerde deskundigheid op het gebied van privacy wordt gebundeld en voor een bredere kring toegankelijk wordt gemaakt. De wijze waarop dit gestalte zal krijgen zal onderdeel uitmaken van het plan van aanpak voor de implementatie van alle in deze brief genoemde maatregelen.

4. Bescherming van persoonsgegevens op andere terreinen dan veiligheid

De verwerking van persoonsgegevens vindt voornamelijk plaats buiten het veiligheidsdomein. Van groot belang voor de verwerking en bescherming van persoonsgegevens op dit terrein is de Wet bescherming persoonsgegevens. Het kabinet ziet, mede naar aanleiding van de evaluatie van deze wet, voldoende aanleiding om deze aan te passen.

Bij de behandeling van de navolgende voorstellen wordt aangesloten bij de in de inleiding aangegeven kernthema's. Dit betekent dat allereerst wordt ingegaan op de mogelijkheden van de Wbp. Vervolgens komt aan bod op welke wijze de nadruk op meer waarborgen voor de burger een grotere rol zou kunnen spelen bij de verwerking van persoonsgegevens.

In het kader van het vormgeven van het tweede kernthema, robuuster, extern toezicht, zal worden ingegaan op de rol van de toezichthouder, het College bescherming persoonsgegevens, en de voorstellen om de positie

van het college te versterken. Tot slot worden mogelijkheden aangedragen om door aanpassingen van de Wbp bij te dragen aan de verwezenlijking van de vier kernthema's van het kabinet.

Het kabinet is zich er daarbij nadrukkelijk van bewust dat de Wbp de verwerking van persoonsgegevens binnen verschillende domeinen reguleert, maar ziet op dit moment onder het regime van de EU-privacyrichtlijn geen reëel alternatief voor het abstracte karakter van de huidige wet. Aanpassing van de specifieke wettelijk kaders – per domein – kan echter zeer verschillend uitvallen. Het kabinet zal bij het uitwerken van de hieronder gepresenteerde voornemens de verschillende belanghebbenden betrekken, waaronder het College bescherming persoonsgegevens en het georganiseerde bedrijfsleven.

4.1. Normering en toekomstbestendigheid van de Wbp

De Wbp is een algemeen en abstract geformuleerde wet. Uit de evaluatie komt naar voren dat de invulling van die abstract geformuleerde normen in praktische situaties niet altijd even gemakkelijk verloopt. De vooronderstelling van de wetgever is altijd geweest dat die algemene normen sectoraal of branchegewijs (met gedragscodes) nader zouden worden ingevuld. Die vooronderstelling blijkt maar zijn ten dele juist te zijn. In het volgende punt wordt daarop nog teruggekomen.

Wel acht het kabinet de evaluatie een bevestiging van het standpunt dat er geen reëel alternatief bestaat voor het bestaande karakter van de Wbp. Daar liggen drie redenen aan ten grondslag. In de eerste plaats zou het verlaten van het algemene en abstracte karakter van de Wbp (één regeling geldend voor alle gegevensverwerkingen, behoudens uitzondering) onvermijdelijk tot gevolg moeten hebben dat de wetgever sectorale normen gaat opstellen.

In de tweede plaats is het de vraag of de ontwikkeling van een stelsel van sectorale normen wel voldoende zal zijn om volledig te voldoen aan de eisen die voortvloeien uit de EU-privacyrichtlijn. De richtlijn is ook algemeen en abstract geformuleerd. In de derde plaats leidt het in het leven roepen van sectorale wetgeving tot een toename van de regeldruk.

Punt van aandacht in het evaluatieonderzoek is geweest of de Wbp – deel van de nationale rechtsorde – de samenleving nog wel afdoende kan beschermen tegen de gevolgen van technologische ontwikkelingen als *radio frequency identification* (RFID), biometrie, internettoepassingen e.d. Uit de evaluatie blijkt dat nieuwe technologische ontwikkelingen, zoals RFID, in de praktijk niet tot grote privacyschendingen hebben geleid die het kabinet thans aanleiding geeft nieuwe wetgeving voor te stellen. Het kabinet is van opvatting dat hier waakzaamheid aan de dag moet worden gelegd. Wanneer de toepassing van nieuwe technologie door de overheid ter hand wordt genomen, die in zijn gebruik consequenties heeft voor de bescherming van persoonsgegevens, behoort dat effect behoorlijk te worden verantwoord.

Voorts is het kabinet van opvatting dat de wet niet aan elke nieuwe technologie moet worden aangepast. De algemene privacybeginselen uit de kaderwet moeten worden vertaald naar specifieke technologische toepassingen. De huidige wet biedt voorlopig nog voldoende ruimte om bescherming van persoonsgegevens mogelijk te maken. Daarom ziet het kabinet bijvoorbeeld geen reden een specifieke RFID-wetgeving in te voeren, maar bij specifieke toepassingen ervan moet wel duidelijk zijn wat de kaderwet betekent voor burger en bedrijf.

Op langere termijn zal zich de noodzaak aandienen voor een meer fundamentele verandering van regelgeving. Verschijnselen als «*cloud computing*», maar ook RFID, leiden op den duur onvermijdelijk tot de noodzaak centrale begrippen uit de richtlijn en de Wbp als «persoonsgegeven» en «verantwoordelijke» opnieuw op hun bruikbaarheid voor de komende decennia te beoordelen. Het eindbeeld van deze ontwikkelingen is nog zo onzeker dat het onmogelijk is daarover nu al vastomlijnde standpunten in te nemen. Dit is bovendien in nationaal perspectief niet zinvol.

Dat Europese antwoord zal bovendien rekening moeten houden met elders in de wereld bestaande principes van gegevensbescherming. De ervaringen met diverse derde landen op het terrein van de passagiersgegevens en op het gebied van de zogeheten Safe Harbor Principles hebben geleerd dat ook de Europese Unie niet teveel kan vertrouwen op de bereidheid van die derde landen om de gedetailleerde regels van de Europese Unie te aanvaarden. Er zal ook gekeken moeten worden naar Azië en de daar gehanteerde maatstaven voor gegevensbescherming. Het is immers daar waar veel gegevens uit Europa feitelijk worden verwerkt. Zoals hiervoor al is aangegeven, heeft de Europese Commissie inmiddels het startsein gegeven voor een proces dat op termijn moet leiden tot een herziening van de richtlijn.

4.2. Het belang van een privacybewuste burger

Een belangrijke rol bij de bescherming van persoonsgegevens is weggelegd voor de burger zelf. Hij is immers de eigenaar van zijn eigen gegevens, is tot zekere hoogte verantwoordelijk voor zijn eigen keuzes en hij is ook degene die schade ondervindt wanneer onzorgvuldig met zijn gegevens wordt omgegaan. Om die reden staat de burger ook centraal in de opvattingen van het kabinet over de omgang met persoonsgegevens, ook al is het merendeel van de beleidsvoornemens gericht op de *professional.*

Wanneer hij schade ondervindt van een onzorgvuldige omgang met zijn persoonsgegevens, is de burger om zijn recht te halen niet uitsluitend afhankelijk van de bestaande strafrechtelijke controle- en handhavingsmechanismen, maar kan hij zelf ook civielrechtelijk actie ondernemen.

Het kabinet vindt het belangrijk om de burger bewuster te maken van de rechten die aan hem zijn toegekend wanneer zijn persoonsgegevens worden verzameld en hem tevens te stimuleren om van deze rechten ook daadwerkelijk gebruik te maken. De overheid wil de burger daarnaast ook bewuster maken van de risico's die zijn verbonden aan een onzorgvuldige omgang met zijn eigen persoonsgegevens.

4.3. Transparantie

Een voldoende mate van transparantie over wat er met zijn gegevens gebeurt, is een noodzakelijke voorwaarde voor een sterkere en bewustere burger. Deze stelling komt ook naar voren in het rapport van Regioplan. Hij kan immers pas keuzes maken wanneer hij ook daadwerkelijk weet voor welk doel zijn gegevens worden verwerkt, met welke andere gegevens die gegevens in verband worden gebracht en vervolgens aan anderen ter beschikking worden gesteld, waar ze beschikbaar zijn en hoe het inzage- en correctierecht kan worden uitgeoefend. Het is echter juist de transparantie die in de huidige samenleving in toenemende mate onder druk lijkt te staan.

Zo kan niet worden voorbijgegaan aan het feit dat het aantal databanken waarin gegevens van burgers zijn opgeslagen is toegenomen[1]. Dat verschijnsel is onvermijdelijk verbonden aan de informatiesamenleving.

[1] In een quick scan onderzoek verricht in opdracht van het Cbp wordt gewag gemaakt van aantallen variërend van 250 tot 1000 databanken waarin de gemiddelde Nederlander zou staan geregistreerd. Zie verder: «Onze digitale schaduw». Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat. Considerati, januari 2009.

Het hoeft ook niet negatief te worden gewaardeerd. Wat wel nodig is, is dat overheid en bedrijfsleven behoorlijk inhoud blijven geven aan hun verplichting tot transparantie en dat ook wordt bezien of de formulering van de verplichting nog wel volledig bij de tijd is. Zo ontbreken specifieke verplichtingen om informatie te verschaffen over verschillende gebruikswijzen van persoonsgegevens, zoals het profileren en de redenen die aan de profielen ten grondslag liggen.

De invloed van het groeiende aantal registraties op de effectiviteit van het inzage- en correctierecht verdient aandacht. Deze gedachte komt ook overeen met de uitkomsten van het onderzoek van Regioplan, waarin ondervraagde burgers aangaven behoefte te hebben aan meer overzicht met betrekking tot van hun geregistreerde persoonsgegevens.

4.3.1. Inzage- en correctierecht

Vanuit de overheid bestaan verschillende initiatieven waarmee een bijdrage wordt geleverd aan de versterking van de transparantie voor de burger met betrekking tot de verwerking van zijn persoonsgegevens. Op de website www. burgerservicenummer.nl kan iedereen nagaan welke organisatie welke gegevens uitwisselen met behulp van het burgerservicenummer (BSN). Op de website www.mijnoverheid.nl kunnen burgers inzien welke informatie bij overheidsorganisaties over hem bekend is. Dit portaal is volop in ontwikkeling. Met de groei van het aantal aangesloten overheidsorganisaties neemt het aanbod van informatie langzaam aan toe en worden in de komende jaren de mogelijkheden tot inzage uitgebreid.

Over het hierboven genoemde recht op inzage- en correctie wordt in het evaluatierapport opgemerkt dat dit recht tot doel heeft om een grotere mate van transparantie te bereiken. Burgers maken echter weinig gebruik van dit recht. Uit hetzelfde rapport blijkt dat dit mede wordt veroorzaakt door een onvoldoende bekendheid met de mogelijkheid. Een andere oorzaak zou kunnen zijn dat burgers niet altijd weten dat hun gegevens verwerkt worden.

Aan de formulering van de rechten als zodanig zal – voor zover het de tekst van de Wbp betreft – niet veel hoeven te veranderen. Voor de publieke sector krijgt de bewustmaking van de burger ten aanzien van de hem door de Wbp toegekende rechten een plaats in het persoonsinformatiebeleid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Verder wil het kabinet verantwoordelijken verplichten om betrokkenen inzicht te geven in categoriseringen die plaatsvinden op basis van verzamelde persoonsgegevens en de achterliggende redenen. Tevens wil het kabinet dat het inzagerecht voorts nader zal worden ondersteund door een (facultatief) klachtrecht.
Dit klachtrecht behoeft niet noodzakelijkerwijs volledig wettelijk te worden geregeld. Wat door maatschappelijke organisaties, bijvoorbeeld door het georganiseerd bedrijfsleven en consumentenorganisaties onderling kan worden geregeld, verdient de voorkeur boven overheidsregelgeving. De wet zou de totstandkoming van een dergelijk klachtrecht wel kunnen faciliteren, bijvoorbeeld door middel van een erkenningsregeling, gecombineerd met een vrijstelling van verplichtingen.

4.4. Bijzondere aandacht voor de beveiliging van persoonsgegevens

Persoonsgegevens worden steeds belangrijker binnen een keur aan terreinen in de maatschappij. Voor niemand zijn deze gegevens echter meer waardevol dan voor de burger zelf. Het kabinet is dan ook van

mening dat de burger zo veel mogelijk in staat dient te worden gesteld om zelf zeggenschap te hebben en te houden over het gebruik van zijn gegevens. Onrechtmatig gebruik maakt een inbreuk op deze autonomie van de burger. Daarom is het kabinet van mening dat een adequate beveiliging van deze gegevens noodzakelijk is en specifieke aandacht behoeft.

Uit de evaluatie blijkt niet direct dat er op dit moment al sprake is van grote problemen rondom de uit de Wbp voortvloeiende verplichting tot beveiliging van persoonsgegevens. Dit lijkt ook niet het geval binnen het veiligheidsdomein. Niettemin is er aanleiding aandacht aan dit onderwerp te schenken. Vooral in het buitenland (Bondsrepubliek Duitsland, Verenigd Koninkrijk) heeft zich een aantal ernstige incidenten voorgedaan. De vraag is of de wetgeving de samenleving wel voldoende beschermt tegen het gevaar dat voortvloeit uit het niet nakomen van de verplichting om persoonsgegevens te beveiligen.

Momenteel is de onzorgvuldige omgang met persoonsgegevens, maar ook andere gegevens, privaatrechtrechtelijk te sanctioneren, via een onrechtmatige daadsactie. Daarnaast is de overtreding van een geheimhoudingsplicht strafbaar gesteld. Via beide wegen worden belanghebbenden beschermd tegen de schade die zij lijden als gevolg van de onrechtmatige omgang met gegevens. Uit de evaluatie komt echter naar voren dat tot op heden slechts in zeer beperkte mate geschillen over de bescherming van persoonsgegevens aan de rechter worden voorgelegd. Met betrekking tot mogelijke aanpassingen van het wettelijk kader zijn drie maatregelen in dit opzicht mogelijk.

In de eerste plaats zou een verzwaring van de bestaande verplichting tot dataminimalisatie overwogen kunnen worden. Dat zou op verschillende manieren kunnen worden vormgegeven. Eén alternatief is dat bedrijven en instellingen verplicht zouden kunnen worden uit te leggen hoe lang ze persoonsgegevens bewaren, welke rechtvaardiging geldt voor die bewaartermijnen en wat er gebeurt met persoonsgegevens na het verstrijken van de bewaartermijn. Een ander alternatief kan een wettelijke opschoonverplichting zijn.

In de tweede plaats zou gedacht kunnen worden aan een afzonderlijke sanctionering van de beveiligingsverplichting in de Wbp zulks in samenhang met – de hieronder te bespreken – versterking van de handhaving van de Wbp. Ook hieraan zijn weer consequenties verbonden. De huidige beveiligingsverplichting is zeer algemeen geformuleerd en beschermt de betrokkene tegen potentiële schade. Sanctionering van een dergelijke verplichting zou verder gaan dan het bestaande recht dat toch vooral beoogt te beschermen tegen reële en onmiddellijk dreigende schade.

In de derde plaats zou een verplichting in het leven kunnen worden geroepen om ernstige doorbraken van beveiligingsmaatregelen van persoonsgegevens te melden. Daarmee wordt potentiële schade aan persoonsgegevens zoveel mogelijk beperkt. Een voorstel daartoe maakt al deel uit van een pakket herzieningsmaatregelen voor het pakket richtlijnen en verordeningen voor de telecommunicatiesector. Deze verplichting kan ook voor andere sectoren geldend worden gemaakt.

4.5. Het College bescherming persoonsgegevens

De toezichthouder op de bescherming van persoonsgegevens, het Cbp, heeft op dit moment een relatief breed takenpakket. Zowel het Cbp zelf, als de opstellers van de beide rapporten zijn van mening dat de meeste aandacht op dit moment uit zou moeten gaan naar de handhavingsrol die het Cbp op grond van de Europese privacyrichtlijn heeft. Het kabinet deelt

deze opvatting en treft verschillende maatregelen om de positie van de toezichthouder te versterken.

De commissie adviseert ons zorg te dragen voor robuust extern toezicht op de naleving en handhaving van de regels voor het omgaan met persoonsgegevens door een sterke en onafhankelijke toezichthouder, die alleen is belast met «toezicht houden en handhaven». De commissie bepleit daarom een gemarkeerde verantwoordelijkheid voor onafhankelijk extern toezicht die zich concentreert op de naleving en met passende handhavingsinstrumenten kan optreden.

De huidige situatie waarin een orgaan, i.c. het College bescherming persoonsgegevens, zowel toezicht houdt op de naleving van de Wet bescherming persoonsgegevens als adviserende en toetsende taken vervult, acht zij ongewenst. De slagvaardigheid van het externe toezicht zou door die concentratie van onderscheiden taken bij een orgaan te lijden hebben. Daarbij spreekt de commissie zich er niet over uit welke taken door het College zouden blijven moeten worden verricht en welke taken zouden moeten overgaan.

Wat betreft de invulling van het externe toezicht verdient de positie van het College bescherming persoonsgegevens (Cbp) in drie opzichten aandacht. In de eerste plaats vervult het Cbp in een aantal opzichten een maatschappelijke adviesfunctie. In de tweede plaats vervult het Cbp de functie van wetgevingsadviseur. In de derde plaats vervult het Cbp de rol van toezichthouder op en handhaver van de Wet bescherming persoonsgegevens. Het kabinet meent dat deze cumulatie van taken heroverweging verdient en wil het als volgt regelen.

4.5.1. Cbp en maatschappelijke advisering

Het Cbp heeft zich het afgelopen decennium in belangrijke mate opgesteld als adviseur van de samenleving in privacykwesties. Daaraan bestond grote behoefte. De Wbp is een wet met veel open en in algemene termen geformuleerde normen. Die wet vereist nadere invulling op sectoraal niveau en vaak ook op het niveau van een individuele verwerking. Grote bedrijven of overheidsinstellingen zijn nog wel in staat met de opbouw van de nodige deskundigheid te voorzien in het voeren van een verantwoord beleid met betrekking tot het verwerken van persoonsgegevens.

Ten aanzien van kleinere bedrijven of individuele burgers kan door middel van vrijstelling van de meldplicht nog wel wat vereenvoudiging in de omgang met de formaliteiten waartoe de Wbp verplicht worden bereikt, maar het vrijstellingenregime beantwoordt niet de vragen die bestaan over de invulling van de inhoudelijke verplichtingen die de Wbp oplegt. Het Cbp heeft zich in de afgelopen jaren ingespannen om veel van die vragen zo goed mogelijk te beantwoorden. Het college meent echter zelf, sinds 2008, dat deze taak anders moet worden ingevuld. Het college wil – op basis van selectiviteit en risicoanalyse – de Wbp nadrukkelijker gaan handhaven, in plaats van adviseren.

Twee omstandigheden leiden ertoe dat dan minder de nadruk komt te liggen op maatschappelijke advisering. In de eerste plaats leidt al te intensieve advisering tot potentiële conflicten met de handhavende rol. Een toezichthouder en handhaver moet onbevangen en onbevooroordeeld kunnen optreden. In de tweede plaats zijn de middelen waarover het college beschikt niet onbeperkt. Aangezien uitbreiding van die middelen geen reële optie is, is prioritering noodzakelijk.

Het kabinet heeft begrip voor deze afwegingen van het Cbp. Dit heeft tot consequentie dat het Cbp zijn adviserende taak in de richting van de samenleving, met name om een zo onbevangen mogelijke handhaving van de Wbp mogelijk te maken, in belangrijke mate kan laten vervallen. Wetgeving is hiervoor niet nodig, aangezien de adviserende taak ten aanzien van de samenleving als geheel niet wettelijk is geregeld.

De adviserende rol die het Cbp thans nog vervult zal in ieder geval voor het desbetreffende terrein kunnen worden meegenomen in door de in de voorgaande paragraaf geuite voornemens van het kabinet met betrekking tot het faciliteren van de *professional*. Het Ministerie van Justitie werkt bovendien aan een leidraad om bijzondere wetgeving goed te kunnen afstemmen op de Wbp.

Overigens vervult het Cbp thans met behulp van zijn website en door middel van het vaststellen van richtsnoeren wel een nuttige *informerende* rol voor de samenleving. Die informerende rol is van algemene aard, en richt zich niet op concrete gevallen. Het kabinet meent dat het Cbp die rol zou kunnen blijven vervullen, omdat deze logisch voortvloeit uit de handhavende taak van het Cbp.

4.5.2. Cbp als wetgevingsadviseur

Het Cbp vervult daarnaast een rol als wetgevingsadviseur. Die rol is geen vrijblijvende kwestie. Richtlijn nr. 95/46/EG legt aan de lidstaten de verplichting op de toezichthouder om advies te vragen voorafgaand aan de vaststelling van wettelijke voorschriften die geheel of grotendeels de bescherming van persoonsgegevens betreffen. Het gaat hierbij niet slechts om advisering op het terrein van de Wbp, maar ook om advisering op het gebied van enkele andere wetten, zoals de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de Wet gemeentelijke basisadministratie persoonsgegevens.

Het kabinet is niet voornemens ten aanzien van deze rol van het Cbp veranderingen voor te stellen. Wel ligt het in de bedoeling om bij gelegenheid van het opstellen van wetgeving voor het Nationaal Instituut voor de Rechten van de Mens nog eens na te gaan of de taakomschrijving van het Cbp op het gebied van de wetgevingsadvisering in alle desbetreffende wetten wel voldoende nauwkeurig is geformuleerd.

4.5.3. Toezichthoudende taak van het Cbp

Het Cbp is belast met het toezicht op de naleving en de bestuursrechtelijke handhaving van de Wbp. De wetgever heeft het Cbp daartoe uitgerust met de bevoegdheid tot het toepassen van bestuursdwang, en daaraan gekoppeld, het opleggen van een last onder dwangsom, alsmede met de mogelijkheid tot het opleggen van een bestuurlijke boete. Die laatste mogelijkheid kan het Cbp echter alleen benutten bij het niet naleven van een aantal formele verplichtingen van de Wbp, zoals het niet naleven van de meldplicht. Het boetemaximum (momenteel € 4500,=) is niet indrukwekkend. Voor overtreding van de materiële normen van de Wbp moet worden teruggevallen op het opleggen van een dwangsom.

Uit de evaluatierapporten over de Wbp kan de conclusie worden getrokken dat er over de hele linie sprake is van een nalevingstekort ten aanzien van deze wet. Het kabinet meent dat daaraan ook iets kan worden gedaan door de handhavingsmogelijkheden te versterken. Een stevige handhaving van de Wbp, aan de hand van aansprekende voorbeelden, is een van de mogelijke middelen die nalevingsgedrag van de samenleving kunnen bevorderen.

De keuze van de wetgever bij de totstandkoming van de Wbp om de overtreding van materiële bepalingen van de Wbp niet te sanctioneren met bestraffende sancties, berustte op de gedachte dat het algemene en open karakter van de materiële normen van de Wbp met zich bracht dat het afstemmen van maatschappelijk gedrag op het enkele feit dat overtreding van een norm tot sanctionering aanleiding zou kunnen geven in concrete situaties onvoldoende voorzienbaar is. Dat uitgangspunt, dat voortvloeit uit het EVRM, huldigt het kabinet nog steeds.

Niettemin heeft de praktijk geleerd dat het Cbp in staat is door middel van richtsnoeren aan te geven in welke gevallen, en op welke wijze hij de Wbp zal handhaven. Richtsnoeren moeten dan natuurlijk wel voldoende concreet zijn, op zorgvuldige wijze worden voorbereid en tijdig worden bekendgemaakt. Bovendien heeft het Cbp beleidsregels vastgesteld met betrekking tot de procedurele aspecten van een boeteoplegging. Wanneer aan deze uitgangspunten wordt voldaan is de voorzienbaarheid van sanctionering naar het oordeel van het kabinet voldoende verzekerd.

Daarnaast blijkt uit onderzoek dat in een aantal ons omringende landen, België, Duitsland en Oostenrijk de materiële bepalingen van de in die landen vastgestelde privacyregelgeving ook met bestraffende sancties zijn bedreigd. Tot fundamentele moeilijkheden heeft dat in die landen geen aanleiding gegeven.

Het kabinet meent daarom dat thans het moment is aangebroken om ook de handhaving van de materiële normen van de Cbp door middel van het opleggen van bestuurlijke boetes wettelijk mogelijk te maken. Het kabinet zal daartoe wetgeving in voorbereiding nemen.

Uit de evaluatie blijkt dat er ook door de rechtspraak nog weinig nadere invulling is gegeven aan de Wbp. Betrokkenen lijken niet snel bereid een geschil over de bescherming van persoonsgegevens aan de rechter voor te leggen. Dat is overigens geen specifiek Nederlands probleem. De jurisprudentie van het Hof van Justitie van de Europese Gemeenschappen over de privacyrichtlijn is ook maar beperkt van omvang, al gaat het daarbij wel om principiële zaken.

De indruk bestaat dat het voorleggen van geschil over de bescherming van persoonsgegevens aan het oordeel van de rechter vooral om financiële redenen gebeurt. Alleen wanneer er een redelijk financieel belang bij een dergelijke zaak betrokken is, heeft het zin een rationele afweging te maken tussen kosten en opbrengsten van een dergelijke zaak. Het oplossen van geschillen van niet-materiële aard, moet op andere wijze geschieden. Dat zou kunnen met behulp van klachtprocedures. Het kabinet acht dit niet primair een zaak voor de overheid, maar vooral een zaak van maatschappelijke organisaties. De overheid kan daarbij wel stimulerend optreden, de wetgever kan het gebruik van dergelijke procedures faciliteren.

De wetgever kan ook overigens verdere rechtsvorming uitlokken. Zo kan het openstellen van bezwaar en beroep tegen de (formele) bevindingen van het Cbp naar aanleiding van een op verzoek van een belanghebbende ingesteld onderzoek naar verwachting jurisprudentie uitlokken. Op jaarbasis gaat het om ongeveer 60 van deze bevindingen. Dat zal wel moeten worden afgewogen tegen het belang van het tegengaan van juridisering van de samenleving in het algemeen en de juridisering van het onderwerp gegevensbescherming in het bijzonder.

4.6. Terugbrengen administratieve lasten

Het kabinet neemt de zorg over de administratieve lasten die in verband met Wbp staan serieus. Hiervoor is in januari 2009 een wetsvoorstel ingediend [*Wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve laten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen Kamerstukken II 2008/09, 31 841, nr. 2*].

Dit wetsvoorstel is voor VNO/NCW aanleiding geweest zich bij brief van 7 mei 2009 tot het kabinet te richten met voorstellen tot verdergaande lastenverlichting voor het bedrijfsleven. Het kabinet beschouwt de brief van VNO/NCW als een belangrijke bijdrage tot de noodzakelijke verdieping van de gedachtevorming over de plaats van de Wbp in de samenleving. De brief is voor het kabinet in elk geval aanleiding geweest een nota van wijziging uit te brengen bij genoemd wetsvoorstel. Daarin worden alle voorstellen van VNO/NCW opgenomen van meer technische aard, die zonder veel fundamentele afwegingen kunnen worden overgenomen.

Verder heeft het kabinet, in samenhang met het wetsvoorstel, een wijziging van, onder meer, het Vrijstellingsbesluit Wbp voor advies en consultatie aan Cbp, Actal en VNO/NCW gezonden, waarin een aanmerkelijk deel van de door VNO/NCW bepleite aanpassingen van dit besluit zijn opgenomen. De meer fundamentele kant van de brief sluit goed aan bij de weg die het kabinet bepleit van het schenken van zoveel mogelijk vertrouwen aan burgers en bedrijven, en waarbij de wet veel meer een begeleidend en stimulerend dan een dwingend karakter heeft.

Voor het overige zal het kabinet een aantal nuttige suggesties uit de brief van VNO/NCW die nog nadere uitwerking behoeven betrekken bij de wetgeving die zal voortvloeien uit dit kabinetsstandpunt.

4.7. Ruimhartiger vrijstellingsbeleid t.a.v. de meldplicht

De meldplicht en het voorafgaand onderzoek beogen een preventieve werking te hebben. De verplichting tot voorafgaande melding van een gegevensverwerking bij toezichthouder of functionaris voor de gegevensbescherming zou de transparantie moeten dienen. Tot op zekere hoogte is dit wellicht ook zo: het doen van een melding kan immers bijdragen aan de gedachtevorming over een voorgenomen verwerking. Uit de evaluatie blijkt echter dat de omvang van de verplichting onduidelijk is, en dat het uitblijven van reactie op de melding niet correspondeert met het verwachtingspatroon van de voor de melding verantwoordelijke. De meldplicht leidt bovendien tot administratieve lasten.

Op grond van de EU-privacyrichtlijn is het niet mogelijk de meldplicht af te schaffen. Wel hebben de lidstaten de nodige vrijheid om die meldplicht nader te regelen. Dit brengt het kabinet ertoe een ruimhartiger vrijstellingsbeleid te gaan voeren dan in de afgelopen jaren is gedaan. De eerste stappen zijn daartoe gezet in de vorm van een inmiddels in consultatie gezonden aanpassing van het Vrijstellingsbesluit Wbp. Dit besluit zal in de loop van 2010 in werking kunnen treden. Het kabinet zal periodiek in samenspraak met het College bescherming persoonsgegevens (Cbp) en het georganiseerd bedrijfsleven beoordelen in hoeverre verdere vrijstellingen kunnen worden verleend.

Het voorafgaand onderzoek (VO) leidt – anders dan de meldplicht – wel tot een verklaring van rechtmatigheid van het Cbp. Het VO is door de wetgever al beperkt tot een aantal relatief ingrijpende gegevensverwerkingen, zoals het gebruik van strafrechtelijke gegevens door particulieren.

Het VO is echter een tijdrovende aangelegenheid. Uit oogpunt van terugdringing van administratieve lasten zal het kabinet in samenspraak met Cbp en georganiseerd bedrijfsleven bezien hoe deze lasten verder kunnen verminderd. Dat kan door het aantal gevallen waarin een VO vereist is verder te beperken en door de procedure aanmerkelijk te verkorten.

4.8. Bevorderen van zelfregulering

Het kabinet is van mening dat zelfregulering in belangrijke mate bijdraagt aan een correcte omgang met persoonsgegevens. Het bevorderen van zelfregulering vormt dan ook een onderdeel van de benadering van het kabinet, wanneer het gaat om de verwerking van persoonsgegevens buiten het veiligheidsdomein. Het erop toezien dat persoonsgegevens op een behoorlijke manier worden verwerkt, is immers niet primair een zaak van de toezichthouder.

De Wbp biedt de mogelijkheid tot sectorgewijze invulling v an de regelgeving door middel van gedragscodes. Verder kunnen bedrijven of instellingen besluiten tot de aanstelling van een functionaris voor de gegevensbescherming (FG). De evaluatie laat zien dat van deze instrumenten weinig gebruik wordt gemaakt. Er zijn slechts acht gedragscodes vastgesteld, die elk bovendien kwalitatief weinig toegevoegde waarde hebben ten opzichte van de wettekst.

Een gering aantal organisaties heeft een FG aangesteld. Zeer grote bedrijven hebben wel Privacy Officers aangesteld. Zij hebben tot taak om binnen de organisatie het privacybeleid te ontwikkelen, maar hebben niet de bevoegdheden die een FG op grond van de Wbp heeft. Uit het evaluatierapport blijkt dat wanneer wel een FG (of Privacy Officer) is aangesteld, dit een belangrijk positief effect heeft op de kwaliteit van de gegevensbescherming binnen de desbetreffende organisatie.

De commissie is van mening dat het inrichten van intern toezicht in de vorm van een functionaris bij organisaties leidt tot een sterkere prikkel om risicoanalyses en risicobeoordelingen met betrekking tot de verwerking van persoonsgegevens op een permanent adequaat niveau te brengen. Bij grotere organisaties raadt de commissie aan om deze taak onder te brengen bij een zgn. functionaris voor de gegevensbescherming (FG). De Wbp voorziet in deze mogelijkheid.

Het kabinet onderschrijft de opvatting van de commissie dat het benoemen van functionarissen die toezien op de naleving van de privacywaarborgen een positieve uitwerking zou kunnen hebben op het niveau van gegevensbescherming. De verantwoordelijkheid voor een behoorlijke omgang met persoonsgegevens is dan ook in de eerste plaats een verantwoordelijkheid van de verwerkende organisaties zelf. De evaluatie laat zien dat zowel van de mogelijkheden met betrekking tot gedragscodes als tot de inzet van FG's weinig gebruik wordt gemaakt.

Het kabinet ambieert echter niet de samenleving het gebruik van gedragscodes of het aanstellen van FG's dwingend te gaan voorschrijven. Burgers en bedrijven moeten zoveel mogelijk vrijheid worden gegund bij de wijze waarop zij invulling geven aan een gecompliceerde wet. Het kabinet ziet meer in het door middel van wetgeving stimuleren van het gebruik van deze instrumenten. Een aandachtspunt daarbij is de verhouding tussen de FG en de toezichthouder. Hierover zal in overleg worden getreden met de toezichthouder en andere relevante partijen. Het is de opvatting van het kabinet dat een versteviging van de positie van de externe toezichthouder niet tot gevolg mag hebben, dat het interne toezicht hierdoor wordt verzwakt.

Conform paragraaf 2.2 van de nota «Vertrouwen in wetgeving» zou de wet de mogelijkheid kunnen bieden bedrijven of instellingen meer vrijheid ten opzichte van de verplichtingen van de Wbp te verlenen (bijvoorbeeld een vrijstelling van de meldplicht bij het Cbp, of vrijstelling van een verplichting een VO te ondergaan) wanneer zij een eigen privacybeleid vaststellen en bekendmaken en een FG of daarmee op één lijn te stellen functionaris aanwijzen.

Aan de inhoud van dat privacybeleid moet de wet dan een aantal inhoudelijke eisen worden stellen: een verplichting tot vaststelling van een klachtbehandelingsregeling of een verplichting tot het voeren van een «compliancebeleid», bijvoorbeeld door regelmatig audits te houden en de resultaten daarvan publiek te maken.

Er kan ook worden gedacht aan de mogelijkheid tot aanstelling van collectieve FG's te verruimen. Daarbij gelden twee belangrijke voorwaarden. De eerste is dat verruiming van de regelgeving niet in strijd met de richtlijn mag zijn. De tweede is dat verruimde regels niet principieel de handhavingsbevoegdheden van het Cbp moeten doorkruisen.

5. Uitgeleide

Een betere uitwisseling van informatie indien dat nodig is voor de veiligheid én meer waarborgen bij de omgang met persoonsgegevens, ondersteund door een stevige handhaving, ook buiten het terrein van veiligheid. Dit vormt in de kern de benadering die het kabinet voorstaat.

In paragraaf twee is aangegeven dat de huidige benadering van gegevensbescherming in de praktijk slechts tot beperkte resultaten leidt wanneer het gaat om de naleving van de materiële beginselen van een behoorlijke omgang met persoonsgegevens.

Om de oorzaken van dit probleem aan te pakken bevat deze brief een aantal voorstellen variërend van (juridische) stimuleringsmaatregelen tot praktische handreikingen. Het kabinet streeft ernaar om door middel van deze maatregelen een eerste stap te zetten naar een nieuwe benadering van de bescherming van de persoonlijke levenssfeer. Daartoe beoogt het kabinet de zorgvuldigheid met betrekking tot de omgang met persoonsgegevens in de dagelijkse praktijk te verankeren en voorts passende prikkels in het leven te roepen om deze zorgvuldigheid te waarborgen. Tevens ziet het kabinet voldoende aanleiding om te beginnen met de aanpak van ineffectief gebleken administratieve lasten, althans voor zover de privacyrichtlijn dit toelaat.

Willen deze maatregelen, die een beroep doen op de eigen verantwoordelijkheid van overheden en bedrijven, het gewenste effect sorteren, dan is het verkrijgen van draagvlak een belangrijke randvoorwaarde. Draagvlak bij de *professional* die de geboden handreikingen daadwerkelijk gaat ervaren als een welkome aanvulling op zijn instrumentarium en ook gaat gebruiken. Maar ook draagvlak bij de organisaties zelf die immers zullen moeten investeren om de benodigde ondersteuning aan hun professionals te geven.

Het kabinet zal daarom voor de nadere uitwerking en invoering van de voorgestelde maatregelen een programmaorganisatie in het leven roepen, waarbij de relevante partijen zullen worden betrokken. Op die manier hoopt het kabinet te bewerkstelligen dat de in deze brief uiteengezette benadering een brede invoering zal krijgen.

De in dit kabinetsstandpunt opgenomen voorstellen hebben ook consequenties voor de wetgeving. Binnenkort zal het kabinet een wetsvoorstel tot wijziging van de Wbp doen opstellen, waarin de aanbevelingen van de commissie, de uit de evaluatie van de Wbp voortvloeiende punten en de gedachten die het kabinet door partijen als VNO/NCW en het Cbp zijn aangereikt zullen worden opgenomen.

Op enige belangrijke onderdelen zijn nadere keuzes nog noodzakelijk. Verder zal het kabinet de inzichten die in dit standpunt zijn verwoord bij de Europese Commissie inbrengen als bijdrage aan de meningsvorming over herziening van de richtlijn.

Op middellange termijn zal de Commissie komen met voorstellen tot herziening van de richtlijn. Zodra de voorstellen daartoe bekend zijn – naar verwachting in 2010 of 2011 – worden de Kamers daarover via de gebruikelijke weg geïnformeerd.

De minister van Justitie,
E. M. H. Hirsch Ballin

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
G. ter Horst

BIJLAGE

Overzicht kabinetsvoornemens

Veiligheid en persoonsgegevens

- Stimuleren gebruik richtinggevend kader Brouwer voor actuele kwesties.
- Meer aandacht voor het hanteren van *privacy-by-design.*
- *Ontwikkeling van een Privacy Impact Assessment* instrument.
  - Najaar 2010
- Gebruik van ANPR.
  - Ontwikkeling beleidskader ANPR in samenspraak met Platform ANPR: zomer 2010
  - Uitwerken technische uitvoering met inachtneming van de beginselen van transparantie en privacybescherming door ontwerp: najaar 2010
  - Uitvoering *Privacy Impact Assessment*: voorjaar 2011
  - Voorbereiding wetgeving met de betrokken departementen en de betrokken toezichthouders, politie en openbaar ministerie: najaar 2011
- Expliciteren artikel 9 Wbp zoals voorgesteld door de commissie
- Vergemakkelijken uitwisseling toezichtsgegevens tussen toezichthouders, politie en OM.
  - Indiening wetsvoorstel: voorjaar 2011
- Inrichten helpdesk voor voorlichting, educatie en oplossingen op maat.
  - Zomer 2010

Bescherming van persoonsgegevens op andere terreinen dan veiligheid

- Verdere bewustmaking van burgers t.a.v. hun rechten, ook in het kader van het civiele recht en bestuursrecht.
- Gegevensbeheerders verplichten inzicht te geven aan betrokkenen over de verwerking van hun gegevens.
  - Indiening wetsvoorstel: voorjaar 2011
- Versterken transparantie door verruiming informatie verplichtingen.
  - Indiening wetsvoorstel: voorjaar 2011.
- Activiteiten n.a.v. de functiescheiding Cbp door het laten vervallen van de huidige maatschappelijke adviesfunctie en nadruk op de handhavingstaken.
  - Inrichten helpdesk: zomer 2010
- Sanctionering materiële bepalingen Wbp.
  - Indiening wetsvoorstel: voorjaar 2011
- Ruimhartiger vrijstellingsbeleid t.a.v. de meldplicht.
  - Jaarlijkse aanpassing Vrijstellingsbesluit Wbp na overleg met bedrijfsleven en Cbp
- Beperken van gevallen van verplicht voorafgaand onderzoek en verkorten procedure.
- Meldplicht en waar mogelijk voorafgaand onderzoek vervallen indien:
  - bedrijven een eigen privacybeleid vaststellen en bekendmaken (wel voorwaarden aan de inhoud verbinden);
  - bedrijven een FG (of soortgelijke functionaris) aanstellen (evt. aanstellen collectieve FG).

Uitgeleide

- Ter uitwerking en uitvoering van bovengenoemde beleidsvoornemens zal een programmaorganisatie in het leven worden geroepen.
  - Najaar 2009, looptijd: huidige kabinetsperiode