COLLEGE **BESCHERMING** PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN De leden van de vaste commissie voor Veiligheid en Justitie en de leden van de vaste commissie voor Immigratie en Asiel / JBZ-Raad
Eerste Kamer der Staten-Generaal
Postbus 20017
2500 EA DEN HAAG

DATUM 5 maart 2012
ONS KENMERK z2011-01054 / z2012-00164
CONTACTPERSOON Mw. drs. K. Verhaar
070-8888500
k.verhaar@cbpweb.nl
UW BRIEF VAN
UW KENMERK

ONDERWERP Afschrift van brief aan Tweede Kamer over EC-voorstel nieuw juridisch raamwerk voor gegevensbescherming

Geachte leden,

Op verzoek van de leden van de vaste commissie voor Veiligheid en Justitie van de Tweede Kamer heb ik deze commissie en de vaste commissie voor Binnenlandse Zaken vrijdagmiddag een brief gezonden met het voorlopige standpunt op hoofdlijnen van het College bescherming persoonsgegevens ten aanzien van een aantal essentiële aspecten van het voorstel van de Europese Commissie voor een nieuw juridisch raamwerk voor gegevensbescherming.

Gelet op uw commissievergadering voorzien voor dinsdag 6 maart aanstaande, doe ik u hierbij graag een afschrift van deze brief inclusief bijlage toekomen.

Hoogachtend,

Mr. J. Kohnstamm
Voorzitter College bescherming persoonsgegevens

b/a Mr. W.B.M. Tomesen
Lid van het College

BIJLAGEN 1
BLAD 1

COLLEGE **BESCHERMING** PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN De leden van de vaste commissie voor Veiligheid en Justitie en de leden van de vaste commissie voor Binnenlandse Zaken
Tweede Kamer der Staten-Generaal

Per email aan cie.vj@tweedekamer.nl

DATUM 2 maart 2012
ONS KENMERK z2011-01054/z2012-00164
CONTACTPERSOON Koosje Verhaar / Anne-Marije Fontein
070-8888528

UW BRIEF VAN

UW KENMERK

ONDERWERP EU voorstel: Herziening EU-wetgeving bescherming persoonsgegevens COM (2012) 10 en COM (2012) 11

Geachte leden,

Op 25 januari 2012 heeft de Europese Commissie een voorstel gedaan voor herziening van de EU-wetgeving ten aanzien van de bescherming van persoonsgegevens. Mede naar aanleiding van het verzoek van de leden van de vaste Commissie voor Veiligheid en Justitie informeer ik u graag over het standpunt op hoofdlijnen van het College bescherming persoonsgegevens (CBP) ten aanzien van een aantal essentiële aspecten van het voorstel van de Europese Commissie (hierna: de Commissie).

Het voorstel omvat een ontwerpverordening ter vervanging van de huidige richtlijn gegevensbescherming 95/46/EG en een ontwerprichtlijn die een specifieke regeling bevat voor gegevensbescherming in de rechtshandhavingssector. Deze komt in de plaats van het huidige kaderbesluit gegevensbescherming derde pijler 2008/977/JBZ.

Het CBP is verheugd over het feit dat de Commissie dit voorstel heeft gedaan. De huidige richtlijn gegevensbescherming dateert van voor het internettijdperk, te weten uit 1995. Technologische ontwikkelingen en de schaal waarop gegevensverwerking plaatsvindt hebben sinds die tijd een enorme vlucht genomen. De huidige richtlijn voldoet niet meer aan de behoeften van de hedendaagse geglobaliseerde informatiemaatschappij. Op grond van de huidige richtlijn blijven er te grote verschillen tussen de lidstaten op het terrein van gegevensbescherming. Deze verschillen worden steeds prangender in een tijdperk waarin (online) gegevensverwerking in toenemende mate een grensoverschrijdend karakter heeft.

Artikel 8 van het Handvest van de grondrechten van de Europese Unie bepaalt dat bescherming van persoonsgegevens een grondrecht is. Artikel 16 van het Verdrag betreffende de werking van de Europese Unie, geïntroduceerd door het Verdrag van Lissabon in 2007, stelt dat iedereen recht heeft op

bescherming van zijn persoonsgegevens en dat Europese wetgeving over bescherming van persoonsgegevens moet worden vastgesteld. Als gevolg van de opheffing van de pijlerstructuur geldt de bepaling ook voor politie en justitie, al kunnen voor die sector op grond van Verklaring 21 bij het Verdrag van Lissabon specifieke voorschriften worden opgesteld.

Tot slot is het belangrijk economische groei en innovatie te stimuleren en administratieve lasten te verlichten. Het huidige voorstel schrapt tot genoegen van het CBP veel administratieve plichten zoals de plicht om gegevensverwerkingen bij de toezichthouder te melden, en leidt tot minder fragmentatie in de EU. De Europese Commissie raamt dat dit pakket een jaarlijkse besparing van 2,3 miljard euro zal opleveren.

Het CBP acht dit voorstel van de Commissie van groot belang. De verordening behoudt de basisprincipes voor persoonsgegevensbescherming en verstevigt en verheldert deze op onderdelen. Zij draagt bij aan de versterking van de rechten van burgers van wie persoonsgegevens worden verwerkt. Het toestemmingsvereiste is versterkt. Daarnaast geldt dat burgers duidelijk en helder moeten worden geïnformeerd over het gebruik van hun gegevens en dat zij hun rechten afdoende moeten kunnen uitoefenen.

De verordening legt voorts een grotere verantwoordelijkheid bij bedrijven en organisaties die persoonsgegevens verwerken. Zij moeten ook kunnen aantonen dat zij persoonsgegevens adequaat beschermen. In het geval dat er sprake is van een datalek, moeten bedrijven dit zo spoedig mogelijk melden bij de nationale privacytoezichthouder.

In de conceptverordening staan duidelijke criteria voor de onafhankelijkheid van de privacytoezichthouders en hun onderzoeksbevoegdheden. Privacytoezichthouders hebben bijvoorbeeld het recht op informatie van bedrijven en organisaties en moeten toegang kunnen krijgen tot hun panden. Ook krijgen de toezichthouders geharmoniseerde en krachtige handhavingsbevoegdheden, inclusief een boetebevoegdheid.

Het uitgangspunt van de herzieningsoperatie voor het wetgevend pakket voor gegevensbescherming zoals ingezet door de Europese Commissie was om te komen tot één alomvattend rechtskader. Het feit dat is gekozen voor meerdere instrumenten doet hieraan in beginsel niets aan af zolang het einddoel – het verzekeren van een hoog gegevensbeschermingsniveau voor de Europese burger – behouden blijft. De tekst van de algemene verordening en de richtlijn voor het terrein van politie en justitie lopen op een aantal essentiële punten echter behoorlijk uiteen, waardoor de alomvattendheid van het wetgevend pakket in gevaar komt.

In de bijlage vindt u de visie van het CBP ten aanzien van een aantal hoofdpunten van het Commissievoorstel. Met het oog op de onderhandelingen over het door de Commissie voorgestelde pakket vraagt het CBP in het bijzonder aandacht voor de volgende punten:

DATUM 2 maart 2012
ONS KENMERK z2011-01054/z2012-00164

1. Toestemming

De verordening versterkt op een aantal essentiële punten de rechten van betrokkenen. Zo is het toestemmingsvereiste nader uitgewerkt. De definitie van toestemming in artikel 4 is aangescherpt en artikel 7 geeft een nadere uitwerking van de voorwaarden waaronder toestemming mogelijk is. Artikel 4, onder 8 van de verordening stelt dat de toestemming "expliciet" dient te zijn. Dit houdt in, zoals ook overweging 25 stelt, dat stilzwijgende instemming of toestemming zonder actie van de burger geen rechtsgeldige toestemming is. Zoals vastgelegd in artikel 7 moet de toestemming voor de gegevensverwerking ook te onderscheiden zijn van toestemming die ziet op een ander onderwerp. Te denken valt aan de toestemming voor de algemene voorwaarden, die dus onderscheiden dient te zijn van de toestemming voor de gegevensverwerking. Deze versterking van de toestemming past in de door de Tweede Kamer consistent ingezette lijn waarbij toestemming als grondslag voor verwerking van persoonsgegevens noodzakelijk wordt geacht. Dit betreft bijvoorbeeld vragen van de Tweede Kamer inzake de verzameling van wifi-gegevens door Google en de cookiewetgeving. Mede in het licht hiervan acht het CBP het van groot belang voor het versterken van de rechten van de burger dat de door de ontwerpverordening gegarandeerde versterking van het toestemmingsvereiste behouden blijft.

2. Lastenverlichting en nalevingskosten

De voorafgaande administratieve plichten voortvloeiend uit de huidige richtlijn gegevensbescherming, zoals de melding van verwerking van persoonsgegevens, zijn vrijwel geheel geschrapt. Tevens heeft de één-loket-functie ervoor gezorgd dat bedrijven in beginsel met één nationale toezichthouder te maken hebben in de EU. Dit voorkomt fragmentatie, draagt bij aan administratieve lastenverlichting en stimuleert innovatie en economische groei. Het CBP is hierover verheugd.
De tegenpool van het schrappen van voorafgaande administratieve plichten is dat de verantwoordelijkheid van de verantwoordelijke dient te worden versterkt. Persoonsgegevens zijn immers 'het nieuwe goud', getuige bijvoorbeeld de beurswaarde van internetbedrijven die gratis diensten aanbieden en zo veel persoonsgegevens verzamelen. Deze "accountability", of "responsibility", zoals vastgelegd in artikel 22 van de verordening, betekent dat bedrijven dienen te investeren in een zorgvuldige omgang met persoonsgegevens, waarbij zij vertrouwen wekken en rekenschap kunnen geven aan hun stakeholders. Dit vertaalt zich in plichten als het zorgdragen voor 'privacy by design', het doen van 'privacy impact assessments' en het garanderen van adequate beveiliging. Dit moet uiteraard 'schaalbaar' worden geïmplementeerd, naar de mate van risico van de gegevensverwerking. Het belang hiervan is door regering en Tweede Kamer onderschreven, getuige de afspraak in het regeerakkoord om de informatieveiligheid te verbeteren en voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens bij de voorbereiding nadrukkelijk te toetsen aan effectiviteit en getuige de kamerbreed aangenomen motie Nicolaï (Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 31) waarin de regering wordt opgeroepen in haar eigen systemen voor de verwerking van persoonsgegevens 'privacy enhancing technologies' toe te passen.

Dergelijke verplichtingen kunnen daarmee niet worden gezien als nalevingskosten die de lasten voor verantwoordelijken verzwaren. Dit zijn investeringen die verantwoordelijken van begin af aan in hun business plan dienen te betrekken, bij gebreke waarvan zij grote risico's lopen op hoge kosten en

ernstige imagoschade. Organisaties die 'accountability' niet van meet af aan meenemen zijn zogezegd 'penny wise pound foolish'. Ook hier geldt: De kost gaat voor de baat uit.

3. Extraterritoriale werking van buitenlandse regelgeving

De regelgeving van sommige landen buiten de EU leidt er soms toe dat Europese verantwoordelijken gedwongen worden om persoonsgegevens te verstrekken aan de autoriteiten van deze landen, in strijd met het EU-grondrecht op bescherming van persoonsgegevens. Dit heeft het afgelopen decennium plaatsgevonden ondanks het feit dat de huidige richtlijn regels stelt ten aanzien van de doorgifte van persoonsgegevens buiten de EU (zie bijvoorbeeld de verstrekking van passagiersgegevens en financiële gegevens aan de Amerikaanse autoriteiten). Om die reden zou de verordening hiertoe een duidelijker regel moeten stellen. Een eerdere – openbaar geworden – conceptversie van de verordening bevatte zo'n bepaling in artikel 42:
"No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any matter, without prejudice to an mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State".
Het CBP dringt er op aan om een dergelijke bepaling weer in de tekst van de verordening op te nemen. Bij gebreke daarvan worden Europese bedrijven klem gezet tussen de vereisten van derde landen – inclusief dreigende sancties – en hun verplichtingen op grond van de Europese privacywetgeving.

4. Eénloketfunctie of one-stop-shop

Artikel 51 lid 2 van de conceptverordening bepaalt dat de toezichthouder van de lidstaat waar de hoofdvestiging [main establishment] van de verantwoordelijke zich bevindt, bevoegd is om toezicht te houden op de verwerkingen van die verantwoordelijke in alle lidstaten. Het doel van deze bepaling is vooral het aanwijzen van een 'lead authority' binnen de EU. Het principe van de one-stop-shop is zeer belangrijk; het draagt bij aan de noodzakelijke consistentie en eenduidigheid van het Europese dataprotectieregime, wat de effectiviteit ten goede komt. Bovendien biedt dit principe voor (grote) bedrijven een goede oplossing; zij hebben in beginsel nog maar met één nationale autoriteit te maken.

Zonder nadere spelregels is deze bepaling echter onvoldoende duidelijk. In de praktijk kan niet altijd zonder meer worden bepaald welke vestiging de hoofdvestiging is. De criteria op basis waarvan vast komt te staan welke toezichthouder bevoegd is en hoe de onderlinge besluitvorming plaatsvindt, moeten dus eenduidiger worden geformuleerd. De verordening zou voorts moeten bepalen dat indien de hoofdvestiging niet eenduidig kan worden vastgesteld de European Data Protection Board (EDPB), het orgaan waarin alle toezichthouders deelnemen, de bevoegdheid krijgt om te bepalen welke autoriteit de leiding neemt bij een zaak en hoe de onderlinge rolverdeling met andere nationale toezichthouders is.

5. Uitzonderingen van verplichtingen voor bedrijven met minder dan 250 fte

In de ontwerpverordening worden bedrijven met minder dan 250 werknemers vrijgesteld van een aantal verplichtingen. Hoezeer het ook juist is om de verplichtingen die voortvloeien uit de verordening ten opzichte van het midden- en kleinbedrijf te matigen, het gekozen criterium waarop de uitzonderingen gebaseerd zijn, is onjuist. Gegeven het fundamentele recht op bescherming van

persoonsgegevens dient niet de grootte van een bedrijf, maar de mate van risico verbonden aan de verwerking bepalend te zijn als besloten wordt om uitzonderingen te creëren. In de informatiemaatschappij kunnen vaak juist bedrijven met slechts enkele medewerkers voor de bescherming van persoonsgegevens zeer risicovolle verwerkingen doen (denk aan de apps-industrie).

6. Verhouding principes gegevensbescherming verordening - richtlijn

Zoals in de inleiding al is genoemd maakt het CBP zich zorgen over de samenhang tussen de verordening en de richtlijn gegevensbescherming in de rechtshandhavingssector. Deze samenhang dient te worden gewaarborgd en op een aantal punten fors te worden versterkt. Dat is in de eerste plaats het geval voor de algemene beginselen voor gegevenswerking. In het bijzonder begrippen als de rechtmatigheid van de verwerking, doelbinding, accuratesse van gegevens, en de noodzaak tot het stellen van heldere bewaartermijn ("niet langer dan strikt noodzakelijk") dienen zowel in de verordening als de richtlijn te worden opgenomen. Daarnaast dienen ook de verplichtingen die van toepassing zijn op de verantwoordelijke en bewerker in beide instrumenten gelijkgeschakeld te worden, waaronder de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor privacy by design. Tot slot dienen de bevoegdheden die worden toegekend aan toezichthouders voor de gegevensbescherming gelijk te worden getrokken.

7. Toepasselijkheid richtlijn ten aanzien van nationale verwerkingen

In tegenstelling tot het kaderbesluit derde pijler zal de richtlijn wél van toepassing zijn op verwerkingen in een strikt nationale context. Het CBP juicht deze keuze van de Commissie toe. De keuze die in het verleden is gemaakt om de geharmoniseerde regels voor gegevensbescherming alleen van toepassing te verklaren op grensoverschrijdende verwerkingen is onlogisch. Het is immers niet bij voorbaat vast te stellen of door de rechtshandhavingsautoriteiten verwerkte gegevens op enig moment grensoverschrijdend zullen worden verwerkt. Het CBP hecht er dan ook aan dat de brede toepasselijkheid van de richtlijn tijdens de onderhandelingen behouden blijft.

Ook voor het CBP geldt dat wij pas enkele weken beschikken over de ontwerpverordening en de ontwerprichtlijn. Het kan dus zijn dat bij nadere studie nieuwe zaken opkomen dan wel dat wij later nuances aanbrengen. Wij zullen u hierover graag informeren. Een compleet overzicht van de hoofdpunten van het voorlopige CBP-standpunt, inclusief de in deze brief uitgelichte, vindt u in de bijlage.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Mr. J. Kohnstamm

Voorzitter College bescherming persoonsgegevens

Bijlage: 1

HOOFDPUNTEN VOORLOPIG CBP-STANDPUNT TAV VOORSTEL VAN DE EUROPESE COMMISSIE VOOR HERZIENING EU-WETGEVING BESCHERMING PERSOONSGEGEVENS COM(2012) 10 en COM(2012) 11
2 MAART 2012

Ten aanzien van de *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012)11*, hierna te noemen "ontwerpverordening"

1. Algemeen oordeel positief

Het College bescherming persoonsgegvens (CBP) staat zeer positief tegen over de harmonisatie van de privacyregelgeving door middel van de ontwerpverordening. Het 'level playing field' dat hiermee in Europa wordt gecreëerd heeft een hogere prioriteit dan het honoreren van culturele verschillen tussen de lidstaten. Ook overigens is het CBP enthousiast over de inhoud van de verordening, maar meent dat op verschillende punten verbetering in de voorstellen kan en moet worden aangebracht.

2. Lastenverlichting en nalevingskosten

De administratieve plichten voortvloeiend uit de huidige richtlijn gegevensbescherming, zoals de melding van verwerking van persoonsgegevens, zijn vrijwel geheel geschrapt. Tevens heeft de één-loket-functie (zie hieronder) ervoor gezorgd dat bedrijven in beginsel met één nationale toezichthouder te maken hebben in de Europese Unie (EU). Dit voorkomt fragmentatie, draagt bij aan lastenverlichting en stimuleert innovatie en economische groei. De Europese Commissie raamt dat dit pakket een jaarlijkse besparing van 2,3 miljard euro zal opleveren. Het CBP is hierover verheugd.

De tegenpool van minder voorafgaande administratieve plichten is dat de verantwoordelijkheid van de verantwoordelijke dient te worden versterkt. Persoonsgegevens zijn immers "het nieuwe goud", getuige bijvoorbeeld de beurswaarde van internetbedrijven die gratis diensten aanbieden en zo veel persoonsgegevens verzamelen. Deze "accountability", of "responsibility", zoals vastgelegd in artikel 22 van de verordening, betekent dat bedrijven dienen te investeren in een zorgvuldige omgang met persoonsgegevens, waarbij zij vertrouwen wekken en rekenschap kunnen geven aan hun stakeholders. Dit vertaalt zich in moderne plichten als het zorgdragen voor privacy by design, het doen van privacy impact assessments en garanderen van adequate beveiliging. Dit alles dient uiteraard 'schaalbaar' te worden geïmplementeerd, naar de mate van risico van de gegevensverwerking. Het belang hiervan is door regering en Tweede Kamer onderschreven, getuige de afspraak in het regeerakkoord om de informatieveiligheid te verbeteren en voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens bij de voorbereiding nadrukkelijk te toetsen aan effectiviteit en getuige de kamerbreed aangenomen motie Nicolaï (Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 31) waarin de regering wordt opgeroepen in haar eigen systemen voor de verwerking van persoonsgegevens privacy enhancing technologies toe te passen.

Dergelijke moderne verplichtingen kunnen daarmee niet worden gezien als nalevingskosten die de lasten voor verantwoordelijken verzwaren. Dit zijn investeringen die verantwoordelijken van

begin af aan in hun business plan dienen mee te nemen, bij gebreke waarvan zij grote risico's lopen op hoge kosten en ernstige imagoschade. Organisaties die "accountability" niet van meet af aan meenemen zijn zogezegd "penny wise pound foolish". Ook hier geldt: De kost gaat voor de baat uit.

3. Uitdrukkelijke toestemming (artikel 4 en artikel 7)

De ontwerpverordening versterkt op een aantal essentiële punten de rechten van betrokkenen. Zo is het toestemmingsvereiste nader uitgewerkt. De definitie van toestemming in artikel 4 is aangescherpt en artikel 7 geeft een nadere uitwerking van de voorwaarden waaronder toestemming mogelijk is. Artikel 4, onder 8 van de verordening stelt dat de toestemming "expliciet" dient te zijn. Dit houdt in, zoals ook overweging 25 stelt, dat stilzwijgende instemming of toestemming zonder actie van de burger geen rechtsgeldige toestemming is. Zoals vastgelegd in artikel 7 moet de toestemming voor de gegevensverwerking ook te onderscheiden zijn van toestemming die ziet op een ander onderwerp. Te denken valt aan de toestemming voor de algemene voorwaarden, die dus onderscheiden dient te zijn van de toestemming voor de gegevensverwerking. Deze versterking van de toestemming past in de door de Tweede Kamer consistent ingezette lijn waarbij toestemming als grondslag voor verwerking van persoonsgegevens noodzakelijk wordt geacht. Dit betreft bijvoorbeeld de verzameling van wifi-gegevens door Google en de cookiewetgeving. Mede in het licht daarvan acht het CBP het van groot belang voor het versterken van de rechten van de burger dat de door de ontwerpverordening gegarandeerde versterking van het toestemmingsvereiste blijft behouden.

4. Definitie persoonsgegevens (artikel 4)

De definitie van betrokkene en persoonsgegevens zoals verwoord in artikel 4 en overweging 24 gaat uit van het principe dat er pas sprake is van een betrokkene, als de natuurlijke persoon daadwerkelijk (direct of indirect) *geïdentificeerd* kan worden. Er is sprake van persoonsgegevens als gegevens betrekking hebben op de geïdentificeerde natuurlijke persoon.

Ook als het niet mogelijk is om een naam, adres of woonplaats te verbinden aan de gegevens (bijvoorbeeld in het geval van profiling d.m.v. algoritmen), kan het verwerken van gegevens over een *geïndividualiseerd* persoon echter vergaande maatschappelijke consequenties hebben. Het is daarom van belang dat ook indien iemand geïndividualiseerd oftewel onderscheiden kan worden de principes en waarborgen van de verordening gelden en dat betrokkenen in beginsel in staat worden gesteld om inzicht te hebben in en zeggenschap te hebben over de beslissingen die aan de hand van die gegevens over hen worden genomen. In het licht van de huidige en toekomstige technologische ontwikkelingen brengt de individualiseerbaarheid mee dat er op basis van die gegevens beslissingen over een persoon kunnen worden genomen die hem raken in het maatschappelijk verkeer. Door de voortschrijding in de techniek volstaan unieke nummers en gegevens die herleidbaar zijn tot een computer of een apparaat immers om iemand te kunnen onderscheiden van anderen.

Het CBP pleit er daarom voor om in de toelichting toe te voegen dat er ook sprake is van identificeerbaarheid van een natuurlijke persoon indien op grond van gegevens een *individu* kan worden *onderscheiden* van anderen ('singled out'). In de toelichting zou vervolgens opgenomen moeten worden dat gegevens die het mogelijk maken een persoon van anderen te onderscheiden, persoonsgegevens zijn als deze persoon op basis daarvan in het maatschappelijk verkeer anders kan worden behandeld of beoordeeld.

5. Doelbinding (artikel 5, onder b en artikel 6, vierde lid)

Artikel 6, vierde lid van de ontwerpverordening doorbreekt in latere fases van gegevensverwerking het principe van doelbinding. In de Verordening wordt verder gebruik bij onverenigbaarheid met het eerdere doel waarvoor de gegevens zijn verzameld mogelijk gemaakt als er een andere dan de oorspronkelijke grondslag kan worden gevonden in de noodzakelijkheid voor de uitvoering van een overeenkomst, wetgeving, vitaal belang, of de uitvoering van een taak in het publieke belang. Het CBP heeft tegen deze bepaling in ieder geval in de huidige vorm ernstige bedenkingen, omdat op deze wijze de kern van het doelbindingsprincipe onderuit wordt gehaald.

Doelbinding is één van de belangrijkste principes van gegevensbescherming. Dit betekent dat een precies doel moet worden aangegeven voor de verwerking van gegevens en dat degenen die gegevens verwerkt, zich moet houden aan het doel waarvoor hij de gegevens (kenbaar)heeft verzameld. Deze scheiding van domeinen waarbinnen gegevens gebruikt mogen worden, vormt, tezamen met de plicht enkel noodzakelijke gegevens te verwerken, de basis van de bescherming van persoonsgegevens. De Staatscommissie Grondwet (2010/2011) adviseerde (in navolging van de conventie 108 van de Raad van Europa) daarom zelfs om in een grondwettelijke bepaling over het recht op de bescherming van persoonsgegevens dit doelbindingsprincipe vast te leggen.

6. Overheid

In de ontwerpverordening zijn voor de overheid afwijkende bepalingen opgenomen. Deze bepalingen zien op het gebruik van bijzondere persoonsgegevens, onverenigbaar gebruik, privacy impact assessments, en op de mogelijkheid van de overheid om beperkingen aan te brengen op de principes en rechten voor bepaalde belangen. Door deze bepalingen wordt afgeweken van de doelstelling voor een nieuw Europees rechtelijk privacy kader, mogelijk gemaakt door het verdrag van Lissabon, te weten om te komen tot een alomvattend privacykader ("comprehensive framework"): een normenstelsel dat én voor de publieke en én voor de private sector zou gelden. Zonder dat allesomvattende privacy kader ontstaat onzekerheid bij burgers en verantwoordelijke instanties over welke normen waarom wel of niet in welke situaties voor hen van toepassing zijn. Het CBP meent dat dit niet wenselijk is.

7. Direct marketing (artikel 19, tweede lid)

Artikel 19, tweede lid van de ontwerpverordening voorziet in een recht van verzet ten aanzien van de verwerking van gegevens voor direct marketing. Dit is in overeenstemming met het huidige regime onder de Europese privacyrichtlijn en de Wet bescherming persoonsgegevens. In de Europese e-privacy regelgeving zijn ten aanzien van toestemming specifieke bepalingen opgenomen. Zo dient er in de regel toestemming te worden gevraagd voor direct marketing, en dient er ondubbelzinnige toestemming te zijn voor online behavioural advertising. Het CBP hecht eraan te onderstrepen dat deze bepalingen uit de e-privacy regelgeving onverkort van toepassing blijven, zoals ook vastgelegd in artikel 89 van de ontwerpverordening.

8. Extraterritoriale werking van buitenlandse regelgeving

De regelgeving van sommige landen buiten de EU leidt er soms toe dat Europese verantwoordelijken gedwongen worden om persoonsgegevens te verstrekken aan de autoriteiten van deze landen, in strijd met het EU grondrecht op bescherming van persoonsgegevens. Dit heeft het afgelopen decennium plaatsgevonden ondanks het feit dat de huidige richtlijn regels stelt ten aanzien van de doorgifte van persoonsgegevens buiten de EU (bijvoorbeeld de verstrekking van passagiersgegevens en financiële gegevens aan de Amerikaanse autoriteiten). Om die reden zou de verordening hiertoe een duidelijker regel moeten stellen. Een eerdere – openbaar geworden – conceptversie van de verordening bevatte zo'n bepaling in artikel 42:

"No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any matter, without prejudice to an mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State".
Het CBP dringt er op aan om een dergelijke bepaling weer in de tekst van de verordening op te nemen. Bij gebreke daarvan worden Europese bedrijven klem gezet tussen de vereisten van derde landen – inclusief dreigende sancties – en hun verplichtingen op grond van het Europese recht op gegevensbescherming.

9. Eén-loket-functie of one-stop-shop-bepaling (artikel 51)

Artikel 51, tweede lid van de ontwerpverordening bepaalt dat de toezichthouder van de lidstaat waar de hoofdvestiging [main establishment] van de verantwoordelijke voor een bepaalde verwerking zich bevindt, bevoegd is om toezicht te houden op die verwerking van de verantwoordelijke in alle lidstaten. Het doel van deze bepaling is met name het aanwijzen van een "lead authority" binnen de EU.

Het principe van de one-stop-shop is zeer belangrijk; het draagt bij aan de noodzakelijke consistentie en eenduidigheid van het Europese dataprotectieregime, wat de effectiviteit ten goede komt. Bovendien biedt dit principe voor (grote) bedrijven een goede oplossing; zij hebben in beginsel nog maar met één nationale toezichthouder te maken, hoezeer laatstgenoemde – achter de schermen - ook in overleg met andere betrokken toezichthouders tot een oordeel over een en ander moet komen.

Zonder nadere spelregels is deze bepaling echter onvoldoende duidelijk. In de praktijk kan niet altijd zonder meer bepaald worden welke vestiging de hoofdvestiging is. Bovendien spelen ook andere zaken een rol bij de vraag welke toezichthoudertoezichthouders (grote) betrokkenheid hebben bij het toezicht, zoals de aanwezigheid van veel betrokkenen in hun land, het aantal klachten, etc. Tevens zal er regelmatig sprake zijn van aanpalende nationale wetgeving. Ten aanzien hiervan is onduidelijk hoe dit aangrijpt op de ontwerpverordening en hoe het toezicht daarop zou moeten plaatsvinden.

De criteria op basis waarvan vast komt te staan welke toezichthouder bevoegd is en hoe de onderlinge besluitvorming plaatsvindt, moeten dus eenduidiger worden geformuleerd. De verordening zou voorts moeten bepalen dat indien de hoofdvestiging niet eenduidig kan worden vastgesteld de European Data Protection Board (EDPB), het orgaan waarin alle toezichthouders deelnemen, de bevoegdheid krijgt om te bepalen welke toezichthouder de leiding neemt bij een zaak en hoe de onderlinge rolverdeling met andere toezichthouders is.

10. Rechtsgang voor burgers (artikelen 73-75)

Burgers zullen zich op basis van het voorgestelde artikel 73 van de ontwerpverordening– weliswaar via iedere willekeurige toezichthouder - tot in potentie 27 verschillende toezichthouders moeten wenden. Dit is vooral een probleem indien een burger op grond van artikel 74 beroep aantekent tegen een besluit van een toezichthouder uit een ander land. Bekendheid van de belanghebbende met het feit dat er een besluit is genomen en met de procedures en termijnen rondom de buitenlandse rechtsgang zijn dan noodzakelijk. Daarnaast zal de toezichthouder van het land waar de belanghebbende woont deze moeten vertegenwoordigen, terwijl deze toezichthouder mogelijk nauw betrokken is geweest bij de besluitvorming in de betreffende zaak. Dit belemmert een goede rechtsgang. Een betere oplossing zou zijn dat de toezichthouder van het land van de belanghebbende de uitspraak moet

volgen, waarna de belanghebbende een zaak aanhangig kan maken tegen zijn eigen toezichthouder.

Verder is het belangrijk dat de burger zijn zaak aanhangig moet kunnen maken bij een rechter in het land waar hij/zij woont, conform de geldende regels van rechtsvordering. De keuze die artikel 75 lid 2 biedt heeft het nadeel dat er procedures over dezelfde kwestie aanhangig kunnen worden gemaakt bij rechters in verschillende lidstaten.
Alhoewel er bepalingen zijn opgenomen (artikel 76 lid 3 en 4) die erop zijn gericht te voorkomen dat in zulke gevallen tegenstrijdige uitspraken worden gedaan, ontstaat mogelijk onhelderheid en tegenstrijdigheid in de rechtspraak, met als gevolg dat de rechtsbescherming van de burger in gevaar komt.

11. Uitzonderingen van verplichtingen voor bedrijven met minder dan 250 fte

In de ontwerpverordening worden bedrijven met minder dan 250 werknemers vrijgesteld van een aantal verplichtingen. Hoezeer het ook juist is om de verplichtingen die voortvloeien uit de verordening ten opzichte van het midden- en kleinbedrijf te matigen, het gekozen criterium waarop de uitzonderingen gebaseerd zijn, is onjuist. Gegeven het fundamentele recht op bescherming van persoonsgegevens dient niet de grootte van een bedrijf, maar de mate van risico verbonden aan de verwerking bepalend te zijn, als besloten wordt om uitzonderingen te creëren. In de informatiemaatschappij kunnen bedrijven met slechts enkele medewerkers juist vaak voor de bescherming van persoonsgegevens zeer risicovolle verwerkingen doen (denk aan de apps-industrie).

12. Verplichtingen voor niet in de EU gevestigde verantwoordelijken (artikel 25)

Buiten de EU gevestigde verantwoordelijken die goederen of diensten in de EU aanbieden of gedrag van burgers in de EU monitoren, dienen op grond van artikel 25 van de ontwerpverordening een verantwoordelijke in de EU aan te wijzen. Hierbij wordt een uitzondering geformuleerd. Indien deze verantwoordelijke minder dan 250 fte's heeft dan wel gevestigd is in een land met een passend beschermingsniveau, hoeft geen verplichte vertegenwoordiger te worden aangewezen. Het CBP meent dat dit een groot risico in zich draagt doordat (kleinere) buitenlandse partijen op gronden die niet relevant zijn voor de bescherming van persoonsgegevens zich aan toezicht en sanctionering binnen de EU kunnen onttrekken.

13. Advisering EDPB bij regelgeving ten aanzien van persoonsgegevens

De rol van de Europese Commissie bij het opstellen van gedelegeerde regelgeving en de invulling van uitvoeringsmaatregelen is deels onmisbaar. In de ontwerpverordening ontbreekt echter een bepaling waardoor de Europese Commissie verplicht wordt om daarbij het advies in te winnen bij de EDPB over voorgenomen gedelegeerde regelgeving of invulling van uitvoeringsmaatregelen. Ook dient de Europese Commissie advies in te winnen bij de EDPB over andere voorgenomen wet- en regelgeving voor de Unie. Het is onevenwichtig om lidstaten te verplichten bij voorgenomen wet- en regelgeving advies in te winnen bij de nationale toezichthouder zonder een vergelijkbare verplichting op te leggen in de richting van de Europese Commissie om in voorkomend geval advies in te winnen van de EDPB.

14. Rol Europese Commissie bij besluiten in individuele casusposities (artikel 59)

Het CBP heeft grote moeite met de rol van de Europese Commissie bij het vaststellen van de juiste interpretatie van de verordening (artikel 59). Het feit dat de Commissie het recht heeft om een voorgenomen maatregel in individuele casusposities te schorsen en op basis van artikel 62 een 'implementing act' te nemen, geeft aanleiding tot zorg over de - door de verordening juist

beoogde (zie artikel 47)- onafhankelijkheid van de toezichthouders. Als de Europese Commissie zich niet kan verenigen met het standpunt van de EDPB en/of het op grond daarvan ingenomen standpunt van de lead toezichthouder, zou zij de voorgenomen maatregel moeten kunnen voorleggen aan een rechterlijke instantie, bijvoorbeeld het Europese Hof van Justitie; het laatste woord over de interpretatie van de verordening – zeker in concrete gevallen – dient niet door een bestuursorgaan maar door een rechterlijke instantie te worden uitgesproken.

15. Risico verschuiving naar ex-ante activiteiten

Het CBP constateert in de ontwerpverordening een verschuiving van ex post naar ex ante werkzaamheden voor de nationale toezichthouders. Uit enkele bepalingen volgt zelfs dat de toezichthouder op de stoel van de verantwoordelijke moet gaan zitten doordat hij dient te bepalen op welke wijze de verantwoordelijke het product of de dienst in moet richten om rechtmatig persoonsgegevens te kunnen verwerken (onder meer ten gevolge van de uitkomst van een voorafgaand onderzoek door de toezichthouder, zie artikel 34). De rol van de toezichthouder wordt daardoor een onzuivere: de combinatie van het zijn van 'adviseur' van verantwoordelijken die zich op een kritiek moment kan ontpoppen tot een met ingrijpende bevoegdheden voorziene handhavende autoriteit is niet wenselijk.

16. Toename kosten toezicht en subsidiariteit

Ook los van het vorenstaande is in de ontwerpverordening sprake van aanzienlijke uitbreiding van verplichtingen en bevoegdheden van de toezichthouder. Te denken valt aan de verschillende boetebevoegdheden en de introductie van de algemene meldplicht datalekken. Daarnaast dienen toezichthouders alle zaken met enige internationale dimensie via de European Data Protection Board te laten verlopen, ook indien deze naar tevredenheid zijn afgehandeld tussen betrokken toezichthouders. Dit roept de vraag op naar de subsidiariteit.

Naast deze extra taken zal door de invoering van de one-stop- shop voor bedrijven de druk op sommige toezichthouders niet onaanzienlijk toenemen. Explicitering van bepalingen omtrent minimumbudget van nationale toezichthouders gerelateerd aan onder meer het aantal inwoners, het bruto nationaal product en het aantal hoofdvestigingen van internationaal opererende bedrijven is onontbeerlijk, bij gebreke waarvan de beoogde werking van de verordening zal falen.

17. Discretionaire bevoegdheden voor nationale toezichthouders

De ontwerpverordening brengt met zich mee dat het CBP verplicht kan worden om onderzoek te doen naar de gegevensverwerking door een bepaalde verantwoordelijke. Dit kan zijn op verzoek van een andere toezichthouder (op basis van artikel 55) of op verzoek van een betrokkene. De laatste kan de toezichthouder op basis van artikel 74 lid 2 door de rechter laten verplichten actie te nemen naar aanleiding van een klacht. Het CBP pleit er voor om in de verordening de discretionaire bevoegdheid van de toezichthouder in dit verband (en daarmee respect voor de nationale rechtsorde) te garanderen.

VOORLOPIG CBP-STANDPUNT ten aanzien van *de Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10,* hierna te noemen "de richtlijn"

1. Samenhang tussen verordening en richtlijn

Het uitgangspunt van de herzieningsoperatie voor het wetgevend pakket voor gegevensbescherming was om te komen tot één alomvattend rechtskader. Het feit dat is gekozen voor meerdere instrumenten doet hier in beginsel niets aan af zolang het einddoel – het verzekeren van een hoog gegevensbeschermingsniveau voor de Europese burger – behouden blijft.

De tekst van de richtlijn en de verordening lopen op een aantal hierna genoemde essentiële punten echter behoorlijk uiteen, waardoor de alomvattendheid van het wetgevend pakket in gevaar komt. Een zeker onderscheid in de regels gesteld in de verordening en richtlijn is begrijpelijk, zeker gelet op het specifieke karakter van de politie- en justitiesector. Het CBP dringt er echter op aan dat tijdens de onderhandelingen scherp in de gaten wordt gehouden dat de samenhang tussen beide instrumenten gewaarborgd wordt en op een aantal punten fors worden versterkt. Dat is in de eerste plaats het geval voor de algemene beginselen voor gegevenswerking. In het bijzonder begrippen als de rechtmatigheid van de verwerking, doelbinding, accuratesse van gegevens, en de noodzaak tot het stellen van heldere bewaartermijn ("niet langer dan strikt noodzakelijk") dienen zowel in de verordening als de richtlijn te worden opgenomen. Daarnaast dienen ook de verplichtingen die van toepassing zijn op de verantwoordelijke en bewerker in beide instrumenten gelijkgeschakeld te worden, waaronder de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor privacy by design. Tot slot dienen de bevoegdheden die worden toegekend gegevensbeschermingsautoriteiten gelijk getrokken te worden.

2. Toepasselijkheid richtlijn / nationale verwerkingen

In tegenstelling tot het kaderbesluit derde pijler zal de richtlijn wél van toepassing zijn op verwerkingen in een strikt nationale context. Het CBP juicht deze keuze van de Commissie toe. De keuze die in het verleden is gemaakt om de geharmoniseerde regels voor dataprotectie alleen van toepassing te verklaren op grensoverschrijdende verwerkingen is onlogisch. Het is immers niet bij voorbaat vast te stellen of door de rechtshandhavings-autoriteiten verwerkte gegevens op enig moment grensoverschrijdend zullen worden verwerkt. Het CBP hecht er dan ook aan dat de brede toepasselijkheid van de richtlijn tijdens de onderhandelingen behouden blijft.

3. Beperkingen aan verwerking van gegevens / codering

In de systematiek van de Wet politiegegevens zijn niet alle door de politie te verwerken gegevens zonder meer voor alle medewerkers toegankelijk. Afhankelijk van de aard van de gegevens en de verwerkingsgrondslag, is een hogere autorisatie vereist. Het CBP vindt dit een belangrijk uitgangspunt, dat ook in de Europese en internationale samenwerking gehandhaafd dient te blijven. Het zou dan ook graag zien dat beperkingen die op grond van nationale wetgeving aan de verwerking van gegevens zijn gesteld ook van toepassing blijven wanneer gegevens worden uitgewisseld naar andere EU-lidstaten, zoals wel al is geregeld voor doorgiften naar derde

landen en internationale organisaties (artikel 37). De richtlijn behoeft op dit punt aanvulling.

4. Onderscheid in categorieën en op basis van juistheid gegevens

Het CBP verwelkomt de keuze om een onderscheid te maken bij de verwerking van gegevens op grond van de positie van de betrokkene (verdachte, slachtoffer, veroordeelde, etc.) en op grond van de kwaliteit van de gegevens (harde en zachte gegevens). Tegelijkertijd betreurt het de beperkingen die aan dit onderscheid zijn gesteld door de toevoeging 'voor zover mogelijk' in zowel artikel 5 lid 1 als artikel 6 lid 1 en 2. Het is zeer goed mogelijk op dit punt een resultaatsverplichting te creëren, die ziet op het vereiste dát onderscheid wordt gemaakt tussen verschillende categorieën betrokkenen dan wel de kwaliteit van de gegevens, maar niet op welke wijze dat gebeurt.

Daarnaast wordt geconstateerd dat de verwerking van gegevens van personen die in geen van de genoemde categorieën vallen (artikel 5 lid 1 sub e) nogal ruim is geformuleerd. Het CBP dringt er op aan dat aan gegevensverwerking op dit punt nadere voorwaarden worden gesteld, met name op het gebied van maximale bewaartermijnen van gegevens in deze "restcategorie".

5. Verwerkingsverbod van gevoelige gegevens

Artikel 8 bevat een algemeen verwerkingsverbod voor gevoelige gegevens. Het CBP heeft hier met instemming kennis van genomen. Tegelijkertijd erkent hij ook dat er situaties zijn waarin het desalniettemin nodig kan zijn voor rechtshandhavingsautoriteiten om gevoelige gegevens te verwerken. De richtlijn zal dan ook in een aantal uitzonderingen op het verwerkingsverbod moeten voorzien. Een algemene uitzondering, zoals nu opgenomen in artikel 8 lid 2 sub a, gaat echter een stap te ver. De facto zou dit immers betekenen dat het verwerkingsverbod teniet kan worden gedaan door het introduceren van een wettelijke bepaling die – weliswaar met de introductie van waarborgen – het verwerken van gevoelige gegevens alsnog in algemene zin autoriseert.

Het CBP constateert daarnaast dat gevoelige gegevens die door betrokkenen actief openbaar worden gemaakt ondanks het verwerkingsverbod door de rechtshandhavingsautoriteiten mogen worden verwerkt op grond van artikel 8 lid 2 sub c. Dit is een vreemde redenering. Het enkele feit dat iemand zelf gegevens over bijvoorbeeld seksuele of politieke voorkeur openbaar maakt, betekent nog niet dat deze ook zonder meer door politie en justitie verwerkt zouden mogen worden. Het CBP adviseert dan ook deze bepaling aan te vullen met een noodzaakscriterium, door de toevoeging *'and the processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in article 1(1)'*.

6. Recht op informatie

Het recht op informatie voor betrokkenen is een belangrijk kernbegrip van het dataprotectierecht, dat zoveel mogelijk onaangetast dient te blijven. In de politie- en justitiesector kan er echter een gerechtvaardigd belang zijn om onder voorwaarden dit recht op informatie te beperken, bijvoorbeeld om lopende onderzoeken of operaties niet in gevaar te brengen. Artikel 11 bevat nu de mogelijkheid om algemene uitzonderingen op de informatieplicht vast te stellen, waarbij volledige categorieën van te verwerken gegevens structureel buiten de informatieplicht kunnen worden gebracht. Deze uitzonderingen zijn naar de zin van het CBP echter veel te ruim. Juist omdat er sprake is van inbreuken op een grondrecht dienen algemene beperkingen en uitzonderingen te worden vermeden. Het CBP hecht er dan ook sterk aan dat in artikel 11 wordt voorzien in een zaakspecifieke afweging door de verantwoordelijke en/of bewerker van de beperkingen op het recht op informatie. Een beperking zou dan bovendien alleen moeten zien op

die informatie die lopende onderzoeken of operaties kan ondermijnen en niet op alle informatie over de betrokkene.

Het CBP meent voorts dat uitzonderingen op de rechten van betrokkenen moeten voldoen aan het EU Handvest van de Grondrechten, het Europees Verdrag voor de Rechten van de Mens en jurisprudentie van het Hof van Justitie en het Europees Hof voor de Rechten van de Mens. Een overweging die dit stipuleerde was opgenomen in een conceptversie van de richtlijn, maar is in de definitieve versie verdwenen.

7. Doorgifte van gegevens naar landen buiten de EU of internationale organisaties

De richtlijn voorziet in artikel 35 in de mogelijkheid om gegevens door te geven naar derde landen of internationale organisaties, zelfs wanneer er geen oordeel is geveld over de adequaatheid van het beschermingsniveau aldaar. In zo'n geval zal de verantwoordelijke zelf moeten beoordelen in hoeverre het beschermingsniveau naar Europese normen adequaat is en welke aanvullende waarborgen nodig zijn. Deze aanvullende waarborgen dienen vervolgens in een juridisch bindend instrument te worden vastgelegd.

Het betreffende artikel bepaalt weliswaar dat het besluit naar aanleiding van de zelfbeoordeling moet worden gedocumenteerd, maar voorziet niet in handvatten om het beschermingsniveau van het land of de organisatie in kwestie te beoordelen. Het CBP hecht eraan dat hierover wel duidelijkheid wordt verstrekt, zowel uit oogpunt van kenbaarheid voor de verantwoordelijke als in het belang van het toezicht op deze risicovolle bepaling, door bijvoorbeeld de elementen op te nemen die nu zijn genoemd in artikel 25 lid 1 van richtlijn 95/46/EG.

Als laatste opmerking ten aanzien van de internationale doorgiften spreekt het CBP zijn zorg uit over de afwijkingen waarin is voorzien in artikel 36, en specifiek de afwijking als genoemd in sub d en sub e. Beide afwijkingen maken het mogelijk om in individuele gevallen data door te geven, ook wanneer er geen adequaat beschermingsniveau is vastgesteld en evenmin passende waarborgen overeen zijn gekomen. Daaraan is weliswaar een noodzakelijkheidsvereiste gekoppeld, maar bij gebreke van een definitie van noodzaak kan in de praktijk wellicht worden volstaan met de mededeling dat de betreffende doorgifte noodzakelijk is. Het CBP acht dit onwenselijk en dringt er op aan dat nadere voorwaarden worden gesteld aan deze bepalingen, zodat zij alleen in échte uitzonderingssituaties kunnen worden toegepast en niet als standaard grondslag voor doorgifte kunnen worden gebruikt.

8. Eén toezichthouder

Artikel 39 lid 2 voorziet in de mogelijkheid voor lidstaten om te bepalen dat de toezichthouder op de richtlijn en de verordening dezelfde kunnen zijn. Het CBP hecht eraan dat dit ook daadwerkelijk het geval is, wederom vanuit het oogpunt van consistentie. Daarnaast voorkomt de keuze voor één toezichthouder onderlinge (nationale) afstemming, bijvoorbeeld ter voorbereiding op vergaderingen van de vergaderingen van de EDPB.

9. European Data Protection Board (EDPB)

Het CBP constateert met tevredenheid dat de samenwerking in het kader van de EDPB zoals voorzien in de verordening zich ook uitstrekt naar de richtlijn. Dit is zeker van belang voor die onderdelen van de richtlijn die na inwerkingtreding nadere interpretatie dan wel afstemming behoeven, zoals de afgelopen jaren ook het geval is geweest voor richtlijn 95/46/EG. Ook de formele advisering op voorstellen in het kader van de Europese politie- en justitiesamenwerking

in strafzaken, waar de afgelopen jaren door de gezamenlijke Europese toezichthouders al een begin mee is gemaakt, wordt zeer verwelkomd.

Naast de reeds voorziene relatie tussen de EDPB en de Commissie op het terrein van de politie- en justitiesamenwerking, zou het CBP graag zien dat een vergelijkbare relatie ook gecreëerd wordt voor het Europees Parlement. Zeker in deze sector zou het Europees Parlement de mogelijkheid moeten krijgen om de EDPB in voorkomende gevallen om advies te vragen. De richtlijn sluit een dergelijke relatie momenteel overigens niet uit, maar het verdient de voorkeur een adviesrecht richting het Europees Parlement ook vast te leggen in de tekst.

10. Sanctiemogelijkheden

In de verordening is een uitgebreid sanctie-arsenaal voor de toezichthouder voorzien in het geval een verantwoordelijke of bewerker handelt in strijd met het dataprotectierecht. Voor de richtlijn blijven de sanctiebepalingen helaas beperkt tot de mededeling dat straffen moeten kunnen worden opgelegd die effectief, proportioneel en afschrikkend zijn. Hoewel een minder uitgebreide beschrijven van het sanctie-arsenaal in deze sector inherent is aan de keuze voor een richtlijn, alsook de specifieke eigenschappen van de diverse nationale rechtstelsels, meent het CBP dat verdergaande harmonisatie mogelijk en gewenst is. Op zijn minst zou aan artikel 55 moeten worden toegevoegd dat onder de mogelijke op te leggen straffen boetes moeten vallen, ongeacht of deze bestuurlijk dan wel strafrechtelijk van aard zijn.

11. Daadwerkelijk alomvattend rechtskader

Het CBP constateert dat ook na inwerkingtreding van de nieuwe richtlijn nog geen daadwerkelijk alomvattend rechtskader voor gegevensbescherming zal zijn gerealiseerd. Juist in de politie- en justitiesector bestaan veel specifieke regelingen, bijvoorbeeld ten aanzien van het Schengeninformatiesysteem of EU-Agentschappen als Europol en Eurojust. De Commissie beoogt, zoals vastgelegd in artikel 61 lid 2, om binnen drie jaar met voorstellen te komen om waar nodig deze specifieke regelingen aan te passen aan de richtlijn. Dit is echter niet genoeg. Artikel 61 zou het uitgangspunt moeten bevatten dat alle specifieke dataprotectieregelingen op het terrein van de voormalige derde pijler, alsook de verdragen tussen de Europese Unie en derde landen op dit terrein, op termijn onder de reikwijdte van de richtlijn dienen te worden gebracht. De enige te rechtvaardigen uitzondering is wanneer er momenteel sprake is van een hoger beschermingsniveau dan dat dat wordt geboden door de richtlijn. De inwerkingtreding van de richtlijn mag immers niet tot gevolg hebben dat een geldend beschermingsniveau naar beneden moet worden bijgesteld.