



Advies nr 35/2012 van 21 november 2012

Betreft: Advies uit eigen beweging over het ontwerp van Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens¹ (CO-A-2012-015)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verslag van de heer Willem Debeuckelaere, Voorzitter en de heer Verschuere, Ondervoorzitter;

Brengt op 21 november 2012 het volgend advies uit:

¹ COM (2012)11 final

I. INLEIDING

1. Onderwerp van onderhavig advies

1. Op 25 januari 2012 publiceerde de Europese Commissie (EC) haar voorstel voor een vernieuwd juridisch kader voor gegevensbescherming in de Europese Unie (Data Protection Package)². Deze nieuwe geplande beschermingsregeling bestaat uit twee wetgevende voorstellen:
 - een voorstel van Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens³ (hierna "het ontwerp van Verordening") en,
 - een voorstel van Richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens door de bevoegde overheden met het oog op preventie en opsporing, onderzoek en vervolging van strafrechtelijke inbreuken, of uitvoering van strafbepalingen en het vrije verkeer van deze gegevens ("het voorstel van Richtlijn")⁴.
2. De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna CBPL) heeft kennis genomen van deze voorstellen en heeft hierover gediscussieerd tijdens haar zittingen van 8 februari, 29 februari, 14 maart, 21 maart, 11 april, 18 april, 25 april, 23 mei, 17 oktober en 21 november 2012.
3. Het huidig advies uit eigen beweging heeft evenwel uitsluitend betrekking op het ontwerp van Verordening. Het betreft een eerste – voornamelijk artikelsgewijze – analyse en de CBPL behoudt zich het recht voor om desgevallend op een later tijdstip een aanvullend advies uit te brengen.
4. De CBPL vestigt er de aandacht op dat onderhavig advies gebaseerd is op de Franse en de Nederlandse tekst van het ontwerp van Verordening. Zij maakt hier melding van omdat zij heeft kunnen vaststellen dat de tekst van het ontwerp op sommige punten verschilt naargelang de taal waarin deze is opgesteld⁵.

² COM (2012)9 final.

³ COM (2012)11 final

⁴ COM (2012)10 final

⁵ Ter illustratie: De laatste zinsnede van artikel 47.3 heeft een andere betekenis in het Frans dan in het Nederlands:

2. Antecedenten

A. De mededeling van de Europese Commissie van 4 november 2010

5. In een mededeling van 4 november 2010 getiteld "*Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie*", somt de Europese Commissie de doelstellingen van de hervorming op⁶:
- Versterking van de rechten van individuen: grotere transparantie voor de betrokkenen, grotere zeggenschap over de eigen gegevens, zorgen voor geïnformeerde en vrije toestemming, bescherming van gevoelige gegevens, corrigerende maatregelen en sancties doeltreffender maken, opdrijven van sensibiliseringsacties in het kader waarvan de betrokkenen bewust worden gemaakt van hun rechten;
 - Verder uitwerken van de internemarktdimensie, onder meer door de administratieve belasting te verminderen, de verantwoordelijkheid van de voor de verwerking verantwoordelijke uit te breiden door aanmoediging van zelfregulering en onderzoek naar EU-certificeringsregelingen;
 - Herziening van de voorschriften inzake gegevensbescherming in het kader van de politie en justitiële samenwerking in strafzaken (voorstel van Richtlijn);
 - Rekening houden met de wereldwijde dimensie van gegevensbescherming: De regels voor internationale doorgifte van gegevens verduidelijken en vereenvoudigen;
 - Het institutionele kader versterken met het oog op een betere naleving van de voorschriften inzake gegevensbescherming: de onafhankelijkheid versterken, het statuut en de bevoegdheden van de nationale overheden voor gegevensbescherming verduidelijken en harmoniseren en de samenwerking en coördinatie onderling verbeteren.
6. De memorie van toelichting bij het ontwerp van Verordening verwoordt de voor de actie weerhouden motieven en de door de EC beoogde objectieven als volgt: "*Het huidige rechtskader is nog steeds valide wat zijn doelstellingen en beginselen betreft, maar heeft niet voorkomen dat persoonsgegevens in de Unie op gefragmenteerde wijze worden beschermd, er sprake is van rechtsonzekerheid en in brede lagen van de bevolking het beeld bestaat dat met name onlineactiviteit aanzienlijke risico's inhoudt. Het is dan ook tijd om een krachtiger en coherenter kader voor gegevensbescherming in de EU tot stand te brengen en bovendien*

- "Les membres de l'autorité de contrôle (...), n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

- De leden van de toezichhoudende autoriteit (...) verrichten gedurende hun ambtstermijn geen andere al dan niet bezoldigde beroepswerkzaamheden".

⁶ Mededeling van de Commissie aan het Europees parlement, de Raad, het Europees economisch en sociaal comité en het Comité van de Regio's: "Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie" COM (2010)609 final

*scherp toe te zien op de handhaving daarvan, zodat de digitale economie zich op de hele interne markt kan ontwikkelen, burgers zelf bepalen wat er met hun gegevens gebeurt en er meer praktische en rechtszekerheid wordt geboden aan bedrijven en overheden"*⁷

B. Vroegere standpunten van de CBPL

a) Bijdrage van de CBPL aan de openbare raadpleging door de EC (november 2010 – januari 2011)

7. In een schrijven van 14 januari 2011 – dat een bijdrage vormt aan de openbare raadpleging ingevolge de voormelde mededeling van 4 november 2010 – legt de CBPL 9 opmerkingen voor aan de Europese Commissie. De eerste slaat op de keuze van de norm: richtlijn of verordening. De CBPL herinnert aan de noodzakelijke eerbiediging van de subsidiariteits- en proportionaliteitsbeginselen⁸ bij deze keuze. Dientengevolge isoleert zij de "multinationale en transnationale" gegevensverwerkingen – zijnde gegevensverwerkingen die op gelijkaardige wijze gebeuren over de grenzen heen van een lidstaat of uitgevoerd worden door één enkele verantwoordelijke voor de verwerking (multinational) in verschillende lidstaten – waarvoor een geharmoniseerde Europese regelgeving op het hoogste niveau gepast lijkt.
8. Voor diezelfde verwerkingen is de CBPL voorstander van de oprichting van een Europese autoriteit voor gegevensbescherming. Deze autoriteit zou op Europees niveau de trans/internationale⁹ kwesties behandelen zonder zich ooit te mengen in de interne organisatie van de openbare overheden van een lidstaat. Voor deze Europese multinationals pleitte de CBPL eveneens voor een uniek Europees aangiftesysteem. Deze opmerking doet niet langer ter zake aangezien het ontwerp van Verordening elke voorafgaande aangifte bij de autoriteit voor gegevensbescherming schrapt.

⁷ COM (2012)11 final

⁸ Minimale verklaring van de beginselen: het subsidiariteitsbeginsel veroorlooft de uitvoering van een aan de Unie toevertrouwde bevoegdheid: het is een voorwaarde voor inwerkingtreding van de bevoegdheid. Zie artikel 5.1, 5.2, 5.3. en 5.4. van het Verdrag betreffende de Europese Unie (VEU): "1. De afbakening van de bevoegdheden van de Unie wordt beheerst door het beginsel van bevoegdheidstoedeling. De uitoefening van die bevoegdheden wordt beheerst door de beginselen van subsidiariteit en evenredigheid.

2. Krachtens het beginsel van bevoegdheidstoedeling handelt de Unie enkel binnen de grenzen van de bevoegdheden die haar door de lidstaten in de Verdragen zijn toegedeeld om de daarin bepaalde doelstellingen te verwezenlijken. Bevoegdheden die in de Verdragen niet aan de Unie zijn toegedeeld, behoren toe aan de lidstaten.

3. Krachtens het subsidiariteitsbeginsel treedt de Unie op de gebieden die niet onder haar exclusieve bevoegdheid vallen, slechts op indien en voor zover de doelstellingen van het overwogen optreden niet voldoende door de lidstaten op centraal, regionaal of lokaal niveau kunnen worden verwezenlijkt, maar vanwege de omvang of de gevolgen van het overwogen optreden beter door de Unie kunnen worden bereikt (...).

4. Krachtens het evenredigheidsbeginsel gaan de inhoud en de vorm van het optreden van de Unie niet verder dan wat nodig is om de doelstellingen van de Verdragen te verwezenlijken (...)."

⁹ Swift, Google, Facebook...

9. Nog in dit schrijven van 14 januari 2011 aan de Europese Commissie merkt de CBPL op dat het nieuwe wettelijke kader (1) de functie van functionaris voor de gegevensbescherming zou moeten bevorderen alsook (2) in de context van de steeds talrijker wordende grensoverschrijdende gegevensstromen, het mechanisme van bindende bedrijfsvoorschriften (BCR) en dit van de wederzijdse erkenning zoals dit toegepast wordt door een aantal overheden voor gegevensbescherming van de Unie¹⁰.

10. Betreffende genetische gegevens dringt de CBPL aan op hun extreme gevoeligheid. In haar ogen zou de verwerking ervan beperkt moeten worden tot de gezondheidszorg en het wetenschappelijk onderzoek of de wetsgeneeskunde. Elke verwerking in een contractuele, politieke, sociale of commerciële context zou moeten worden uitgesloten.

11. De CBPL is voorstander van de invoering van een verplichte privacyeffectbeoordeling aangezien alle efficiënte en proportionele veiligheidsmaatregelen moeten bepaald worden in functie van het risico dat veroorzaakt wordt door de verwerking en een redelijke beheersing van de risico's moet mogelijk maken zonder evenwel een efficiënte en effectieve dienstverlening aan de burgers en ondernemingen in de weg te staan, noch de goede werking van deze laatste of van de openbare diensten.

12. Gesteund door de kennis die werd verworven bij de organisatie van de conferentie "Privacy and research : from obstruction to construction" richt de CBPL ook enkele aanbevelingen aan de Europese Commissie die afkomstig zijn uit haar conclusies en die bestemd zijn om tegemoet te komen aan de noodzakelijke bescherming van de gegevens van de proefpersonen, alsook aan de rechtmatige belangen van de onderzoekers. Verduidelijkingen betreffende de toepassing van de reglementering op overleden personen en verduidelijkingen betreffende de voorwaarden waaronder onderzoek kan gebeuren in Europa en betreffende het invoeren van andere wettigheidsgronden dan de toestemming, maken onder meer deel uit van de geformuleerde suggesties.

¹⁰ De wederzijdse erkenning is een akkoord dat afgesloten werd tussen verschillende overheden teneinde de Europese samenwerkingsprocedure voor de BCR te versnellen. Volgens dit akkoord zullen, eens de leidende autoriteit (lead authority) oordeelt dat de BCR beantwoordt aan de vereisten die bepaald werden in de werkdocumenten van de Groep 29 en haar analyse werd nagekeken door twee andere autoriteiten, de andere autoriteiten die het principe van de wederzijdse erkenning aanvaarden, gaan ermee akkoord dat deze analyse een voldoende basis vormt om hun eigen nationale machtiging of goedkeuring van de BCR te verlenen, of om een gunstig advies te verstrekken aan het organisme dat de machtiging moet verstrekken.

b) Hoorzitting van het Voorzitterschap van de CBPL door de Commissie "Justitie" bij de Kamer van volksvertegenwoordigers

13. Een jaar later, begin maart 2012, vestigt het voorzitterschap van de CBPL de aandacht van de Commissie "Justitie" van de Kamer van volksvertegenwoordigers op de keuze die gemaakt werd door de Europese Commissie om het geheel van gegevensverwerkingen te regelen via een Verordening (met uitzondering van de verwerkingen "politie en justitie" die gedekt worden door het voorstel van Richtlijn).
14. In het algemeen waarschuwt de CBPL de Belgische wetgever voor de belangrijke wijzigingen die veroorzaakt zouden worden door het ontwerp van Verordening eens deze is goedgekeurd. De CBPL maakt zich vooral zorgen van het lot dat zal voorbehouden worden aan de bestaande sectorale comités (bijvoorbeeld Sectoraal comité van de Sociale zekerheid en van de Gezondheid (SCSZ & G), Sectoraal comité voor de Federale overheid (SCFO), Statistisch Toezichtscomité (SC STAT) en Sectoraal comité van het Rijksregister (SCRR)) wat betreft hun voorafgaande machtigingsbevoegdheid. Het ontwerp van Verordening beperkt immers de gevallen waarin vooraf een machtiging moet gevraagd worden aan de autoriteit voor gegevensbescherming (artikel 34). Het mechanisme van machtigingen zoals deze worden verleend door voormelde sectorale comités schijnt niet voorzien in de bepalingen van het ontwerp. In eenzelfde redenering stelt de CBPL zich vragen bij het gebruik in de toekomst (al dan niet geoorloofd?) van het Rijksregisternummer.
15. Ter ondersteuning van deze overwegingen vraagt de CBPL de Kamer van volksvertegenwoordigers haar politieke controle a priori uit te oefenen die haar sinds het Verdrag van Lissabon werd verleend door artikel 6 van het Protocol nr. 2 *betreffende de toepassing van de beginselen van subsidiariteit en evenredigheid*, aangehecht aan het Verdrag¹¹.
16. Op 20 maart 2012 werden de voorzitter, de ondervoorzitter en commissaris B. De Schutter gehoord door de Commissie "Justitie" bij de Kamer van volksvertegenwoordigers¹².

¹¹ Artikel 6 van het Protocol nr. 2: "*Ieder nationaal parlement en iedere kamer van een van die parlementen kan binnen een termijn van acht weken vanaf de datum van toezending van een ontwerp van wetgevingshandeling aan de voorzitters van het Europees Parlement, de Raad en de Commissie, in de officiële talen van de Unie, een gemotiveerd advies toezenden waarin wordt uiteengezet waarom het betrokken ontwerp zijns inziens niet strookt met het subsidiariteitsbeginsel. (...)*".

¹² Voorstel van verordening van het Europees Parlement en de Raad *betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens* COM (2012) 0011; Voorstel van richtlijn Europees Parlement en de Raad *betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens door de bevoegde overheden met het oog op preventie en opsporing, onderzoek en vervolging van strafrechtelijke inbreuken, of uitvoering van strafbepalingen en het vrije verkeer van deze gegevens* COM (2012) 0010, Subsidiariteitsadvies, verslag van 6 april 2012 namens de Commissie voor de Justitie door R. Landuyt, Kamer van volksvertegenwoordigers, Parl. Doc. DOC 53 2145/001, blz. 13-16.

17. Tot besluit van haar subsidiariteitsadvies neemt de Commissie Justitie bij de Kamer van volksvertegenwoordigers het volgende standpunt in :

Betreffende de subsidiariteit

- De grensoverschrijdende dimensie van de bescherming van persoonsgegevens, gecombineerd met de toegenomen internationalisering en het alomtegenwoordige internet rechtvaardigen een optreden op Europees niveau;
- De lidstaten moeten naar eigen inzicht de Europese reglementering in hun rechtsorde kunnen omzetten;
- De keuze voor een Verordening stuit op bezwaren inzake subsidiariteit omdat via de keuze voor een Verordening, die rechtstreeks toepasselijk is in de interne rechtsorde en geen verdere omzetting in de interne rechtsorde behoeft, de Europese Commissie voorbij gaat aan de bestaande praktijk en de kenmerken die eigen zijn aan de organisatie van gegevensbescherming in België;
- De keuze voor een Richtlijn dringt zich op, een Verordening kan slechts worden gebruikt voor bepaalde specifieke onderwerpen waarover tussen de lidstaten een draagvlak bestaat om dit via Verordening te regelen (zoals de uitwisseling van gegevens met landen buiten de EU);
- De bevoegdheid waarover de Europese Commissie zou beschikken om beslissingen van de overheden voor gegevensbescherming op te schorten, wordt als overmatig beschouwd (bevoegdheidsoverschrijding); een versterking van het Europees Comité voor gegevensbescherming (European Data Protection Board- EDPB) verdient de voorkeur;
- De Europese Commissie zou met het in het ontwerp van Verordening voorgestelde artikel 62 over ruimere bevoegdheden beschikken met betrekking tot het bepalen van uitvoeringswetgeving. De regelgeving zelf zou reeds zo volledig mogelijk moeten zijn teneinde de betrokkenheid van alle actoren, het Europees parlement en de Raad te verzekeren.

Betreffende de proportionaliteit

- Het ontwerp van Verordening zou de thans bestaande verwerkingen van persoonsgegevens door de publieke sector in hun geheel beïnvloeden of veranderen (toezichtmechanisme van de sectorale comités);
- Machtigingen afgeleverd door de sectorale comités vooraleer sommige verwerkingen met persoonsgegevens kunnen worden uitgevoerd zouden niet langer toegelaten zijn indien de voorgestelde Verordening wordt goedgekeurd;

- De lidstaten dienen bij wet te kunnen bepalen welke verwerkingen voorafgaande machtigingen vereisen;
- De vraag stelt zich of het gebruik van een unieke identificatiemiddel, zoals het rijksregisternummer niet problematisch wordt: de lidstaten dienen bij nationale wet voorwaarden vast te kunnen stellen waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt;
- De Verordening zou eveneens toepasselijk moeten zijn op de Europese instellingen zelf.

II. ARTIKELSGEWIJZE ANALYSE VAN HET ONTWERP VAN VERORDENING

1. Territoriale toepassingsfeer (artikel 3)

18. In toepassing van artikel 3.1, is het ontwerp van Verordening van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verantwoordelijke voor de verwerking of een verwerker in de Unie. In de hypothese waarin een verantwoordelijke voor de verwerking die buiten de EU gevestigd is beroep doet op een verwerker die in de EU gevestigd is, meent de CBPL dat zou moeten worden verduidelijkt of enkel de verwerker onderworpen is aan de toepassing van het ontwerp van Verordening, dan wel of daarentegen ook de verantwoordelijke voor de verwerking onderworpen is aan het geheel van verplichtingen die in het ontwerp van Verordening worden vastgelegd.
19. Artikel 3.2. beoogt de toepassing van het ontwerp van Verordening in de gevallen waarin de verantwoordelijke voor de verwerking niet gevestigd is in de Unie. Het feit dat de verwerking gekoppeld is aan een aanbod van goederen of diensten aan betrokkenen die woonachtig zijn in de Unie (of gepaard gaat met het observeren van hun gedrag), is in dat geval het criterium voor de territoriale toepassingsfeer van het ontwerp van Verordening.
20. Het criterium van de "middelen" dat gehanteerd werd door de Richtlijn 95/46/EG (artikel 4.1.c) heeft vaak geleid tot interpretatieproblemen en dit nieuwe criterium wil deze moeilijkheden vermijden en toch de Europese burgers doelgericht beschermen. Het zou niettemin nuttig zijn het begrip "aanbod van goederen of diensten" te verduidelijken teneinde dit te beperken tot de situaties waar de goederen niet eenvoudig verkrijgbaar zijn voor de Europese burgers, maar wel waar het aanbod van goederen of diensten duidelijk aan hen wordt geadresseerd, wat bijvoorbeeld blijkt uit het gebruik van domeinnamen van EU-lidstaten, uit het feit dat bijzondere leveringsmogelijkheden worden voorzien en/of uit het feit dat in het aanbod wordt rekening gehouden met de taal/cultuur/tradities/gebruiken van een bepaalde lidstaat, enz.

(zgn. "target approach"). Dit om te vermijden dat elke buitenlandse handelswebsite binnen de toepassingsfeer van het ontwerp van Verordening zou vallen.

2. Definities (artikel 4)

A. Algemene opmerking

21. De CBPL stelt zich de vraag waarom de definities pas in artikel 4 van het ontwerp van Verordening aan bod komen. In de artikelen 1 t.e.m. 3 worden immers al heel wat noties gebruikt die pas in artikel 4 worden gedefinieerd. Zij is dan ook van oordeel dat het instrument logischer zou opgebouwd zijn, mocht het luik over de definities in het eerste artikel worden opgenomen.

B. Persoonsgegevens en betrokkene

22. De CBPL staat positief ten aanzien van de aanpassing van de definities van "persoonsgegevens" en "betrokkene" en in het bijzonder over de precisering dat rekening moet worden gehouden met het geheel van middelen die redelijkerwijs kunnen worden ingezet om de betrokkene te identificeren, hetzij door de verantwoordelijke voor de verwerking, hetzij door iemand anders. Deze verduidelijking bevond zich in considerans 26 van de Richtlijn 95/46/EG en wordt thans ingevoegd in de definitie zelf, wat voor meer duidelijkheid en rechtszekerheid zorgt.

C. Gegevens betreffende de gezondheid

23. De definitie, vermeld in artikel 4.12, moet gelezen worden in het licht van considerans 26¹³ die voorziet in een zeer ruime interpretatie van dit begrip: het gaat niet alleen om gegevens betreffende de fysieke of mentale gezondheid maar eveneens om iedere informatie over de verlening van een gezondheidsdienst aan een persoon (zoals registratie van de patiënt voor de zorg, informatie betreffende betalingen).

¹³ Overweging 26 van het ontwerp van Verordening: Persoonsgegevens betreffende de gezondheid dienen met name alle gegevens te omvatten die betrekking hebben op de gezondheidstoestand van de betrokkene, informatie over de registratie van de persoon voor de verlening van gezondheidsdiensten, informatie over betalingen of voorwaarden voor gezondheidszorg met betrekking tot de persoon; een aan een persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van de persoon geldt voor gezondheidsdoeleinden; informatie over de persoon die tijdens de verstrekking van gezondheidszorg aan hem is verzameld; informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van biologische monsters; de identificatie van een persoon als verstrekker van gezondheidszorg aan de betrokkene; of informatie over bv. ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de feitelijke fysiologische of biomedische staat van de betrokkene, ongeacht de bron, zoals een arts of een andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een invitrodiagnostiek

24. De CBPL is van mening dat de door het ontwerp van Verordening voorgestelde definitie (veel) te ruim is en onvoldoende rekening houdt met de talrijke contexten waarin verwerkingen van dergelijke gegevens zich kunnen voordoen, alsook met het doeleinde dat met de verwerking wordt nagestreefd. Deze definitie dreigt ongewenste, verregaande gevolgen te hebben. Ter illustratie:
- a. Op videobeelden van bewakingscamera's is te zien dat een persoon een gebroken been heeft. Op basis van de definitie in het ontwerp van Verordening betreft dit een persoonsgegeven betreffende de gezondheid.
 - b. Een overheidsdienst is bevoegd om een belastingvermindering of een ander sociaal voordeel toe te kennen aan personen die een handicap hebben. Het feit dat deze overheidsdienst in zijn gegevensbanken opslaat dat een persoon binnen deze categorie valt (zonder te specificeren om welke handicap het juist gaat), volstaat om te beweren dat deze dienst persoonsgegevens betreffende de gezondheid verwerkt in de zin van het ontwerp van Verordening.
25. Tot slot, hoewel artikel 4.12 (definities) de term "gegevens over gezondheid" gebruikt, heeft men het in de ontwerptekst ook regelmatig over "gegevens betreffende de gezondheid". Een uniforme terminologie/vertaling zou moeten voorgesteld worden.

D. Belangrijkste vestiging

26. Voor gevallen waarin de gegevensverwerking plaatsvindt in het kader van de activiteiten van een verantwoordelijke voor de verwerking of een verwerker die in verschillende lidstaten gevestigd is, bepaalt het ontwerp van Verordening dat de bevoegde autoriteit enkel deze is waar de belangrijkste vestiging van de verantwoordelijke voor de verwerking zich bevindt (cf. infra).
27. Het ontwerp van Verordening voorziet ook in een criterium van belangrijkste vestiging voor de verwerkers en het gaat hier om de plaats van de centrale administratie in de Unie (artikel 4.13 in fine).
28. De CBPL maakt enig voorbehoud op dit punt aangezien er geen enkele zekerheid bestaat dat een centrale administratie, bijvoorbeeld de hoofdzetel of "headquarter" van een groep ondernemingen die optreedt als verwerker, concreet betrokken is bij de gegevensverwerking of de overeenkomst die de verwerkende onderneming bindt aan de verantwoordelijke voor de verwerking. De aangeduide bevoegde overheid zou voor de verwerkers zo dicht mogelijk bij de beschikbare informatie moeten staan (plaats van verwerking of van de technische of

organisatorische beslissingen betreffende de verwerking) en bij de juridische verantwoordelijkheid (persoon juridisch verbonden aan de verwerkingsovereenkomst) zoals dit het geval is in het ontwerp van Verordening voor de verantwoordelijke voor de verwerking. In de veronderstelling dat de centrale administratie (of hoofdzetel) geen weet heeft van de verwerkingsovereenkomst en op generlei wijze betrokken is bij de uitvoering van deze overeenkomst, zou de bevoegde autoriteit immers toch een beroep moeten doen op haar collega's om er informatie over te verkrijgen.

E. Bindende bedrijfsvoorschriften

29. De CBPL waardeert de expliciete erkenning van bindende bedrijfsvoorschriften. Er zou echter moeten voor gezorgd worden dat deze oplossing eveneens kan toegepast worden voor ondernemingen die niet in de Unie gevestigd zijn maar krachtens het ontwerp van Verordening desondanks toch verplicht zijn om te voorzien in een passende bescherming in het raam van gegevensdoorgiften vanuit de Europese Unie (zie artikel 4.17)¹⁴.

F. Het kind

30. Considerans 29 van het ontwerp van Verordening verduidelijkt dat *"voor de vaststelling of een persoon een kind is, dient in deze verordening de in het vn-verdrag inzake de rechten van het kind vervatte definitie te worden overgenomen"*. Aangezien de meeste EU-lidstaten het Verdrag inzake de rechten van het kind hebben geratificeerd¹⁵, lijkt de keuze voor deze referentiedefinitie "democratisch" relevant. Volgens artikel 4.18 van het ontwerp van Verordening wordt het kind gedefinieerd als *"iedere persoon die jonger is dan achttien jaar"*. De volledige tekst van het vn-verdrag verduidelijkt evenwel *"behalve indien de meerderjarigheid vroeger wordt bereikt ingevolge de op hem toepasselijke wetgeving"*. Bijgevolg zou een betere coherentie moeten verzekerd worden tussen considerans 29 en de definitie van het kind zoals vermeld in artikel 4.18.
31. Een op leeftijd gebaseerde definitie biedt het voordeel van rechtszekerheid. De CBPL is echter van mening dat de willekeurige vaststelling van een leeftijd (voor meerderjarigheid) inzake bescherming van persoonsgegevens moeilijk te rijmen valt met de realiteit van het gebruik, van onder meer het internet, door (soms heel jonge) jongeren. Naar analogie van wat is voorzien in de *recommandation R(2002)9 du Comité des Ministres du Conseil de l'Europe sur la*

¹⁴ De modelcontractbepalingen 2010/87/EU bieden bijvoorbeeld een juridische oplossing voor de doorgiften van gegevens naar ondernemingen die gevestigd zijn in derde landen en die optreden als verwerker. Er zou moeten worden vermeden dat bindende bedrijfsvoorschriften voor verwerkers enkel kunnen geboden worden aan ondernemingen die gevestigd zijn in de Unie terwijl zij gebruik kunnen maken van modelcontractbepalingen.

¹⁵ België ratificeerde het Internationale Verdrag inzake de rechten van het kind in 1991.

protection des données à caractère personnel collectées et traitées à des fins d'assurance, (Aanbeveling Rec (2002) 9 van het Comité van Ministers aan de lidstaten betreffende de bescherming van persoonsgegevens verzameld en verwerkt voor verzekeringsdoeleinden) beveelt de CBPL aan het kind te informeren, te raadplegen en vanaf een zekere leeftijd rekening te houden met zijn wensen, ofwel het in functie van zijn beoordelingsvermogen geleidelijk te betrekken bij de te nemen beslissingen bijvoorbeeld wat de uitoefening van zijn rechten betreft. Deze benadering weerspiegelt het streven van de CBPL om de jongere te stimuleren tot het aannemen van een geïnformeerde, verantwoordelijke en zichzelf en anderen respecterende houding bij het gebruik van informatie- en communicatietechnologieën¹⁶.

3. Beginselen inzake de verwerking van persoonsgegevens (artikel 5)

32. Hoewel de CBPL volledig achter het principe staat dat gegevens toereikend en niet overmatig dienen te zijn ten opzichte van het beoogde doeleinde (het bestaande proportionaliteitsbeginsel), meent zij dat het minimaliseringsbeginsel zoals geformuleerd in artikel 5.c) te ver gaat. Dit beginsel impliceert immers dat de verwerkte gegevens moeten beperkt worden tot wat minimaal nodig is en dat moet worden nagegaan of de doeleinden niet kunnen worden verwezenlijkt zonder verwerking van persoonsgegevens. Een dergelijk principe is in de ogen van de CBPL te beperkend, daar het in sommige gevallen de verwezenlijking van het doeleinde zou kunnen belemmeren door verwerkingen van gegevens die op het eerste zicht niet onontbeerlijk lijken te verbieden, maar waarvan uiteindelijk a posteriori blijkt dat ze onmisbaar zijn voor de verwerking (bijvoorbeeld inzake wetenschappelijk onderzoek).

4. Rechtmatigheid van de verwerking (artikel 6)

33. De CBPL vestigt er vooreerst de aandacht op dat de term "rechtmatigheid" in deze context aanleiding kan geven tot verwarring. Er zou immers kunnen uit afgeleid worden dat verwerkingen van persoonsgegevens die gesteund kunnen worden op één van de grondslagen vervat in artikel 6.1. automatisch op alle vlakken conform zijn aan het ontwerp van Verordening, terwijl dit evident niet het geval is. Daarom pleit de CBPL ervoor om de term "toelaatbaarheid" te hanteren. Laatstgenoemd begrip heeft immers een beperktere draagwijdte dan "rechtmatigheid" en geeft aldus beter weer dat artikel 6 slechts een eerste stap is bij de beoordeling of een verwerking van persoonsgegevens voldoet aan de verplichtingen die in het ontwerp van Verordening zijn vastgelegd.

¹⁶ Zie in die zin advies 2/2009 van 11 februari 2009 van de Groep 29 *over de bescherming van persoonsgegevens van kinderen (Algemene richtlijnen en het bijzondere geval van scholen)*.

34. Verder heeft de CBPL bedenkingen bij artikel 6.1.f) van het ontwerp van Verordening, waarin het openbare overheden wordt verboden om hun verwerkingen te rechtvaardigen indien zij optreden op basis van hun gerechtvaardigde belangen die prevaleren op de rechten en belangen van de betrokkenen. Zij meent dat deze basis voor toelaatbaarheid van de verwerking, niet mag worden geschrapt. Het is immers niet denkbeeldig dat er zich situaties voordoen waarin een openbare overheid geen andere keuze heeft dan sommige verwerkingen te baseren op haar gerechtvaardigde belangen (bijvoorbeeld in het kader van haar personeelsbeheer).
35. Meer in het algemeen, heeft de Commissie overigens ook een nota uitgewerkt waarin zij elementen van antwoord heeft samengebracht omtrent de vraag of een afzonderlijk wettelijk, reglementair raamwerk nodig is voor de publieke en de private sector. Deze nota is in bijlage bij onderhavig advies gevoegd.
36. Tot slot heeft de CBPL een aantal opmerkingen bij artikel 6.4 van het ontwerp van Verordening, dat het volgende bepaalt: *"Wanneer het doel van verdere verwerking niet verenigbaar is met het doel waarvoor de persoonsgegevens zijn verzameld, moet de verwerking minstens in één van de in lid 1, onder a) tot en met e), genoemde gronden een rechtsgrondslag hebben. (...)."*
- Ofwel is de verwerking verenigbaar, ofwel is ze dit niet en in laatstgenoemd geval gaat het om een nieuwe verwerking die moet voldoen aan alle wettelijke voorwaarden en die aldus een andere rechtmatige basis moet bezitten. Alle hypotheses van artikel 6 a) tot f) zouden in dit geval moeten toegepast kunnen worden en de CBPL begrijpt dan ook niet waarom in het ontwerp van Verordening enkel de hypotheses bedoeld in de punten a) tot e) worden vermeld.
- De CBPL is ook van oordeel dat in artikel 5, punt b) van het ontwerp van Verordening een duidelijke verwijzing zou moeten opgenomen worden naar artikel 6.4. Beide bepalingen zijn immers nauw met mekaar verbonden.

5. Toestemming van de betrokkene (artikel 7)

37. Wanneer de verantwoordelijke voor de verwerking zijn verwerking rechtvaardigt op basis van de toestemming, bepaalt het ontwerp van Verordening dat deze uitdrukkelijk moet zijn (artikel 4.8) en dat de bewijslast van de toestemming duidelijk berust bij de verantwoordelijke voor de verwerking (artikel 7.1). Considerans 25 verduidelijkt dat de toestemming kan worden verleend op elke passende wijze, hetzij via een verklaring, hetzij via een ondubbelzinnige, actieve handeling of een duidelijke indicatie waaruit in de gegeven context blijkt dat de verwerking van persoonsgegevens wordt aanvaard. Deze aanpassingen beogen een versterking van de

rechten van de betrokkenen en een responsabilisering van de verantwoordelijken voor de verwerking voor het bewaren van bewijselementen.

38. Het ontwerp van Verordening voorziet eveneens dat de verleende toestemming voortaan op elk ogenblik kan worden ingetrokken zonder rechtvaardiging of motivering. Deze bepaling wordt voorgesteld als een versterking van de rechten van de betrokkene en van de controle die hij moet kunnen uitoefenen op het gebruik van zijn gegevens. De CBPL wijst er niettemin op dat een mogelijke unilaterale en niet-gerechtvaardigde intrekking van een wettelijk bekrachtigde toestemming waardoor wordt geraakt aan de belangen van derden, de activiteiten van de verantwoordelijken voor de verwerking kan hypothekeren en dat deze regel het evenwicht dreigt op de helling te zetten dat bekrachtigd werd in Richtlijn 95/46/EG tussen de rechten van de betrokkene en de belangen van de verantwoordelijken voor de verwerking. Deze mogelijkheid op unilaterale intrekking dient overigens beoordeeld te worden in het licht van het recht op verzet tegen de verwerking en de voorwaarden voor uitoefening van dit recht (cf. infra).
39. De CBPL meent in het algemeen dat een overwaardering van de toestemming moet worden vermeden. De toestemming is toegelaten als basis voor rechtmatigheid maar men moet alert blijven voor de kwetsbaarheid ervan en niet alle verwerkingen willen baseren op de toestemming. Talrijke bepalingen van het ontwerp van Verordening baseren zich op de toestemming als basis voor rechtmatigheid zoals artikel 8.1 betreffende de toestemming van minderjarigen in de context van diensten van de informatiemaatschappij (zie supra). Welnu, in die context wordt er veel vaker gebruik gemaakt van aansluitingscontracten in welk geval men niet meer echt gewag kan maken van een toestemming.
40. Het ontwerp van Verordening sluit overigens de toestemming uit als geldige rechtsgrondslag voor verwerking wanneer er een aanzienlijke onevenwichtigheid bestaat tussen de positie van de betrokkene en die van de verantwoordelijke voor de verwerking (artikel 7.4). Considerans 34 verduidelijkt dat het gaat om het geval wanneer de betrokkene zich in een situatie van afhankelijkheid jegens de verantwoordelijke voor de verwerking bevindt, bijvoorbeeld als zijn persoonsgegevens worden verwerkt door zijn werkgever in het raam van zijn arbeidsrelatie. Men wenst aldus formeel te erkennen dat het vrije karakter van de toestemming een probleem kan vormen in een professionele context ingevolge het bestaan van een band van ondergeschiktheid¹⁷.

¹⁷ Zie in dit verband eveneens de aanbevelingen nr. 01/2002 van de CBPL en werkdocumenten WP 48 en WP 168 (punt 66) van de Groep 29.

41. Het gebruik van de toestemming in een professionele context in alle gevallen uitsluiten, kan aldus de CBPL echter leiden tot meer rechtsonzekerheid voor de verantwoordelijke voor de verwerking en dit voor de verwerkingen die niet strikt noodzakelijk zijn voor de uitvoering van de arbeidsovereenkomst. Opdat gegevensverwerkingen in die gevallen toelaatbaar zouden zijn, moet de verantwoordelijke voor de verwerking zelf a priori de belangen afwegen (artikel 6.1.f van het ontwerp van Verordening), met het risico dat hij a posteriori door de rechter wordt teruggefloten.
42. Aldus de CBPL zou de toestemming van een werknemer daarom in sommige gevallen toch een toelaatbaar grondslag moeten kunnen vormen. Er kan hiertoe inspiratie worden gevonden in het bestaande nationaal regelgevend kader. Artikel 27 van het Koninklijk besluit van 13 februari 2001, genomen ter uitvoering van de WVP, voorziet met name in het verbod voor de werkgever om de verwerking van **gevoelige** gegevens uitsluitend te baseren op de toestemming, **behalve wanneer de verwerking erop gericht is de betrokken persoon een voordeel te verstrekken**. De CBPL pleit er voor om deze uitzondering over te nemen in het ontwerp van Verordening.

6. Verwerking van persoonsgegevens van kinderen (artikel 8)

43. Het ontwerp van Verordening voert het beginsel in van een specifieke bescherming voor minderjarigen (kinderen) "*aangezien zij zich allicht minder bewust zijn van de risico's, gevolgen, beschermingsmaatregelen en rechten in verband met de verwerking van persoonsgegevens*" (considerans 29).
44. De CBPL staat positief ten aanzien van dit initiatief, dat overigens in het bijzonder aangewezen is in de context van online activiteiten, sociale netwerken en marketingactiviteiten die speciaal gericht zijn op jongeren. De CBPL herinnert aan het initiatief dat zij in dit verband nam met haar speciale website voor minderjarigen (jongeren en adolescenten) en hun ouders en leerkrachten¹⁸, waarmee zij anticipeerde op de uitnodiging in het ontwerp van Verordening om sensibiliseringsacties te houden voor deze categorie betrokkenen (artikel 52).
45. Betreffende de garanties waarin voorzien is in het ontwerp van Verordening, staat de CBPL positief tegenover de verduidelijking die aangebracht werd aan artikel 6 f). Deze bepaling schrijft voor dat het feit dat een persoon minderjarig is in aanmerking moet genomen worden bij de beoordeling van de eventuele voorrang van belangen, vrijheden of fundamentele rechten van de betrokkene tegenover de gerechtvaardigde belangen van de verantwoordelijke

¹⁸ Website "Ik beslis" : <http://www.ikbeslis.be/>

voor de verwerking. In diezelfde zin deelt zij het verlangen van de Europese Commissie om grote databanken betreffende minderjarigen te onderwerpen aan een voorafgaande privacyeffectbeoordeling (artikel 33), sensibiliseringsacties door de autoriteiten voor gegevensbescherming aan te moedigen (artikel 52), specifieke gedragscodes op te stellen (artikel 38) alsook de verantwoordelijken voor de verwerking te verzoeken het nodige te doen om een verifieerbare toestemming te verkrijgen bij de aanbidding van diensten van de informatiemaatschappij (artikel 8).

46. Aangaande het rechtstreeks aanbieden van diensten van de informatiemaatschappij aan kinderen, stelt artikel 8 dat *"de verwerking van persoonsgegevens van een kind jonger dan 13 jaar in het kader van deze verordening slechts rechtmatig is wanneer en voor zover de ouder of voogd van het kind daartoe toestemming heeft gegeven of machtiging tot toestemming heeft verleend"* (artikel 8.1) Tegelijk bepaalt artikel 8.2 het volgende: *"Lid 1 laat het algemene overeenkomstenrecht van de lidstaten, zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van een overeenkomst ten opzichte van een kind, onverlet"*.
47. De CBPL begrijpt deze bepaling als een uitnodiging om een onderscheid te maken tussen de rechtmatigheid (gebaseerd op de toestemming) van de verwerking van gegevens van een minderjarige van minder dan 13 jaar, en de wettigheid van zijn contractuele verbintenis in het licht van het nationaal (burgerlijk) recht. Het zou nuttig zijn om een bevestiging van deze lezing en een illustratie van wat moet worden verstaan onder "het rechtstreeks aanbieden van diensten van de informatiemaatschappij" op te nemen in de consideransen.
48. Bovendien maakt de CBPL zich de bedenking hoe de strikte geldigheidsvereisten van een toestemming krachtens artikel 7 van het ontwerp van Verordening, te rijmen zijn met de toestemming van een minderjarige ouder dan 13.
49. De CBPL herinnert er tot slot aan dat, los van elke specifieke bescherming, rekening kan en moet gehouden worden met de bijzondere situatie van kinderen bij de toepassing van de bepalingen van het ontwerp van Verordening (voorbeeld: de kennisgeving moet begrijpelijk zijn wat inhoudt dat de verantwoordelijke voor de verwerking zijn taalgebruik aanpast wanneer hij zich specifiek tot kinderen richt). Hetzelfde geldt voor andere categorieën personen. De CBPL denkt hierbij aan personen die weinig vertrouwd zijn met informaticatoepassingen en informatie- en communicatietechnologieën (ouderen, digitale kloof)¹⁹.

¹⁹ Hoewel de reglementering inzake "gegevensbescherming" in het algemeen geleidelijk complexer is geworden en de *verwerkingen* en *gegevens* vandaag in het middelpunt van de belangstelling staan (economisch en juridisch), dient immers toch niet uit het oog te worden verloren dat de doelstelling van de reglementering van dit grondrecht in de eerste plaats de bescherming van de *persoon* betreft (ten opzichte van de verwerking van zijn gegevens...).

50. In dit verband merkt de CBPL ook op dat het ontwerp van Verordening in een algemene bepaling zou kunnen voorzien met betrekking tot de vertegenwoordiging van handelingsonbekwamen. Deze bepaling zou de nadruk kunnen leggen op het feit dat wanneer deze vertegenwoordigers hun toestemming geven, zij niet uit het oog mogen verliezen dat zij toestemming verlenen voor een derde en niet voor zichzelf, en dat de bescherming van diegene die zij vertegenwoordigen hierbij hun leidraad moet zijn.

7. Verwerking van bijzondere categorieën persoonsgegevens (artikel 9)

51. Artikel 9.1., dat de bijzondere categorieën persoonsgegevens definieert (gevoelige gegevens) vermeldt eveneens de genetische gegevens. Dit was niet het geval in artikel 8.1 van de Richtlijn 95/46/EG. De CBPL staat positief tegenover deze inlassing.

52. De CBPL is een stuk terughoudender met betrekking tot de wijziging van de omschrijving van de gerechtelijke gegevens zoals vermeld in artikel 8.5 van de Richtlijn 95/46/EG en meer in het bijzonder wat betreft de schrapping van de term "overtredingen" ("offences" in het Engels). Laatstgenoemde notie liet nochtans toe om administratieve overtredingen of burgerlijke veroordelingen eveneens als gerechtelijke gegevens te kwalificeren (zie artikel 8 § 1 van de WVP).

53. Verder stelt de CBPL vast dat het aantal gevallen waarin de verwerking van gerechtelijke gegevens toelaatbaar wordt geacht, aanzienlijk is uitgebreid in vergelijking met wat in artikel 8.5. van de Richtlijn 95/46/EG is voorzien. Zo vormen bijvoorbeeld de toestemming van de betrokkene of de openbaarmaking van de gegevens door de betrokkene, krachtens artikel 9.2., punten a) en e), van het ontwerp van Verordening, uitzonderingsgronden op het verwerkingsverbod, terwijl deze grondslagen niet worden voorzien in de Richtlijn. De CBPL stelt zich de vraag wat de motivatie is voor deze versoepeling.

54. Wat de verwerking van gegevens betreffende de gezondheid aangaat, wordt het standpunt van de CBPL hoger uiteengezet.

8. Verwerking die geen identificatie toelaat (artikel 10)

55. Artikel 10 van het ontwerp van Verordening bepaalt dat wanneer de verwerkte gegevens niet toelaten een natuurlijke persoon te identificeren, de verantwoordelijke voor de verwerking niet verplicht is om aanvullende informatie te verkrijgen ter identificatie van de betrokkene om zodoende aan de bepalingen van deze verordening te voldoen. De CBPL meent dat de bedoelingen achter deze bepaling moeten verduidelijkt worden en dat in elk geval moet

vermeden worden dat hieruit wordt afgeleid dat de verantwoordelijke voor de verwerking tot geen enkele verplichting meer gehouden is.

9. Transparantie (artikelen 11 en 14)

56. De CBPL verwelkomt de algemene verplichting om te beschikken over transparante, makkelijk toegankelijke, completere privacy policies en zij staat positief tegenover het feit dat iedere informatieverstrekking of communicatie vanwege de verantwoordelijke voor de verwerking moet gebeuren in een duidelijke taal, die aangepast is aan de betrokkene (artikel 11).
57. Het ontwerp van Verordening voorziet verder in een ruimere inhoud van de door de verantwoordelijke voor de verwerking te verstrekken informatie (Vergelijk artikel 14.1 tot 14.3 van het ontwerp ten opzichte van artikel 10 en 11 van de Richtlijn 95/46/EG).
58. De CBPL waardeert de bijkomende informatie betreffende de oorsprong van de gegevens (artikel 14.3) die meteen de facto een grotere controle toelaat voor de betrokkenen over hun eigen gegevens.
59. Wat de informatieverstrekking betreft met betrekking tot de rechten van de betrokkenen (artikel 14.1.d), meent de CBPL dat eveneens melding zou moeten gemaakt worden van de nieuwe rechten die in het ontwerp van Verordening worden gecreëerd (recht om te worden vergeten, recht op overdraagbaarheid, profileringmaatregelen). Tevens zou de informatieverstrekking betreffende de internationale doorgiften (artikel 14.1.g) de passende waarborgen moeten omvatten waarin werd voorzien door de verantwoordelijke voor de verwerking, aangezien deze waarborgen voor de betrokkenen vaak rechten creëren .
60. De CBPL merkt ook op dat het ontwerp van Verordening (artikel 14, punt 1, c)) het principe vastlegt dat bij de informatieverstrekking aan de betrokkene meteen ook de vooropgestelde bewaartermijn van de verwerkte gegevens wordt vermeld. De CBPL deelt de idee dat dit principe een hogere graad van transparantie aan de verwerking van persoonsgegevens zou geven in de gevallen waarin de verantwoordelijke voor de verwerking vooraf een duidelijk zicht heeft op de bewaarduur (bv. omdat deze in de regelgeving is verankerd), maar ze wijst er tegelijk op dat het voor de verantwoordelijke voor de verwerking in de praktijk vaak onmogelijk is om vooraf een exacte bewaartermijn vast te leggen. Heel wat beraadslagingen van het Sectoraal Comité voor de Federale Overheid illustreren dit.
De CBPL vreest dan ook dat deze nieuwe regel er in de praktijk vaak zal toe leiden dat de verantwoordelijke voor de verwerking op het moment van de informatieverstrekking aan de betrokkene hoogstens een ruwe schatting zal kunnen maken van de bewaartermijn. Wellicht

zal de verantwoordelijke zelfs 'veiligheidshalve' een langere termijn vragen dan wat strikt noodzakelijk is.

61. Tot slot vestigt de CBPL er de aandacht op dat – op grond van artikel 14.5., punt c) van het ontwerp van Verordening – de informatieplicht niet van toepassing is *wanneer (de gegevens niet worden verzameld bij de betrokkene en) de vastlegging of verstrekking van de gegevens uitdrukkelijk bij wet is voorgeschreven*.
62. De CBPL meent dat deze bepaling enerzijds een verstrenging lijkt in te houden ten aanzien van de Richtlijn 95/46/EG, omdat het woord "uitdrukkelijk" werd toegevoegd (vergelijk artikel 11.2., in fine van Richtlijn 95/46/EG). Anderzijds lijkt tegelijk ook op een versoepeling te worden aangestuurd, aangezien de verplichting ten aanzien van de lidstaten – die in artikel 11.2., in fine, van de Richtlijn 95/46/EG was opgenomen – om in "*passende waarborgen*" te voorzien voor de gevallen waarin onderhavige uitzondering op de informatieplicht kan worden ingeroepen, niet wordt herhaald in het ontwerp van Verordening.
63. De CBPL stelt zich dan ook de vraag of de Europese Commissie bij de redactie van artikel 14.5., punt c), van het ontwerp van Verordening, de bedoeling had om een wijziging door te voeren ten aanzien van de huidige situatie. Heeft zij met andere woorden een verstrenging, een versoepeling of een *status quo* voor ogen?
64. De CBPL is in elk geval van oordeel dat een verstrenging van deze uitzondering op de informatieplicht zou kunnen impliceren dat heel wat gegevensfluxen in de Belgische overheidssector onderhevig zullen worden aan de informatieplicht, terwijl totnogtoe vaak de uitzondering kon worden inroepen van zodra voor de verwerking steun kon worden gevonden in de regelgeving. Het ontwerp van Verordening zou aldus belangrijke praktische implicaties kunnen hebben voor gegevensverwerkingen in de publieke sector. Er dreigt zich met name een grootschalige oefening op te dringen, om na te gaan of het regelgevend kader van elk domein volstaat om de uitzondering op de informatieplicht te rechtvaardigen, dan wel of wetgevende ingrepen vereist zijn of de informatieplicht desgevallend toch moet vervuld worden.
65. De CBPL heeft ernstige twijfels bij de wenselijkheid van een dergelijke oefening en zij pleit er daarom voor om in artikel 14.5., punt c), van het ontwerp van Verordening duidelijk te opteren voor het behoud van de bestaande situatie zoals voorzien in artikel 11.2., in fine, van de Richtlijn 95/46/EG.

10. Procedure en mechanismen voor de uitoefening van de rechten van de betrokkene (artikel 12)

66. De CBPL waardeert de verplichting die rust op de verantwoordelijke voor een geautomatiseerde verwerking om aan de betrokkene de middelen ter beschikking te stellen om zijn rechten en verzoeken elektronisch uit te oefenen (artikel 12.1), de invoering van een termijn voor het verstrekken van een antwoord (artikel 12.2) en het gratis principe (behoudens ingeval van misbruik) (artikel 12.4).

11. Recht op toegang (artikelen 15 en 20)

67. De CBPL meent dat het recht op toegang (artikel 15) ook zou moeten gelden voor de passende waarborgen waarin werd voorzien bij internationale doorgiften. De bestaande waarborgen zoals de bindende bedrijfsvoorschriften en de modelcontractbepalingen van de Europese Commissie bevatten vaak een mogelijkheid voor de betrokkenen op toegang tot de inhoud. Deze waarborgen voorzien immers voor de betrokkenen vaak in rechten (als derde begunstigden).

68. Aangezien het ontwerp van Verordening in de mogelijkheid voorziet voor de verwerkers om zelf passende waarborgen te bieden (artikel 42) en zij niet noodzakelijk in contact staan met de betrokkenen, zou aldus de CBPL ook een grotere transparantie en toegang door de betrokkenen tot de passende waarborgen die door verwerkers worden geboden, moeten ingeschreven worden in het ontwerp van Verordening zelf²⁰.

69. Overigens voorziet Richtlijn 95/46/EG in haar artikel 12 in de verplichte mededeling aan de betrokkene van de logica die ten grondslag ligt aan de automatische verwerking van zijn gegevens, in elk geval als het gaat om de geautomatiseerde besluiten als bedoeld in artikel 15, lid 1. De "geautomatiseerde maatregelen" waarvoor in artikel 15 van de Richtlijn 95/46/EG specifieke regels zijn vastgelegd, worden in artikel 20 van het ontwerp van Verordening gecombineerd met "profileringmaatregelen". De CBPL is evenwel van oordeel dat er ook geautomatiseerde verwerkingen denkbaar zijn die niet in de context van profilering worden uitgevoerd (cf infra). Zij betreurt dat er in het ontwerp van Verordening voor die gevallen geen specifieke regel is vastgesteld die de verantwoordelijke voor de verwerking verplicht om de betrokkenen te informeren omtrent de logica die aan de basis ligt van de geautomatiseerde verwerking van hun gegevens.

²⁰ Wat zou verzekeren dat de verantwoordelijke voor de verwerking de door de verwerkers geboden passende waarborgen ter beschikking moet stellen.

12. Recht op verbetering (artikel 16)

70. De CBPL is van oordeel dat wanneer de gegevens objectief gezien onjuist zijn, deze eenvoudig zouden moeten verbeterd worden. De mogelijkheid om de in artikel 16 voorziene rectificerende verklaring toe te voegen, zou daarentegen slechts van toepassing mogen zijn wanneer de gegevens betrekking hebben op subjectieve informatie (bijvoorbeeld een beoordeling) en de betrokkene oordeelt dat ze onjuist zijn terwijl de verantwoordelijke voor de verwerking het hier niet mee eens is (dit laat toe in de praktijk de beide versies van de gegevens te bewaren).

13. Recht om te worden vergeten en om gegevens te laten wissen (artikel 17)

71. De rechten om te worden vergeten en om gegevens te laten wissen (artikel 17) zouden duidelijk moeten worden onderscheiden aangezien het twee verschillende concepten betreft.

72. Verder stelt de CBPL vast dat artikel 17 voorziet in het recht voor de betrokkene om de gegevens te laten wissen wanneer zij niet langer noodzakelijk zijn voor de verwezenlijking van het doeleinde waarvoor zij werden ingezameld of wanneer de toegestane termijn voor opslag is verstreken terwijl een andere rechtsgrond voor de verwerking van de gegevens ontbreekt. Aldus de CBPL zou de betrokkene in deze gevallen niet moeten verzoeken om uitwissing van de gegevens, aangezien dit in elk geval automatisch zou moeten gebeuren. Zij meent dan ook dat het ontbreken van automatisme een zekere verzwakking betekent van de bescherming ten opzichte van de huidige situatie.

73. De CBPL deelt tot slot het standpunt dat nauwlettend moet worden toegezien op de juistheid en de bijwerking van gegevens van minderjarigen en op hun uitwissing eens hun bewaring niet langer gerechtvaardigd is. Er wordt echter geen enkel juridisch gevolg gekoppeld aan de zinsnede "met name waar het gaat om persoonsgegevens die door de betrokkene als kind beschikbaar zijn gesteld" (artikel 17.1). Dit gebrek aan juridische gevolgen kan leiden tot verwarring en een zeker gevoel van rechtsonzekerheid.

14. Recht op overdraagbaarheid van gegevens (artikel 18)

74. De CBPL verwelkomt dit principe – dat tot doel heeft de positie van de betrokkenen te versterken door hen meer controle te bieden over hun gegevens – maar meent dat waakzaamheid zal geboden zijn bij de vaststelling van de uitvoeringsmaatregelen van dit beginsel. De thans in het ontwerp van Verordening voorziene modaliteiten zijn aldus de CBPL echter onvoldoende uitgewerkt om dit artikel in de praktijk te kunnen toepassen.

15. Recht op verzet (artikel 19)

75. Met de inwerkingtreding van het ontwerp van Verordening zal het in de WVP voorziene recht op verzet verdwijnen in de gevallen waarin de toestemming van de betrokkene de rechtsbasis vormt van een gegevensverwerking²¹. Dit standpunt is onaanvaardbaar aangezien dit een verzwakking van de rechten van de betrokkenen zou betekenen. Het recht op verzet is essentieel aangezien het inhoudt dat de verantwoordelijke voor de verwerking de gegevens waarvoor de betrokkene zijn recht op verzet heeft uitgeoefend niet meer mag verwerken.
76. Het recht op verzet biedt thans sterkere waarborgen dan de mogelijkheid op intrekking van de toestemming die is voorzien in het ontwerp van Verordening. Deze stelt immers het volgende "*De intrekking van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet*" (artikel 7.3. van het ontwerp van Verordening). In ieder geval moet men ervan uitgaan dat de intrekking van een toestemming slechts concrete gevolgen kan hebben voor de toekomst. Een dergelijke bepaling verzwakt in belangrijke mate de bescherming die in de huidige regelgeving geboden wordt door uitoefening van het recht op verzet.
77. Bij de uitvoering van het recht op verzet tenslotte, verleent het ontwerp van Verordening aan de verantwoordelijke voor de verwerking de mogelijkheid om dwingende legitieme gronden voor de verwerking aan te tonen die zwaarder wegen dan de belangen of de grondrechten en fundamentele vrijheden van de betrokkene. (art. 19.1). Op het eerste gezicht gaat het om een versterking van de rechten van de betrokkenen die in het kader van de uitoefening van hun recht op verzet niet langer zwaarwegende en gerechtvaardigde redenen moeten aantonen die

²¹ De lidstaten waren krachtens artikel 14 van de Richtlijn 95/46/EG verplicht om in minimum in een aantal gevallen (met name in de gevallen bedoeld in artikel 7, punten e) en f) en bij direct marketing) in een recht van verzet te voorzien, maar verder waren ze vrij om dit recht ook in andere gevallen te verankeren (alle verwerkingen ongeacht hun wettelijke basis).

In de WVP werd er effectief voor gekozen om dit recht naar andere gevallen uit te breiden. Concreet bepaalt artikel 12 van deze wet het volgende:

"(...) Eenieder is bovendien gerechtigd om wegens zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie, zich ertegen te verzetten dat hem betreffende gegevens het voorwerp van een verwerking vormen, behalve wanneer de rechtmatigheid van de verwerking gesteund is op de in artikel 5, b) (verwerking noodzakelijk voor de uitvoering van een overeenkomst en c), (verwerking noodzakelijk is om een verplichting na te komen waaraan de verantwoordelijke voor de verwerking is onderworpen) bedoelde redenen (...)".

Kortom, de WVP voorziet twee bijkomende hypothesen aan het minimum vereist door de Richtlijn 95/46/EG, namelijk wanneer de verwerking gerechtvaardigd is door de vrijwaring van een vitaal belang van de betrokkene (art. 5d) WVP) en wanneer de verwerking gerechtvaardigd wordt door de toestemming van de betrokkene (art. 5a) WVP)

Het ontwerp van Verordening bepaalt daarentegen het volgende: (art.19)" *De betrokkene heeft het recht te allen tijde op gronden die verband houden met zijn bijzondere situatie bezwaar te maken tegen de verwerking op basis van artikel 6, lid 1, onder d), e) en f), van persoonsgegevens, tenzij de voor de verwerking verantwoordelijke dwingende legitieme gronden voor de verwerking aantoont die zwaarder wegen dan de belangen of de grondrechten en fundamentele vrijheden van de betrokkene"*.

Het recht op verzet is aldus uitgesloten ingeval van verwerkingen gebaseerd op de toestemming (art. 6 1 a) van het ontwerp van Verordening), de overeenkomst (6.1.b) en de wet in het algemeen (6.1.c) – wettelijke verplichting van de verantwoordelijke voor de verwerking).

verband houden met hun bijzondere situatie (zie artikel 14. a) van de Richtlijn 95/46/EG). In de plaats daarvan, wil het ontwerp van Verordening voortaan aan de verantwoordelijke voor de verwerking de mogelijkheid bieden om de uitoefening van dit recht te weigeren. Aldus de CBPL doet deze nieuwe regel het risico ontstaan dat verantwoordelijken voor de verwerking voortdurend hun gerechtvaardigd belang inroepen om zich te verzetten tegen de uitoefening van het recht op verzet door de betrokkene²².

78. De CBPL is ook bezorgd omwille van het feit dat artikel 19.3 van het ontwerp van Verordening eveneens het onvoorwaardelijk karakter van het recht op verzet inzake direct marketing, voorzien in artikel 12, 3^{de} lid van de WVP ("zonder enige motivering"), opnieuw in vraag lijkt te stellen aangezien dit artikel bepaalt : "*Wanneer een bezwaar op grond van de leden 1 en 2 (direct marketing) gegrond wordt verklaard....*".

16. Profilering (artikel 20)

79. De CBPL meent dat de waarborgen van de betrokkenen steeds het recht op een menselijke tussenkomst zouden moeten omvatten (wat momenteel alleen voorzien wordt in het ontwerp van Verordening onder artikel 20.2.a). Daarnaast zou ook steeds het recht moeten gelden om zijn standpunt te doen gelden (artikel 15.2.a van de Richtlijn 95/46/EG) Beide waarborgen zouden aldus duidelijk van toepassing moeten zijn in al de gevallen van artikel 20.2 van het ontwerp van Verordening (ingeval van overeenkomst, toepassing van een wet of toestemming).
80. Bij lezing van artikel 20 van het ontwerp van Verordening is het trouwens niet vanzelfsprekend om uit te maken of profilering die uitgevoerd wordt voor direct marketingdoeleinden, en die zich uit in de vorm van specifieke reclameboodschappen, onder de toepassings sfeer valt van dit artikel, aangezien het geen rechtsgevolgen heeft ten opzichte van de betrokkene (behoudens wanneer het vergezeld is van een korting en dus een prijsopofferte) en hem niet noodzakelijk op belangrijke wijze raakt. De CBPL meent niettemin dat dit soort profilering zou moeten onderworpen worden aan de bijzondere voorwaarden van artikel 20.
81. De CBPL betreurt verder dat het ontwerp van Verordening zich ertoe beperkt om in een considerans te vermelden dat de profilering geen betrekking mag hebben op kinderen (considerans 58). De CBPL pleit ervoor dat artikel 20 zelf (maatregelen op basis van profilering) rekening zou houden met deze wens en zou verbieden dat gesteund wordt op de

²² Artikel 19.3 van het ontwerp van Verordening biedt hier geen soelaas aangezien het bepaalt: "*Wanneer een bezwaar (...) gegrond wordt verklaard, worden de betrokken persoonsgegevens door de voor de verwerking verantwoordelijke niet langer gebruikt of anderszins verwerkt*".

toestemming van een kind, aangezien zij van mening is dat in de context van profilering nooit kan voldaan zijn aan de voorwaarde dat er geen gebrek aan evenwicht mag bestaan tussen de belangen van de betrokkene (kind) en de verantwoordelijke voor de verwerking (artikel 7 (4) van het ontwerp van Verordening: voorwaarden voor toestemming).

82. Ten slotte beoogt artikel 20.3 de uitsluiting van geautomatiseerde gegevensverwerkingen, bedoeld om bepaalde persoonlijke aspecten eigen aan een natuurlijke persoon te evalueren, wanneer deze uitsluitend gebaseerd zijn op bijzondere categorieën gegevens (gevoelige gegevens). De CBPL stelt zich de vraag in hoeverre de openbare besturen door deze bepaling niet zullen beperkt worden in hun openbaar beleid inzake gezondheidszorg. In de ogen van de CBPL zou ter zake een oplossing kunnen gevonden worden in het raam van de uitvoering van artikel 21 van het ontwerp van Verordening. Bovendien maakt de CBPL zich de bedenking in welke mate een dergelijke verwerking uitsluitend gebaseerd kan zijn op gevoelige gegevens.

17. Responsabilisering van de verantwoordelijke voor de verwerking (artikel 22)

83. De CBPL waardeert de verankering van het responsabiliseringsbeginsel voor de verantwoordelijken voor de verwerking dat hen verplicht in preventieve maatregelen te voorzien die elke eventuele aantasting van de gegevensbescherming moeten vermijden. Het is inderdaad beter dit vooraf aan te pakken door preventieve mechanismen te gebruiken die een schending beletten, dan gebonden te zijn door beginselen en eventuele sancties bij niet-naleving. Dit beginsel wordt heden reeds toegepast in de bindende bedrijfsvoorschriften.
84. De CBPL merkt evenwel een gebrek aan coherentie door het feit dat het beginsel enkel de verantwoordelijken voor de verwerking beoogt (artikel 22.1), terwijl de lijst met opgesomde mechanismen voor de uitvoering van het responsabiliseringsbeginsel eveneens rechtstreeks betrekking heeft op de verwerker (artikel 22.2).
85. De CBPL is verder van oordeel dat de verplichtingen bedoeld in artikel 22.3 zouden moeten worden verduidelijkt. Dit artikel handelt over een verplichte audit en het is niet duidelijk of de "evenredigheid" die in de laatste zin van dit artikel 22.3. wordt vermeld van toepassing is op de verplichting zelf (de audit zou m.a.w. niet verplicht zijn tenzij de situatie dit rechtvaardigt) of alleen op het feit dat hij zal uitgevoerd worden door interne of externe controleurs (m.a.w.: naargelang de situatie zal de verplichting al dan niet de tussenkomst van externe controleurs vergen). De verschillen in de vertalingen van het ontwerp van Verordening dragen enkel bij tot nog meer verwarring.

86. De CBPL meent in elk geval dat de verantwoordelijke voor de verwerking het beste geplaatst is om zelf te oordelen – hierbij rekening houdend met aard van de verwerkte gegevens, de risico's, het eventuele bestaan van andere beschermingsmechanismen, enz. – of de uitvoering van een externe audit in zijn organisatie een nuttige maatregel betreft, dan wel of een interne controle volstaat. .

18. Privacy by design en by default (artikel 23)

87. De CBPL steunt de invoering van deze beginselen maar onderstreept dat de ontwikkeling van verwerkingssystemen soms niet in handen is van de verantwoordelijken voor de verwerking maar in deze van product- en softwareontwikkelaars.

19. De vertegenwoordiger (artikel 25)

88. Ingeval van toepassing van artikel 3.2²³ van het ontwerp van Verordening, voorziet artikel 25 van het ontwerp van Verordening in de aanduiding van een vertegenwoordiger in de Unie.

89. De rol van de vertegenwoordiger zou moeten uitgeklaard worden. Fungeert hij enkel als contactpersoon binnen de Unie voor de autoriteiten voor gegevensbescherming of vervult hij eveneens een rol als juridisch verantwoordelijke? Artikel 4.14 van het ontwerp van Verordening bepaalt dat hij door de toezichthoudende autoriteiten kan worden aangesproken (in de Engelse versie, "may be addressed by **any** supervisory authority"). Deze rol als contactpersoon wordt bevestigd door artikel 53.1.c) over de bevoegdheden van de gegevensbeschermingsautoriteiten (in toepassing van deze bepaling kunnen zij hem gelasten om alle nuttige informatie mee te delen), alsook door artikelen 28.3 en 29. Inzake juridische verantwoordelijkheid is het op z'n minst verbazend dat artikel 78, betreffende de mogelijkheid voor de lidstaten om sancties te voorzien, eveneens van toepassing is op de vertegenwoordiger, hoewel nergens naar hem wordt verwezen in artikel 79 (administratieve sancties) of in artikel 77 (burgerlijke aansprakelijkheid). Overigens, door niet duidelijk te bepalen dat de juridische verplichtingen die rusten op de verantwoordelijke voor de verwerking eveneens van toepassing zijn op de vertegenwoordiger, kan de invoering van een rechtstreekse strafrechtelijke verantwoordelijkheid voor problemen zorgen aangezien men

²³ "Deze Verordening is van toepassing op de verwerking van persoonsgegevens van in de Unie wonende betrokkenen door een niet in de Unie gevestigde voor de verwerking verantwoordelijke, wanneer de verwerking betrekking heeft op:

a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie; of
b) het observeren van hun gedrag."

normaal gezien niet strafrechtelijk verantwoordelijk kan gesteld worden voor de fouten van anderen²⁴.

90. Verder voorziet het ontwerp van Verordening in verschillende uitzonderingen op de verplichting tot het aanstellen van een vertegenwoordiger (artikel 25.2) en de CBPL heeft hier een aantal bedenkingen bij.
91. Vooreerst meent zij dat het nuttig blijft om een vertegenwoordiger aan te duiden, zelf in het geval waar de verantwoordelijke voor de verwerking gevestigd is in een derde land dat een passend beschermingsniveau waarborgt (artikel 25.2 a). De CBPL onderschrijft op dit punt het advies van ICO²⁵, dat stelt dat een verantwoordelijke voor de verwerking die gevestigd is in een derde land dat een passend beschermingsniveau waarborgt, de Verordening zou kunnen schenden zonder echter de wet van dit derde land te overtreden.
92. Ten tweede voorziet het ontwerp van Verordening eveneens in een uitzondering voor ondernemingen die minder dan 250 personeelsleden tewerkstellen (artikel 25.2.b), hoewel het aantal medewerkers aldus de CBPL geen relevant criterium kan zijn voor het evalueren van de risico's (cf. infra).
93. Bovendien, wat de uitzondering betreft voor de verantwoordelijke voor de verwerking die slechts occasioneel goederen of diensten aanbiedt aan in de Unie wonende betrokkenen (artikel 25.2. d), kan het criterium "incidenteel aanbieden van goederen en diensten" toepassingsproblemen veroorzaken (één enkele inzameling van gevoelige gegevens betreffende 1.000.000 personen zou occasioneel kunnen zijn?).
94. Tot slot pleit de CBPL voor een volledige schrapping van elke uitzondering op de verplichting tot het aanstellen van een vertegenwoordiger, in de gevallen waarin gevoelige gegevens worden verwerkt.

20. Documenten (artikel 28)

95. De CBPL kan instemmen met het schrappen van de verplichte aangifte om deze te vervangen door een verplichte interne documentatie van de verwerkingen. De wezenlijke elementen van de persoonsgegevensverwerkingen zouden makkelijk toegankelijk moeten zijn voor de

²⁴ Het geval van strafrechtelijke verantwoordelijkheid voor rechtspersonen uitgezonderd, maar hier gaat het om een specificiteit.

²⁵ Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework, 27 februari 2012, blz. 17.

betrokkenen en zouden ter beschikking moeten gehouden worden van de DPA's. Bijvoorbeeld via de functionaris voor de gegevensbescherming of via een website.

96. De CBPL heeft kunnen vaststellen dat het bijzonder belang van de aangifte niet zozeer bestaat uit de gecreëerde transparantie (aangezien weinig burgers het openbaar register raadplegen) maar wel uit het feit dat zij elke verantwoordelijke voor de verwerking verplicht zich pertinente vragen te stellen met betrekking tot de voorgenomen gegevensbescherming. Het is dan ook zaak ervoor te zorgen dat deze oefening bij het opzetten en uitrollen van een verwerking steeds gebeurt. Het opmaken, updaten en het bijhouden van een interne documentatie laat bijgevolg toe de voordelen van de aangifte te behouden (bewustzijn van de noodzaak om de wetten na te leven). De nadelen van de verplichte aangifte (onnodige bureaucratie, kosten voor onderhoud van een weinig geraadpleegd openbaar register) kunnen vermeden worden.
97. De CBPL stelt vast dat de uitzonderingen voorzien op de verplichte documentatie (lid 4) te ruim zijn aangezien elke verantwoordelijke in ieder geval steeds een basisdocumentatie zou moeten bijhouden met de belangrijkste elementen betreffende de gegevensverwerking : contactgegevens van de verantwoordelijke voor de verwerking en wie in concreto onmiddellijk kan aangesproken worden door de betrokkene voor de uitoefening van diens rechten (maar ook de identiteit van de verwerkers, van de eventuele vertegenwoordiger, van de functionaris voor gegevensbescherming, beknopte beschrijving van de verwerkingen (zoals de doeleinden, de categorieën gegevens en de ontvangers)).
98. Voormelde uitzondering kan ook niet gelden voor de 'gevoelige persoonsgegevens'.
99. In elk geval moet erover gewaakt dat de DPA snel en volledig kan ingelicht worden bij het opvragen van documentatie en inlichtingen (terecht verder uit te werken zoals door lid 5 en 6 voorzien op uniforme wijze door de Commissie (na advies van de DPA's).
100. Tot slot dient te worden opgemerkt dat de lijst van informatiegegevens die wordt opgesomd in artikel 28, lid 2 verregaand is. En voor sommige verwerkingen moeilijk als niet onmogelijk toe te passen. Zo is de CBPL van oordeel dat het voor de verantwoordelijke voor de verwerking niet mogelijk is om steeds vooraf te bepalen hoe lang hij de gegevens zal bewaren. De verplichting zal dan ook voldoende soepel moeten worden geschreven, uitgewerkt en gehandhaafd om een concrete toepassing, case by case, toe te laten. Ruimte moet dus gelaten worden om de verantwoordelijke of verwerker toe te laten bepaalde informatie niet aan te leveren in zoverre op redelijke grond kan gemotiveerd worden waarom dit moeilijk of onmogelijk is. Dit sluit niet uit dat basiselementen steeds zullen moeten gedocumenteerd worden. Het is zaak dat de verordening dit onderscheid maakt.

21. Medewerking met de toezichhoudende autoriteiten (artikel 29)

101. De CBPL waardeert de invoeging van dit beginsel (artikel 29) maar de verplichte mededeling van informatie mag niet beperkt moeten worden tot de hypothesen van onderzoek (53.2a) maar moet ruimer zijn en onder meer betrekking hebben op artikel 53.1c..
102. De DPA moet in staat gesteld worden voor het geheel van haar taken van controle en toezicht de verantwoordelijke c.q. verwerker alle relevante informatie dwingend op te vragen.
103. Tevens zal moeten worden voorzien hoe en wie antwoorden moet in het kader van het unieke loketsysteem (toepassing artikel 51.2.) en welke de investituur is voor de andere DPA's. Teneinde hiaten te vermijden moet erin voorzien worden dat elke DPA beroep kan doen op deze medewerkingsplicht, zonder dat enige bevoegdheidsexceptie kan ingeroepen worden.

22. Beveiliging van de verwerking (artikel 30)

104. De CBPL waardeert dat het ontwerp van Verordening de verplichtingen inzake beveiliging eveneens rechtstreeks oplegt aan de verwerker (artikel 30.1). In de praktijk sluit dit aan bij onze nationale bepalingen (artikel 16 §4 WVP).
105. De CBPL onderstreept eveneens het nut dat uitdrukkelijk wordt vereist dat de onderrichtingen die aan de verwerker worden gegeven schriftelijk worden vastgelegd (artikel 26.3) en meent dat dit eveneens het geval zou moeten zijn voor het service- of waarborgniveau betreffende de veiligheidsmaatregelen die opgelegd worden door de verantwoordelijke voor de verwerking.
106. Artikel 26.4 voorziet overigens dat wanneer een verwerker persoonsgegevens verwerkt anders dan volgens de instructies, hij de verantwoordelijke voor de verwerking wordt en onderworpen wordt aan de bepalingen die van toepassing zijn op de gezamenlijke verantwoordelijken. Artikel 24, dat de regels bepaalt die van toepassing zijn op de gezamenlijke verantwoordelijken, stelt dat deze door middel van een onderlinge regeling hun respectieve verantwoordelijkheden vaststellen en dat de niet-nakoming van deze verplichting bestraft kan worden met een geldboete tot 500 000 euro of, bij een onderneming, een geldboete van 1 % van haar jaarlijkse wereldwijde omzet (artikel 79.5.e). De CBPL wijst er echter op dat wanneer een verwerker gegevens gebruikt voor de verwezenlijking van een eigen doeleinde, hij de initiële verantwoordelijke voor de verwerking niet noodzakelijk op de hoogte brengt van deze activiteiten. Bijgevolg (en hoewel de CBPL het idee steunt dat de

verwerker in onderhavige situatie beschouwd dient te worden als verantwoordelijke voor de verwerking) zou er moeten over gewaakt worden dat de initiële verantwoordelijke voor de verwerking – die zoals gezegd geen weet heeft van deze nieuwe verwerkingen – niet gestraft kan worden wegens het niet sluiten van een overeenkomst in de zin van artikel 24 van het ontwerp van Verordening..

107. Met betrekking tot de voorwaarden die de verwerker toelaten een beroep te doen op een verdere verwerker (artikel 26.2d), wenst de CBPL het feit te onderstrepen dat naast de voorafgaande toestemming van de verantwoordelijke, deze verdere onderaanneming eveneens het onderwerp moet vormen van een overeenkomst die de latere verwerker aan dezelfde verplichtingen onderwerpt als de oorspronkelijke verwerker. Dit beginsel is vervat in de modelcontractbepalingen 2010/87/EU die goedgekeurd werden door de Europese Commissie en meer in het bijzonder in artikel 11. Dit artikel bepaalt eveneens dat ingeval van tekortkoming van de latere verwerker aan de verplichtingen inzake gegevensbescherming waaraan hij bij overeenkomst is onderworpen, de eerste verwerker ten volle verantwoordelijk blijft ten opzichte van de verantwoordelijke voor de verwerking.

23. Melding van inbreuken aan de DPA's en betrokkene (artikel 31 en 32)

108. Het ontwerp van Verordening verduidelijkt niet of iedere inbreuk op de veiligheid (schending van gegevens) gemeld moet worden aan de DPA. De tekst delegeert aan de Europese Commissie de taak om via een gedelegeerde handeling te bepalen in welke omstandigheden de verantwoordelijken voor de verwerking ertoe gehouden zijn de schending te melden (artikel 31.5). Men zou dus terecht kunnen denken dat bij gebrek aan goedkeuring van gedelegeerde handelingen, iedere schending van de veiligheid gemeld zou moeten worden aan de DPA, hetgeen wellicht een te ruime en onwerkbare verplichting zou vormen. Het behoort eveneens toe aan de Europese Commissie om de omstandigheden te bepalen waarin inbreuken mogelijk de gegevens of de persoonlijke levenssfeer van de betrokkenen kunnen schenden. Deze criteria zouden toelaten de inbreuken te bepalen die eveneens gemeld moeten worden aan de betrokkenen.
109. De CBPL meent dat duidelijke criteria in de tekst zelf zouden moeten ingelast worden en niet achteraf bepaald via gedelegeerde handelingen. Vooreerst dient een overmatige mededeling van kleine inbreuken aan de DPA's vermeden te worden zodat enkel de inbreuken met ernstige gevolgen of die betrekking hebben op een zeer groot aantal personen zouden moeten gemeld worden. Overigens zouden ook de risico's op financiële verliezen moeten ingelast worden in de criteria die een melding aan de betrokkenen vergen.

110. Overigens voorziet het ontwerp van Verordening in een uitzondering op de melding van een inbreuk aan de betrokkene indien de verantwoordelijke voor de verwerking bewijst, tot tevredenheid van de DPA, dat hij de passende technologische beschermingsmaatregelen heeft genomen opdat de gegevens onbegrijpelijk zouden zijn voor iedere persoon die geen toegangsmachtiging bezit (encryptiemaatregelen). De CBPL onderstreept het feit dat de encryptiemaatregelen technisch niet voor gevolg mogen hebben de lezing van de gegevens voor iedereen totaal onbegrijpelijk²⁶ te maken maar hebben dit als doelstelling. De eis zou veeleer deze doelstelling moeten beogen met een vereist technisch karakter, gekoppeld aan de aard van de gegevens, de stand van de techniek en de kosten.
111. Tenslotte meent de CBPL dat het nuttig zou zijn dat in de overeenkomst tussen de verantwoordelijke voor de verwerking en de verwerker wordt bepaald dat ingeval van veiligheidsincident, de verantwoordelijke voor de verwerking en de verwerker samenwerken om de oorzaken van het incident te achterhalen en palliatieve of corrigerende maatregelen te nemen.
112. De CBPL oordeelt dat de huidige tekst nog zovele vragen oproept dat een aanname van de voorliggende tekst tot onmogelijke situaties zal leiden, zowel voor de DPA als voor de verantwoordelijke c.q. verwerker als voor de betrokkene. De zogenaamde data breach melding is vrij nieuw en vraagt nog heel veel onderzoek en experiment. De CBPL is dan ook van oordeel dat voor de uitrol een realistisch stappenplan wordt opgemaakt zodat deze verplichting geleidelijk kan worden ingevoerd. Tevens zal moeten voorzien worden in een nauwlettende opvolging van de voor- en nadelen van het mechanisme, de administratieve en financiële gevolgen en de saldo voor de rechten van de betrokkene. De schaarse ervaringen van de CBPL zijn op desbetreffende niet meteen positief. De CBPL formuleert dan ook een ernstig voorbehoud en verwacht dat voor dit mechanisme nog voldoende voorafgaand onderzoek wordt gedaan naar de haalbaarheid en effectiviteit ervan met centraal de vraag : wordt de burger hier beter van ?

24. Privacyeffectbeoordeling (artikel 33)

113. Naast de omstandigheden voorzien onder 33.1. is het aangewezen de DPA de macht te geven een PIA op te leggen bij gemotiveerd besluit. Dit moet de DPA toelaten gemoduleerd en passend op te treden.

²⁶ De CBPL suggereert de term "onbegrijpelijk" (unintelligible) te vervangen door ontoegankelijk (unaccessible).

114. De CBPL begrijpt niet wat de 'specifieke risico's' zouden zijn bij 33.2.c : de openbaar toegankelijke ruimten zijn op vandaag bij uitstek plaatsen die door optisch-elektronische apparatuur bewaakt worden. Behoudens uitzonderlijke omstandigheden waar de DPA kan optreden en PIA opleggen valt niet in te zien waarom (grootschalige) videobewaking van openbaar toegankelijke ruimten (draagwijdte van het begrip?) specifieke risico's oplevert (behalve wanneer speciale applicaties zouden worden ingezet zoals bijvoorbeeld facial recognition of wanneer de camera's en/of de beelden niet op een wijze zouden worden gebruikt die strookt met de redelijke verwachtingen van het grote publiek). Dit spoort in elk geval niet met de ervaringen van de CBPL met camerabewaking.
115. Artikel 33.4. is niet duidelijk en kan op velerlei manieren geïnterpreteerd of genegeerd worden. Deze bepaling moet worden geschrapt of verduidelijkt.
116. De CBPL vraagt zich af waarom artikel 33.5 verwijst naar verwerkingen die uitgevoerd worden in het raam van de EU-wetgeving en niet eveneens deze van de lidstaten. Bij het aannemen van nationale wetgeving zou steeds een privacyeffectbeoordeling moeten gebeuren (zie considerans 73). De CBPL ziet dan ook niet in waarom enkel EU-wetgeving en niet de andere wetgevingsinstrumenten (aangenomen door een parlementaire assemblee) worden vrijgesteld. Deze uitzondering moet voor elke wetgeving gelden maar moet wel gecompenseerd worden door verplichte advisering door de betrokken DPA (artikel 52.1.f.): in het kader van deze raadpleging zal de bevoegde DPA dan wel uitmaken of een PIA en op welke manier deze moet uitgevoerd worden nuttig en nodig is).
117. De CBPL is voorstander van het instrument "privacyeffectbeoordeling". Zij kan het principe dan ook volkomen onderschrijven.
118. De CBPL heeft evenwel de ervaring dat een goede PIA niet te zwaar mag worden en ook niet mag verwateren tot een stieriele stijloefening waarin veel wordt geschreven door duur betaalde consultants. Er moet daarentegen alles op alles gezet worden om van een PIA een trefzeker en concreet instrument te maken dat zo onbevagen en duidelijk mogelijk aangeeft wat de bedoelingen, finaliteit is van de beoogde verwerking, wat de risico's zijn, wat de keuzemogelijkheden inhouden, hoe de verplichtingen van de verantwoordelijke cq verwerker zijn nagekomen. De kardinale vraag daarbij moet steeds zijn of de burger, de betrokkene, baat dan wel schade kan ondervinden en wat eraan gedaan wordt om de rechten en de vrijheden van die burger te versterken.

119. De wijze waarop deze verplichting verder wordt geconcretiseerd, zoals voorzien onder artikelen 33.6. en 33.7. is dan ook belangrijk. Ook hiervoor vraagt de CBPL een doordachte invoering en geregelde monitoring. Zie *mutatis mutandis supra*.

25. Voorafgaande toestemming en voorafgaande raadpleging van de DPA (artikel 34)

120. Het ontwerp van Verordening wil de bevoegdheid voor voorafgaande toestemmingen vanwege de autoriteiten voor gegevensbescherming strikt beperken tot de internationale gegevensdoorgiften (artikel 34.1). De huidige Belgische regelgeving op het vlak van gegevensbescherming voorziet echter in een systeem van voorafgaande machtigingen voor welbepaalde gegevensdoorgiften vanuit Belgische overheidsdiensten. Artikel 34 dreigt dit systeem aldus op de helling te zetten.

121. De beschermings- en proceduremaatregelen die in België werden uitgewerkt voorzien immers onder andere in de oprichting van Sectorale comités (Sociale Zekerheid en Gezondheid, Rijksregister, Federale Overheid, Statistieken, Phenix (Justitie), Kruispuntbank van Ondernemingen) die een voorafgaande machtigingsbevoegdheid bezitten. Deze comités werden opgericht in de schoot van onze DPA maar zijn gemengd, want samengesteld uit een deel leden van de CBPL en een deel deskundigen of leden van openbare overheden. Deze comités dienen te waken over gegevensverwerkingen door openbare besturen, vooral via voorafgaande machtigingen. Vooraleer deze openbare besturen bepaalde persoonsgegevens kunnen ter beschikking stellen van andere overheden of derden, dient hiertoe een machtiging te worden bekomen van een dergelijk comité. Dit is bijvoorbeeld het geval voor de toegang en het gebruik van het Rijksregisternummer en de toegang tot de bevolkingsregisters.

122. De procedure van voorafgaande machtiging door deze comités kan de openbare sector op nuttige wijze begeleiden bij de invoering van een flux persoonsgegevens. Deze comités vervullen de rol van gids ten aanzien van de verantwoordelijken voor de verwerking. Zij kunnen niet alleen een toegang volledig machtigen of weigeren, maar zij kunnen ook machtigingen toekennen waaraan (opschortende) voorwaarden worden gekoppeld

123. De invoering van voorafgaande raadplegingen, zoals voorzien in het ontwerp van Verordening zal daarentegen systematisch leiden tot ofwel een gebrek aan reactie van de DPA (wat tot rechtsonzekerheid leidt in hoofde van de verantwoordelijke voor de verwerking), of tot een verbod²⁷ op de verwerkingen, wanneer deze niet conform zijn aan de wetgeving (artikel

²⁷ Artikel 34, punt 3, voorziet wel in de verplichting ten aanzien van de DPA om in geval van een verbod "passende voorstellen" te doen "om alsnog aan deze verordening te voldoen". Vandaag kunnen de Belgische sectorale comités - in de gevallen waarin nog verbeterpunten qua privacybescherming gedetecteerd worden - meteen een machtiging verlenen waaraan zij een (opschortende) voorwaarde koppelen. In het systeem van het ontwerp van verordening zal de

34.3). Bovendien zou een dergelijk verbod zelfs kunnen opgelegd worden in gevallen waarin de verwerking vastgelegd is in een wet, wat overmatig is.

124. De CBPL merkt in ondergeschikte orde ook op dat in artikel 34.4 van het ontwerp van Verordening aan de autoriteiten voor de gegevensbescherming de keuze wordt geboden om een lijst op te stellen van verwerkingen die een voorafgaande raadpleging vergen. De CBPL meent dat dit een overmatige bevoegdheid betreft, aangezien dergelijke keuzes democratisch (en dus door de wetgever) dienen te worden gemaakt.

125. **Samenvatten, meent de CBPL dan ook dat het Belgische systeem van sectorale comités, opgericht ter bescherming van persoonsgegevens in de openbare sector onverkort zou moeten kunnen behouden blijven** en dat het ontwerp van Verordening aldus niet zou mogen raken aan louter nationale systemen die geen beletsel vormen voor het vrije verkeer van gegevens. De huidige tekst van het ontwerp van Verordening voorziet deze mogelijkheid evenwel niet (noch in artikel 34, noch in Hoofdstuk IX). Naar verluidt zou de vertegenwoordiger van de Europese Commissie – in het kader van de DAPIX-vergaderingen – nochtans verklaard hebben dat men begrip heeft voor dit Belgisch standpunt. De CBPL verzoekt dan ook om de tekst van het ontwerp van Verordening effectief in deze zin aan te passen.

26. De functionaris voor gegevensbescherming (artikelen 35 t.e.m. 37)

126. Het ontwerp van Verordening wijdt een volledige afdeling van het hoofdstuk betreffende de verplichtingen van de verantwoordelijke voor de verwerking en de verwerker aan de functie van functionaris voor de gegevensbescherming (artikelen 35-37).

127. De CBPL verwelkomt deze formele erkenning van de functionaris voor gegevensbescherming en zijn bijstandsrol²⁸ voor de verantwoordelijke voor de verwerking en de verwerker bij de uitvoering van de verschillende verplichtingen die op hen rusten krachtens de Verordening. De aanduiding van een functionaris voor de gegevensbescherming draagt bij tot de uitvoering van het beginsel "accountability" en de "internal privacy management" benadering van de Verordening waarbij toch een nauwe band blijft bestaan met de autoriteit voor gegevensbescherming en de betrokkenen.

gegevensbeschermingsautoriteit in dergelijke situaties steeds moeten weigeren en "passende voorstellen" doen, wat de facto impliceert dat de aanvrager nadien een nieuwe aanvraag moet indienen, wat weinig flexibel en inefficiënt is..

²⁸ Opmerking bij de vertaling: de CBPL merkt op dat de formulering « monitor the implementation and application of the policies..» die gebruikt wordt in artikel 37 §1 b) in het Frans vertaald werd door « contrôler la mise en œuvre..». Zij is van mening dat deze vertaling niet passend is. De formulering «veiller à (surveiller) et assister» (in de zin van bijvoorbeeld een hartmonitor) verdient de voorkeur.

128. Indien het ontwerp van Verordening op een dag in werking zou treden zal de rol en het statuut van de "functionaris voor de gegevensbescherming" in de zin van artikel 17bis eindelijk worden gepreciseerd; precisering waarop de CBPL reeds vele jaren aandringt bij de Belgische executieve²⁹.
129. De CBPL stelt tevreden vast dat de functionaris voor gegevensbescherming een persoon kan zijn die tewerkgesteld wordt door de verantwoordelijke voor de verwerking of een derde persoon (artikel 35.8) en eveneens de rol van contactpersoon krijgt toevertrouwd voor de uitoefening door betrokkenen van hun rechten. De door de verantwoordelijke voor de verwerking en de verwerker te verstrekken informatie is in dit opzicht essentieel (artikel 14.1.a)).
130. Wat de medewerking betreft met de autoriteit voor gegevensbescherming, deelt de CBPL de visie van het ontwerp van Verordening (artikel 37 § 1 h)). Een relatie, onder meer inzake uitwisseling van informatie, lijkt essentieel.
131. De CBPL is in het algemeen ook tevreden over de waarborgen op onafhankelijkheid die vereist worden door het ontwerp van Verordening en zij keurt de verplichtingen goed die opgelegd worden aan de verantwoordelijken voor de verwerking en de verwerkers om de functionaris voor gegevensbescherming toe te laten zijn functie ten volle uit te oefenen (artikel 35 § 5, 6, 7 en artikel 36). Deze waarborgen voegen zich bij deze die zij herhaaldelijk heeft gewenst bij de uitoefening van haar adviesbevoegdheid³⁰. Zij stelt evenwel het totaal ontbreken vast van mechanisme/procedure/garanties tegen ontslag van de functionaris ingevolge de uitoefening van zijn functies. Zij zou het ten minste nuttig geacht hebben dat de autoriteiten voor gegevensbescherming hierover geïnformeerd zouden worden en/of dat aan de functionaris voor gegevensbescherming de mogelijkheid zou geboden worden van aanhangigmaking bij de autoriteit voor gegevensbescherming ingeval van (gepland) ontslag³¹.
132. Trouw aan haar rechtspraak is de CBPL verder van oordeel dat de functie van functionaris voor gegevensbescherming samen met een andere functie kan uitgeoefend worden voor zover de functionaris voor gegevensbescherming in deze hoedanigheid alle nodige vrijheid en onafhankelijkheid geniet om zijn opdrachten tot een goed einde te brengen³². De CBPL

²⁹ Zie onder meer CBPL, Advies 15/2002 van 2 mei 2002 houdende een Ontwerp van koninklijk besluit ter uitvoering van artikel 3, §6, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (§ 17).

³⁰ Zie adviezen avis 01/2007, 16/2007 en 39/2008

³¹ Zie bijvoorbeeld de Franse wet 78-17 van 6 januari 1978 relative à l'informatique, aux fichiers et aux libertés (Chapitre IV) en het décret d'application 2005-1309 van 20 oktober 2005

³² CBPL, Advies 33/2002 van 22 augustus 2002 houdende een Ontwerp van wet houdende oprichting van het Federaal Kenniscentrum voor de Gezondheidszorg (punt 21). In dezelfde zin, CBPL, Advies 19/2002 van 10 juni 2002 houdende een (1) Ontwerp van wet tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke

onderstreept in dit verband dat de onafhankelijkheid van de functionaris voor gegevensbescherming redelijkerwijs niet absoluut kan zijn, al was het maar omdat de functionaris voor gegevensbescherming, tenminste in sommige gevallen, gebonden is door een arbeidsovereenkomst aan de verantwoordelijke voor de verwerking.

133. **Niettegenstaande de gunstige beoordeling die voorafgaat, is de CBPL geen voorstander van de keuze die gemaakt werd om de aanduiding van een functionaris voor de gegevensbescherming in sommige gevallen verplicht te stellen.** In haar ogen dient de aanduiding van een functionaris voor de gegevensbescherming optioneel te blijven. De aanduiding van een functionaris voor de gegevensbescherming is een maatregel – onder al deze die bijdragen tot de accountability – die de verantwoordelijke voor de verwerking vrij moet kunnen nemen, rekening houdend met de uitgevoerde verwerkingen, de aard van de verwerkte gegevens, de risico's, het bestaan van andere beschermingsmechanismen en de reële winst voor de gegevensbescherming die de aanduiding van een functionaris voor de gegevensbescherming in dat geval zou meebrengen.

134. In ondergeschikte orde heeft de CBPL ook opmerkingen omtrent de criteria die in het ontwerp van Verordening worden gebruikt om te bepalen of een aangestelde voor de gegevensverwerking al dan niet verplicht is:

- a. Eén van de criteria betreft de situatie waarin de verwerking wordt uitgevoerd door een onderneming met minimaal 250 werknemers. De Commissie is van oordeel dat het aantal werknemers geen goed criterium betreft om te bepalen of een aangestelde voor de gegevensbescherming nodig is. Een onderneming kan immers 1000 werknemers tewerkstellen maar amper (gevoelige) verwerkingen van persoonsgegevens verrichten, terwijl een klein bedrijf met 10 werknemers juist heel veel gevoelige verwerkingen kan uitvoeren.
- b. De CBPL stelt zich de vraag hoe de volgende zinsnede in artikel 35, punt 1, c) moet worden geïnterpreteerd: "*(...) verwerkingen die vanwege hun aard, hun omvang en/of hun doel regelmatige en stelselmatige observatie van betrokkenen vereisen.*" De CBPL vraagt dat in de tekst zelf van artikel 35, of op zijn minst in een considerans zou opgehelderd worden wat hieronder moet begrepen worden. Aangezien het gaat om een hypothese waarin een functionaris voor de gegevensbescherming verplicht moet worden aangeduid, kan deze verduidelijking

personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen. (2) Ontwerp van koninklijk besluit betreffende de identiteitskaarten. (3) Ontwerp van koninklijk besluit houdende overgangsmaatregelen in verband met de elektronische identiteitskaart in België; CBPL, Advies 23/2006 van 12 juli 2006 betreffende het voorontwerp van wet betreffende de omkadering van de negatieve lijsten (punten 42 tot 44).

niet wachten op de gedelegeerde handeling die de Europese Commissie zichzelf in artikel 35.11 voorbehoudt, goed te keuren.

27. Gedragscodes

135. De CBPL meent dat het niet de bevoegdheid van de Europese Commissie maar wel van het Europees comité voor gegevensbescherming zou moeten zijn om vast te stellen of een gedragscode algemeen toepasselijk is op het grondgebied van de Unie (artikel 38.4).

28. Doorgifte van persoonsgegevens naar derde landen of naar internationale instellingen

136. De CBPL meent dat in het ontwerp van Verordening de regels inzake grensoverschrijdende gegevensdoorgiften duidelijker zijn omschreven. Dit is met name het geval voor de definitie van de beoordelingscriteria van een gepaste bescherming van derde landen of voor de uitdrukkelijke erkenning van de bindende bedrijfsvoorschriften.

137. De CBPL staat ook achter de wens om de verplichtingen van de ondernemingen te vereenvoudigen via de opheffing van de verplichte nationale machtigingen wanneer er gebruikt wordt gemaakt van bindende bedrijfsvoorschriften of van modelcontractbepalingen.

138. Voor wat nu specifiek het artikel 42.5 betreft, meent de CBPL dat het aan duidelijkheid te wensen overlaat. Dit artikel lijkt betrekking te hebben op de overheidssector en zou zich daartoe uitdrukkelijk moeten beperken. Het is van wezenlijk belang dat er oplossingen worden aangeboden voor de internationale gegevensstromen voor de overheidssector. Modelcontractbepalingen of bindende bedrijfsvoorschriften dienen niet om gebruikt te worden in de overheidssector. De samenwerkingsakkoorden of de unilaterale verbintenissen die in de overheidssector worden gebruikt, zouden moeten blijven voortbestaan en zouden in de tekst zelfs uitdrukkelijk moeten worden erkend.

139. Aangaande de bindende bedrijfsvoorschriften, wil het ontwerp van Verordening de voorwaarden oplist waaraan moet worden voldaan en het baseert zich hiervoor op de bestaande vereisten die in de documenten van de Groep van het artikel 29³³ omschreven staan. Het ontwerp van Verordening herneemt evenwel niet de bestaande vereiste inzake de noodzaak om binnen een ondernemingsgroep een intern systeem in te voeren voor de

³³ Hoofdzakelijk WP153 maar ook WP74 en WP108

klachtenbehandeling van de betrokken personen evenals de invoering van een passend opleidingsprogramma³⁴. Deze verplichtingen zijn niet duidelijk vastgelegd en zijn slechts terug te vinden in de omschrijving van de opdrachten van de functionaris voor de gegevensbescherming. Indien die laatste moet worden ingelicht van klachten die betrekking hebben op persoonsgegevens, wil dit niet zeggen dat hijzelf noodzakelijk deze opdrachten moet vervullen (klachtenbehandeling³⁵, opleiding werknemers) en bovendien garandeert de uitdrukkelijke verwijzing naar artikel 35 in het artikel 43.2.h niet altijd zijn bestaan. De documenten van de Groep artikel 29 vereisen overigens van de leden van de ondernemingsgroep een engagement om bij een conflict tussen een buitenlandse wetgeving en bindende bedrijfsvoorschriften, te aanvaarden dat interne transparantie (binnen de groep) noodzakelijk is en dat zij zich bij twijfel ook moeten onderwerpen aan de Europese gegevensbeschermingsautoriteiten³⁶. Deze voorwaarde werd niet opnieuw opgenomen in artikel 43 van het ontwerp van Verordening. En zoals hoger werd benadrukt, zou de toepassing van de gedefinieerde, bindende bedrijfsvoorschriften zich niet alleen moeten beperken tot de multinationals die een vestiging hebben binnen de Unie.

140. De afwijking in artikel 44.1.h. inzake de mogelijkheid voor de verantwoordelijke voor de verwerking om zelf de omstandigheden van een doorgifte te beoordelen en de passende, noodzakelijke garanties te bieden is niet alleen in strijd met het stelsel van de bindende bedrijfsvoorschriften "ad hoc" en de BCR waarbij een tussenkomst van de overheid noodzakelijk is, maar brengt ze ook in gevaar.

29. De gegevensbeschermingsautoriteiten (artikelen 46 t.e.m. 54)

141. Hoofdstuk VI van het ontwerp van Verordening is volledig gewijd aan de toezichthoudende autoriteiten (gegevensbeschermingsautoriteiten). Hun statuut, de regels betreffende hun vestiging, hun competenties, functies en bevoegdheden zijn talrijker en uitdrukkelijker omschreven dan in de Richtlijn 95/46/EG.

142. Het ontwerp van Verordening wil de onafhankelijkheid van de gegevensbeschermingsautoriteiten versterken en houdt daarbij rekening met het arrest van 9 maart 2010 van het Hof van Justitie van de Europese Unie tegen de Republiek Duitsland³⁷.

³⁴ Punten 2.1. en 2.2. van WP153.

³⁵ Het klachtenbeheer moet evenwel worden toevertrouwd aan een persoon of een departement die in de uitoefening van zijn functie een gepaste graad van onafhankelijkheid heeft (zie WP 153 van de Groep van het artikel 29 maar ook de aanbeveling 01/2006 van de CBPL inzake whistleblowing).

³⁶ Punt 6.3. van WP153.

³⁷ Europees Hof van Justitie (Grande chambre) , 9 maart 2010, affaire C-518/07.

143. De CBPL staat gunstig tegenover de vereisten omschreven in artikel 47 van het ontwerp van Verordening betreffende de onafhankelijkheid van de gegevensbeschermingsautoriteiten, inzonderheid het *globale* begrip van die onafhankelijkheid: onafhankelijkheid van zijn leden (commissarissen CBPL), voldoende human resources en eigen personeel (secretariaat CBPL), technische middelen, gepaste financiële middelen onderworpen aan een financieel toezicht die de onafhankelijkheid niet bedreigt en de ter beschikkingstelling van de noodzakelijke lokalen en infrastructuur om haar taken en bevoegdheden naar behoren te kunnen uitoefenen. Op dit punt vestigt de CBPL de aandacht van de bevoegde Belgische overheid op de nieuwe functies die zij zal toegewezen krijgen en de daaruit voortvloeiende gevolgen inzake personele en financiële middelen. Als voorbeelden kunnen hier vermeld worden: de voorafgaande privacyeffectbeoordeling (artikel 33), de behandeling van de meldingen van inbreuken op de gegevens en het onderzoek naar de vraag of de verantwoordelijke voor de verwerking de passende maatregelen heeft genomen om schadelijke gevolgen te voorkomen (artikel 31-32), bijstand aan haar Europese ambtgenoten, de samenwerking met die laatsten en haar deelname aan het Europees Comité voor Gegevensbescherming (hoofdstuk VII), evenals haar nieuwe bevoegdheid om administratieve straffen op te leggen (artikel 53.4 en artikelen 79.4, 5 en 6).

144. In verband met de algemene voorwaarden die van toepassing zijn op de leden van de toezichthoudende autoriteit (artikel 48), heeft de CBPL twee opmerkingen:

- a. Vooreerst is zij van mening dat de gevolgen verbonden aan het feit dat een lid de noodzakelijke voorwaarden voor de uitoefening van zijn functie niet langer vervult of die een ernstige fout heeft begaan, aan de beoordeling van de nationale wetgever moet worden overgelaten. De CBPL is van oordeel dat de Europese Commissie haar bevoegdheden overschrijdt door in die gevallen erin te voorzien dat een lid zijn ontslag neemt of uit zijn pensioenrechten en andere voordelen wordt ontzet.
- b. Ten tweede is zij van oordeel dat de leden van de toezichthoudende autoriteiten steeds door het parlement zouden moeten benoemd worden en niet door de Regering (artikel 48, punt 1, laat ter zake de keuze aan de lidstaten). In het parlement zetelen immers vertegenwoordigers van alle politieke strekkingen, wat een bredere democratische controle garandeert. Een benoeming van de leden door het Parlement sluit aldus de CBPL nauwer aan bij de onafhankelijkheidsvoorwaarden die in het arrest van het Hof van Justitie van 9 maart 2010 worden gesteld..

145. Wanneer de gegevensverwerking plaatsvindt in het kader van de activiteiten van een verantwoordelijke voor de verwerking of een verwerker die in verschillende lidstaten gevestigd is, bepaalt het ontwerp van Verordening dat de bevoegde autoriteit enkel deze is waar de "belangrijkste vestiging" van de verantwoordelijke voor de verwerking zich bevindt (artikel 51.2). De Europese gegevensbeschermingsautoriteiten hebben dit gekwalificeerd als de **one-stop-shop** voor de verantwoordelijken voor de verwerking, namelijk het principe van een uniek loket voor die laatsten.
146. Hoewel dit *prima facie* een aantrekkelijk principe betreft³⁸, heeft de CBPL toch ernstige bedenkingen bij de werkbaarheid ervan.
147. Zo betreft de notie "belangrijkste vestiging" één van de cruciale elementen in artikel 52 en de definitie die aan deze notie wordt gegeven (artikel 4, punt 13) is allesbehalve duidelijk, vooral wat de volgende zinsnede betreft: "(...) *wanneer in de Unie geen besluiten over het doel van of de voorwaarden en middelen voor de verwerking van persoonsgegevens worden genomen, is de belangrijkste vestiging de plaats waar de voornaamste gegevensverwerking in het kader van de activiteiten van een vestiging van een voor de verwerking verantwoordelijke in de Unie plaatsvindt. (...)*". De CBPL stelt zich ook de vraag hoe bevoegdheidsconflicten tussen DPA's – die er onvermijdelijk zullen ontstaan op basis van dit onduidelijk artikel 52 – zullen opgelost worden.
148. Verder is de CBPL bezorgd over de juridische en praktische consequenties van de aanduiding van één bevoegde autoriteit in een bepaalde zaak. Zij meent dat deze bezorgdheid het beste kan geïllustreerd worden aan de hand van een aantal voorbeelden:
- a. Een Belgische werknemer die in België is tewerkgesteld voor een onderneming waarvan de "belangrijkste vestiging" gesitueerd is in Ierland, dient bij de Belgische DPA een klacht in tegen zijn werkgever omdat zijn telefoon wordt afgeluisterd. De Belgische DPA maakt de zaak over aan de Ierse DPA, die in dit geval de bevoegde autoriteit zou zijn. Stel dat de Ierse DPA een schikking treft tussen de werkgever en de werknemer. Dient de Ierse DPA dan – naast het ontwerp van Verordening – bijvoorbeeld ook rekening te houden met het Belgisch sociaal –en strafrecht?
Indien deze vraag bevestigend wordt beantwoord, impliceert dit dat de Ierse DPA dus de Belgische wetgeving dient toe te passen. Een consequente toepassing van

³⁸ De CBPL begrijpt in het algemeen de bedoeling van de invoering van een uniek loket ("one stop shop") die erin bestaat dat voor eenzelfde verwerking die uitgevoerd wordt in verschillende lidstaten, verschillende autoriteiten parallel zouden bevoegd zijn en er bijgevolg verschillende beslissingen zouden kunnen genomen worden.

een dergelijke benadering zou ook inhouden dat iedere DPA potentieel de regelgeving van de andere 26 EU-lidstaten moet kunnen toepassen wanneer deze krachtens artikel 51 is aangeduid als bevoegde DPA en wanneer de desbetreffende zaak niet alleen een invloed heeft op de privacy-Verordening, maar ook op andere nationale rechtsregels (wat vaak het geval is). De CBPL stelt zich ernstige vragen bij de haalbaarheid van een dergelijk systeem

Indien deze vraag ontkennend wordt beantwoord, is de kans reëel dat in het voorbeeld de schikking van de Ierse DPA op gespannen voet zal komen te staan met Belgische dwingende rechtsbepalingen uit het sociaal –en strafrecht. In laatstgenoemde hypothese zal een Belgische rechter de schikking van de Ierse DPA niet kunnen respecteren³⁹.

- b. Een Chinees bedrijf heeft een vestiging in België van waaruit telefonisch producten worden verkocht aan Belgische burgers. Het bedrijf heeft meerdere vestigingen in de EU, waarvan de Poolse de "belangrijkste" is. Het bedrijf stelt voor om alle telefoongesprekken tussen haar werknemers en klanten op te nemen en legt uit dat dit enkel tot doel heeft om de opleiding en vorming van de werknemers te verbeteren. De vakbonden vrezen echter dat de geregistreerde gesprekken voor geheel andere doeleinden (met name controle van de werknemers) zullen gebruikt worden en vragen aan de Belgische DPA om te bemiddelen. De Belgische DPA – die nochtans het beste de sociale verhoudingen, de maatschappelijke problemen, alsook de taal van alle betrokkenen kent – zal de vakbond echter moeten vragen om zicht tot de Poolse DPA te wenden...
- c. Een Amerikaans ICT-bedrijf die meerdere vestigingen heeft in de EU, waarvan de "belangrijkste vestiging" in Parijs gesitueerd is, installeert samen met een Belgisch bedrijf een cloud-toepassing en in het kader daarvan ontstaat een security breach waardoor gegevens van Belgische burgers openbaar gemaakt worden. Welke DPA is bevoegd? Wellicht de Franse. Dient de Belgische DPA dan alle benadeelde burgers naar de CNIL door te sturen?

149. Samengevat vreest de CBPL aldus dat er zich door artikel 52, punt 2, eideloze bevoegdheidsconflicten en discussies tussen de gegevensbeschermingsautoriteiten zullen

³⁹ Dit voorbeeld vestigt overigens ook de aandacht op een ander probleem, met name het feit dat de bevoegdheidsregels die ten aanzien van DPA's gelden niet coherent zijn met deze van de rechterlijke macht en dit terwijl het eerder zeldzaam is dat de feiten van een inbreuk op de Verordening uitsluitend betrekking hebben op gegevensbescherming: de strafbare feiten bestaan meestal uit meerdere inbreuken waarvan één aspect de "gegevensbescherming" betreft en waarvan de andere aspecten enkel door de rechterlijke macht kunnen beoordeeld worden. Een concreet geschil moet in de praktijk echter vaak in zijn totaliteit behandeld worden (ongeacht het aantal rechtstakken waaraan de zaak raakt en ongeacht welke DPA/rechtbank er bevoegd is) om tot een goede oplossing te komen.

voordoen en zij meent eveneens dat deze bevoegdheidsregel tot onlogische en onwerkbare situaties zal leiden. **De CBPL verwerpt daarom het criterium "belangrijkste vestiging"**.

150. Zij is er zich tegelijk van bewust dat de discussie over de aanduiding van de bevoegde DPA een moeilijke oefening betreft die nog heel wat reflectie zal vergen. Ten einde een eerste bijdrage te leveren aan deze discussie, onderlijnt zij dat dit volgens haar één van de mogelijke alternatieve criteria zou kunnen zijn: een DPA is bevoegd in gevallen waarin de verantwoordelijke voor de verwerking zich met zijn activiteiten tot een bepaald cliënteel/bepaalde markt richt op het grondgebied van de lidstaat waar deze DPA opereert.

30. Samenwerking en conformiteit (artikelen 55 t.e.m. 72)

151. Gelet op de globalisering van de verwerkingen van persoonsgegevens, acht de CBPL het zeker nuttig om de bestaande samenwerkingssystemen tussen de Europese autoriteiten te versterken met mechanismen van wederzijdse bijstand (artikel 55), gezamenlijke operaties (artikel 56) en conformiteitstoetsing (artikelen 57 tot 63).

152. De CBPL is daarentegen van oordeel dat de mogelijkheid in hoofde van de Europese Commissie om te verzoeken om een maatregel van een DPA te schorsen die aldus deze Commissie tot een incorrecte of inconsequente toepassing van de Verordening dreigt te leiden (artikel 60), te ver gaat. Hoe kan een gegevensbeschermingsautoriteit immers in alle onafhankelijkheid beslissingen nemen, wanneer deze achteraf door de uitvoerende macht kunnen in vraag gesteld worden? Een dergelijke benadering is aldus de CBPL in strijd met artikel 8, 3^{de} lid, van het Handvest van de Grondrechten van de Europese Unie.

153. De oprichting van een vast secretariaat voor de Groep 29 (toekomstig Europees Comité voor gegevensbescherming – ECGB) (artikel 71) acht de CBPL nuttig, gelet op het voortdurende stijgend aantal onderwerpen die binnen deze groep worden behandeld. Ze drukt evenwel haar twijfels uit over de termijn die werd vastgelegd voor de goedkeuring van adviezen binnen de ECGB (1 maand) (artikel 58.7).

31. Sancties (artikelen 78 en 79)

154. Vooreerst heeft de CBPL ernstige twijfels omtrent het nut van een uniform, administratief straffenstelsel, dat de gegevensbeschermingsautoriteiten moeten uitvoeren. De CPBL vraagt zich af waarom dit vandaag wordt voorgesteld, aangezien zij in de bestaande situatie ter zake niet als problematisch ervaart. Ter illustratie verwijst zij naar het dossier Google Street View en het illegaal inwinnen van gegevens van internetverbindingen (Wi-Fi), waarin de betrokken

gegevensbeschermingsautoriteiten volgens hun beleid en eigen wetgeving het controlestelsel hebben toegepast en desgevallend het beschikbare bestraffingstelsel zonder dat zich daarbij moeilijkheden hebben voorgedaan: het Nederlandse College Beschermingspersoonsgegevens bestrafte Google met een dwangsom, de Franse CNIL legde een boete op en de CBPL droeg het dossier over aan het openbaar ministerie dat aan Google een minnelijke schikking van 150.000 euro voorstelde.

155. Bovendien verzet de CBPL zich tegen het feit dat zij zelf bevoegd zou zijn om sancties op te leggen, met name omwille van haar gehechtheid aan het principe van de scheiding der machten. Hiermee samenhangend, wenst de CBPL te weten of het samengaan van alle bevoegdheden die de hare zouden zijn krachtens het ontwerp van Verordening, te verenigen zijn met de onpartijdigheidsvereiste die op zijn minst bij de uitoefening van bepaalde van die bevoegdheden noodzakelijk is. Deze vraag zou grondig moeten worden onderzocht, vooral in het licht van de jurisprudentie van het Europees Hof voor Rechten van de Mens⁴⁰. Een grondige reorganisatie van CBPL zou nodig zijn (op organisatorisch niveau, bijvoorbeeld middels gescheiden kamers, naar voorbeeld van het systeem dat de Franse CNIL heeft ingevoerd).

156. In dit verband merkt de Commissie ook op dat

- a. vanuit grondwettelijk standpunt uitsluitend de rechterlijke macht bevoegd is om te controleren of de wet wordt toegepast en om de niet-naleving ervan te bestraffen. Die bevoegdheid is aldus toevertrouwd aan onafhankelijke magistraten.
- b. het eerder zeldzaam is dat de feiten van een inbreuk op de Verordening uitsluitend betrekking hebben op gegevensbescherming: de strafbare feiten bestaan meestal uit meerdere inbreuken waarvan één aspect de "gegevensbescherming" betreft. In die gevallen zal de bevoegdheid van de gegevensbeschermingsautoriteit verhinderen dat die laatste de feiten op een globale manier kan bevatten. Zij zal zich moeten beperken tot de het aspect "gegevensbescherming", want zij kan op haar niveau geen beroep doen op de techniek van de samenloop van strafbare feiten, volgens dewelke de hoogste straf op de aangeklaagde feiten wordt toegepast. Alleen de hoven en rechtbanken kunnen zich baseren op deze techniek en de strafbare feiten in hun geheel vatten.

⁴⁰ Arrest Dubus vs. Frankrijk van 11 juni 2009.

157. De Commissie stelt zich verder de vraag of in artikel 78 administratieve dan wel strafrechtelijke sancties geïmplementeerd worden. Dit artikel bepaalt het volgende : *“De lidstaten stellen de regels inzake sancties vast die van toepassing zijn op schendingen van deze Verordening en treffen alle maatregelen die nodig zijn om de daadwerkelijke toepassing van die sancties te garanderen (...). De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn”*.
158. Gelet op de keuze voor een Verordening (in plaats van een Richtlijn) en na samenlezing van artikel 78 met de in de preambule aangegeven juridische basis voor het ontwerp van Verordening, besluit de CBPL dat de opdracht voor de lidstaten er hier in bestaat om administratieve sancties te voorzien. Immers, wanneer de EU de lidstaten wil opdragen strafrechtelijke sancties in het nationale recht in te schrijven, dient daartoe artikel 83.2 van Verdrag betreffende de werking van de EU⁴¹ als juridische basis te worden aangewend. Dit artikel vereist duidelijk dat het aannemen van minimumstandaarden met betrekking tot strafrechtelijke sancties door een *Richtlijn* dient te gebeuren (en niet door een *Verordening*).
159. Ook omtrent de kwalificatie van de sancties die in artikel 79 zijn vastgelegd, heeft de CBPL ernstige bedenkingen. Hoewel deze sancties expliciet zijn omschreven als zijnde “administratieve sancties”, is de CBPL van oordeel dat het hier veeleer strafrechtelijke sancties betreft en dit gelet op de vaste rechtspraak van het Europees Hof voor de Rechten van de Mens⁴² en gelet op het beleid van de Europese Unie⁴³. Het essentiële belang van de vaststelling dat hier om strafrechtelijke sancties gaat, betreft het feit dat artikel 6 van het Europees Verdrag voor de Rechten van de Mens en artikel 6 van het Verdrag betreffende de Europese Unie voorschrijven dat in een dergelijke context in voldoende rechtswaarborgen moet voorzien worden (zoals bijvoorbeeld een beroepsmogelijkheid bij een onafhankelijke rechter). In de tekst van het ontwerp van Verordening wordt hier helemaal geen gewag van gemaakt.
160. Of het nu administratieve of strafrechtelijke sancties betreft, het is duidelijk dat het ontwerp van Verordening twee systemen (artikel 78 en 79) invoert en het samenspel tussen de twee zal aldus de CBPL tot problemen leiden. Zij is met name van mening dat een cumulatieve toepassing van de twee bestraffingsstelsels, kan leiden tot een schending van het algemene

⁴¹ “(...) Indien onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten op het gebied van het strafrecht nodig blijkt voor een doeltreffende uitvoering van beleid van de Unie op een gebied waarop harmonisatiemaatregelen zijn vastgesteld, kunnen bij richtlijnen minimumvoorschriften worden vastgesteld met betrekking tot de bepaling van strafbare feiten en de sancties op het betrokken gebied. (...)”

⁴² Cf. Engel-Arrest van 8 juni 1976.

⁴³ Cf. artikel 6.3. van het Verdrag betreffende de Europese Unie, op grond waarvan kan besloten worden dat de EU zich aansluit bij de criteria die het Europees Hof voor de Rechten van de Mens gebruikt om strafzaken van andere zaken te onderscheiden. Het Europees Hof van Justitie heeft dat uitdrukkelijk bevestigd in onder andere het Spector-arrest van 23 december 2009 (§42, C-45/08)

rechtsprincipe volgens hetwelk niemand vervolgd of bestraft kan worden op basis van dezelfde feiten (non bis in idem).

161. Ter ondersteuning van haar analyse vermeldt De CBPL het arrest van 10 februari 2009, van de Grote Kamer van het Europees Hof voor Rechten van de Mens (Zolotoukhine v. Rusland) dat vaststelde dat wanneer er een administratieve en een strafrechtelijke straf gecumuleerd worden, er een schending is van artikel 4 van het protocol nr. 7 volgens hetwelk: *“nul ne peut être poursuivi ou puni pénalement par les juridictions du même Etat en raison d’une infraction pour laquelle il a déjà été acquitté ou condamné par un jugement définitif conformément à la loi et à la procédure pénale de cet Etat”* (niemand kan door de rechtbanken van dezelfde Staat strafrechtelijk vervolgd of bestraft worden op grond van een overtreding waarvoor hij reeds werd vrijgesproken of veroordeeld met een definitief vonnis overeenkomstig de wet en de strafrechtelijke procedure van die Staat) (vrije vertaling). Het Hof meende in dit geval inderdaad dat de procedure die tegen de eiser werd opgestart, hoewel ze werd gekwalificeerd als administratief intern recht, beoordeeld moet worden als een strafrechtelijke procedure, met name omwille van de aard van de overtreding en de zwaarte van de straf.
162. De Commissie vestigt er ook de aandacht op dat in een Rechtstaat alleen inbreuken kunnen worden bestraft die voldoende werden omschreven, ongeacht of dit gebeurt via de strafrechtelijke dan wel administratieve straffen. De CBPL stelt hier vast dat tal van inbreuken bedoeld in artikel 79, 4^{de} tot 6^{de} lid of de inbreuken waaraan de nationale wetgever desgevallend in toepassing van artikel 78 sancties zal koppelen, de algemene verplichtingen hernemen en zijn omschreven in algemene om niet te zeggen vage bewoordingen die op zijn minst een aanzienlijke beoordelingsmarge laten aan de verantwoordelijken voor de verwerking. Wat is in dit geval de voorspelbaarheid? De CBPL vermeldt aldus de artikelen 5a) (rechtmatige, eerlijke en transparante verwerking), 5 e) (niet overmatige bewaartermijn uitgaande van de verwezenlijking van de doeleinden), 5 f) (verwerking onder het gezag van de verantwoordelijkheid voor de verwerking die toeziet op de conformiteit van iedere verwerking), 6 e) (verwerking die noodzakelijk is voor de verwezenlijking van een opdracht van openbaar belang) en 6 i) (gerechtvaardigd belang van de verantwoordelijke voor de verwerking die niet voorgaat op de belangen of fundamentele rechten en vrijheden van de betrokken personen).
163. Tot slot merkt de CBPL op dat artikel 79 van het ontwerp van Verordening heel weinig appreciatie-ruimte laat aan de DPA's. Zij kunnen met name geen rekening houden met de specifieke omstandigheden waarin de inbreuken werden gepleegd. Slechts in een beperkt aantal gevallen waarin een verantwoordelijke een eerste, onopzettelijke inbreuk pleegt, kan een sanctie worden vervangen door een waarschuwing. De CBPL meent dat hier meer flexibiliteit aangewezen is.

32. Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerkingen (artikelen 80 t.e.m. 85)

A. De bestaande nationale regels voor de overheidssector

164. Hoofdstuk IX heeft betrekking op de verschillende sectoren die nationaal van elkaar verschillen, en waarvan wordt aangenomen dat deze divergenties gerechtvaardigd zijn door het verschil in cultuur en juridische tradities. Bijvoorbeeld op het gebied van vrije meningsuiting, de verwerking van gegevens die de gezondheid betreffen, sociale zekerheid of tewerkstelling. Om die reden werden de Staten verzocht om voor deze facetten hun eigen nationale wetgevingen uit te werken.
165. Sinds de invoering en de ontwikkeling van de fundamentele rechten, meer in het bijzonder van het recht op eerbiediging van de privacy in het algemeen en van het recht op bescherming van de persoonsgegevens in het bijzonder, hebben verschillende Europese landen er heel specifiek naar gestreefd om deze rechten in hun administratief en grondwettelijke weefsel in te voegen. Deze regels betreffende de bescherming van de privacy in het kader van gegevensverwerkingen die door de overheid worden verricht, verschillen nationaal zo van elkaar, dat de CBPL van mening is dat de bestaande systemen binnen elke lidstaat bewaard zouden moeten kunnen blijven.
166. Bijvoorbeeld, hoewel er op het gebied van de verwerking van gezondheidsgegevens een actiekader werd gelaten aan de lidstaten voor medische doeleinden, volksgezondheid of sociale zekerheid, werd in dit hoofdstuk geen enkele manoeuvreerruimte gelaten voor de verwerking van andere persoonsgegevens (dan deze betreffende de gezondheid) in het kader van de sociale zekerheid (en de gegevensverwerkingen binnen deze sector hebben evident niet enkel betrekking op de eenvoudige terugbetaling van de gezondheidskosten; ze kunnen bijvoorbeeld ook betrekking hebben op de uitbetalingen voor werkloosheid of pensioenen).
167. Een tweede voorbeeld betreft het bestaande Belgische systeem van sectorale comités, dat werd opgericht ter bescherming van persoonsgegevens in de openbare sector, en waarvan de CBPL meent dat het onverkort zou moeten kunnen behouden blijven (cf. supra).
168. De CBPL is dan ook van oordeel dat de mogelijkheid moet voorzien worden om sommige bepalingen van het ontwerp van Verordening niet van toepassing te verklaren op verwerkingen van persoonsgegevens binnen de overheidssector, zodat bestaande nationale systemen – met eigen waarborgen ter bescherming van de privacy (bv. systeem van voorafgaande

machtigingen), die in de loop der jaren in het juridisch kader werden verankerd – niet in het gedrang komen en verder op het niveau van de lidstaten kunnen geregeld worden.

B. Gebruik van het identificatienummer van het Rijksregister

169. De CBPL betreft de schrapping van artikel 8.7 van de Richtlijn 95/46/EG, dat de staten toelaat de voorwaarden te bepalen waaronder een nationaal identificatienummer of ieder ander algemeen identificatiemiddel kan worden verwerkt. Deze bepaling wordt geschrapt zonder verdere uitleg en wordt niet vervangen door een specifieke regel gewijd aan dit bijzonder gegeven.

170. De vrees bestaat dan ook dat het identificatienummer van het Rijksregister niet meer zou kunnen gebruikt worden in België. Dit nummer vormt echter één van de hoekstenen van de belangrijkste bestaande egovernment-projecten en een verbod op het gebruik ervan legt *de facto* een bom onder al deze projecten, terwijl daarvoor vanuit privacy-overwegingen geen ernstige verantwoording voor bestaat. De Belgische wetgeving voorziet immers in een bijzonder beschermend systeem van controle en machtiging voor het gebruik van het identificatienummer van het Rijksregister. Zoals hoger reeds aangehaald, wenst de CBPL dat dit systeem van voorafgaande machtigingen zou behouden blijven.

171. Naar verluidt zou de vertegenwoordiger van de Europese Commissie op de DAPIX-vergadering verklaard hebben dat de oude regeling die wordt voorzien in artikel 8.7. van Richtlijn 95/46/EG effectief opnieuw een plaats zou moeten krijgen en dat het aldus niet de bedoeling was om de creatie en het gebruik van identificatienummers te beletten. De CBPL is alvast verheugd omtrent dit standpunt en zij staat er ook op dat de tekst van het ontwerp van Verordening in die zin wordt aangepast.

C. De gegevensverwerkingen betreffende de gezondheid

172. Artikel 81 van het ontwerp van Verordening bevat specifieke bepalingen voor de verwerking van persoonsgegevens betreffende de gezondheid.

173. Deze regels moeten samen gelezen worden met de definitie van de notie "persoonsgegevens betreffende de gezondheid", die wordt vermeld in artikel 4.12. Laatstgenoemde bepaling dient op haar beurt gelezen te worden in het licht van considerans 26⁴⁴. Deze lectuur leert dat aan dit begrip een zeer ruime interpretatie wordt gegeven: het

⁴⁴ Persoonsgegevens betreffende de gezondheid dienen met name alle gegevens te omvatten die betrekking hebben op de gezondheidstoestand van de betrokkene, informatie over de registratie van de persoon voor de verlening van

gaat niet alleen om gegevens betreffende de fysieke of mentale gezondheid maar eveneens om iedere informatie over de verlening van een gezondheidsdienst aan een persoon (zoals registratie van de patiënt voor de zorg, informatie betreffende betalingen of verkiesbaarheid van de patiënt voor gezondheidszorgen).

174. De CBPL is vooreerst van mening dat deze door het ontwerp van Verordening voorgestelde definitie (veel) te ruim is en onvoldoende rekening houdt met de talrijke contexten waarin verwerkingen van dergelijke gegevens zich kunnen voordoen.

175. Bovendien stelt zij vast dat in artikel 81 ook nog specifieke voorwaarden worden opgelegd (verplichting van het bestaan van een specifieke wettelijke basis, het verplichte beroepsgeheim of de gelijkwaardige vertrouwelijkheidsplicht) om dergelijke gegevens te verwerken en deze modaliteiten doen vragen rijzen:

- a. De CBPL acht de vereiste dat bijvoorbeeld gegevensverwerkingen met als doel het factureren van ziekenhuisdiensten noodzakelijkerwijs zou moeten omkaderd worden door een specifieke wet, weinig zinvol/realistisch
- b. Het is voor de CBPL belangrijk dat het begrip "gelijkwaardige vertrouwelijkheidsplicht" (artikel 81, punt 1, a)) niet wordt opgevat als zijnde beperkt tot het beroepsgeheim, aangezien dit met zich mee zou brengen dat voor al deze verwerkingen het toezicht vereist is van een beroepsbeoefenaar in de gezondheidszorg (ook voor de gegevensverwerkingen die worden verricht in het kader van de sociale zekerheid en de terugbetaling van gezondheidszorgen).
- c. De relatie tussen artikel 81 en artikel 9 van het ontwerp van Verordening is aldus de CBPL geheel onduidelijk. Laatstgenoemd artikel voorziet in een lijst van uitzonderingsgronden waarin de verwerking van gezondheidsgegevens toegelaten is. Eén van deze grondslagen wordt vermeld in artikel 81 (met name artikel 9, punt 2, h) en artikel 81 lijkt enkel op deze specifieke situatie betrekking te hebben. Nochtans kunnen medische gegevens ook op basis van andere gronden worden verwerkt die worden opgesomd in artikel 9, punt 2, en voor die verwerkingen wordt geen enkele link gelegd met artikel 81.

gezondheidsdiensten, informatie over betalingen of voorwaarden voor gezondheidszorg met betrekking tot de persoon; een aan een persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van de persoon geldt voor gezondheidsdoeleinden; informatie over de persoon die tijdens de verstrekking van gezondheidszorg aan hem is verzameld; informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van biologische monsters; de identificatie van een persoon als verstrekker van gezondheidszorg aan de betrokkene; of informatie over bv. ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de feitelijke fysiologische of biomedische staat van de betrokkene, ongeacht de bron, zoals een arts of een andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een invitrodiagnostiek

Bovendien overlappen sommige van de andere uitzonderingsgronden die vervat liggen in artikel 9, punt 2, met de drie gronden die opgesomd worden in artikel 81, punt 1, zonder dat dit specifiek gemotiveerd wordt.

De CBPL verzoekt aldus om de link tussen de artikelen 9 en 81 grondig te herbekijken.

D. De gegevensverwerkingen voor historische, statistische of wetenschappelijke doeleinden

176. Het ontwerp van Verordening wijdt een volledig artikel aan historisch, statistisch of wetenschappelijk onderzoek (artikel 83), wat zeker de lezing vergemakkelijkt van de wettelijke voorwaarden voor de gegevensverwerkingen die worden verricht in het kader van een wetenschappelijk onderzoek⁴⁵. De voorwaarden uiteengezet in artikel 83.1, die het gebruik van anonieme of gecodeerde gegevens aanmoedigt in wetenschappelijke onderzoek, liggen perfect in lijn met onze nationale wetgeving en andere internationale standaarden⁴⁶. Desalniettemin meent de CBPL dat de tekst van artikel 83, punt 1, nog duidelijker het principe zou moeten verwoorden dat gegevensverwerkingen in de mate van het mogelijke moeten worden verricht op basis van anonieme gegevens en dat indien dit onmogelijk is, de verwerking dient plaats te vinden op basis van gecodeerde gegevens en dat enkel indien ook dit niet mogelijk is, een verwerking van identificeerbare gegevens toelaatbaar mag zijn.

177. De CBPL acht het verder nuttig dat het historisch, statistisch of wetenschappelijk onderzoek werd erkend als een wettelijke grond voor de verwerking van gevoelige gegevens (artikel 9.2.i)⁴⁷. De Richtlijn 95/46/EG liet toe dat de Lidstaten het wetenschappelijk onderzoek konden erkennen als redenen van zwaarwegend, openbaar belang (considerans 40) en er bestonden ter zake verschillende nationale implementaties.

178. De CBPL heeft meer voorbehoud ten aanzien van artikel 6.2. dat lijkt toe te laten dat er verwerkingen van niet-gevoelige gegevens worden verricht voor wetenschappelijke doeleinden zonder dat het eerste lid van artikel 6 wordt nageleefd. Het is in de ogen van de CBPL nochtans van wezenlijk belang dat ieder onderzoeksproject deze verplichte wettelijkheidstest ondergaat om te vermijden dat er onethische onderzoeksprojecten zouden worden toegelaten.

⁴⁵ Vandaag is de nuttige informatie verspreid over de Richtlijn 95/46/EG, met name over de consideransen 29, 34 en 40; evenals in de artikelen 6.1.b, 6.1.e, 11.2, 13.2).

⁴⁶ Hoofdstuk II van het koninklijk besluit van 13/02/2001 maar zie ook artikel 40 van de Duitse federale wet, artikel 46 van de Oostenrijkse federale wet (DSG 2000), artikel 16 van de Estse wet en artikel 3 van de Aanbeveling Rec (2006)4 van de Raad van Europa over het onderzoek dat gebruik maakt van menselijk lichaamsmateriaal.

⁴⁷ Het internationaal congres over het wetenschappelijk onderzoek dat de CBPL organiseerde in november 2010 leidde eveneens tot deze vaststelling.

179. Artikel 5.e. voorziet in de uitdrukkelijke mogelijkheid om de gegevens langer te bewaren voor historische, statistische of wetenschappelijke doeleinden, het legitimeert de openbare archieven en herneemt artikel 6.1.e. van de Richtlijn 95/46/EG. Krachtens dit artikel moeten de lidstaten voorzien in gepaste waarborgen en deze waarborgen worden rechtstreeks voorgesteld in de tekst van het ontwerp omdat het de bedoeling is dat het onmiddellijk toepasbaar wordt. De voorwaarde is dat periodiek wordt onderzocht of de verdere bewaring nog noodzakelijk is. De CBPL acht het nuttig om nog andere waarborgen toe te voegen, zoals de noodzaak om het doeleinde van het onderzoek strikt te eerbiedigen en het invoeren van beveiligingsmaatregelen zodat toegang alleen mogelijk is in het kader van het historische, statistisch of wetenschappelijk onderzoek.

180. De CBPL verbaast er zich over dat de uitzonderingen die in de Richtlijn 95/46/EG betreffende de uitoefening van de rechten van de betrokken personen (artikelen 11.2, en 13.2) werden opgenomen, niet meer terug te vinden zijn in het ontwerp van Verordening, tenzij onder de vorm van een eventuele goedkeuring van gedelegeerde handelingen (artikel 83.3). De uitzonderingen zouden moeten vermeld worden in de tekst zelf, zodat kan worden gegarandeerd dat ze van bij de inwerkingtreding bestaan en ze zouden de gepaste waarborgen moeten bevatten waarin de lidstaten vandaag hebben voorzien. Gelet op haar ervaring die de CBPL heeft opgedaan in het kader van de internationale conferentie "Privacy and research: from obstruction to construction" die zij in november 2010⁴⁸ organiseerde, heeft zij een concreet tekstvoorstel:

- *In addition to the circumstances referred to in Article 14(5), paragraphs 1 to 4 of Article 14 shall not apply where the data are directly⁴⁹ or indirectly obtained from the data subject, under condition that the information or part of the information referred to in Article 14 (1 to 3) is likely to render impossible or seriously impair the achievement of the objectives of the scientific research⁵⁰. From the moment that the information is not any more likely to render impossible or seriously impair the achievement of the objectives of the scientific research, the data subject shall be informed without delay.*
- *Article 15 shall not apply under condition that the information or part of the information referred to in Article 14 (1 to 3) is likely to render impossible or seriously impair the achievement of the objectives of the scientific research, unless*

⁴⁸ <http://www.privacyandresearch.be/>

⁴⁹ Une exemption en cas de collecte directe est déjà prévue dans différentes législations nationales, telles que la loi fédérale allemande (Art.33), la loi portugaise (Art. 10) ainsi que la loi luxembourgeoise (art. 27).

⁵⁰ Informer clairement des finalités précises de la recherche peuvent évidemment influencer et dès lors compromettre ses résultats. Une exception similaire se retrouve dans la loi polonaise (Art. 25 de la loi du 29 août 1997) pour les collectes indirectes de données.

the interests of the research are overridden by the interests or the fundamental rights and freedoms of the data subject. From the moment that the information is not any more likely to render impossible or seriously impair the achievement of the objectives of the scientific research, the controller or processor shall grant the data subject access to the data without delay.

E. Gegevensbeschermingsregels van kerken en religieuze verenigingen

181. De CBPL stelt zich de vraag welke de draagwijdte is van artikel 85 van het ontwerp van Verordening.

33. Gedelegeerde handeling en uitvoeringshandelingen

182. Het ontwerp van Verordening wordt gekenmerkt door een groot aantal gedelegeerde handelingen en uitvoeringshandelingen (artikelen 86 en 87).

183. De CBPL is van mening dat in quasi alle gevallen, de voorziene delegaties de voorwaarden niet naleven waaronder de gedelegeerde handelingen toegelaten zijn (artikel 29 §1, 1^{ste} lid TFUE). Het voorwerp van een gedelegeerde handeling dient er normaal op gericht te zijn om een wettelijke handeling aan te vullen door bepaalde technische elementen te preciseren, of om de niet-wezenlijke elementen van de wettelijke handeling zelf te wijzigen. Niettegenstaande de strikte interpretatie die werd gegeven aan het begrip wezenlijke elementen en diens gevolgde de uitgebreidheid van de toegelaten delegaties⁵¹, is de CBPL van oordeel dat de Europese Commissie in dit geval haar bevoegdheden overschrijdt gelet op het aantal toegestane delegaties (artikel 86.2), de onderwerpen van deze en het feit dat bij ontstentenis van sommige, de bepalingen in het ontwerp van Verordening geen (nuttige) uitwerking kunnen hebben.

184. Het ontwerp van Verordening geeft overigens geen enkele informatie over de al dan niet bestaande intentie van de Europese Commissie om deze vele gedelegeerde handelingen goed te keuren, noch over de termijn waarin deze mogelijks goedgekeurd zullen worden. Quid in afwachting van deze gedelegeerde handelingen? Het kan toch niet de bedoeling zijn om een bestaand systeem dat goed werkt te vervangen door nieuwe rechtsregels die nog heel wat cruciale punten gedelegeerde handelingen of uitvoeringshandelingen behoeven (waaromtrent de inhoud en de timing waarbinnen ze zullen genomen worden, hoogst onduidelijk is), vooraleer ze in de praktijk toepasbaar zijn?

⁵¹ N. de Sadeleer, I Hachez " Hiérarchie et typologie des actes juridiques de l'Union européenne", in *les innovations du Traité de Lisbonne : incidences pour le praticien*, Brussel, 2011.

185. De CBPL dringt er dan ook ten stelligste op aan om gedelegeerde handelingen en uitvoeringshandelingen strikt te beperken tot de niet-wezenlijke elementen. Dit impliceert derhalve dat quasi alle artikelen van het ontwerp van Verordening waar het nemen van een dergelijke handeling wordt mogelijk gemaakt, zouden moeten herzien worden.

De Wnd. Administrateur,

De Voorzitter,

(get.) Patrick Van Wouwe

(get.) Willem Debeuckelaere

Bijlage: Bedenkingen over onderscheid publiek-privaat naar aanleiding van het voorstel tot verordening gegevensbescherming COM(2012)11 van 25/01/2012

1.1. Centraal staat de vraag of een afzonderlijk wettelijk, reglementair raamwerk nodig is voor de publieke en de private sector. Hierbij wordt abstractie gemaakt van de specifieke noden voor politie en justitie aangezien de facto hiervoor reeds een ander instrument wordt voorgesteld⁵².

1.2. Een dergelijke aanpak dient zoveel mogelijk vermeden te worden. In de mate van het mogelijke moeten alle regelingen, zowel de basisbeginselen als de concrete uitwerking, zoveel mogelijk gelijkgeschakeld worden. Dit geldt zeker voor de basisprincipes (de grondslagen voor de verwerking, de basisbeginselen, de rechten van de betrokkene, de rechtshandhaving, internationale gegevensuitwisseling). Maar ook voor de concrete uitwerking, procedures, onafhankelijke toezichthouder, uitzonderingen en dergelijke meer moet zoveel mogelijk hetzelfde instrument en juridische raamwerk gelden.

Vandaag maken de internationale, reglementaire teksten inzake bescherming van privacy en persoonsgegevens, dit onderscheid niet en het is de bedoeling dat ze zowel in de particuliere als de openbare sector van toepassing zijn.

Op dit punt kan het Verdrag 108 van de Raad van Europa (1981) geciteerd worden, meer bepaald artikel 3, §1 (toepassingsgebied) dat uitdrukkelijk stelt: "De Partijen verbinden zich dit Verdrag toe te passen op de geautomatiseerde bestanden van persoonsgegevens en op de geautomatiseerde verwerking van persoonsgegevens in de openbare en particuliere sector." Een toepassing in de openbare en particuliere sector is in het proces van de modernisering/herziening van het Verdrag 108 dat momenteel lopende, is op geen enkele manier in vraag gesteld.

Het toelichtend verslag bij het Verdrag 108 formuleert uitdrukkelijk dit brede toepassingsgebied (punten 33 en volgende):

"According to paragraph 1 the convention applies to the public as well as the private sector. Although most international data traffic occurs in the private sector, the convention is nevertheless of great importance for the public sector and this for two reasons. First, Article 3 imposes obligations on the member States to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders. Secondly, the convention offers assistance to data

⁵² Wat meteen tot tal van problemen zal leiden aangezien er geen duidelijke aflijning is gemaakt tussen de wereld van politie en justitie en de private actoren die daarin meespelen (advocaten, notarissen, gerechtsdeurwaarders, gemeentelijke administratieve sancties, private bewaking, privédetectives, enz.). Er zal hoe dan ook nood zijn aan een wettelijk instrument om dit te kaderen.

subjects who wish to exercise their right to be informed about their record kept by a public authority in a foreign country.

*The distinction public sector/private sector is not found in the other provisions of the convention, especially since these terms may have a different meaning in different countries. **But it may play a role in the declarations which the Parties may make with regard to the scope of the convention (paragraph 2).** (geen officiële Nederlandse vertaling beschikbaar).*

Bepaalde landen maken gebruik van de in artikel 3, §2 geboden mogelijkheid om af te wijken van het toepassingsgebied van het Verdrag (zie ook het toelichtend verslag hierboven), met name voor bepaalde bestanden uit de openbare sector⁵³. Gelet op de verklaringen vermeld in de voetnoot, blijkt dat deze uitsluiting van het toepassingsgebied plaatsvond toen de nationale wet voor dit soort bestanden een kader regelde (flexibiliteit voor de openbare sector – rol van de nationale wet).

Het is interessant te weten dat de Belgische staat daarvan geen gebruik heeft gemaakt. Maar het moet gezegd dat destijds de bescherming van persoonsgegevens nog in zijn kinderschoenen stond (het allereerste bindende, juridisch instrument) en dat het een internationaal Verdrag betrof dat in het "nationaal recht moest worden omgezet" (zie verklaring van België van 28/05/1993).

<http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=&DF=&CL=FRE&VL=0>

De Europese richtlijn 95/46/EG dekt op dezelfde manier de openbare en particuliere sector (met de onder randnummer 1.1. vermelde nuance aangaande de politieke en justitiële sectoren en de domeinen die niet onder de bevoegdheid van de Europese wetgever vallen maar onder de nationale soevereiniteit). Dit staat niet alleen letterlijk en uitdrukkelijk in het Verdrag 108 maar wordt ook afgeleid uit de bepalingen van de richtlijn. Zie bijvoorbeeld de definitie van de verantwoordelijke voor de verwerking die ook de "overheid" impliceert. Deze optie wordt in het voorstel van verordening van de Europese Commissie niet in vraag gesteld en werd in de evaluatieverslagen van diezelfde Commissie ook niet als problematisch aanzien.

De instrumentenkeuze van de Europese Commissie, namelijk een rechtstreeks, toepasselijke verordening (i.p.v. een richtlijn die moet worden omgezet in het interne recht) komt ook voor in de

⁵³ Voorbeelden van voorbehoud betreffende "openbare sector": zie de verklaring van Andorra: geen toepassing van het Verdrag op de "openbare registers die uitdrukkelijk geregeld zijn door de wet in Andorra". Liechtenstein heeft dan weer de verwerkingen die het Ministerie van Financiën, de Parlementaire assemblees en Commissies verrichten, uit het toepassingsgebied geschrapt (idem voor Zwitserland voor de parlementaire assemblees). Zie ook de verklaring van Luxemburg die de toepassing van het Verdrag uitsluit op gegevensbanken die krachtens een wet of verordening voor het publiek toegankelijk zijn. Nederland maakte op zijn beurt hetzelfde voorbehoud aangaande talrijke bestanden: archieven aangewezen door de wet, bestanden die dienen voor de uitvoering van de kieswet, het register van de burgerlijk staat, het centraal register van studenten van het hoger onderwijs, opgemaakt in het kader van de wet betreffende het universitair onderwijs (Meer klassiek sloten talrijke landen de gegevensbestanden uit die verband houden met de nationale veiligheid, de openbare veiligheid en strafrechtelijke overtredingen).

analyse. Daar waar een omzetting - die bij een richtlijn door zijn aard noodzakelijk is - aan de nationale wetgever een zekere manoeuvreerruimte liet, met name voor eventuele gegevensverwerkingen van de openbare sector, laat de rechtstreeks toepasselijke eigenschap van een verordening geen nuances toe, tenzij de verordening zelf in zijn tekst zou voorzien in specifieke, genuanceerde of voldoende flexibele bepalingen die rekening houden met de bijzonderheden van deze sector. De lezing van het ontwerp van verordening en de uitleg die de Europese Commissaris V. Reding, daarover verstrekte, geven aan dat de tekst eerst werd bedacht voor ondernemingen en multinationals, vanuit eens treven naar vereenvoudiging, rechtszekerheid en vrij verkeer van gegevens in een gemonialiseerde context. Als men kijkt naar wat de Raad van Europa reeds in 1981 vaststelde, namelijk dat het grootste deel van het (internationaal) gegevensverkeer de particuliere sector betrof, krijgt het streven van de EU betekenis. Dat betekent evenwel niet dat een zekere soepelheid ten opzichte van gegevensverwerkingen uit de openbare sector – zeer duidelijk, geïdentificeerde en afgebakende verwerkingen – de verwezenlijking van die doelstellingen van de particuliere sector in de weg zouden staan. De bescherming van persoonsgegevens in/door de openbare sector zou de verordening eerbiedigen middels specifieke aanpassingen en er zou met de nationale regelgeving ook meer rekening worden gehouden (traditioneler meer van toepassing op die sector, of toch meer dan op de particuliere sector).

1.3. Eén van de moeilijkheden die men steeds ontmoet wanneer een dergelijk onderscheid wordt gemaakt is de vraag naar het criterium dat moet gehanteerd worden. Zal men organiek werken, of verkiest men een materiële aanpak. En wat met de intermediaire instellingen en taken (p&p). De rechtspraak van de Raad van State en het Hof van Cassatie (conflicten van attributie) over bvb. de vraag of vrije onderwijsinstellingen nu al dan niet administratieve overheden zijn is een mooi voorbeeld van een discussie die toch nooit echt beslecht wordt: never ending story. Maar er zijn uiteraard nog tal van andere voorbeelden te geven: sociale zekerheid, gezondheidszorg ...

2.1. Dit betekent niet dat openbare instellingen, bestuursorganen, administraties of wat nog meer tot de openbare overheid behoort *sensu stricto* of *lato* geen nood heeft aan eigen regelingen. De openbare sector beschikt over specifieke kenmerken die eigen zijn aan de overheid: *privilège du préalable*, directe uitvoeringsmacht, het monopolierecht, democratische controle vanuit wetgever en uitvoerende macht, enz. Hiermee moet rekening gehouden worden bij de concrete uitwerking van de basisprincipes en zeker met de procedures en vormen van toezicht en rechtshandhaving.

2.2. Een ander aspect is het bewaken en bewaren van het bereikte acquis: tal van overheidsinstellingen beschikken over een verfijnd instrumentarium voor het verwerken van persoonsgegevens. In vele gevallen bestaat die verwerking ook uit privacy- en veiligheidsregelingen. In vele gevallen werken deze mechanismen bevredigend, om niet te zeggen zeer goed. Bij wijze van voorbeeld kan verwezen worden naar het geheel van de werking van de Kruispuntenbank sociale

zekerheid. Dit systeem thans in vraag stellen door zonder meer de theoretische uitgangspunten van het voorstel EU Verordening persoonsgegevensverwerking te laten prevaleren dreigt voor gigantische bestuurlijke problemen te zorgen en voor het vernietigen van een verfijnd en werkbaar instrumentarium aan persoonsgegevensbescherming. Zie op dezelfde manier de wet op het Rijksregister en het Sectoraal machtigingscomité, een extra mechanisme conform de vereisten van de richtlijn 95/46/EG betreffende de omkadering van de verwerkingen van unieke identificatiemiddelen (zie hierna).

2.3. Evenmin kan voorbijgegaan worden aan de merites van de Richtlijn 95/46: het heeft geen zin om de kwaliteiten van deze richtlijn zomaar opzij te zetten. Bij wijze van voorbeeld: artikel 8 punt 7,⁵⁴ dit heeft in België basis gegeven voor het verder gebruiken van het rijksregisternummer en het uitbouwen van het rijksregister zelf. Uiteraard op een wettelijke en gereguleerde manier, onder meer via het sectoraal comité rijksregister. Het gaat ter zake om een belangrijk instrument in het bestuursrecht, e-government, dat vooreerst voor de publieke sector bedoeld is.⁵⁵

Dit is maar één voorbeeld van de kwaliteit van de vroegere richtlijn die op dit ogenblik jammer genoeg niet werd hernomen in het Europese voorstel. In het kader van specifieke regelingen voor zowel private als publieke toepassingen verdient het dat op de verworvenheden van de Richtlijn 95/46 kan voortgebouwd worden.

2.4. Respect voor de democratische verworvenheden en controle. Hier kan verwezen worden naar de Belgische algemeen verbindend verklaarde collectieve arbeidsovereenkomsten die vanuit het sociaal overleg belangrijke bijdragen hebben geleverd in de privacybescherming en de acceptatie ervan door de sectoren. Maar hetzelfde geldt voor bijvoorbeeld de sociale zekerheid: dit wordt aangestuurd door paritaire vertegenwoordiging en onder controle van het sectoraal comité sociale zekerheid. In het geheel van de privacybescherming zijn er tal van voorbeelden te vinden van privacybescherming die werd uitgewerkt, niet door de overheid *sensu stricto* maar door het middenveld, sociale partners en het geheel van de actoren in een bepaalde sector: zie ter zake de gezondheidssector. Deze verworvenheden vervangen door "delegated acts" is een manifeste afbraak van democratische verworvenheden. Zie ter zake het artikel 81 en 82 van het EU voorstel.

3. Concrete problemen p&p in het huidige voorstel verordening.

⁵⁴ De lidstaten stellen de voorwaarden vast waaronder een nationaal identificatienummer of een ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt.

⁵⁵ Machtigingen worden verleend aan de openbare en private instellingen van het Belgisch recht voor de informatie die zij nodig hebben voor het vervullen van taken van algemeen belang die hen zijn toevertrouwd door of krachtens een wet ... of voor taken die uitdrukkelijk als zodanig erkend worden door het voormelde sectoraal comité (artikel 5, eerste lid, 2^o van de wet van 8 augustus 1983 Rijksregister)

3.1. Artikel 6,1,f (afgewogen belang): het valt niet in te zien waarom thans het artikel 6, rechtmatigheid van de verwerking, de "overheidsinstanties" uitsluit voor deze verwerkingsgrond. Considerans 38 preciseert dat "Aangezien het aan de wetgever is om de rechtsgrondslag te creëren voor gegevensverwerkingen door overheidsinstanties, dient deze rechtsgrond niet van toepassing te zijn op de verwerking door overheidsinstanties in het kader van de uitvoering van hun taken". Die motivatie kan de CBPL niet overtuigen. Zie de redenering in het ontwerp van advies over het voorstel van verordening.

3.2. Quid artikel 21 van het voorstel.

3.3. Het artikel van het voorstel dat het meeste zorgen baart is artikel 34: voorafgaande toestemming en voorafgaande raadpleging. Een volgehouden toepassing van de geest van deze bepaling moet leiden tot het verbieden van het geheel van voorafgaande machtigingen waarop het systeem van de sectorale comités en van de regionale toezichthouders is gebaseerd. Het basismechanisme is immers een voorafgaandelijke machtiging na aanvraag door de verantwoordelijke van de verwerking, het opbouwen van een dossier, het voldoen aan basisverplichtingen (waaronder veiligheid), advies van referentie-instellingen en beoordeling door een paritair samengesteld bestuursorgaan.

De "oplossing" die er voor de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer erin bestaat gebruik te maken van de mogelijkheid, bedoeld in artikel 34§4 (raadplegingsmechanisme), kan volgens de Commissarissen, in de huidige tekst zeker en vast dezelfde bescherming bieden als het mechanisme van de bestaande sectorale comités.

Artikel 34 §4 bepaalt immers: *"De toezichthoudende autoriteit stelt een lijst op van verwerkingen waarover uit hoofde van lid 2, onder b), voorafgaande raadpleging moet plaatsvinden en publiceert deze. De toezichthoudende autoriteit deelt deze lijsten mee aan het Europees Comité voor gegevensbescherming"*.

Artikel 34, §2 b) vermeldt dan weer dat de verantwoordelijke voor de verwerking de gegevensbeschermingsautoriteit raadpleegt als: *"de toezichthoudende autoriteit het nodig acht om vooraf tot raadpleging over te gaan over verwerkingen die naar hun aard, hun omvang en/of hun doel waarschijnlijk specifieke risico's voor de rechten en vrijheden van betrokkenen met zich brengen en die overeenkomstig lid 4 zijn gespecificeerd"*.

MAAR ...

- Het Belgische machtigingssysteem van de Sectorale comités is niet uitsluitend gebaseerd op het risico (soms zelfs op het niet bestaan van risico's, bijvoorbeeld Kruispuntbank van ondernemingen) maar ook / vooral op een sectorale benadering;
- Wat de samenstelling betreft die voor de helft een afspiegeling is van de betrokken sector kunnen er vragen gesteld worden over de verenigbaarheid ervan met artikel 47 §3 (onafhankelijkheid) van het voorstel van verordening dat vermeldt dat "De leden van de toezichthoudende autoriteit onthouden zich van alle handelingen die onverenigbaar zijn met hun taken en verrichten gedurende hun ambtstermijn geen andere al dan niet bezoldigde beroepswerkzaamheden";
- En VOORAL, de lijst met verwerkingen die de CBPL zou goedkeuren (en die een afspiegeling is van de bevoegdheden van de huidige sectorale comités) is in toepassing van artikel 58, §2 c) voor advies voorgelegd aan het Europees Comité voor gegevensbescherming en dientengevolge voor eventueel advies en een mogelijke opschortingsmaatregel van de Europese Commissie (artikels 59 e.v., hoofdstuk dat handelt over samenwerking en een coherentiemechanisme).

3.4. Artikel 51.2, competentie: het uniek loket principe: stelt bijzondere problemen voor overheden, meer in het bijzonder bij relaties, contracten, samenwerking bij internationale bedrijven en organisaties (bvb ict, inzonderheid cloud, farmaceutica, financial ...). Aangezien de bevoegde dpa veelal niet de nationale toezichthouder zal zijn stelt zich wel het probleem hoe een buitenlandse privacycommissie zal kunnen omgaan met de eigen bestuurlijke en administratieve, staatsrechterlijke opbouw van al die andere landen...

3.5. Hoofdstuk IX, Bepalingen in verband met specifieke situaties op het gebied van de gegevensverwerking, inzonderheid de artikelen 81, 82, in zekere mate 83 en 85 stellen bijzondere vragen en problemen voor de publieke sector. Op het eerste zicht openen deze mogelijkheden voor de overheid om op te treden in bepaalde domeinen vanuit hun overheidsopdracht. Deze zijn evenwel als een uitzonderingsregeling voorzien waardoor in het geheel van het concept van de verordening geen ruimte wordt gegeven voor andere domeinen waarop de overheid actief is. Daarenboven zijn deze uitzonderingen dermate scherp en beperkend geformuleerd dat deze eerder een keurslijf worden dan een reële mogelijkheid voor eigen overheidsop treden.

4. Een basisprobleem, dat veel verder gaat dan het doel van deze nota p&p vloeit voort uit de totalitaire aanspraak van het EU voorstel.

4.1. Het verwerken van persoonsgegevens is geen op zich staande activiteit. De bescherming van persoonsgegevens is een bij uitstek transversaal en relatief grondrecht. Transversaal omdat dit recht op quasi alle menselijke activiteiten inspeelt en toegepast moet worden. Relatief omdat het recht

quasi nooit alleen staat maar steeds in balans en evenwicht moet gebracht worden met andere rechten en vrijheden.

4.2. Het formuleren van een absoluut geldend systeem van persoonsgegevensbescherming dat geen ruimte (meer) laat voor andere rechten en vrijheden, verankerd in de staatsrechterlijke, bestuurlijke en organisatorische opbouw van een staat, samenleving en maatschappij dreigt dan ook in botsing te komen met die andere grondvesten en grondrechten.