I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbeschermingbetreffende de mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's — „Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie"

(2011/C 181/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag betreffende de werking van de Europese Unie, en met name op artikel 16,

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op artikel 7 en 8,

Gelet op Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([1]),

Gelet op Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens ([2]), en met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

A. ALGEMEEN DEEL

1. Inleiding

1.1. *Een eerste algemene analyse*

1. Op 4 november 2010 heeft de Commissie de mededeling „Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie" (de „mededeling") vastgesteld ([3]). De mededeling werd voor advies naar de EDPS gestuurd. Het verheugt de EDPS dat hij geraadpleegd is door de Commissie overeenkomstig artikel 41 van Verordening (EG) nr. 45/2001. Reeds voor de goedkeuring van de mededeling werd de EDPS in de gelegenheid gesteld informele opmerkingen te maken. Een deel van deze opmerkingen is in de definitieve versie van het document in aanmerking genomen.
2. In de mededeling stelt de Commissie de aanpak vast voor een herziening van de wettelijke regeling van de EU voor de bescherming van persoonsgegevens op alle werkterreinen van de Unie, waarbij zij in het bijzonder rekening houdt met de uitdagingen die voortvloeien uit de globalisering en de nieuwe technologieën ([4]).
3. De EDPS is over het geheel genomen ingenomen met de mededeling. Hij is er namelijk van overtuigd dat het huidige rechtskader van de EU inzake gegevensbescherming moet worden herzien, om effectieve bescherming te garanderen in een zich almaar verder ontwikkelende informatiemaatschappij. Al in zijn advies van 25 juli 2007 over de toepassing van de richtlijn gegevensbescherming ([5]) kwam hij tot de conclusie dat een wijziging van Richtlijn 95/46/EG op langere termijn onvermijdbaar zou zijn.
4. De mededeling is een belangrijke stap op weg naar een wijziging van de wetgeving, welke de belangrijkste ontwikkeling op het gebied van gegevensbescherming in de Europese Unie zou zijn sinds de goedkeuring van Richtlijn 95/46/EG, die over het algemeen wordt gezien als de hoeksteen van gegevensbescherming in de Europese Unie (en de ruimere Europese Economische Ruimte).
5. De mededeling creëert een passend kader voor een gerichte herziening, onder meer omdat zij een algemeen overzicht bevat van de voornaamste problemen en uitdagingen. De EDPS is het met de Commissie eens dat ook in de toekomst een solide gegevensbeschermingssysteem noodzakelijk blijft, ervan uitgaande dat de bestaande algemene beginselen van gegevensbescherming nog steeds gelden in een maatschappij die fundamentele veranderingen ondergaat als gevolg van snelle technologische ontwikkelingen en globalisering. Daartoe dienen alle bestaande wettelijke regelingen onder de loep te worden genomen.

([1]) PB L 281 van 23.11.1995, blz. 31.
([2]) PB L 8 van 12.1.2001, blz. 1.
([3]) COM(2010) 609 definitief.
([4]) Zie blz. 5 van de mededeling, eerste lid.
([5]) Advies van de EDPS van 25 juli 2007 inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming, (PB C 255 van 27.10.2007, blz. 1).

6. In de mededeling wordt terecht beklemtoond dat de uitdagingen enorm zijn. De EDPS is het daar volledig mee eens en onderstreept dat de voorgestelde oplossingen dan ook ambitieus moeten zijn en de doeltreffendheid van de bescherming moeten verbeteren.

1.2. *Doel van het advies*

7. De in de mededeling voorgestelde oplossingen worden in dit advies op basis van twee criteria beoordeeld, namelijk ambitie en doeltreffendheid. De evaluatie is over het geheel genomen positief. De EDPS steunt de mededeling, maar staat tegelijkertijd kritisch tegenover een aantal aspecten waarvoor een ambitieuzere aanpak naar zijn mening tot een doeltreffender regeling zou leiden.

8. De EDPS wil met dit advies bijdragen tot de verdere ontwikkeling van het rechtskader inzake gegevensbescherming. Hij kijkt uit naar het in medio 2011 verwachte voorstel van de Commissie en hoopt dat zijn suggesties in aanmerking zullen worden genomen bij de totstandkoming van dat voorstel. Hij merkt ook op dat de mededeling een aantal gebieden van het algemene instrument uitsluit, zoals gegevensverwerking door de instellingen en de organen van de EU. Indien de Commissie daadwerkelijk zou besluiten om in dit stadium bepaalde gebieden achterwege te laten, wat de EDPS zou betreuren, vraagt hij de Commissie met drang haar uiterste best te doen om binnen een vooraf gespecificeerde, korte termijn een allesomvattende architectuur tot stand te brengen.

1.3. *Bouwstenen van dit advies*

9. Dit is geen opzichzelfstaand advies. Het is gebaseerd op eerdere standpunten die de EDPS en de Europese gegevensbeschermingsautoriteiten herhaaldelijk hebben ingenomen. In het bijzonder dient te worden benadrukt dat de EDPS in het bovengenoemde advies van 25 juli 2007 reeds een aantal hoofdelementen voor toekomstige wijzigingen heeft aangestipt en uitgewerkt ([6]). Het is ook gebaseerd op overleg met andere belanghebbenden op het gebied van privacy en gegevensbescherming. Hun bijdragen leverden een zeer nuttige achtergrond voor zowel de mededeling als dit advies. Gesteld kan worden dat er een zekere mate van overeenstemming bestaat over de wijze waarop de gegevensbescherming doeltreffender kan worden gemaakt.

10. Het document „The Future of Privacy", de gezamenlijke bijdrage van de Groep gegevensbescherming artikel 29 („Groep artikel 29") en de Groep politie en justitie aan de raadpleging van de Commissie van 2009 (het „verslag van de werkgroepen over de toekomst van privacy") is eveneens een belangrijke bouwsteen van dit advies ([7]).

11. Meer recent heeft de EDPS tijdens een persconferentie op 15 november 2010 zijn eerste reacties op deze mededeling gegeven. In dit advies gaat hij dieper in op de algemene standpunten die hij tijdens die persconferentie heeft aangehaald ([8]).

12. Tot slot stoelt dit advies ook op een aantal eerdere adviezen van de EDPS, evenals op documenten van de Groep artikel 29. Waar relevant wordt op diverse plaatsen in dit advies naar die adviezen en documenten verwezen.

2. **Context**

13. De herbeoordeling van de regelgeving inzake gegevensbescherming komt op een cruciaal historisch moment. De mededeling bevat een uitgebreide en overtuigende beschrijving van de situatie. Op basis daarvan identificeert de EDPS de vier hoofdfactoren die bepalend zijn voor de context waarin het herzieningsproces plaatsvindt.

14. De eerste bepalende factor is technologische ontwikkeling. De technologie die we vandaag de dag kennen, is niet meer dezelfde als toen Richtlijn 95/46/EG werd opgesteld en goedgekeurd. Technologische fenomenen als cloud computing (het online beschikbaar stellen van software, hardware en gegevens), behavioural advertising (gerichte reclame op basis van het surfgedrag), sociale netwerken, apparatuur voor de inning van tol op wegen alsook gps-toestellen hebben de manier waarop gegevens worden verwerkt danig veranderd en zetten de gegevensbescherming zwaar onder druk. Deze druk zal bij een herziening van de Europese regelgeving inzake gegevensbescherming moeten worden aangepakt.

15. De tweede bepalende factor is de globalisering. Door het geleidelijk verdwijnen van handelsbelemmeringen krijgen bedrijven steeds meer een mondiale dimensie. Grensoverschrijdende gegevensverwerking en de internationale doorgifte van gegevens zijn de afgelopen jaren sterk toegenomen. Bovendien is gegevensverwerking thans alomtegenwoordig als gevolg van de informatie- en communicatietechnologie: dankzij het internet en cloud computing kunnen waar ook ter wereld grote hoeveelheden gegevens worden verwerkt. In de afgelopen tien jaar is ook de internationale politiële en justitiële activiteit toegenomen om terrorisme en andere vormen van internationale georganiseerde misdaad te bestrijden, met behulp van een

([6]) Met name (zie punt 77 van het advies): er hoeven geen nieuwe beginselen te worden geïntroduceerd, maar er bestaat een duidelijke noodzaak van andere administratieve regelingen; het ruime toepassingsgebied van het gegevensbeschermingsrecht, dat van toepassing is op alle gebruik van persoonsgegevens, moet ongewijzigd blijven; het gegevensbeschermingsrecht moet het mogelijk maken in concrete gevallen een evenwichtige aanpak te volgen en moet de gegevensbeschermingsautoriteiten de mogelijkheid bieden prioriteiten te stellen; het systeem moet volledig van toepassing zijn op het gebruik van persoonsgegevens ten behoeve van de rechtshandhaving, hoewel er passende bijkomende maatregelen nodig kunnen zijn om speciale problemen op dit gebied aan te pakken.

([7]) Document WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). De voornaamste boodschap is dat een wijziging van de wetgeving de gelegenheid biedt om een aantal belangrijke regels en beginselen te verduidelijken (bijv. toestemming en transparantie), een aantal nieuwe beginselen vast te stellen (bijv. ingebouwde privacy en controleerbaarheid), de doeltreffendheid te verbeteren door de regelingen te moderniseren (bijv. door bestaande meldingseisen te beperken) en alle regels en beginselen in één allesomvattend rechtskader te verenigen (met inbegrip van politiële en justitiële samenwerking).

([8]) De speaking points voor de persconferentie kunnen worden geraadpleegd op de EDPS-website op: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

grootschalige uitwisseling van informatie voor wetshandhavingsdoeleinden. Gezien het voorgaande dient ernstig te worden nagedacht over de wijze waarop de bescherming van persoonsgegevens in de geglobaliseerde wereld doeltreffend kan worden gewaarborgd zonder al te veel hinder voor de internationale verwerkingsactiviteiten.

16. De derde bepalende factor is het Verdrag van Lissabon. De inwerkingtreding van het Verdrag van Lissabon luidt een nieuw tijdperk in voor gegevensbescherming. Artikel 16 VWEU verleent niet alleen een individueel recht aan de betrokkene, maar vormt ook een directe rechtsgrondslag voor een sterke Europese regelgeving inzake gegevensbescherming. Bovendien verplicht de afschaffing van de pijlerstructuur het Europees Parlement en de Raad om gegevensbescherming op alle terreinen van de EU-wetgeving te voorzien. Het maakt met andere woorden een allesomvattend rechtskader inzake gegevensbescherming mogelijk dat van toepassing is op de private sector, de openbare sector in de lidstaten en de instellingen en organen van de EU. In het programma van Stockholm ([9]) is bepaald dat de Unie een allesomvattende strategie moet uitwerken om gegevens in de EU en in haar betrekkingen met andere landen te beschermen.

17. De vierde bepalende factor zijn de parallelle ontwikkelingen die zich in het kader van internationale organisaties voordoen. Er worden verschillende discussies gevoerd over de modernisering van de huidige rechtsinstrumenten inzake gegevensbescherming. Dienaangaande dient ook melding te worden gemaakt van de huidige reflectie over de toekomstige herziening van Verdrag nr. 108 van de Raad van Europa ([10]) en van de richtsnoeren van de OESO inzake de bescherming van de persoonlijke levenssfeer ([11]). Nog een belangrijke ontwikkeling heeft betrekking op de vaststelling van internationale normen inzake gegevensbescherming en privacy, welke uiteindelijk kan leiden tot de goedkeuring van een wereldwijd bindend instrument inzake gegevensbescherming. Al deze initiatieven verdienen alle mogelijke steun. Zij moeten er alle op gericht zijn een doeltreffende, consistente bescherming te waarborgen in een door technologische ontwikkelingen gestuurde en geglobaliseerde wereld.

3. **Belangrijkste perspectieven**

3.1. *Gegevenbescherming bevordert het vertrouwen en moet andere (openbare) belangen dienen*

18. Een solide kader voor gegevensbescherming is het noodzakelijke gevolg van het belang dat in het Verdrag van Lissabon aan gegevensbescherming wordt gehecht, met name in artikel 8 van het Handvest van de grondrechten van de Europese Unie en artikel 16 VWEU, alsook van de sterke band met artikel 7 van het Handvest ([12]).

19. Een solide kader inzake gegevensbescherming dient ook ruimere openbare en private belangen in een informatiemaatschappij waar gegevensverwerking alomtegenwoordig is. Gegevenbescherming bevordert het vertrouwen en vertrouwen is cruciaal voor de goede werking van onze samenleving. Het is essentieel dat regelingen inzake gegevensbescherming zodanig worden opgezet dat zij andere legitieme rechten en belangen zoveel mogelijk actief ondersteunen in plaats van deze te belemmeren.

20. Belangrijke voorbeelden van andere legitieme belangen zijn een sterke Europese economie, de veiligheid van personen en de verantwoordingsplicht van regeringen.

21. De economische ontwikkeling van de EU gaat hand in hand met het op de markt en in de handel brengen van nieuwe technologieën en diensten. In de informatiemaatschappij hangt de ontwikkeling en succesvolle introductie van informatie- en communicatietechnologieën en gerelateerde diensten af van vertrouwen. Zonder vertrouwen in ICT is de kans op mislukking groot ([13]). Vertrouwen in ICT is evenwel slechts mogelijk indien de gegevens efficiënt worden beschermd. Gegevensbescherming dient dan ook in technologieën en diensten te worden ingebouwd. Een solide kader voor gegevensbescherming bevordert de Europese economie indien het niet alleen sterk is, maar ook passend. Verdere harmonisatie op EU-niveau en het beperken van de administratieve rompslomp tot een minimum zijn daarbij essentieel (zie hoofdstuk 5 van dit advies).

22. De afgelopen jaren is veel gesproken over de behoefte aan evenwicht tussen privacy en veiligheid, vooral met betrekking tot instrumenten voor gegevensverwerking en -uitwisseling op het gebied van politiële en justitiële samenwerking. ([14]) Gegevensbescherming werd vrij vaak voorgesteld als een obstakel voor de volledige bescherming van de fysieke veiligheid van personen ([15]), of op zijn minst als een onvermijdelijke voorwaarde die door de wetshandhavingsautoriteiten moest worden gerespecteerd. Dat is echter niet het hele verhaal. Een solide kader voor gegevensbescherming kan de veiligheid aanscherpen en vergroten. Volgens de beginselen voor gegevensbescherming, indien ze goed worden toegepast, hebben de voor verwerking verantwoordelijken de plicht ervoor te zorgen dat hun informatie correct en actueel is en dat overtollige persoonsgegevens die niet voor wetshandhavingsdoeleinden vereist zijn uit de systemen worden verwijderd. Er kan

([9]) Het programma van Stockholm — Een open en veilig Europa ten dienste en ter bescherming van de burger, (PB C 115 van 4.5.2010, blz. 1), op blz. 10.

([10]) Verdrag nr. 108 van de Raad van Europa ter bescherming van de mens bij de automatische verwerking van op de persoon betrekking hebbende gegevens, ETS nr. 108, 28. januari 1981.

([11]) Richtlijnen van de OESO over de bescherming van de persoonlijke levenssfeer en grensoverschrijdende stromen van persoonsgegevens, gepubliceerd op http://www.oecd.org

([12]) Het Hof van Justitie heeft het belang van gegevensbescherming en de band met de persoonlijke levenssfeer in het Handvest benadrukt in zijn arrest van 9 november 2010, gevoegde zaken C-92/09 en C-93/09, *Schecke*, nog niet in de jurisprudentie bekendgemaakt.

([13]) Zie het advies van de EDPS van 18 maart 2010 inzake het vergroten van het vertrouwen in de informatiemaatschappij door de bevordering van gegevensbescherming en privacy, (PB C 280 van 16.10.2010, blz. 1), punt 113.

([14]) Zie het advies van de EDPS van 10 juli 2009 over de mededeling van de Commissie aan het Europees Parlement en de Raad betreffende een ruimte van vrijheid, veiligheid en recht ten dienste van de burger, (PB C 276 van 17.9.2009, blz. 8).

([15]) Veiligheid is een ruimer begrip dan fysieke veiligheid, maar ter illustratie van de betrokken argumenten wordt de term hier in zijn engere betekenis gebruikt.

ook worden gewezen op de verplichting om technologische en organisatorische maatregelen te treffen teneinde de veiligheid van de systemen te waarborgen, zoals voorzieningen ter bescherming tegen ongeoorloofde bekendmaking van gegevens of ongeoorloofde toegang, zoals deze op het gebied van gegevensbescherming is vastgesteld.

23. Naleving van de beginselen van gegevensbescherming door de wetshandhavingsautoriteiten kan bovendien meer zekerheid bieden dat zij binnen het wettelijke kader werken, wat het vertrouwen in hun gedrag en bijgevolg ook bij uitbreiding in onze samenleving zal bevorderen. De rechtspraak op grond van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens verzekert dat politie en justitie alle gegevens kunnen verwerken die relevant zijn voor hun werk, maar er gelden wel beperkingen. Gegevensbescherming vereist controles (zie hoofdstuk 9 van het advies over politie en justitie).

24. In een democratische maatschappij kan de regering verantwoordelijk worden gesteld voor al zijn activiteiten, ook voor het gebruik van persoonsgegevens voor de verschillende openbare belangen die zij dienen. Dit gebruik gaat van de publicatie van gegevens op het internet ter wille van transparantie tot het gebruik van gegevens ter ondersteuning van beleidsmaatregelen op gebieden zoals volksgezondheid, vervoer en fiscaliteit en het toezicht op personen voor wetshandhavingsdoeleinden. Dankzij een solide kader voor gegevensbescherming kan een regering zijn verantwoordelijkheden nemen en verantwoording afleggen, als onderdeel van goed bestuur.

3.2. *Gevolgen voor het rechtskader inzake gegevensbescherming*

3.2.1. Verdere harmonisatie dringt zich op

25. In de mededeling wordt terecht gewezen op een van de essentiële tekortkomingen van het huidige kader, namelijk dat de lidstaten over te veel vrijheid beschikken bij de omzetting van de Europese bepalingen in nationaal recht. Het gebrek aan harmonisatie heeft een aantal negatieve gevolgen in een informatiemaatschappij waarin de fysieke grenzen tussen de lidstaten almaar minder belangrijk worden (zie hoofdstuk 5 van het advies).

3.2.2. Algemene beginselen van gegevensbescherming blijven geldig

26. Een eerste, meer formele reden waarom de algemene beginselen van gegevensbescherming niet mogen en kunnen worden veranderd, is van wettelijke aard. Deze beginselen zijn vastgelegd in Verdrag nr. 108 van de Raad van Europa, dat bindend is voor alle lidstaten. Dat verdrag vormt de basis voor gegevensbescherming in de EU. Bovendien zijn enkele basisbeginselen uitdrukkelijk opgenomen in artikel 8 van het Handvest van de grondrechten van de Europese Unie. Om deze beginselen te wijzigen, zouden dus ook de verdragen moeten worden gewijzigd.

27. Dat is echter niet het hele verhaal. Er zijn ook inhoudelijke gronden om niet aan de algemene beginselen te raken. De EDPS is er vast van overtuigd dat een informatiemaatschappij niet kan en mag functioneren zonder een passende bescherming van de persoonlijke levenssfeer en persoonsgegevens. Wanneer meer informatie wordt verwerkt, is ook betere bescherming vereist. Een informatiemaatschappij waarin grote hoeveelheden informatie over alle burgers worden verwerkt, dient te stoelen op het beginsel van zeggenschap door de persoon, zodat hij of zij als persoon kan handelen en vrijheden als de vrijheid van meningsuiting in een democratische maatschappij kan benutten.

28. Bovendien is het moeilijk voor te stellen dat individuen controle houden wanneer de voor verwerking verantwoordelijken niet verplicht zijn om deze verwerking te beperken overeenkomstig de beginselen van noodzakelijkheid, evenredigheid en specificiteit. Controle door de personen is al even moeilijk wanneer de betrokkenen geen rechten hebben, zoals het recht op toegang tot hun gegevens en het recht om hun gegevens te corrigeren, te wissen of af te schermen.

3.2.3. Vanuit het oogpunt van de grondrechten

29. De EDPS benadrukt dat gegevensbescherming erkend wordt als een grondrecht. Dat betekent niet dat gegevensbescherming altijd *voorrang* moet hebben op andere belangrijke rechten en belangen in een democratische samenleving, maar het heeft wel gevolgen voor de aard en de reikwijdte van de bescherming die op grond van een Europees rechtskader moet worden geboden, om ervoor te zorgen dat altijd *afdoende* rekening wordt gehouden met de voorschriften inzake gegevensbescherming.

30. De belangrijkste gevolgen kunnen als volgt worden omschreven:

— de bescherming moet doeltreffend zijn; een rechtskader moet voorzien in instrumenten die ervoor zorgen dat personen hun rechten daadwerkelijk kunnen uitoefenen;

— het kader moet gedurende lange tijd stabiel blijven;

— de bescherming moet in alle omstandigheden worden geboden en mag niet afhangen van de politieke voorkeuren in een bepaald tijdsbestek;

— uitoefening van het recht moet mogelijk worden beperkt. Deze beperkingen moeten evenwel uitzonderlijk zijn, moeten met passende redenen worden omkleed en mogen de essentiële elementen van het recht zelf niet in het gedrang brengen ([16]).

De EDPS adviseert de Commissie met deze gevolgen rekening te houden wanneer zij wetgevingsoplossingen voorstelt.

3.2.4. Er is behoefte aan nieuwe wettelijke regelingen

31. De mededeling is terecht toegespitst op de behoefte aan aangescherpte wettelijke regelingen op het gebied van gegevensbescherming. Tegen deze achtergrond is het goed eraan te herinneren dat de gegevensbeschermingsautoriteiten in het verslag van de werkgroepen over de toekomst van privacy ([17]) hebben aangedrongen op een ruimere rol

([16]) Zie ook punt 17 van het advies van de EDPS van 25 juli 2007 inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming, dat voortbouwt op de rechtspraak van het Europees Hof van de rechten van de mens en het Hof van Justitie.

([17]) Vgl voetnoot 7.

voor de verschillende partijen die bij gegevensbescherming betrokken zijn, met name de personen waarop de gegevens betrekking hebben, de voor verwerking verantwoordelijken en de toezichthoudende instanties zelf.

32. Onder de belanghebbenden lijkt een brede consensus te bestaan dat aangescherpte wettelijke regelingen, waarin rekening wordt gehouden met de technologische ontwikkelingen en de globalisering, ook in de toekomst de sleutel zullen zijn voor een ambitieuze en doeltreffende gegevensbescherming. Zoals reeds werd aangehaald in punt 7, zijn dit de criteria waaraan de EDPS iedere voorgestelde oplossing toetst.

3.2.5. Alomvattendheid als basisvoorwaarde

33. Zoals in de mededeling wordt aangehaald, is Richtlijn 95/46/EG van toepassing op iedere verwerking van persoonsgegevens in de lidstaten, zowel in de openbare als in de privésector, met uitzondering van verwerkingsactiviteiten die buiten het toepassingsgebied van vroegere communautaire wetgeving vallen ([18]). Deze uitzondering was noodzakelijk zolang het vorige verdrag van kracht was, maar dat is niet meer het geval sinds de inwerkintreding van het Verdrag van Lissabon. Bovendien is de uitzondering in strijd met — de tekst en in ieder geval de strekking van — artikel 16 VWEU.

34. Volgens de EDPS is een alomvattend rechtsinstrument inzake gegevensbescherming dat ook politiële en justitiële samenwerking in strafzaken omvat een van de belangrijkste verbeteringen die in een nieuw rechtskader kan worden aangebracht. Het is een basisvoorwaarde voor doeltreffende gegevensbescherming in de toekomst.

35. De EDPS zet zijn voorgaande woorden kracht bij met de volgende argumenten:

— het onderscheid tussen de activiteiten van de particuliere sector en de wetshandhavingsector vervaagt. Entiteiten uit de particuliere sector kunnen gegevens verwerken die uiteindelijk voor wetshandhavingsdoeleinden worden gebruikt (bijvoorbeeld PNR-gegevens ([19])), terwijl zij in andere gevallen verplicht zijn gegevens voor wetshandhavingsdoeleinden bij te houden (bijvoorbeeld op grond van de richtlijn gegevensbewaring ([20]));

— er is geen fundamenteel verschil tussen de politiële en justitiële autoriteiten en andere wetshandhavingsautoriteiten (belastingen, douane, fraudebestrijding en immigratie) die onder Richtlijn 95/46/EG vallen;

— zoals terecht in de mededeling wordt vermeld, is het rechtsinstrument inzake gegevensbescherming dat van toepassing is op politie en justitiële autoriteiten (Kaderbesluit 2008/977/JBZ ([21])) ontoereikend;

— de meeste lidstaten hebben Richtlijn 95/46/EG en Verdrag nr. 108 in nationaal recht omgezet, waardoor zij ook van toepassing zijn op hun politiële en justitiële autoriteiten.

36. De opname van politie en justitie in het algemene rechtsinstrument zou de burger niet alleen meer garanties bieden, maar ook de taak van de politieautoriteiten vergemakkelijken. De toepassing van verschillende regelgevingspakketten is lastig, neemt onnodig veel tijd in beslag en zet een rem op de internationale samenwerking (zie hoofdstuk 9 van het advies). Dit pleit ook voor de opname van de verwerkingsactiviteiten van nationale veiligheidsdiensten in het instrument, voor zover dat mogelijk is op grond van de huidige EU-wetgeving.

3.2.6. Technologische neutraliteit

37. De periode sinds de goedkeuring van Richtlijn 95/46/EG in 1995 kan op technologisch gebied veelbewogen worden genoemd. Regelmatig zijn nieuwe technologieën en apparatuur geïntroduceerd. In vele gevallen heeft dit geleid tot fundamentele veranderingen in de manier waarop persoonsgegevens van individuen worden verwerkt. De informatiemaatschappij kan niet langer worden gezien als een parallelle wereld waaraan individuen op vrijwillige basis kunnen deelnemen en is een integrerend deel van ons dagelijkse leven geworden. Een voorbeeld is het internet van de dingen ([22]), dat fysieke voorwerpen aan online-informatie over die voorwerpen koppelt.

38. De technologische vooruitgang zal blijven doorgaan. Dat heeft gevolgen voor het nieuwe rechtskader. Het moet doeltreffend zijn gedurende vele jaren en mag tegelijkertijd de verdere technologische ontwikkeling niet in de weg staan. Daarom moeten de wettelijke regelingen technologisch neutraal zijn. Het kader moet bedrijven en individuen echter ook meer rechtszekerheid bieden. Zij moeten begrijpen wat van hen wordt verwacht en moeten hun rechten kunnen uitoefenen. Daarom moeten de wettelijke regelingen nauwkeurig zijn.

39. Volgens de EDPS moet een algemeen rechtsinstrument inzake gegevensbescherming in de mate van het mogelijke op een technologisch neutrale manier worden opgesteld. Dat betekent dat de rechten en plichten van de verschillende betrokken partijen op een algemene en neutrale wijze moeten worden geformuleerd, zodat zij in beginsel geldig en uitvoerbaar blijven ongeacht de technologie die voor de verwerking van persoonsgegevens wordt gebruikt.

([18]) Dit advies is hoofdzakelijk toegespitst op de vroegere derde pijler (politiële en justitiële samenwerking in strafzaken), aangezien de vroegere tweede pijler niet alleen een complexer onderdeel van de EU-wetgeving is (zoals ook wordt erkend in artikel 16 VWEU en artikel 39 VEU), maar ook minder relevant is voor gegevensbescherming.

([19]) Zie bijvoorbeeld de mededeling van de Commissie over de algemene aanpak van doorgifte van passagiersgegevens (Passenger Name Record — PNR) aan derde landen, COM(2010) 492 definitief.

([20]) Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (PB L 105 van 13.4.2006, blz. 54).

([21]) Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (PB L 350 van 30.12.2008, blz. 60).

([22]) Zoals gedefinieerd in „Het internet van de dingen — een actieplan voor Europa", COM(2009) 278 definitief.

Er is geen andere mogelijkheid, gezien het snelle tempo waarin de technologie tegenwoordig evolueert. De EDPS stelt voor bovenop de bestaande beginselen van gegevensbescherming nieuwe „echnologisch neutrale" rechten vast te stellen die van bijzonder belang zouden kunnen zijn in de snel veranderende elektronische omgeving (zie hoofdzakelijk de hoofdstukken 6 en 7).

3.2.7. Lange termijn: rechtszekerheid gedurende langere tijd

40. Richtlijn 95/46 is in de EU al vijftien jaar lang het belangrijkste rechtsinstrument inzake gegevensbescherming. Zij werd door de lidstaten omgezet in nationaal recht en wordt door de verschillende betrokken partijen toegepast. Met de jaren werd zij beter toegepast dankzij de opgedane praktische ervaring en nadere richtsnoeren van de Commissie, de gegevensbeschermingsautoriteiten (op nationaal niveau en in het kader van de Groep gegevensbescherming artikel 29) en nationale en Europese rechtbanken.

41. Benadrukt dient te worden dat deze ontwikkelingen tijd vergen en dat die tijd nodig is om voor rechtszekerheid en stabiliteit te zorgen, vooral omdat het een algemeen kader betreft dat tot doel heeft een grondrecht te doen gelden. Er dient een nieuw algemeen rechtsinstrument te worden opgesteld dat gedurende langere tijd rechtszekerheid en stabiliteit kan brengen, zonder dat uit het oog wordt verloren dat de verdere ontwikkeling van de technologie en de globalisering erg moeilijk kan worden voorspeld. Hoe het ook zij, de EDPS staat volledig achter het voornemen om gedurende langere tijd rechtszekerheid te verzekeren, wat ook de bedoeling was van Richtlijn 95/46. Kortom: wanneer de technologie snel evolueert, moet de wetgeving stabiel zijn.

3.2.8. Korte termijn: bestaande instrumenten beter benutten

42. Op korte termijn is het van essentieel belang de doeltreffendheid van de bestaande wettelijke regelingen te waarborgen, in de eerste plaats door extra aandacht te besteden aan handhaving op nationaal en Europees niveau (zie hoofdstuk 11 van dit advies).

B. ELEMENTEN VAN EEN NIEUW KADER

4. Integrale aanpak

43. De EDPS staat volledig achter de integrale aanpak van gegevensbescherming, die niet alleen de titel maar ook het uitgangspunt van de mededeling is en noodzakelijkerwijs voorziet in de uitbreiding van de algemene regelgeving inzake gegevensbescherming met politiële en justitiële samenwerking in strafzaken ([23]).

44. Hij merkt echter ook op dat de Commissie niet voornemens is alle gegevensverwerkingsactiviteiten in dit algemene rechtsinstrument op te nemen. Met name gegevensverwerking door de instellingen, organen, instanties en agentschappen van de EU zullen niet onder het instrument vallen. De Commissie zegt enkel dat zij zal „afwegen of andere wettelijke instrumenten moeten worden aangepast aan het nieuwe algemene gegevensbeschermingskader".

45. De EDPS geeft er duidelijk de voorkeur aan gegevensverwerking op EU-niveau in het algemene rechtskader op te nemen. Hij herinnert eraan dat dit de oorspronkelijke bedoeling was van het vroegere artikel 286 VEG, waarin gegevensbescherming voor het eerst op het niveau van het Verdrag werd vermeld. Artikel 286 VEG bepaalde dat rechtsinstrumenten inzake de verwerking van persoonsgegevens ook op de instellingen van toepassing waren. Nog belangrijker is dat één enkele rechtstekst het risico op tegenstrijdigheden tussen bepalingen vermijdt en het meest geschikt zou zijn voor de gegevensuitwisseling tussen de EU en de entiteiten uit de openbare en de particuliere sector in de lidstaten. Eén alomvattende tekst zou ook het risico voorkomen dat er na de wijziging van Richtlijn 95/46/EG geen politieke wil meer is om Verordening (EG) nr. 45/2001 te wijzigen of voldoende prioriteit aan deze wijziging te verlenen om tegenstrijdige data van inwerkintreding te voorkomen.

46. De EDPS vraagt de Commissie met klem — indien zij tot het besluit zou komen dat gegevensverwerking op EU-niveau niet in het algemene rechtsinstrument kan worden opgenomen — zich ertoe te verbinden zo snel mogelijk en bij voorkeur vóór eind 2011 een wijzigingsvoorstel voor Verordening (EG) nr. 45/2001 in te dienen (in plaats van af te wegen of andere wettelijke instrumenten moeten worden aangepast).

47. Even belangrijk is dat de Commissie ervoor zorgt dat andere terreinen niet achterblijven, met name:

— gegevensbescherming in het gemeenschappelijk buitenlands en veiligheidsbeleid, op grond van artikel 39 VEU ([24]);

— sectorspecifieke gegevensbeschermingsregelingen voor EU-organen als Europol en Eurojust en voor grote informatiesystemen, voor zover deze aan het nieuwe rechtskader moeten worden aangepast;

— e-privacyrichtlijn 2002/58, voor zover deze aan het nieuwe rechtskader moet worden aangepast.

48. Ten slotte kan een algemeen rechtsinstrument inzake gegevensbescherming, en moet het wellicht zelfs, vervolledigd worden met aanvullende sectorale en specifieke regelgeving, bijvoorbeeld op het gebied van politiële en justitiële samenwerking, maar ook op andere gebieden ([25]). Dergelijke regelgeving dient indien nodig en overeenkomstig het subsidiariteitsbeginsel op EU-niveau te worden vastgesteld. De lidstaten kunnen indien nodig op welbepaalde gebieden aanvullende regels vaststellen (zie 5.2).

([23]) Zie blz. 14 van de mededeling en punt 3.2.5 van dit advies.

([24]) Zie ook het advies van de EDPS van 24 november 2010 over de mededeling van de Commissie aan het Europees Parlement en de Raad, „Het terrorismebestrijdingsbeleid van de EU: belangrijkste resultaten en nieuwe uitdagingen", punt 31.

([25]) Zie ook het verslag van de werkgroepen over de toekomst van privacy (voetnoot 7), punten 18-21.

5. **Verdere harmonisatie en vereenvoudiging**

5.1. *De behoefte aan harmonisatie*

49. Harmonisatie is uitermate belangrijk voor het EU-recht inzake gegevensbescherming. In de mededeling wordt terecht beklemtoond dat gegevensbescherming een belangrijke internemarktdimensie heeft, omdat deze het vrije verkeer van persoonsgegevens tussen de lidstaten op de interne markt moet waarborgen. De huidige richtlijn heeft evenwel tot onvoldoende harmonisatie geleid. De Commissie erkent in de mededeling dat dit een van de belangrijksten punten is waarover belanghebbenden zich steeds weer zorgen maken. Zij wijzen vooral op de noodzaak van een grotere rechtszekerheid, minder administratieve lasten en gelijke mededingingsvoorwaarden voor ondernemingen. Zoals de Commissie terecht opmerkt, is dit met name het geval voor de voor gegevensverwerking verantwoordelijken die in verschillende lidstaten zijn gevestigd en de (eventueel verschillende) voorschriften van de nationale wettelijke regelingen inzake gegevensbescherming moeten naleven ([26]).

50. Harmonisatie is niet alleen belangrijk voor de interne markt, maar ook om passende gegevensbescherming te waarborgen. Artikel 16 VWEU bepaalt dat „eenieder" recht heeft op bescherming van zijn persoonsgegevens. Om ervoor te zorgen dat dit recht daadwerkelijk wordt geëerbiedigd, dient in de hele EU een gelijkwaardige bescherming gegarandeerd te worden. In hun verslag over de toekomst van privacy onderstrepen de werkgroepen dat verschillende bepalingen betreffende de standpunten van de betrokkenen niet in alle lidstaten zijn omgezet of niet door alle lidstaten op dezelfde manier zijn uitgelegd ([27]). In een geglobaliseerde en geïnterconnecteerde wereld kunnen deze verschillen de bescherming van de individuen ondermijnen of beperken.

51. De EDPS meent dat een verdere en betere harmonisatie tot de hoofddoelstellingen van de herziening behoort. De EDPS is verheugd dat de Commissie zich ertoe heeft verbonden na te gaan hoe de regelgeving inzake gegevensbescherming op EU-niveau verder kan worden geharmoniseerd. Hij stelt echter met enige verwondering vast dat de Commissie in dit stadium geen concrete mogelijkheden in de mededeling aanhaalt. Daarom stipt hij zelf een aantal terreinen aan waarop de behoefte aan meer samenhang het grootst is (zie 5.3). De regelgeving op deze terreinen zou niet alleen verder moeten worden geharmoniseerd door de vrijheid van de lidstaten in te perken, maar ook door een foutieve omzetting door de lidstaten te voorkomen (zie ook hoofdstuk 11) en te zorgen voor een meer samenhangende en gestructureerde handhaving (zie ook hoofdstuk 10).

([26]) Mededeling, blz. 10.

([27]) Zie het document van de werkgroepen over de toekomst van de persoonlijke levenssfeer (voetnoot 7), punt 70. Het document verwijst in het bijzonder naar aansprakelijkheidsbepalingen en de mogelijkheid om schadevergoeding te eisen voor geleden immateriële schade.

5.2. *De vrijheid die de richtlijn bij de omzetting laat beperken*

52. De richtlijn bevat een aantal bepalingen die ruim geformuleerd zijn en daardoor heel wat ruimte voor interpretatie laten. Overweging 9 van de richtlijn bevestigt uitdrukkelijk dat de lidstaten een zekere vrijheid krijgen en dat binnen de grenzen daarvan ongelijkheden kunnen voorkomen in de omzetting van de richtlijn. Meerdere bepalingen werden op een verschillende manier door de lidstaten omgezet, waaronder ook een aantal essentiële bepalingen ([28]). Deze situatie is niet bevredigend en meer samenhang in de regelgeving dringt zich op.

53. Dit betekent niet dat verscheidenheid zonder meer moet worden uitgesloten. Op bepaalde gebieden kan flexibiliteit nodig zijn om gerechtvaardigde specifieke kenmerken, belangrijke openbare belangen of de institutionele autonomie van de lidstaten in stand te houden. Volgens de EDPS dienen verschillen tussen de lidstaten beperkt te worden tot met name de volgende specifieke situaties:

— vrijheid van meningsuiting: op grond van het huidige kader (artikel 9) kunnen de lidstaten ontheffingen en uitzonderingen voorzien met betrekking tot gegevensverwerking voor journalistieke, artistieke en literaire doeleinden. Deze flexibiliteit lijkt op zijn plaats, uiteraard binnen de grenzen van het Handvest en het EVRM, gezien de verschillende tradities en de culturele verschillen die op dit gebied tussen de lidstaten kunnen bestaan. Dit zou een eventuele aanpassing van het huidige artikel 9 aan de ontwikkelingen op het internet evenwel niet in de weg staan;

— specifieke openbare belangen: op grond van het huidige kader (artikel 13) kunnen de lidstaten wetgevingsmaatregelen aannemen om de reikwijdte van de rechten en plichten in te perken wanneer dat noodzakelijk is om belangrijke openbare belangen te vrijwaren, zoals nationale veiligheid, landsverdediging, openbare veiligheid, enz. De lidstaten beschikken terecht over deze bevoegdheid. In de mate van het mogelijke dient de uitlegging van de uitzonderingen evenwel verder te worden geharmoniseerd (zie punt 9.1). Bovendien lijkt het huidige artikel 6, lid 1, onnodig veel ruimte te laten voor uitzonderingen;

— rechtsmiddelen, sancties en administratieve procedures: een Europees kader dient de belangrijkste voorwaarden te bepalen, maar op grond van de huidige EU-wetgeving dient het vaststellen van sancties, rechtsmiddelen, procedurevoorschriften en de modaliteiten van inspecties zoals deze van toepassing zijn op nationaal niveau aan de lidstaten te worden overgelaten.

([28]) Ook met betrekking tot manuele gegevens lopen de benaderingen enigszins uiteen.

5.3. *Terreinen voor verdere harmonisatie*

54. *Definities* (artikel 2 van Richtlijn 95/46). Definities zijn de hoeksteen van het rechtsstelsel en dienen eenvormig te worden uitgelegd in alle lidstaten, zonder enige ruimte voor interpretatie. Op grond van het huidige kader zijn verschillen ontstaan, onder andere wat het begrip „verantwoordelijke" betreft ([29]). De EDPS stelt voor de huidige lijst van artikel 2 uit te breiden om de rechtszekerheid te bevorderen, bijvoorbeeld met de begrippen anonieme gegevens, onder pseudoniem opgeslagen gegevens, justitiele gegevens, doorgifte van gegevens en functionaris voor gegevensbescherming.

55. *Rechtmatigheid van de verwerking van persoonsgegevens (artikel 5)*. De kernelementen die de rechtmatigheid van gegevensverwerking bepalen, dienen zo nauwkeurig mogelijk in het nieuwe rechtsinstrument te worden omschreven. Artikel 5 van de richtlijn (alsook overweging 9 van genoemde richtlijn), dat de lidstaten opdraagt de voorwaarden voor een wettige verwerking van gegevens nader te bepalen, is in een nieuw kader misschien niet langer nodig.

56. *Gronden voor gegevensverwerking* (artikelen 7 en 8). Het vaststellen van de voorwaarden voor gegevensverwerking is een essentieel onderdeel van alle regelgeving inzake gegevensbescherming. De lidstaten mogen de gronden voor gegevensverwerking niet kunnen aanvullen of wijzigen, noch bepaalde gronden kunnen uitsluiten. De mogelijkheid om uitzonderingen toe te staan, dient te worden uitgesloten of beperkt (met name wat gevoelige gegevens betreft ([30])). De gronden voor gegevensverwerking dienen duidelijk te worden geformuleerd in het nieuwe rechtsinstrument, zodat de ruimte voor interpretatie bij de omzetting of de handhaving ervan beperkt blijft. Met name het begrip toestemming dient wellicht nader te worden omschreven (zie punt 6.5). Bovendien leidt de grond op basis van het gerechtvaardigde belang van de voor verwerking verantwoordelijke (artikel 7, onder f)) door zijn flexibele aard tot sterk uiteenlopende interpretaties. Nadere specificatie dringt zich op. Een andere bepaling die mogelijk eveneens verder moet worden uitgewerkt, is artikel 8, lid 2, onder b), dat verantwoordelijken toelaat gevoelige gegevens te verwerken om hun uit het arbeidsrecht voortvloeiende verplichtingen na te komen en hun specifieke rechten op dat gebied uit te oefenen ([31]).

57. *Rechten van betrokkenen* (artikelen 10 tot 15). Dit is een van de gebieden waarop niet alle elementen van de richtlijn consistent door de lidstaten zijn omgezet en uitgelegd. De rechten van de betrokkenen spelen een centrale rol in een doeltreffende regeling voor gegevensbescherming. De speelruimte dient dan ook aanzienlijk te worden ingeperkt. De EDPS beveelt aan dat de voor verwerking verantwoordelijken overal in de EU dezelfde informatie aan de betrokkenen verstrekken.

58. *Internationale doorgifte* (artikelen 25 en 26). Dit gebied is sterk gekritiseerd wegens het gebrek aan eenvormigheid in de EU. Belanghebbenden betoogden dat de lidstaten de besluiten van de Commissie inzake adequaatheid op zeer uiteenlopende manieren interpreteren en ten uitvoer leggen. Ook wat bindende bedrijfsvoorschriften betreft, beveelt de EDPS verdere harmonisatie aan (zie hoofdstuk 9).

59. *Nationale gegevensbeschermingsautoriteiten* (artikel 28). De regelgeving inzake nationale gegevensbeschermingsautoriteiten loopt sterk uiteen in de 27 lidstaten, met name wat hun statuut, middelen en bevoegdheden betreft. De vage formulering van artikel 28 heeft deze verschillen mee in de hand gewerkt ([32]); het dient dan ook nader te worden omschreven, in overeenstemming met het arrest van het Europees Hof van Justitie in zaak C-518/07 ([33]) (zie hoofdstuk 10).

5.4. *Vereenvoudiging van het aanmeldingssysteem*

60. De lidstaten hebben tot dusver ook op het gebied van aanmeldingseisen (artikelen 18 tot 21 van Richtlijn 95/46/EG) heel wat vrijheid gekregen. Er wordt in de mededeling terecht opgemerkt dat een geharmoniseerd systeem zowel de kosten als de administratieve rompslomp van de voor verwerking verantwoordelijken zou verminderen ([34]).

61. Op dit gebied dient vooral gestreefd te worden naar vereenvoudiging. De evaluatie van het gegevensbeschermingskader is een unieke kans om het toepassingsgebied van de huidige aanmeldingseisen verder te vereenvoudigen en/of te beperken. In de mededeling wordt erkend dat er onder de belanghebbenden een algemene consensus bestaat dat het bestaande aanmeldingssysteem vrij omslachtig is en op zichzelf niet bijdraagt tot de bescherming van persoonsgegevens ([35]). De EDPS is dan ook verheugd dat de Commissie zich ertoe heeft verbonden verschillende mogelijkheden te onderzoeken om het bestaande aanmeldingssysteem te vereenvoudigen.

62. Volgens hem dient de vereenvoudiging gebaseerd te worden op een verschuiving van een systeem waar aanmelding de regel is, behoudens andersluidende bepalingen (met name een „systeem van ontheffingen"), naar een gerichter systeem. Het systeem van ontheffingen is weinig doelmatig gebleken aangezien het niet door alle lidstaten op dezelfde manier wordt toegepast ([36]). De EDPS stelt voor de volgende alternatieven in overweging te nemen:

([29]) Zie advies 1/2010 van de Groep gegevensbescherming artikel 29 betreffende de begrippen „verantwoordelijke" en „verwerker" (WP 169).

([30]) Op grond van artikel 8, leden 4 en 5, kunnen de lidstaten momenteel onder bepaalde voorwaarden aanvullende uitzonderingen met betrekking tot gevoelige gegevens voorzien.

([31]) Zie dienaangaande het eerste verslag van de Commissie over de toepassing van de richtlijn gegevensbescherming, zoals eerder genoemd, blz. 14.

([32]) Verslag van de werkgroepen over de toekomst van privacy, lid 87.

([33]) Zaak C-518/07, *Commissie/Duitsland,* nog niet bekendgemaakt.

([34]) Vgl. voetnoot 26.

([35]) Vgl. voetnoot 26.

([36]) Verslag van de Groep gegevensbescherming artikel 29 over de verplichte aanmelding bij de nationale toezichthoudende autoriteiten, het optimale gebruik van uitzonderingen en vereenvoudigingen en de rol van functionarissen voor gegevensbescherming in de Europese Unie, WP 106, 2005, blz. 7.

— beperking van de aanmeldingsplicht tot specifieke soorten verwerkingshandelingen die welbepaalde risico's inhouden (aan deze meldingen kunnen verdere stappen worden verbonden, zoals een voorafgaande controle van de verwerking);

— een eenvoudige registratieplicht voor de voor verwerking verantwoordelijken (in tegenstelling tot een uitgebreide registratie van iedere verwerking van gegevens).

Bovendien kan een pan-Europees standaardaanmeldingsformulier worden opgesteld om ervoor te zorgen dat overal dezelfde informatie wordt gevraagd.

63. De herziening van het huidige aanmeldingssysteem mag geen obstakel zijn voor het aanscherpen van de verplichtingen inzake voorafgaande controle voor bepaalde verwerkingsverplichtingen die wellicht specifieke risico's inhouden (zoals grootschalige informatiesystemen). De EDPS is er voorstander van om in het nieuwe rechtsinstrument een niet-exhaustieve lijst op te nemen van gevallen waarin een dergelijke voorafgaande controle vereist is. Verordening (EG) nr. 45/2001 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen en organen van de EU reikt daarvoor een nuttig model aan ([37]).

5.5. *Een verordening, geen richtlijn*

64. Ten slotte is de EDPS van mening dat de herziening ook een gelegenheid is om het voor gegevensbescherming gebruikte soort rechtsinstrument opnieuw te bekijken. Een verordening, één enkel instrument dat rechtstreeks van toepassing is in de lidstaten, is de meest doeltreffende manier om het grondrecht van gegevensbescherming te beschermen en een echte interne markt tot stand te brengen waarop het vrije verkeer van persoonsgegevens wordt gewaarborgd en het beschermingsniveau overal gelijk is, ongeacht het land of de sector waarin de gegevens worden verwerkt.

65. Een verordening beperkt de ruimte voor tegenstrijdige interpretaties en ongerechtvaardigde verschillen in de omzetting en de toepassing van de wetgeving. Met een dergelijk rechtsinstrument wordt het bepalen van de toepasselijke wetgeving voor verwerkingsactiviteiten in de EU, een van de meest omstreden aspecten van de huidige regeling (zie hoofdstuk 9), bovendien minder belangrijk.

66. Op het gebied van gegevensbescherming is een verordening des te meer gerechtvaardigd, aangezien:

— artikel 16 VWEU het recht op bescherming van persoonsgegevens naar het niveau van het Verdrag heeft opgetild en een eenvormig beschermingsniveau voor het individu in de hele EU beoogt of zelfs gelast;

— gegevens in een elektronische omgeving worden verwerkt waarin de binnengrenzen tussen de lidstaten minder belangrijk zijn geworden.

([37]) Zie artikel 27 van de verordening, (PB L 8 van 12.1.2001, blz. 1).

67. Indien voor een verordening als algemeen instrument wordt gekozen, kunnen zo nodig rechtstreeks aan lidstaten gerichte bepalingen worden opgenomen wanneer flexibiliteit vereist is. De keuze voor een verordening heeft ook geen invloed op de bevoegdheid van de lidstaten om, zo nodig, aanvullende regels inzake gegevensbescherming vast te stellen, in overeenstemming met het EU-recht.

6. **De rechten van personen beter beschermen**

6.1. *Het belang van een betere bescherming van de rechten*

68. De EDPS staat volledig achter de mededeling wat het voorstel betreft om de rechten van personen beter te beschermen, aangezien de bestaande rechtsinstrumenten onvoldoende bescherming bieden in deze almaar complexere gedigitaliseerde wereld.

69. Enerzijds zorgt de ontwikkeling van een gedigitaliseerde wereld voor een scherpe toename van het verzamelen, het gebruik en de doorgifte van persoonsgegevens op een bijzonder ingewikkelde en ondoorzichtige wijze. Personen zijn zich er vaak niet van bewust of begrijpen niet hoe dat gebeurt, wie hun gegevens verzamelt en hoe zij controle kunnen uitoefenen. Een voorbeeld daarvan is de monitoring van de onlineactiviteiten van personen door aanbieders van advertentienetwerken, met behulp van cookies en soortgelijke middelen, met de bedoeling gerichte advertenties te kunnen sturen. Wanneer gebruikers websites bezoeken, verwachten zij niet dat een onzichtbare derde partij deze bezoeken registreert en gebruikersprofielen opstelt op basis van informatie over hun levensstijl en hun voorkeuren en afkeren.

70. Anderzijds moedigt de ontwikkeling personen aan om hun persoonlijke informatie proactief te delen, bijvoorbeeld op sociale netwerken. Steeds meer jongeren worden lid van een sociaal netwerk en wisselen informatie uit met hun leeftijdgenoten. Het valt te betwijfelen dat (jonge) leden van dergelijke netwerken zich bewust zijn van de reikwijdte van de informatie die zij bekendmaken en van de gevolgen op lange termijn van hun handelingen.

6.2. *Transparantie bevorderen*

71. Transparantie is uitermate belangrijk voor elke regeling inzake gegevensbescherming, niet alleen door de intrinsieke waarde ervan, maar ook omdat zij de toepassing van andere beginselen van gegevensbescherming mogelijk maakt. Pas wanneer personen weten dat hun gegevens worden verwerkt, kunnen zij hun rechten uitoefenen.

72. Verschillende bepalingen van Richtlijn 95/46/EG hebben betrekking op transparantie. Op grond van de artikelen 10 en 11 moeten personen van wie persoonsgegevens worden verzameld daarover worden ingelicht. Bovendien wordt in artikel 12 het recht van personen erkend om in begrijpelijke vorm een afschrift te krijgen van hun eigen persoonsgegevens (recht van toegang). In artikel 15 wordt erkend dat betrokkenen het recht hebben de achterliggende gedachte te kennen van geautomatiseerde besluiten die rechtsgevolgen voor hen hebben. Tot slot houdt artikel 6, lid 1, onder a), volgens welk gegevens eerlijk moeten worden verwerkt, ook een transparantievereiste in. Persoonsgegevens kunnen niet om verborgen of geheime redenen worden verwerkt.

73. De Commissie stelt in de mededeling voor een algemeen transparantiebeginsel toe te voegen. In reactie op dat voorstel beklemtoont de EDPS dat het begrip transparantie al een integrerend onderdeel van het huidige rechtskader inzake gegevensbescherming uitmaakt, zij het impliciet. Dit kan worden afgeleid van de verschillende bepalingen die betrekking hebben op transparantie, zoals in het voorgaande lid werd aangehaald. Volgens de EDPS had de opname van een *uitdrukkelijk* transparantiebeginsel, al dan niet gekoppeld aan de bestaande bepaling betreffende eerlijke verwerking, een meerwaarde geboden. De uitdrukkelijke vermelding van het beginsel zou de rechtszekerheid bevorderen en bevestigen dat voor de verwerking verantwoordelijken persoonsgegevens in alle omstandigheden op een transparante wijze moeten verwerken, en niet alleen op verzoek of wanneer een specifieke wettelijke bepaling hen daartoe verplicht.

74. Het is echter misschien belangrijker de bestaande bepalingen inzake transparantie uit te breiden, zoals de bestaande artikelen 10 en 11 van Richtlijn 95/46/EG. Die bepalingen specificeren welke informatie moet worden verstrekt, maar blijven vaag over de wijze waarop dat moet gebeuren. Concreet stelt de EDPS voor de bestaande bepalingen uit te breiden door:

— de voor verwerking verantwoordelijken te verplichten informatie over de gegevensverwerking te verstrekken die vlot toegankelijk en gemakkelijk te begrijpen is en opgesteld is in duidelijke en eenvoudige taal ([38]). De informatie moet duidelijk zijn en in het oog springen. De bepaling kan ook vereisen dat de informatie gemakkelijk te begrijpen moet zijn. Op grond van die eis zou een ondoorzichtig of moeilijk te begrijpen privacybeleid bij wet niet langer zijn toegestaan;

— te eisen dat de informatie vlot en rechtstreeks aan de betrokkenen wordt verstrekt. De informatie dient ook permanent toegankelijk te zijn en mag niet na een korte tijd van een elektronisch medium verdwijnen. Daardoor zouden gebruikers informatie gemakkelijker kunnen opslaan en op een later tijdstip raadplegen, wat de toegankelijkheid ten goede komt.

6.3. *Steun voor een kennisgevingsplicht voor beveiligingsinbreuken*

75. De EDPS pleit voor de opname in het algemene instrument van een bepaling betreffende kennisgeving van inbreuken op persoonsgegevens, die de in de herziene e-privacyrichtlijn vastgestelde verplichting voor bepaalde aanbieders uitbreidt naar alle voor verwerking verantwoordelijken, zoals in de mededeling wordt voorgesteld. Volgens de e-privacyrichtlijn geldt de verplichting enkel voor aanbieders van elektronische communicatiediensten (aanbieders van telefonie, met inbegrip van VoIP, en internettoegang). Andere voor verwerking verantwoordelijken hoeven zich er niet aan te houden. De redenen voor de verplichting gelden evenzeer voor andere voor verwerking verantwoordelijken dan aanbieders van elektronische communicatiediensten.

76. De kennisgeving van beveiligingsinbreuken dient verschillende doeleinden. Zoals in de mededeling wordt benadrukt, is zij in de eerste plaats een middel om personen te wijzen op het gevaar dat zij lopen wanneer hun persoonsgegevens gecompromitteerd raken. Dit kan hen helpen de nodige maatregelen te nemen om dergelijke risico's te beperken. Wanneer bijvoorbeeld bankgegevens gecompromitteerd zijn, kunnen de betrokken personen onder meer hun wachtwoorden wijzigen of hun rekeningen sluiten. Bovendien draagt de kennisgeving van beveiligingsinbreuken bij tot de doeltreffende toepassing van andere in de richtlijn vastgestelde beginselen en verplichtingen. De verplichte kennisgeving van beveiligingsinbreuken moedigt de voor verwerking verantwoordelijken bijvoorbeeld aan strengere veiligheidsmaatregelen te treffen om inbreuken te voorkomen. De kennisgeving van beveiligingsinbreuken is ook een middel om de verantwoordelijkheid van de voor verwerking verantwoordelijken aan te scherpen, in het bijzonder om verantwoording te bevorderen (zie hoofdstuk 7). Tot slot is het ook een handhavingshulpmiddel voor gegevensbeschermingsautoriteiten. De kennisgeving van een inbreuk aan de gegevensbeschermingsautoriteiten kan leiden tot een onderzoek van de algemene praktijken van een voor verwerking verantwoordelijke.

77. De specifieke voorschriften inzake beveiligingsinbreuken in de gewijzigde e-privacyrichtlijn werden uitgebreid besproken in het parlementaire stadium van de wetgevingsprocedure die aan de goedkeuring van de e-privacyrichtlijn voorafging. Daarbij werden de adviezen van de Groep gegevensbescherming artikel 29 en de EDPS alsook de standpunten van andere belanghebbenden in overweging genomen. De voorschriften geven de standpunten van de verschillende belanghebbenden weer. Alle belangen zijn daarbij in evenwicht: de criteria die kennisgeving verplichten volstaan in beginsel om personen te beschermen, zonder dat omslachtige, nutteloze eisen worden gesteld.

6.4. *Uitbreiding van de voorschriften inzake het verlenen van toestemming*

78. Artikel 7 van de richtlijn gegevensbescherming voorziet in zes rechtsgrondslagen voor de verwerking van persoonsgegevens, waaronder toestemming van de betrokkene. Een voor verwerking verantwoordelijke mag persoonsgegevens verwerken voor zover de betrokkenen met kennis van zaken toestemming hebben gegeven voor de verzameling en verdere verwerking van hun gegevens.

79. In de praktijk hebben gebruikers slechts weinig controle over hun gegevens, met name in technologische contexten. In sommige gevallen wordt gebruik gemaakt van impliciete toestemming, met andere woorden toestemming die wordt afgeleid. Toestemming kan worden afgeleid uit een handeling van de betrokkene (bijv. het gebruik van een website wordt gezien als het verlenen van toestemming om de gegevens van de gebruiker te registreren

([38]) Zie mededeling, blz. 6.

voor marketingdoeleinden). Zij kan ook worden afgeleid uit stilzwijgen of het niet verrichten van een handeling (het niet verwijderen van een vinkje in een aangekruist vak wordt als toestemming beschouwd).

80. Volgens de richtlijn is de toestemming geldig indien zij geïnformeerd en specifiek is en vrijwillig wordt verleend. Zij moet een geïnformeerde uitdrukking zijn van de wensen van de betrokkene, waarmee deze aangeeft in te stemmen met de verwerking van zijn of haar persoonsgegevens. De toestemming moet op ondubbelzinnige wijze worden gegeven.

81. Toestemming die wordt afgeleid uit een handeling en met name uit stilzwijgen of het niet verrichten van een handeling is vaak geen ondubbelzinnige toestemming. Het is evenwel niet altijd duidelijk wat echte, ondubbelzinnige toestemming betekent. Bepaalde voor verwerking verantwoordelijken profiteren van deze onzekerheid om methoden te hanteren die niet geschikt zijn om echte, ondubbelzinnige toestemming te geven.

82. Gezien het voorgaande is de EDPS het met de Commissie eens dat het begrip toestemming duidelijker moet worden afgelijnd en dat ervoor moet worden gezorgd dat enkel op een behoorlijke wijze verleende toestemming als dusdanig wordt beschouwd. Tegen deze achtergrond stelt de EDPS het volgende voor ([39]):

— de situaties waarin uitdrukkelijke toestemming is vereist, welke momenteel beperkt zijn tot gevoelige gegevens, eventueel uitbreiden;

— aanvullende voorschriften vaststellen voor het verlenen van toestemming op het internet;

— aanvullende voorschriften vaststellen voor het verlenen van toestemming voor de verwerking van gegevens voor bijkomende doeleinden (met name wanneer de verwerking secundair is ten opzichte van de primaire verwerking of niet voor de hand ligt);

— in een aanvullend rechtsinstrument, dat al dan niet door de Commissie op grond van artikel 290 VWEU wordt goedgekeurd, bepalen welk type toestemming vereist is, bijvoorbeeld om te specificeren in welke mate toestemming moet worden verleend voor de verwerking van gegevens van RFID-tags op consumptiegoederen of voor andere specifieke technieken.

6.5. *Gegevensportabiliteit en het recht om te worden vergeten*

83. Gegevensportabiliteit en het recht om te worden vergeten zijn twee verwante begrippen die in de mededeling worden gebruikt om de rechten van betrokkenen beter te beschermen. Zij vullen de al in de richtlijn vastgestelde beginselen aan. Zij geven betrokkenen namelijk het recht zich tegen de verdere verwerking van hun persoonsgegevens te verzetten en verplichten de voor verwerking verantwoordelijken informatie te wissen zodra deze niet meer noodzakelijk is voor de verwerking.

84. Deze twee nieuwe begrippen zijn vooral nuttig in de context van een informatiemaatschappij, waarin almaar meer gegevens automatisch worden opgeslagen en voor onbepaalde duur worden bijgehouden. In de praktijk blijkt dat betrokkenen in werkelijkheid bijzonder weinig controle hebben over hun persoonsgegevens, zelfs indien zij de gegevens zelf in een systeem hebben geladen. Dit is te meer zo gezien het gigantische geheugen dat het internet vandaag de dag vertegenwoordigt. Bovendien is het verwijderen van gegevens voor een voor verwerking verantwoordelijke economisch gezien duurder dan ze te bewaren. Door hun rechten uit te oefenen, gaan personen bijgevolg tegen de natuurlijke economische tendens in.

85. Zowel gegevensportabiliteit als het recht om te worden vergeten kunnen helpen de weegschaal te doen doorslaan in het voordeel van de betrokkenen. Gegevensportabiliteit heeft ten doel personen meer controle te geven over hun informatie, terwijl het recht om te worden vergeten ervoor zorgt dat de informatie automatisch verdwijnt na een bepaalde termijn, zelfs indien de betrokkenen geen actie ondernemen of zelfs niet weten dat hun gegevens ooit zijn bewaard.

86. Gegevensportabiliteit is meer bepaald het vermogen van gebruikers om hun voorkeur betreffende de verwerking van hun gegevens te veranderen, met name in verband met diensten op basis van nieuwe technologieën. Dit geldt steeds meer voor diensten in het kader waarvan informatie wordt bewaard, met inbegrip van persoonsgegevens, zoals mobiele telefonie en bewaardiensten voor foto's, e-mails en andere informatie, waarbij in bepaalde gevallen gebruik wordt gemaakt van cloud computing.

87. Personen moeten gemakkelijk en vrij kunnen overstappen naar een andere aanbieder en hun persoonsgegevens naar de nieuwe aanbieder kunnen overdragen. De EDPS is van mening dat de bestaande rechten in Richtlijn 95/46/EG beter kunnen worden beschermd door een portabiliteitsrecht te voorzien in het kader van diensten van de informatiemaatschappij, teneinde personen te helpen ervoor te zorgen dat aanbieders en andere voor de verwerking verantwoordelijken hen toegang geven tot hun persoonsgegevens en er tegelijkertijd voor te zorgen dat de oude aanbieders of andere voor verwerking verantwoordelijken de desbetreffende informatie wissen, zelfs indien zij deze eigenlijk zouden willen bewaren voor hun eigen rechtmatige doeleinden.

88. De vaststelling van een nieuw „recht om te worden vergeten" zou garanderen dat de persoonsgegevens worden gewist of het verbod op verder gebruik ervan wordt nageleefd zonder dat de betrokkene hoeft tussen te komen, zij het op voorwaarde dat de desbetreffende gegevens reeds gedurende een bepaalde termijn zijn bewaard. De

([39]) De Groep gegevensbescherming artikel 29 werkt momenteel aan een advies over het begrip „toestemming". Dat advies kan tot aanvullende voorstellen leiden.

gegevens krijgen als het ware een soort van vervaldatum. Dit beginsel werd reeds bevestigd in nationale rechtszaken en wordt toegepast in bepaalde sectoren, bijvoorbeeld voor politiedossiers, strafregisters en tuchtdossiers: volgens bepaalde nationale wetten dient informatie over personen automatisch te worden gewist of mag deze niet verder worden gebruikt of verspreid, in het bijzonder na een bepaalde termijn, zonder dat vooraf een analyse van elk geval afzonderlijk vereist is.

89. Een nieuw „recht om te worden vergeten" dient dan ook samen te gaan met gegevensportabiliteit. De meerwaarde is dat de betrokkenen zonder enige inspanning en zonder te hoeven aandringen hun gegevens kunnen laten wissen, aangezien dat automatisch op een objectieve wijze dient te gebeuren. Een voor verwerking verantwoordelijke kan de gegevens slechts in zeer specifieke omstandigheden langer bijhouden wanneer daartoe een specifieke behoefte wordt vastgesteld. Het „recht om te worden vergeten" legt aldus de bewijslast bij de voor verwerking verantwoordelijke en niet bij de betrokkene en vormt een standaardinstelling voor de verwerking van persoonsgegevens die maximale privacy biedt („privacy by default").

90. De EDPS is van mening dat het recht om te worden vergeten bijzonder nuttig kan zijn in het kader van diensten van de informatiemaatschappij. Een verplichting om informatie na een bepaalde termijn te wissen of niet verder te verspreiden is vooral zinvol in de media en op het internet, met name voor sociale netwerken. Zij zou ook nuttig zijn wat eindapparatuur betreft: gegevens die zijn opgeslagen op mobiele toestellen of computers worden na een bepaalde termijn automatisch gewist of geblokkeerd wanneer zij niet langer in het bezit zijn van de betrokken persoon. Het recht om te worden vergeten kan dan ook worden vertaald in een verplichting tot ingebouwde privacy („privacy by design").

91. Kortom: de EDPS is van mening dat gegevensportabiliteit en het recht om te worden vergeten nuttige begrippen zijn. De opname ervan in het rechtsinstrument kan zinvol zijn, maar dan wellicht alleen voor elektronische diensten.

6.6. *Verwerking van persoonsgegevens van kinderen*

92. Er zijn geen specifieke voorschriften over de verwerking van persoonsgegevens van kinderen op grond van Richtlijn 95/46/EG. Dit betekent dat niet wordt erkend dat kinderen in bepaalde omstandigheden extra moeten worden beschermd door hun kwetsbaarheid en door de rechtsonzekerheid die met name op de volgende gebieden bestaat:

— het verzamelen van gegevens van kinderen en de manier waarop deze kinderen van die handeling in kennis moeten worden gesteld;

— de manier waarop de toestemming van kinderen wordt verkregen. Aangezien er geen specifieke voorschriften gelden voor de wijze waarop de toestemming van kinderen moet worden verkregen noch voor de leeftijdsgrens waaronder kinderen als dusdanig worden beschouwd, worden deze kwesties in de nationale wetgeving geregeld, die van lidstaat tot lidstaat verschilt ([40]);

— de manier waarop en de voorwaarden waaronder kinderen of hun wettelijke vertegenwoordigers hun uit de richtlijn voortvloeiende rechten kunnen uitoefenen.

93. De EDPS is van mening dat de bijzondere belangen van kinderen beter beschermd zouden worden indien aanvullende bepalingen in het nieuwe rechtsinstrument worden opgenomen, met name wat het verzamelen en het verwerken van gegevens van kinderen betreft. Dergelijke specifieke bepalingen zouden ook meer rechtszekerheid bieden op dit bepaalde gebied en zouden ten goede komen aan de voor verwerking verantwoordelijken, die momenteel geconfronteerd worden met uiteenlopende wettelijke voorschriften.

94. De EDPS stelt voor de volgende bepalingen in het rechtsinstrument op te nemen:

— een verplichting om informatie aan te passen aan kinderen in zoverre kinderen daardoor gemakkelijker kunnen begrijpen wat het verzamelen van hun gegevens betekent;

— andere informatieverplichtingen die op kinderen zijn afgestemd, over de manier waarop de informatie moet worden verstrekt en eventueel ook over de inhoud;

— een specifieke bepaling die kinderen beschermt tegen behavioural advertising;

— een strengere beperking van de toegelaten gebruiksdoeleinden voor gegevens van kinderen;

— een verbod op het verzamelen van bepaalde categorieën gegevens van kinderen;

— een leeftijdsgrens. Onder deze grens mag in het algemeen enkel informatie van kinderen worden verzameld indien een van de ouders uitdrukkelijk en controleerbaar toestemming heeft gegeven;

— indien de toestemming van een van de ouders vereist is, regels over de manier waarop de leeftijd van het kind kan worden geauthenticeerd, met andere woorden de manier waarop kan worden nagegaan of een kind minderjarig is en waarop de toestemming van de

([40]) Toestemming is doorgaans gekoppeld aan de leeftijd waarop kinderen contractuele verplichtingen kunnen aangaan. Dat is de leeftijd waarop kinderen geacht worden een bepaalde mate van volwassenheid te hebben bereikt. Zo vereist de Spaanse wetgeving dat ouders toestemming geven voor het verzamelen van gegevens van kinderen jonger dan 14 jaar. Boven die leeftijd wordt ervan uitgegaan dat kinderen zelf toestemming kunnen geven. In het Verenigd Koninkrijk bevat de Wet bescherming persoonsgegevens („Data Protection Act") geen verwijzing naar een specifieke leeftijd of grens. De Britse gegevensbeschermingsautoriteit heeft de wet echter zo geïnterpreteerd dat kinderen ouder dan 12 jaar toestemming kunnen geven. Kinderen jonger dan 12 kunnen dus geen toestemming geven. Om hun persoonsgegevens te verkrijgen, is de voorafgaande toestemming van een van de ouders of van een voogd vereist.

ouders kan worden geverifieerd. Dienaangaande kan de EU zich inspireren op de regelgeving van andere landen, zoals de Verenigde Staten ([41]).

6.7. *Mechanismen voor collectieve schadeacties*

95. Het heeft geen zin de bepalingen betreffende de rechten van personen uit te breiden indien er geen doeltreffende procedures bestaan om dergelijke rechten te handhaven. In deze context beveelt de EDPS aan mechanismen voor collectieve schadeacties wegens inbreuken op de gegevensbeschermingsvoorschriften in het EU-recht vast te stellen. Met name mechanismen voor collectieve schadeacties waarmee een groep burgers hun individuele claims kunnen bundelen, kunnen in grote mate tot de handhaving van de regelgeving inzake gegevensbescherming bijdragen ([42]). Ook de gegevensbeschermingsautoriteiten hebben zich in het document van de werkgroepen over de toekomst van privacy voor dergelijke mechanismen uitgesproken.

96. In gevallen waar de gevolgen beperkt zijn, is de kans klein dat de slachtoffers van een inbreuk op de gegevensbeschermingsvoorschriften ieder afzonderlijk een vordering instellen tegen de voor verwerking verantwoordelijken door de kosten, de lange wachttijd, de onzekerheid, de risico's en de lasten die dit voor hen meebrengt. Deze obstakels kunnen worden weggewerkt of aanzienlijk beperkt door een regeling voor collectieve schadeacties die de slachtoffers van inbreuken in staat stelt hun individuele claims te bundelen. De EDPS is er ook voor gewonnen gekwalificeerde entiteiten, zoals consumentenorganisaties en overheidsinstanties, te machtigen om schadevergoedingsacties te starten in naam van de slachtoffers van inbreuken op de gegevensbescherming. Deze acties mogen geen afbreuk doen aan het recht van de betrokkenen om individuele vorderingen in te stellen.

97. Collectieve acties zijn niet alleen belangrijk om een volledige compensatie of andere correctieve maatregelen te garanderen, maar doen indirect ook dienst als afschrikmiddel. Het risico dat door dergelijke acties een dure collectieve schadevergoeding moet worden betaald, is voor de voor verwerking verantwoordelijken een belangrijke prikkel om toe te zien op de effectieve naleving van de regelgeving. Een betere private handhaving in de vorm van mechanismen voor collectieve schadeacties zou dus een aanvulling vormen op de openbare handhaving.

98. In de mededeling wordt dienaangaande geen standpunt ingenomen. De EDPS heeft weet van de discussie op Europees niveau over de invoer van collectieve schadeacties voor consumenten. Hij is zich ook bewust van het risico op uitwassen dat deze mechanismen met zich kunnen meebrengen, gezien de ervaring hiermee in andere rechtsstelsels. Deze factoren wegen naar zijn mening evenwel niet tegen de mogelijke voordelen op om de invoering van de mechanismen in de wetgeving inzake gegevensbescherming af te wijzen of uit te stellen ([43]).

7. **Een belangrijkere rol voor organisaties en de voor verwerking verantwoordelijken**

7.1. *Algemeen*

99. De EDPS is van mening dat een modern rechtsinstrument voor gegevensbescherming naast ruimere rechten voor personen ook de nodige hulpmiddelen moet bevatten die de verantwoordelijkheid van de voor verwerking verantwoordelijken bevorderen. Het kader dient de voor verwerking verantwoordelijken van de private en de openbare sector met name te stimuleren om gegevensbeschermingsmaatregelen in hun bedrijfsprocessen op te nemen. Deze hulpmiddelen zouden ten eerste nuttig zijn omdat, zoals eerder al werd gezegd, de technologische ontwikkelingen tot een forse toename hebben geleid van het verzamelen, het gebruik en de doorgifte van persoonsgegevens, wat leidt tot grotere risico's voor de privacy en de bescherming van persoonsgegevens die op een doeltreffende wijze moeten worden gecompenseerd. Ten tweede ontbreken dergelijke hulpmiddelen in het huidige kader, met uitzondering van een aantal welomschreven bepalingen (zie verder), en kunnen de voor verwerking verantwoordelijken gegevensbescherming en privacy reactief benaderen en pas optreden nadat zich een probleem heeft voorgedaan. Deze aanpak blijkt ook uit de statistieken, die aangeven dat een gebrekkige naleving van de regelgeving en gegevensverlies een telkens terugkerend probleem zijn.

100. Volgens de EDPS volstaat het huidige kader niet om de doeltreffende bescherming van persoonsgegevens nu en in de toekomst te waarborgen. Hoe groter de risico's, hoe groter de behoefte aan concrete maatregelen die informatie op een praktisch niveau beschermen en doeltreffende bescherming bieden. Tenzij deze proactieve maatregelen daadwerkelijk worden ingevoerd, zullen de fouten, incidenten en nalatigheid wellicht aanhouden, waardoor de privacy van personen in deze almaar sterker gedigitaliseerde maatschappij in gevaar komt. Daarom stelt de EDPS de onderstaande maatregelen voor.

7.2. *Uitbreiding van de verantwoordingsplicht van de voor verwerking verantwoordelijken*

101. De EDPS beveelt aan een nieuwe bepaling in het rechtsinstrument op te nemen die de voor verwerking verantwoordelijken verplicht passende en doeltreffende maatregelen te nemen om de in het rechtsinstrument vastgestelde beginselen en voorschriften na te leven en dit op verzoek aan te tonen.

([41]) In de VS vereist de COPPA (wet betreffende de bescherming van kinderen op het internet) dat uitbaters van commerciële websites en onlinediensten voor kinderen jonger dan 13 jaar toestemming van de ouders moeten krijgen voordat zij persoonsgegevens verzamelen en dat uitbaters van commerciële websites voor het brede publiek feitelijk op de hoogte zijn van het feit dat ook kinderen de website raadplegen.

([42]) Zie ook het advies van de EDPS van 25 juli 2007 over de toepassing van de richtlijn gegevensbescherming inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming, (PB C 255 van 27.10.2007, blz. 10).

([43]) Sommige lidstaten hebben reeds soortgelijke mechanismen in hun wetgeving opgenomen.

102. Dit type bepaling is niet helemaal nieuw. Artikel 6, lid 2, van Richtlijn 95/46/EG verwijst naar de beginselen inzake gegevenskwaliteit en bepaalt: „Op de voor de verwerking verantwoordelijke rust de plicht om voor de naleving van het bepaalde in lid 1 zorg te dragen". Evenzo vereist artikel 17, lid 1, dat voor de verwerking verantwoordelijken zowel technische als organisatorische maatregelen nemen. Het toepassingsgebied van deze bepalingen is evenwel beperkt. De vaststelling van een algemene bepaling over verantwoording zou voor de verwerking verantwoordelijken aanmoedigen proactieve maatregelen te nemen om alle onderdelen van de wetgeving inzake gegevensbescherming te kunnen naleven.

103. Een bepaling over verantwoording zou tot gevolg hebben dat de voor verwerking verantwoordelijken interne mechanismen en controlesystemen moeten opzetten om naleving van de in het kader vastgestelde beginselen en voorschriften te waarborgen. Dit zou bijvoorbeeld betrokkenheid van de hoogste kaderleden bij het gegevensbeschermingsbeleid vereisen, alsook procedures voor het in kaart brengen en correct identificeren van alle gegevensverwerkingsactiviteiten, een bindend gegevensbeschermingsbeleid dat permanent wordt herzien en geactualiseerd zodat nieuwe verwerkingsactiviteiten erin worden opgenomen, naleving van de beginselen inzake gegevenskwaliteit, aanmelding, beveiliging, toegang, enz. In bepaalde gevallen dienen de voor verwerking verantwoordelijken ook verplicht te worden het brede publiek te bewijzen dat zij de wetgeving naleven. Dat is bijvoorbeeld mogelijk door hen te verplichten het thema gegevensbescherming op te nemen in openbare (jaar)verslagen, wanneer dergelijke verslagen op andere gronden verplicht zijn.

104. De te nemen interne en externe maatregelen dienen uiteraard passend te zijn en hangen af van de feiten en omstandigheden van elk geval afzonderlijk. Er is een groot verschil tussen een voor verwerking verantwoordelijke die enkele honderden klantendossiers verwerkt waarin enkel namen en adressen zijn opgenomen en een voor verwerking verantwoordelijke die dossiers van miljoenen patiënten verwerkt, met inbegrip van hun medische anamnese. Hetzelfde geldt voor de specifieke manieren waarop de doeltreffendheid van de maatregelen dient te worden geëvalueerd. Er is behoefte aan schaalbaarheid.

105. In het algemene integrale rechtsinstrument betreffende gegevensbescherming mogen geen specifieke voorschriften inzake verantwoording worden vastgesteld, maar slechts de essentiële onderdelen ervan. De mededeling voorziet in bepaalde elementen om de verantwoordelijkheid van de voor verwerking verantwoordelijken te vergroten, wat een goede zaak is. De EDPS staat meer bepaald volledig achter het verplicht stellen van functionarissen voor privacy en gegevensbescherming en effectbeoordelingen, onder bepaalde drempelvoorwaarden.

106. Bovendien beveelt de EDPS aan de Commissie op grond van artikel 290 VWEU te machtigen om de noodzakelijke basisvereisten inzake verantwoording aan te vullen. Het gebruik van deze bevoegdheid zou de voor verwerking verantwoordelijken meer rechtszekerheid bieden en de voorwaarden voor de naleving van de verantwoordingsplicht in de hele EU harmoniseren. De Groep gegevensbescherming artikel 29 en de EDPS dient over dergelijke specifieke instrumenten te worden geraadpleegd.

107. Tot slot kunnen de concrete maatregelen die de voor verwerking verantwoordelijken op het gebied van verantwoording moeten nemen ook door de gegevensbeschermingsautoriteiten worden opgelegd in het kader van hun handhavingsbevoegdheid. Daartoe dienen aan de gegevensbeschermingsautoriteiten nieuwe bevoegdheden te worden verleend, zodat zij correctieve maatregelen of sancties kunnen opleggen. Te voorziene maatregelen zijn onder meer het opzetten van interne programma's voor het toezicht op de naleving van de wetgeving, ingebouwde privacy voor specifieke producten en diensten, enz. Corrigerende maatregelen mogen enkel worden opgelegd indien deze passend, evenredig en doeltreffend zijn om de naleving van de toepasselijke en afdwingbare wettelijke normen te garanderen.

7.3. Ingebouwde privacy

108. Ingebouwde privacy is de inachtneming van gegevensbescherming en privacy vanaf de ontwerpfase van nieuwe producten, diensten en procedures in het kader waarvan persoonsgegevens worden verwerkt. Volgens de EDPS maakt „privacy by design" deel uit van de verantwoordingsplicht. Dientengevolge zouden de voor verwerking verantwoordelijken ook moeten aantonen dat zij het beginsel van ingebouwde privacy in voorkomend geval hebben toegepast. Recent heeft de 32e Internationale Conferentie van commissarissen voor gegevensbescherming en privacy een resolutie aangenomen waarin privacy wordt erkend als een essentieel onderdeel van fundamentele privacybescherming ([44]).

109. Een aantal bepalingen van Richtlijn 95/46/EG moedigen ingebouwde privacy aan ([45]), maar nergens is er uitdrukkelijk sprake van een verplichting. De EDPS is verheugd dat ingebouwde privacy in de mededeling wordt gezien als een middel om de naleving van de gegevensbeschermingsvoorschriften te waarborgen. Hij stelt een bindende bepaling voor waarin de toepassing van het ingebouwde-privacybeginsel verplicht wordt gesteld en die kan worden gebaseerd op de formulering van overweging 46 van Richtlijn 95/46/EG. De bepaling zou de voor verwerking

([44]) Resolutie betreffende ingebouwde privacy (Resolution on Privacy by Design), aangenomen tijdens de 32e Internationale Conferentie van commissarissen voor gegevensbescherming en privacy, Jeruzalem 27-29 oktober 2010.

([45]) De richtlijn bevat bepalingen die in verschillende situaties indirect de toepassing van ingebouwde privacy vereisen. Met name artikel 17 bepaalt dat de voor verwerking verantwoordelijken passende technische en organisatorische maatregelen ten uitvoer dienen te leggen om persoonsgegevens te beschermen tegen onwettige verwerking. De e-privacyrichtlijn is explicieter. Artikel 14, lid 3 bepaalt het volgende: Zo nodig kunnen maatregelen worden goedgekeurd om ervoor te zorgen dat de eindapparatuur gebouwd is op een wijze die verenigbaar is met het recht van gebruikers om het gebruik van hun persoonsgegevens te beschermen en te controleren, in overeenstemming met Richtlijn 1995/5/EG en met Beschikking 87/95/EEG van de Raad van 22 december 1986 betreffende de normalisatie op het gebied van de informatietechnologieën en de telecommunicatie.

verantwoordelijken meer bepaald verplichten technische en organisatorische maatregelen te nemen, zowel in de ontwerpfase van het verwerkingssysteem als bij de verwerking zelf, met name om de bescherming van de persoonsgegevens te garanderen en onrechtmatige verwerking te voorkomen ([46]).

110. Op grond van een dergelijke bepaling dienen de voor verwerking verantwoordelijken er onder meer voor te zorgen dat hun gegevensverwerkingssystemen dusdanig zijn opgevat dat zo weinig mogelijk persoonsgegevens worden verwerkt, dat de standaardinstellingen van hun systemen maximale privacy bieden („privacy by default"), bijvoorbeeld in sociale netwerken, dat profielen van personen standaard van andere personen worden afgeschermd en dat gebruikers over middelen beschikken om hun persoonsgegevens beter te beveiligen (bijv. toegangscontrole, encryptie, enz.).

111. Het voordeel van een meer uitdrukkelijke verwijzing naar ingebouwde privacy kan als volgt worden samengevat:

— het zou het belang van het beginsel op zich benadrukken, als een middel dat helpt ervoor te zorgen dat privacy vanaf de ontwerpfase in processen, producten en diensten wordt ingebouwd;

— het zou het misbruik van privacy verminderen, het onnodige verzamelen van gegevens tot een minimum beperken en personen in staat stellen echte keuzes te maken met betrekking tot hun persoonsgegevens;

— het zou voorkomen dat later lapmiddelen moeten worden gebruikt om problemen weg te werken die nauwelijks of niet kunnen worden opgelost;

— het zou de doeltreffende toepassing en handhaving van dit beginsel door de gegevensbeschermingsautoriteiten vergemakkelijken.

112. Het gecombineerde effect van deze verplichting zal de vraag naar producten en diensten met ingebouwde privacy stimuleren, wat de sector zal aanmoedigen op die vraag in te spelen. Bovendien zou een afzonderlijke verplichting moeten worden overwogen voor ontwerpers en fabrikanten van nieuwe producten en diensten die wellicht gevolgen hebben voor de gegevensbescherming en de privacy. De EDPS stelt voor een dergelijke afzonderlijke verplichting te voorzien, die de voor verwerking verantwoordelijken kan helpen hun eigen verplichting na te komen.

113. De opname van ingebouwde privacy in de wetgeving kan worden aangevuld met een bepaling met algemene sectoroverschrijdende eisen inzake ingebouwde privacy voor producten en diensten, zoals maatregelen die gebruikers meer controle geven, die in overeenstemming met het beginsel dient te worden vastgesteld.

114. De EDPS beveelt tevens aan de Commissie op grond van artikel 290 VWEU te machtigen om, indien nodig, de basisvoorschriften inzake ingebouwde privacy voor bepaalde producten en diensten aan te vullen. Het gebruik van deze bevoegdheid zou de voor verwerking verantwoordelijken meer rechtszekerheid bieden en de voorwaarden voor de naleving van de regelgeving in de hele EU harmoniseren. De Groep gegevensbescherming artikel 29 en de EDPS dienen over dergelijke specifieke instrumenten te worden geraadpleegd (zie ook punt 106 betreffende verantwoording).

115. Tot slot dienen de gegevensbeschermingsautoriteiten gemachtigd te worden om correctieve maatregelen en sancties op te leggen, onder dezelfde beperkende voorwaarden als die welke zijn vermeld in punt 107, wanneer voor verwerking verantwoordelijken kennelijk verzuimd hebben concrete maatregelen te nemen wanneer dat verplicht was.

7.4. *Certificeringsdiensten*

116. In de mededeling wordt de noodzaak erkend van de invoering van EU-certificeringsregelingen voor producten en diensten die aan de privacyregels voldoen. De EDPS staat volledig achter dit standpunt en stelt voor dergelijke regelingen en de mogelijke toepassing ervan in de hele EU vast te stellen in een bepaling, die later eventueel verder kan worden uitgewerkt in aanvullende wetgeving. De bepaling dient aan te sluiten op de bepalingen inzake verantwoording en ingebouwde privacy.

117. Met vrijwillige certificeringsregelingen zou kunnen worden gecontroleerd of de voor verwerking verantwoordelijken maatregelen hebben genomen om zich naar het rechtsinstrument te schikken. Bovendien hebben gecertificeerde voor verwerking verantwoordelijken — en zelfs hun producten of diensten — wellicht concurrentievoordeel ten opzichte van anderen. Dergelijke regelingen helpen de gegevensbeschermingsautoriteiten ook bij hun toezichts- en handhavingstaak.

8. **Globalisering en toepasselijk recht**

8.1. *Een duidelijke behoefte aan een consistentere bescherming*

118. Zoals eerder werd vermeld in hoofdstuk 2, is de doorgifte van persoonsgegevens over de EU-grenzen heen fors toegenomen door de ontwikkeling van nieuwe technologieën, de rol van multinationals en de toenemende inmenging van overheden in de verwerking en het delen van persoonsgegevens op internationaal niveau. Dat is een van de voornaamste redenen voor de herziening van het huidige rechtskader. Het is dan ook een van de terreinen waarop de EDPS aandringt op ambitie en doeltreffendheid, aangezien er duidelijk behoefte is aan een consistentere bescherming van gegevens die buiten de EU worden verwerkt.

([46]) In het huidige kader moedigt overweging 46 de voor verwerking verantwoordelijken aan om dergelijke maatregelen te nemen, maar een overweging is uiteraard niet bindend.

8.2. *Investeren in internationale voorschriften*

119. Volgens de EDPS moet meer worden geïnvesteerd in de ontwikkeling van internationale voorschriften. Een verdere harmonisatie van het beschermingsniveau van persoonsgegevens over de hele wereld zou de na te leven beginselen en de voorwaarden voor gegevensoverdracht aanzienlijk verduidelijken. Deze mondiale voorschriften dienen het vereiste hoge gegevensbeschermingsniveau — met inbegrip van de kernelementen van de gegevensbeschermingsregels van de EU — met specifieke regionale situaties te verzoenen.

120. De EDPS steunt de ambitieuze inspanningen die tot nu toe in het kader van de Internationale Conferentie van commissarissen voor gegevensbescherming zijn geleverd om de zogeheten „normen van Madrid" vast te stellen en te verspreiden, teneinde deze op te nemen in een bindend instrument en eventueel een intergouvernementele conferentie te openen ([47]). Hij roept de Commissie op de nodige initiatieven te nemen om de verwezenlijking van deze doelstelling te vergemakkelijken.

121. Volgens de EDPS is het ook belangrijk te zorgen voor samenhang tussen zijn initiatief voor internationale normen, de huidige herziening van het EU-kader inzake gegevensbescherming en andere ontwikkelingen zoals de momenteel aan de gang zijnde herziening van de privacyrichtsnoeren van de OESO en van Verdrag nr. 108 van de Raad van Europa, dat nog door derde landen kan worden ondertekend (zie ook punt 17). De EDPS is van mening dat daarbij een specifieke rol is weggelegd voor de Commissie, die moet verduidelijken hoe zij een dergelijke samenhang in de onderhandelingen van de OESO en de Raad van Europa zal bevorderen.

8.3. *Toepasselijke wettelijke eisen verduidelijken*

122. Aangezien volledige samenhang moeilijk te verwezenlijk is, zullen op zijn minst in de nabije toekomst verschillen blijven bestaan tussen de wetgevingen in de EU en meer nog buiten de EU. De EDPS is van mening dat een nieuw rechtsinstrument de criteria moet verduidelijken die het toepasselijke recht bepalen en moet voorzien in gestroomlijnde mechanismen voor gegevensstromen en een verantwoordingsplicht voor de partijen die bij gegevensstromen betrokken zijn.

123. Het rechtsinstrument dient er in de eerste plaats voor te zorgen dat de EU-wetgeving van toepassing is op de verwerking van persoonsgegevens buiten de EU-grenzen wanneer daar een gegronde reden voor is. Niet-Europese cloud-computingdiensten voor inwoners van de EU illustreren waarom dat nodig is. Op een domein waarop gegevens niet fysiek worden bewaard en niet op een vaste locatie worden verwerkt, waarop dienstverleners en gebruikers die zich in verschillende landen bevinden invloed op gegevens uitoefenen, is het erg moeilijk te bepalen wie verantwoordelijk is voor de naleving van welke gegevensbeschermingsbeginselen. In dergelijke gevallen verstrekken vooral de gegevensbeschermingsautoriteiten advies over de uitlegging en de toepassing van Richtlijn 95/46/EG, maar advies alleen volstaat niet om in deze nieuwe omgeving rechtszekerheid te garanderen.

124. In een recent advies heeft de Groep gegevensbescherming artikel 29 nadruk gelegd op de behoefte aan een nauwkeuriger rechtskader en een eenvoudiger criterium om het toepasselijke recht op het grondgebied van de EU te bepalen ([48]).

125. Volgens de EDPS verdient een verordening als rechtsinstrument de voorkeur omdat op die manier in alle lidstaten identieke voorschriften gelden. Met een verordening wordt het bepalen van het toepasselijke recht minder belangrijk. Dat is een van de redenen waarom de EDPS een groot voorstander is van een verordening. Bovendien kan een verordening de lidstaten ook nog enige vrijheid laten. Indien het nieuwe instrument aanzienlijke vrijheid laat, steunt de EDPS het voorstel van de werkgroep voor een verschuiving van een distributieve toepassing van de verschillende nationale wetgevingen naar een gecentraliseerde toepassing van één enkele wetgeving in alle lidstaten waar voor de verwerking verantwoordelijken vestigingen hebben. Hij pleit tevens voor meer samenwerking en coördinatie tussen de gegevensbeschermingsautoriteiten in transnationale zaken en klachten (zie hoofdstuk 10).

8.4. *Mechanismen voor gegevensstromen stroomlijnen*

126. Er moet rekening worden gehouden met de behoefte aan samenhang en een benchmark van hoog niveau, niet alleen met het oog op mondiale gegevensbeschermingsbeginselen, maar ook voor de internationale doorgifte van gegevens. De EDPS staat volledig achter de doelstelling van de Commissie om de bestaande procedures voor de internationale doorgifte van gegevens te stroomlijnen en te zorgen voor een meer eenvormige en samenhangende aanpak ten aanzien van derde landen en internationale organisaties.

127. Het mechanisme voor gegevensstromen omvat zowel de doorgifte van gegevens in de particuliere sector, met name via contractuele bepalingen of bindende bedrijfsvoorschriften, als de doorgifte van gegevens tussen openbare instanties. Bindende bedrijfsvoorschriften vormen een van de gebieden waarop een meer samenhangende en gestroomlijnde aanpak wenselijk is. De EDPS beveelt aan de voorwaarden voor bindende bedrijfsvoorschriften uitdrukkelijk aan bod te laten komen in het nieuwe rechtsinstrument ([49]), door:

— bindende bedrijfsvoorschriften uitdrukkelijk te erkennen als een hulpmiddel dat passende waarborgen biedt;

— de voornaamste onderdelen van en voorwaarden voor bindende bedrijfsvoorschriften vast te stellen;

([47]) Zoals voorgesteld in de resolutie betreffende internationale normen, aangenomen tijdens de 32e Internationale Conferentie van commissarissen voor gegevensbescherming en privacy, Jeruzalem 27-29 oktober 2010.

([48]) Advies 8/2010 van de Groep gegevensbescherming artikel 29 betreffende het toepasselijke recht, WP 179.

([49]) Betreffende de internationale doorgifte van gegevens, zie ook hoofdstuk 8 van het advies.

— samenwerkingsprocedures voor de vaststelling van bindende bedrijfsvoorschriften te voorzien, met inbegrip van criteria voor de selectie van een toezichthoudende instantie die de leiding heeft (centraal aanspreekpunt).

9. **Politie en justitie**

9.1. *Het algemene instrument*

128. De Commissie heeft meermaals het belang onderstreept van een betere gegevensbescherming op het gebied van rechtshandhaving en misdaadpreventie, in het kader waarvan de uitwisseling en het gebruik van persoonsgegevens aanzienlijk is toegenomen. Bovendien heeft de Europese Raad een solide gegevensbeschermingsregeling in het programma van Stockholm aangemerkt als de eerste noodzakelijke voorwaarde voor de EU-strategie voor het beheer van rechtshandhavingsinformatie op dat gebied ([50]).

129. De herziening van het algemene kader voor gegevensbescherming biedt de gelegenheid om dienaangaande vooruitgang te boeken, vooral omdat Kaderbesluit 2008/977 in de mededeling ontoereikend wordt genoemd ([51]).

130. De EDPS legt in punt 3.2.5 van dit advies uit waarom politiële en justitiële samenwerking in het algemene instrument dient te worden opgenomen. De opname van politie en justitie biedt extra voordelen. Het betekent dat de voorschriften niet langer alleen maar voor de grensoverschrijdende uitwisseling van gegevens gelden ([52]), maar ook voor de binnenlandse verwerking van gegevens. Er is meer garantie op een passende bescherming in de uitwisseling van persoonsgegevens met derde landen, ook ten aanzien van internationale overeenkomsten. Bovendien krijgen de gegevensbeschermingsautoriteiten dezelfde uitgebreide en geharmoniseerde bevoegdheden ten aanzien van politie en justitiële instanties als die welke zij hebben ten aanzien van andere voor verwerking verantwoordelijken. Tot slot dient het huidige artikel 13, dat de lidstaten machtigt specifieke wetgeving vast te stellen om de uit het algemene instrument voortvloeiende rechten en plichten voor bepaalde openbare belangen te beperken, even restrictief te worden toegepast als op andere gebieden. In het bijzonder de specifieke beschermingsmaatregelen waarin in het algemene instrument is voorzien, dienen ook in de nationale wetgeving voor politiële en justitiële samenwerking te worden nageleefd.

9.2. *Aanvullende specifieke voorschriften voor politie en justitie*

131. Een dergelijke opname sluit evenwel geen speciale voorschriften en afwijkingen uit die inspelen op de specifieke behoeften van de betrokken sector, zoals vermeld in de aan het Verdrag van Lissabon gehechte Verklaring nr. 21. De rechten van betrokkenen kunnen worden beperkt, maar de opgelegde beperkingen dienen noodzakelijk en evenredig te zijn en mogen niet aan de essentiële onderdelen van het recht zelf niet raken. Hierbij dient te worden onderstreept dat Richtlijn 95/46/EG, met inbegrip van artikel 13 daarvan, momenteel van toepassing is op de rechtshandhaving op diverse gebieden (bijv. belastingen, douane en fraudebestrijding) die in wezen niet verschillen van vele politiële en justitiële activiteiten.

132. Bovendien dienen ter compensatie van de betrokkenen specifieke beschermingsmaatregelen te worden ingebouwd om hen extra bescherming te bieden op een gebied waarop de verwerking van hun persoonsgegevens ingrijpender kan zijn.

133. Gezien het voorgaande is de EDPS van mening dat het nieuwe kader minstens de volgende elementen moet omvatten, overeenkomstig Verdrag nr. 108 en Aanbeveling R (87) 15:

— een onderscheid tussen verschillende categorieën gegevens en dossiers op basis van hun nauwkeurigheid en betrouwbaarheid, ter toepassing van het beginsel dat feitelijke gegevens moeten worden onderscheiden van gegevens die zijn gebaseerd op meningen of persoonlijke oordelen;

— een onderscheid tussen verschillende categorieën betrokkenen (verdachten van delicten, slachtoffers, getuigen, enz.) en dossiers (tijdelijke, permanente en inlichtingendossiers). Voor de verwerking van gegevens van niet-verdachten moeten specifieke voorwaarden en beschermingsmaatregelen worden voorzien;

— mechanismen die garanderen dat gegevens periodiek worden gecontroleerd en gecorrigeerd om de kwaliteit van de verwerkte gegevens te waarborgen;

— specifieke bepalingen en/of beschermingsmaatregelen met betrekking tot de (steeds belangrijkere) verwerking van biometrische en genetische gegevens op het gebied van rechtshandhaving. Het gebruik van dergelijke gegevens moet worden beperkt tot gevallen waarin geen minder ingrijpende middelen voorhanden zijn die tot hetzelfde resultaat kunnen leiden ([53]);

— voorwaarden voor de overdracht van persoonsgegevens aan onbevoegde instanties en particuliere partijen, alsook voor de toegang tot en het verdere gebruik door wetshandhavingsinstanties van door derden verzamelde persoonsgegevens.

([50]) Zie het advies van de EDPS van 30 september 2010 over de mededeling van de Commissie aan het Europees Parlement en de Raad, „Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht", punten 9-19.

([51]) Zie het voorgaande hoofdstuk 3.2.5.

([52]) Dit is momenteel het beperkte toepassingsgebied van Kaderbesluit 2008/977.

([53]) Zie dienaangaande het verslag van de werkgroepen over de toekomst van privacy, punt 112.

9.3. *Sectorspecifieke regelingen inzake gegevensbescherming*

134. De Commissie stelt in de mededeling: „[…] het kaderbesluit [komt] niet in de plaats van de diverse sectorspecifieke wetgevingsinstrumenten voor politiële en justitiële samenwerking in strafzaken die op EU-niveau zijn vastgesteld, onder meer die betreffende de werking van Europol, Eurojust, het Schengeninformatiesysteem (SIS) en het douane-informatiesysteem, die voorzien in bijzondere gegevensbeschermingsregelingen en/of gewoonlijk verwijzen naar de gegevensbeschermingsinstrumenten van de Raad van Europa".

135. Volgens de EDPS dient een nieuw rechtskader zo duidelijk, eenvoudig en consistent mogelijk te zijn. Wanneer te veel verschillende regelingen gelden voor bijvoorbeeld Europol, Eurojust, SIS en Prüm, blijft het naleven van de voorschriften moeilijk of wordt het zelfs nog moeilijker. Dat is een van de redenen waarom de EDPS voorstander is van een omvattend rechtsinstrument voor alle sectoren.

136. De EDPS begrijpt evenwel dat het op elkaar afstemmen van de verschillende regelingen heel wat werk vraagt, dat zorgvuldig moet worden uitgevoerd. De EDPS is van mening dat een geleidelijke aanpak als bedoeld in de mededeling zinvol is zolang het engagement om een hoog gegevensbeschermingsniveau op een consistente en doeltreffende manier te garanderen duidelijk en zichtbaar blijft. Meer concreet:

— dient het algemene wetgevingsinstrument inzake gegevensbescherming in een eerste stadium toepasselijk te worden gemaakt op elke verwerkingsactiviteit in het kader van politiële en justitiële samenwerking, met inbegrip van de aanpassingen voor politie en justitie (als bedoeld in 9.2);

— dienen de sectorspecifieke gegevensbeschermingsregelingen in een tweede stadium op dit algemene instrument te worden afgestemd. De Commissie dient zich ertoe te verbinden binnen een vooraf gespecificeerde, korte termijn voorstellen aan te nemen voor dit tweede stadium.

10. **De gegevensbeschermingsautoriteiten en hun onderlinge samenwerking**

10.1. *De rol van de gegevensbeschermingsautoriteiten uitbreiden*

137. De EDPS staat volledig achter de doelstelling van de Commissie om het vraagstuk van het statuut van de gegevensbeschermingsautoriteiten te regelen en meer bepaald om hun onafhankelijkheid, middelen en handhavingsbevoegdheden uit te breiden.

138. De EDPS beklemtoont ook dat het essentiële begrip onafhankelijkheid van de gegevensbeschermingsautoriteiten in het nieuwe wetgevingsinstrument moet worden verduidelijkt. Het Europees Hof van Justitie heeft dienaangaande recent een arrest uitgesproken in zaak C-518/07 ([54]), waarin het benadrukte dat onafhankelijkheid betekent dat er geen enkele externe beïnvloeding is. Een gegevensbeschermingsautoriteit mag niemand om instructies vragen noch van iemand instructies aanvaarden. De EDPS stelt voor deze elementen betreffende onafhankelijkheid uitdrukkelijk in de wetgeving vast te leggen.

139. Teneinde hun taken te kunnen uitvoeren, moeten gegevensbeschermingsautoriteiten over voldoende personele en financiële middelen beschikken. De EDPS stelt voor dit vereiste in de wetgeving vast te leggen ([55]). Tot slot beklemtoont hij dat ervoor moet worden gezorgd dat de autoriteiten over volledig geharmoniseerde bevoegdheden beschikken om onderzoeken in te stellen en voldoende afschrikkende correctieve maatregelen en sancties op te leggen. Dit zou de rechtszekerheid voor de betrokkenen en de voor verwerking verantwoordelijken vergroten.

140. De versterking van de onafhankelijkheid van de gegevensbeschermingsautoriteiten en de uitbreiding van hun middelen en bevoegdheden dienen gepaard te gaan met een intensievere multilaterale samenwerking, met name met het oog op het toenemende aantal problemen inzake gegevensbescherming op Europees niveau. De Groep gegevensbescherming artikel 29 dient uiteraard de belangrijkste structuur van deze samenwerking te zijn.

10.2. *De rol van de Groep gegevensbescherming artikel 29 uitbreiden*

141. Bij een terugblik zien we dat de werking van de Groep gegevensbescherming artikel 29 (de „Groep artikel 29") sinds de oprichting ervan in 1997 is geëvolueerd. Hij is onafhankelijker geworden en kan in de praktijk mogelijk niet meer als een gewone raadgevende werkgroep van de Commissie worden gezien. De EDPS stelt verdere verbeteringen voor de werking van de Groep artikel 29 voor, ook wat de infrastructuur en de onafhankelijkheid ervan betreft.

142. De EDPS is van mening dat de kracht van de Groep artikel 29 schuilt in de onafhankelijkheid en de bevoegdheden van de leden. De onafhankelijkheid van de Groep dient te worden gegarandeerd in het nieuwe rechtskader, overeenkomstig de criteria voor volkomen onafhankelijkheid van de gegevensbeschermingsautoriteiten die door het Hof van Justitie werden vastgesteld in het kader van zaak C-518/07. De EDPS vindt dat de Groep ter ondersteuning van zijn werkzaamheden tevens over voldoende personele en financiële middelen alsook over een uitgebreider secretariaat moet kunnen beschikken.

143. De EDPS waardeert dat het secretariaat van de Groep artikel 29 deel uitmaakt van de administratieve eenheid Gegevensbescherming van DG Justitie, met het voordeel dat de Groep zelf kan beschikken over efficiënte en flexibele contacten en actuele informatie over de ontwikkelingen op het gebied van gegevensbescherming. Anderzijds stelt hij zich vragen bij het feit dat de Commissie (en meer bepaald de administratieve eenheid) tegelijkertijd lid, secretariaat en begunstigde van de adviezen van de Groep is. Dit rechtvaardigt een grotere onafhankelijkheid van het secretariaat. De EDPS moedigt de Commissie aan om, in nauw overleg met de belanghebbenden, na te gaan hoe de onafhankelijkheid kan worden gewaarborgd.

([54]) Zaak C-518/07, *Commissie/Duitsland*, nog niet in de jurisprudentie bekendgemaakt.

([55]) Zie bijvoorbeeld artikel 43, lid 2, van Verordening (EG) nr. 45/2001, waarin een dergelijk vereiste is vastgesteld voor de EDPS.

144. Ruimere bevoegdheden voor de gegevensbeschermingsautoriteiten vereisen tot slot ook ruimere bevoegdheden voor de Groep artikel 29, met een transparantere structuur die ook betere regels en beschermingsmaatregelen omvat, zowel voor de raadgevende als voor de handhavingsfunctie van de groep.

10.3. *De raadgevende functie van de Groep gegevensbescherming artikel 29 uitbreiden*

145. De adviezen die de Groep artikel 29 in zijn hoedanigheid van raadgever aan de Commissie uitbrengt, moeten effectief worden toegepast, met name wat de uitlegging en de toepassing van de beginselen van de richtlijn en andere gegevensbeschermingsinstrumenten betreft. Het gezag van de adviezen van de Groep moet met andere woorden worden gewaarborgd. De gegevensbeschermingsautoriteiten moeten onderling verder overleg plegen om uit te maken hoe dit in het wetgevingsinstrument kan worden vastgesteld.

146. De EDPS beveelt oplossingen aan die de adviezen van de Groep artikel 29 meer gezag geven zonder dat de werking van de Groep drastisch wijzigt. De EDPS stelt voor de gegevensbeschermingsautoriteiten en de Commissie te verplichten zoveel mogelijk rekening te houden met de adviezen en gemeenschappelijke standpunten van de Groep artikel 29, op basis van het model dat werd goedgekeurd voor de adviezen van het Orgaan van Europese regelgevende instanties voor elektronische communicatie (Berec) ([56]). Bovendien kan het nieuwe rechtsinstrument de Groep artikel 29 uitdrukkelijk opdragen „uitleggingsaanbevelingen" goed te keuren. Deze alternatieve oplossingen zouden de adviezen van de Groep artikel 29 meer gezag geven, ook in de rechtbank.

10.4. *Gecoördineerde handhaving door de Groep artikel 29*

147. Het huidige kader laat de handhaving van de gegevensbeschermingswetgeving in de lidstaten over aan 27 gegevensbeschermingsautoriteiten die voor bepaalde zaken weinig gecoördineerd te werk gaan. In zaken waarbij meerdere lidstaten betrokken zijn of die duidelijk een mondiale dimensie hebben, lopen de kosten voor ondernemingen op, aangezien deze voor dezelfde activiteit met verschillende overheidsinstanties te maken krijgen. Bovendien vergroot het gebrek aan coördinatie het risico van inconsequente toepassing van de regelgeving: in uitzonderlijke gevallen kan een bepaalde verwerkingsactiviteit rechtmatig worden bevonden door de ene gegevensbeschermingsautoriteit, terwijl een andere haar verboden acht.

148. Sommige gevallen zijn strategisch van aard en vereisen een gecentraliseerde aanpak. De Groep artikel 29 vergemakkelijkt de coördinatie en de handhavingsacties van de gegevensbeschermingsautoriteiten ([57]) voor belangrijke vraagstukken inzake gegevensbescherming met een dergelijke internationale dimensie. Dit is het geval voor sociale netwerken en zoekmachines ([58]), alsook voor de gecoördineerde controles die in verschillende lidstaten worden uitgevoerd met betrekking tot problemen inzake telecommunicatie en ziektekostenverzekeringen.

149. De handhavingsacties die de Groep artikel 29 kan uitvoeren zijn ingevolge het huidige kader evenwel beperkt. De Groep kan gemeenschappelijke standpunten aannemen, maar er is geen instrument dat ervoor zorgt dat deze standpunten ook daadwerkelijk worden toegepast.

150. De EDPS stelt voor aanvullende bepalingen in het wetgevingsinstrument op te nemen die tot een betere gecoördineerde handhaving bijdragen, met name:

— een dwingende bepaling die ervoor zorgt dat de gegevensbeschermingsautoriteiten en de Commissie *zoveel mogelijk rekening te houden met de adviezen en gemeenschappelijke standpunten* van de Groep artikel 29 ([59]);

— een verplichting voor de gegevensbeschermingsautoriteiten om loyaal met elkaar en met de Commissie en de Groep artikel 29 samen te werken ([60]). Als praktisch voorbeeld van een loyale samenwerking kan een procedure worden vastgesteld volgens welke de gegevensbeschermingsautoriteiten nationale handhavingsmaatregelen met een grensoverschrijdend karakter aan de Commissie of de Groep artikel 29 melden, net zoals de procedure die in het huidige kader is voorzien voor nationale besluiten inzake adequaatheid;

— een nadere omschrijving van de stemvoorschriften om de gegevensbeschermingsautoriteiten te verplichten de besluiten van de Groep artikel 29 ten uitvoer te leggen. Er zou kunnen worden bepaald dat de Groep handhavingsbesluiten bij consensus neemt en wanneer een consensus niet mogelijk is, bij gekwalificeerde

([56]) Verordening (EG) nr. 1211/2009 van het Europees Parlement en de Raad van 25 november 2009 tot oprichting van het Orgaan van Europese regelgevende instanties voor elektronische communicatie (BEREC) en het Bureau, (PB L 337 van 18.12.2009, blz. 1).

([57]) Naast de Groep gegevensverwerking artikel 29 heeft de Europese Conferentie van commissarissen voor gegevensbescherming een tiental jaar geleden een permanente werkgroep opgericht die grensoverschrijdende klachten op een gecoördineerde wijze behandelt. Hoewel deze werkgroep ontegenzeglijk nuttig is door de contacten tussen het personeel van de gegevensbeschermingsautoriteiten en een betrouwbaar netwerk van contactpunten biedt, kan hij niet worden beschouwd als een coördinatiemechanisme voor de besluitvorming.

([58]) Zie de brieven van de Groep artikel 29 van 12 mei 2010 en 26 mei 2010, die zijn gepubliceerd op diens website (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Zoals hierboven reeds werd vermeld, is een soortgelijke verplichting vastgesteld in Verordening (EG) nr. 1211/2009, waarin de rol van het Orgaan van Europese regelgevende instanties voor elektronische communicatie (BEREC) wordt gespecificeerd.

([60]) Zie dienaangaande het hierboven genoemde artikel 3 van Verordening (EG) nr. 1211/2009.

meerderheid. Aanvullend zou in een overweging kunnen worden opgenomen dat de gegevensbeschermingsautoriteiten die voor een document hebben gestemd, verplicht zijn of de politieke wil moeten hebben om het desbetreffende document op nationaal niveau ten uitvoer te leggen.

151. De EDPS maakt een voorbehoud bij de invoering van strengere maatregelen, zoals het bindend maken van de adviezen van de Groep artikel 29. Een dergelijke maatregel zou de onafhankelijkheid van de afzonderlijke gegevensbeschermingsautoriteiten die de lidstaten in hun nationaal recht moeten garanderen, in gevaar brengen. Indien de besluiten van de Groep directe gevolgen hebben voor derde partijen zoals de voor verwerking verantwoordelijken, dienen nieuwe procedures te worden voorzien, met onder meer beschermingsmaatregelen als transparantie en schadeloosstelling, met inbegrip van de mogelijkheid om beroep aan te tekenen bij het Europees Hof van Justitie.

10.5. *Samenwerking tussen de EDPS en de Groep artikel 29*

152. De samenwerking tussen de EDPS en de Groep artikel 29 is eveneens voor verbetering vatbaar. De EDPS is lid van de Groep en draagt bij tot diens adviezen over de belangrijkste strategische ontwikkelingen in de EU, waarbij hij tegelijkertijd toeziet op de samenhang met zijn eigen adviezen. De EDPS stelt zowel in de openbare als in de particuliere sector een stijging vast van het aantal privacyproblemen die in vele lidstaten gevolgen hebben op nationaal niveau en met betrekking waartoe de Groep artikel 29 een eigen taak te vervullen heeft.

153. De EDPS heeft de aanvullende taak om adviezen te geven over de ontwikkelingen in de EU, wat zo moet blijven. Hij oefent deze raadgevende bevoegdheid ten aanzien van de EU-instellingen uit als een orgaan van de EU net zoals de nationale gegevensbeschermingsautoriteiten dat doen voor hun regeringen.

154. De EDPS en de Groep artikel 29 geven advies vanuit een verschillend, maar complementair perspectief. Om die reden dient de coördinatie tussen de Groep artikel 29 en de EDPS behouden te blijven en misschien zelfs verbeterd, teneinde ervoor te zorgen dat zij samen naar oplossingen zoeken voor de belangrijkste problemen op het gebied van gegevensbescherming, bijvoorbeeld door hun agenda geregeld op elkaar af te stemmen ([61]) en door te zorgen voor transparantie in vraagstukken met een meer nationale of een specifieke EU-dimensie.

155. Coördinatie wordt in de huidige richtlijn niet vermeld om de eenvoudige reden dat de EDPS nog niet bestond toen de richtlijn werd goedgekeurd, maar in de zes jaar na de instelling van de EDPS is de complementariteit van de EDPS en de Groep artikel 29 duidelijk geworden en zou deze formeel kunnen worden erkend. De EDPS herinnert eraan dat hij ingevolge Verordening 45/2001 verplicht is samen te werken met de nationale gegevensbeschermingsautoriteiten en deel te nemen aan de werkzaamheden van de Groep artikel 29. De EDPS beveelt aan samenwerking uitdrukkelijk in het nieuwe wetgevingsinstrument op te nemen en deze indien nodig te structureren, bijvoorbeeld door de vaststelling van een samenwerkingsprocedure.

10.6. *Gezamenlijk toezicht op EU-regelingen door de EDPS en de gegevensbeschermingsautoriteiten*

156. Deze overwegingen gelden ook voor gebieden waarop het toezicht op Europees en op nationaal niveau moet worden gecoördineerd. Dat is het geval voor EU-organen die aanzienlijke hoeveelheden door nationale instanties verstrekte gegevens verwerken en voor grote informatiesystemen met een Europese en een nationale component.

157. De huidige regeling voor bepaalde EU-organen en grote informatiesystemen — Europol, Eurojust en het Schengeninformatiesysteem (SIS) van de eerste generatie hebben bijvoorbeeld gemeenschappelijke controleorganen met vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten — is een overblijfsel van de intergouvernementele samenwerking van vóór het Verdrag van Lissabon en is niet in overeenstemming met de institutionele structuur van de EU, waarvan Europol en Eurojust een integrerend deel zijn geworden en waarin ook het „Schengenacquis" is opgenomen ([62]).

158. De Commissie kondigt in de mededeling aan dat zij in 2011 de belanghebbenden zal raadplegen over de herziening van deze toezichtsregelingen. De EDPS vraagt de Commissie met klem om in de discussie over toezicht zo snel mogelijk (binnen een vooraf gespecificeerde, korte termijn, zie hierboven) een standpunt in te nemen. Hij neemt in deze discussie het onderstaande standpunt in.

159. In de eerste plaats dient te worden gewaarborgd dat alle toezichthoudende instanties voldoen aan de essentiële criteria van onafhankelijkheid, voldoende middelen en handhavingsbevoegdheden. Bovendien dient ervoor te worden gezorgd dat rekening wordt gehouden met de gezichtspunten en de expertise op EU-niveau. Dat betekent dat de nationale autoriteiten niet alleen onderling moeten samenwerken, maar ook met de Europese gegevensbeschermingsautoriteiten (momenteel de EDPS). De EDPS acht een model dat aan deze vereisten voldoet noodzakelijk ([63]).

160. In de afgelopen jaren werd het model van „gecoördineerd toezicht" ontwikkeld. Dit toezichtsmodel, dat nu operationeel is in Eurodac en in delen van het Douane-informatiesysteem, zal binnenkort ook worden gebruikt voor het visuminformatiesysteem (VIS) en het Schengeninformatiesysteem van de tweede generatie (SIS II). Het model omvat

([61]) Bijv. op basis van het overzicht van de wetgevende activiteiten dat jaarlijks wordt gepubliceerd, geregeld wordt geactualiseerd en op de website van de EDPS kan worden geraadpleegd.

([62]) Ingevolge Verordening (EG) nr. 45/2001 is de EDPS verplicht met deze organen samen te werken.

([63]) Voor Eurojust dient een model er ook voor te zorgen dat de onafhankelijkheid van de rechterlijke macht niet in het gedrang komt door het toezicht op de gegevensbescherming, voor zover Eurojust gegevens verwerkt in het kader van strafrechtelijke procedures.

drie niveaus: 1. op nationaal niveau staan de gegevensbeschermingsautoriteiten in voor het toezicht; 2. op Europees niveau staat de EDPS in voor het toezicht; 3. ter coördinatie worden geregeld bijeenkomsten bijeengeroepen door de EDPS, die het secretariaat van dit coördinatiemechanisme verzorgt. Het model is succesvol en doeltreffend gebleken en gebruik ervan zou ook voor andere informatiesystemen moeten worden overwogen.

C. **HOE DE TOEPASSING VAN HET HUIDIGE KADER TE BEVORDEREN**

11. **Korte termijn**

161. Tijdens het herzieningsproces dienen inspanningen te worden geleverd om ervoor te zorgen dat de huidige voorschriften volledig en effectief worden toegepast. Deze voorschriften blijven van toepassing tot het nieuwe kader wordt goedgekeurd en door de lidstaten in nationaal recht wordt omgezet. In die zin zijn meerdere maatregelen mogelijk.

162. Ten eerste moet de Commissie de naleving van Richtlijn 95/46/EG door de lidstaten blijven monitoren en, in voorkomend geval, haar bevoegdheden overeenkomstig artikel 258 VWEU gebruiken. Recent werden inbreukprocedures ingesteld wegens het niet correct omzetten van artikel 28 van de richtlijn wat de onafhankelijkheidseis voor gegevensbeschermingsautoriteiten betreft ([64]). Ook op andere gebieden moet de naleving van alle regelgeving worden gemonitord en gehandhaafd ([65]). De EDPS is dan ook verheugd over en staat volledig achter het engagement waarvan de Commissie in de mededeling heeft blijkgegeven om een actief inbreukbeleid te voeren. De Commissie dient ook de structurele dialoog met de lidstaten over de omzetting in nationaal recht van de regelgeving voort te zetten ([66]).

163. Ten tweede moet handhaving op nationaal niveau worden aangemoedigd om de praktische toepassing van de gegevensbeschermingsvoorschriften te garanderen, ook op nieuwe technologische fenomenen en mondiale actoren. De gegevensbeschermingsautoriteiten moeten hun bevoegdheden om onderzoeken in te stellen en sancties op te leggen ten volle gebruiken. Het is ook van belang dat de bestaande rechten van betrokkenen, met name het recht op toegang, in de praktijk volledig worden toegepast.

164. Ten derde lijkt op korte termijn een grotere coördinatie op het gebied van handhaving noodzakelijk. De rol van de Groep artikel 29 en diens uitleggingsdocumenten zijn daarbij essentieel, maar ook de gegevensbeschermingsautoriteiten moeten hun uiterste best doen om deze ten uitvoer te leggen. Voorkomen moet worden dat in Europese of mondiale zaken verschillende uitkomsten worden bereikt en binnen de Groep artikel 29 kunnen en moeten gemeenschappelijke benaderingen worden overeengekomen. Ook Europese gecoördineerde onderzoeken onder leiding van de Groep artikel 29 kunnen een aanzienlijke meerwaarde bieden.

165. Ten vierde dienen de gegevensbeschermingsbeginselen proactief te worden „ingebouwd" in nieuwe regelgeving die direct of indirect gevolgen heeft voor gegevensbescherming. Op Europees niveau levert de EDPS aanzienlijke inspanningen om bij te dragen tot een verbetering van de Europese wetgeving, wat navolging moet krijgen op nationaal niveau. De gegevensbeschermingsautoriteiten dienen dan ook hun raadgevende bevoegdheden ten volle te benutten om een proactieve aanpak te garanderen. De gegevensbeschermingsautoriteiten, met inbegrip van de EDPS, kunnen ook een proactieve rol spelen bij de monitoring van de technologische ontwikkelingen. Monitoring is belangrijk om opkomende tendensen in een vroeg stadium te kunnen herkennen, eventuele gevolgen voor gegevensbescherming onder de aandacht te brengen, oplossingen die de gegevensbescherming bevorderen te ondersteunen en bewustwording onder de belanghebbenden te stimuleren.

166. Tot slot moet actief worden gewerkt aan een betere samenwerking tussen de verschillende actoren op internationaal niveau. Het is dan ook van belang de internationale samenwerkingsinstrumenten te versterken. Initiatieven zoals de normen van Madrid en de lopende werkzaamheden van de Raad van Europa en de OESO verdienen dan ook alle steun. In deze context is het bijzonder positief dat ook de Amerikaanse Federal Trade Commission is toegetreden tot de Internationale Conferentie van commissarissen voor privacy en gegevensbescherming.

D. **CONCLUSIES**

ALGEMENE OPMERKINGEN

167. De EDPS is over het geheel genomen ingenomen met de mededeling. Hij is er namelijk van overtuigd dat een evaluatie van het huidige rechtskader voor gegevensbescherming in de EU noodzakelijk is om effectieve bescherming in een zich almaar verder ontwikkelende en geglobaliseerde informatiemaatschappij te garanderen.

168. In de mededeling worden de voornaamste problemen en uitdagingen op een rijtje gezet. De EDPS is het met de Commissie eens dat er ook in de toekomst behoefte zal zijn aan een solide gegevensbeschermingssysteem, ervan uitgaande dat de bestaande algemene beginselen van gegevensbescherming nog steeds gelden in een maatschappij die fundamentele veranderingen ondergaat. De EDPS is het eens met de verklaring in de mededeling dat de uitdagingen enorm zijn en beklemtoont dat de voorgestelde oplossingen dan ook even ambitieus moeten zijn en tot de doeltreffendheid van de bescherming moeten bijdragen. Daarom vraagt hij om een meer ambitieuze aanpak op een aantal punten.

169. De EDPS staat volledig achter de integrale aanpak van gegevensbescherming. Hij betreurt evenwel dat de mededeling een aantal domeinen, zoals gegevensverwerking door de instellingen en organen van de EU, van het algemene instrument lijkt uit te sluiten. Indien de Commissie

([64]) Zie de bovengenoemde zaak C-518/07 en persbericht IP/10/1430 van de Commissie van 28 oktober 2010.

([65]) De Commissie heeft een inbreukprocedure ingesteld tegen het VK voor een vermeende inbreuk op verschillende bepalingen inzake gegevensbescherming, met inbegrip van de vertrouwelijkheidseis voor elektronische communicatie met betrekking tot behavioural advertising. Zie persbericht IP/09/570 van de Commissie van 9 april 2009.

([66]) Zie het eerste verslag van de Commissie over de toepassing van de richtlijn gegevensbescherming, zoals eerder genoemd, blz. 22 e.v.

besluit deze gebieden weg te laten, verzoekt de EDPS de Commissie met klem zo snel mogelijk en bij voorkeur voor eind 2011 een voorstel voor het EU-niveau in te dienen.

BELANGRIJKSTE PERSPECTIEVEN

170. Voor de EDPS zijn de uitgangspunten van het herzieningsproces de volgende:

— gegevensbeschermingsregelingen moeten andere legitieme belangen zoveel mogelijk actief ondersteunen in plaats van deze te hinderen (zoals de Europese economie, de veiligheid van personen en de verantwoordingsplicht van regeringen);

— de algemene beginselen van gegevensbescherming mogen en kunnen niet worden gewijzigd;

— verdere harmonisering moet een van de hoofddoelstellingen van de herziening zijn;

— de grondrechten moeten een centrale plaats in het herzieningsproces innemen. Een grondrecht heeft tot doel burgers in alle omstandigheden te beschermen;

— het nieuwe wetgevingsinstrument moet ook betrekking hebben op politie en justitie;

— het nieuwe wetgevingsinstrument moet zoveel mogelijk op een technologisch neutrale wijze worden geformuleerd en moet rechtszekerheid bieden op lange termijn.

ELEMENTEN VAN EEN NIEUW KADER

Harmonisatie en vereenvoudiging

171. De EDPS is verheugd dat de Commissie zich ertoe heeft verbonden na te gaan hoe de regelgeving inzake gegevensbescherming op EU-niveau verder kan worden geharmoniseerd. De EDPS stelt gebieden vast waarop meer en betere harmonisatie dringend is: definities, gronden voor gegevensverwerking, rechten van de betrokkenen, internationale doorgifte van gegevens en gegevensbeschermingsautoriteiten.

172. De EDPS stelt voor de volgende alternatieven in overweging te nemen om het toepassingsgebied van de aanmeldingsvoorschriften te vereenvoudigen en/of te beperken:

— beperking van de aanmeldingsplicht tot bepaalde soorten verwerkingshandelingen die specifieke risico's inhouden;

— een eenvoudige registratieplicht voor de voor verwerking verantwoordelijken (in tegenstelling tot een uitgebreide registratie van iedere verwerking van gegevens);

— invoering van een pan-Europees standaardformulier voor de aanmelding van verwerkingshandelingen.

173. Volgens de EDPS is een verordening, één enkel instrument dat direct van toepassing is in alle lidstaten, het meest doeltreffende middel om het grondrecht op gegevensbescherming te beschermen en de interne markt verder te doen convergeren.

De rechten van personen beter beschermen

174. De EDPS staat achter het in de mededeling opgenomen voorstel om de rechten van personen beter te beschermen. Hij stelt het volgende voor:

— opname van een transparantiebeginsel in de wetgeving. Het is echter belangrijker de bestaande bepalingen inzake transparantie verder uit te werken (zoals de bestaande artikelen 10 en 11 van Richtlijn 95/46/EG);

— opname in het algemene instrument van een bepaling over verplichte kennisgeving bij een inbreuk in verband met persoonsgegevens, die de in de herziene e-privacyrichtlijn vastgestelde verplichting voor bepaalde aanbieders naar alle voor verwerking verantwoordelijken uitbreidt;

— duidelijke afbakening van het begrip toestemming. Er dient te worden nagedacht over een uitbreiding van de gevallen waarin uitdrukkelijke toestemming vereist is alsook over aanvullende regels voor het internet;

— vaststelling van aanvullende rechten, zoals gegevensportabiliteit en het recht om te worden vergeten, met name voor onlinediensten van de informatiemaatschappij;

— betere bescherming van de belangen van kinderen met een aantal aanvullende bepalingen, met name betreffende het verzamelen en de verdere verwerking van gegevens van kinderen;

— opname in de EU-wetgeving van regelingen voor collectieve schadeacties wegens inbreuken op de gegevensbeschermingsvoorschriften, zodat gekwalificeerde entiteiten procedures kunnen starten in naam van groepen personen.

De verplichtingen van organisaties en de voor verwerking verantwoordelijken uitbreiden

175. Het nieuwe kader moet de voor verwerking verantwoordelijken aanzetten om proactief gegevensbeschermingsmaatregelen in hun bedrijfsprocessen op te nemen. De EDPS stelt voor algemene bepalingen inzake verantwoording en 'privacy by design' vast te stellen. Er dient ook een bepaling betreffende certificeringsregelingen op het gebied van privacy te worden voorzien.

Globalisering en toepasselijk recht

176. De EDPS staat achter de ambitieuze inspanningen van de Internationale Conferentie van commissarissen voor gegevensbescherming om de zogeheten „normen van Madrid" op te stellen, met de bedoeling deze in een bindend instrument te gieten en mogelijk een intergouvernementele conferentie te openen. De EDPS roept de Commissie op om in die zin concrete stappen te ondernemen in nauwe samenwerking met de OESO en de Raad van Europa.

177. Een nieuw wetgevingsinstrument moet de criteria voor het bepalen van het toepasselijke recht verduidelijken. Er dient voor te worden gezorgd dat gegevens die buiten de grenzen van de EU worden verwerkt, niet buiten het rechtsgebied van de EU vallen wanneer er een gegronde reden is om het EU-recht toe te passen. Indien het rechtskader in de vorm van een verordening wordt vastgesteld, gelden in alle lidstaten dezelfde voorschriften en wordt het bepalen van het toepasselijke recht minder belangrijk (binnen de EU).

178. De EDPS staat volledig achter de doelstelling om tot een meer eenvormige en samenhangende aanpak ten aanzien van derde landen en internationale organisaties te komen. Bindende bedrijfsvoorschriften dienen in het wetgevingsinstrument te worden opgenomen.

Politie en justitie

179. Een omvattend instrument dat ook betrekking heeft op politie en justitie kan ruimte laten voor bijzondere voorschriften die afdoende rekening houden met de specifieke behoeften van deze sector, overeenkomstig de aan het Verdrag van Lissabon gehechte Verklaring nr. 21. Ter compensatie van de betrokkenen dienen specifieke beschermingsmaatregelen te worden ingebouwd, teneinde hen extra bescherming te bieden op een gebied waarop de verwerking van hun persoonsgegevens ingrijpender van aard is.

180. Het nieuwe rechtskader moet zo duidelijk, eenvoudig en consistent mogelijk zijn. Voorkomen moet worden dat verschillende regelingen van toepassing zijn op bijvoorbeeld Europol, Eurojust, het SIS en Prüm. De EDPS begrijpt dat de voorschriften van de verschillende regelingen met zorg en geleidelijk op elkaar zullen moeten worden afgestemd.

De gegevensbeschermingsautoriteiten en hun onderlinge samenwerking

181. De EDPS staat volledig achter de doelstelling van de Commissie om het statuut van de gegevensbeschermingsautoriteiten te regelen en hun onafhankelijkheid, middelen en handhavingsbevoegdheden uit te breiden. Hij beveelt aan:

— het essentiële begrip onafhankelijkheid van de gegevensbeschermingsautoriteiten in het nieuwe wetgevingsinstrument vast te leggen, zoals gespecificeerd door het Europese Hof van Justitie;

— in de wetgeving te bepalen dat gegevensbeschermingsautoriteiten voldoende middelen ter beschikking moeten hebben;

— autoriteiten geharmoniseerde bevoegdheden te verlenen om onderzoeken in te stellen en sancties op te leggen.

182. De EDPS stelt verdere verbeteringen in de werking van de Groep artikel 29 voor, ook wat de infrastructuur en de onafhankelijkheid ervan betreft. De Groep zou ook over voldoende middelen en een uitgebreider secretariaat moeten kunnen beschikken.

183. De EDPS stelt voor de raadgevende taak van de Groep artikel 29 uit te breiden door de gegevensbeschermingsautoriteiten en de Commissie te verplichten *zoveel mogelijk rekening te houden met de adviezen en gemeenschappelijke standpunten* van de Groep. De EDPS is er geen voorstander van om de standpunten van de Groep bindend te maken, met name wegens de onafhankelijkheid van de individuele gegevensbeschermingsautoriteiten. De EDPS beveelt de Commissie aan specifieke bepalingen vast te stellen om de samenwerking met de EDPS in het nieuwe wetgevingsinstrument te verbeteren.

184. De EDPS vraagt de Commissie met klem zo snel mogelijk een standpunt in te nemen over het toezicht op EU-organen en grote informatiesystemen, er rekening mee houdend dat alle toezichthoudende instanties aan de essentiële criteria moeten voldoen, namelijk onafhankelijkheid, voldoende middelen en handhavingsbevoegdheden, en dat ervoor moet worden gezorgd dat het EU-standpunt goed wordt vertegenwoordigd. De EDPS staat achter het model van „gecoördineerd toezicht".

Verbeteringen in het kader van de huidige regeling

185. De EDPS moedigt de Commissie aan om:

— de naleving van Richtlijn 95/46/EG door de lidstaten te blijven monitoren en, in voorkomend geval, haar bevoegdheden overeenkomstig artikel 258 VWEU te gebruiken;

— handhaving op nationaal niveau en coördinatie van de handhavingsactiviteiten aan te moedigen;

— gegevensbeschermingsbeginselen proactief in te bouwen in nieuwe regelgeving die direct of indirect gevolgen heeft voor gegevensbescherming;

— actief te werken aan een betere samenwerking tussen de verschillende actoren op internationaal niveau.

Gedaan te Brussel, 14 januari 2011.

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming