EUROPESE COMMISSIE

Brussel, 4.11.2010
COM(2010) 609 definitief

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

"Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie"

1. NIEUWE UITDAGINGEN OP HET GEBIED VAN DE BESCHERMING VAN PERSOONSGEGEVENS

De gegevensbeschermingsrichtlijn van 1995[1] vormde een mijlpaal in de geschiedenis van de bescherming van persoonsgegevens in de Europese Unie. De richtlijn stoelt op twee van de oudste en tevens belangrijkste ambities van het Europese integratieproces: de bescherming van de fundamentele rechten en vrijheden van personen en in het bijzonder het fundamentele recht op gegevensbescherming aan de ene kant, en de verwezenlijking van de interne markt – het vrije verkeer van persoonsgegevens in dit geval – aan de andere kant.

Vijftien jaar later is deze tweeledige doelstelling nog steeds actueel en blijven de in de richtlijn neergelegde beginselen een gezond uitgangspunt. **De snelle technologische ontwikkelingen en de globalisering hebben de wereld om ons heen echter grondig veranderd en nieuwe uitdagingen in het leven geroepen met betrekking tot de bescherming van persoonsgegevens.**

Met de technologie van vandaag kunnen personen gemakkelijk informatie uitwisselen over hun gedragingen en voorkeuren en die informatie op een nooit geziene schaal publiek en wereldwijd toegankelijk maken. Sociale netwerksites met honderden miljoenen leden over de hele wereld zijn wellicht het meest in het oog springende, maar niet het enige voorbeeld hiervan. "Cloud computing" – computeren met internet, waarbij de software, gedeelde bronnen en informatie zich op verre servers ("in the cloud") bevinden – kan eveneens afbreuk doen aan de gegevensbescherming, aangezien personen geen controle meer hebben over hun potentieel gevoelige informatie wanneer zij gegevens opslaan met behulp van programma's die gehost worden op hardware van iemand anders. Een recente studie heeft bevestigd dat – onder gegevensbeschermingsautoriteiten, bedrijfsorganisaties en consumentenorganisaties – vrijwel algemeen wordt aangenomen dat er sprake is van een toename van de risico's voor de privacy en de bescherming van persoonsgegevens die aan onlineactiviteiten verbonden zijn[2].

Terzelfder tijd **zijn de manieren om persoonsgegevens te verzamelen steeds geavanceerder en moeilijker opspoorbaar geworden.** Zo kunnen ondernemingen met behulp van geavanceerde instrumenten potentiële klanten gerichter aanspreken omdat zij hun gedrag kunnen nagaan. Het toenemende gebruik van procedures die automatische gegevensverzameling mogelijk maken, zoals de verkoop van elektronische vervoerbewijzen, de inning van tolgelden op autowegen of het gebruik van geolocatie-apparatuur, maakt het gemakkelijker vast te stellen waar een persoon zich bevindt, gewoon omdat hij een mobieltje

---

[1] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24.10.1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

[2] Zie de *Study on the economic benefits of privacy enhancing technologies*, London Economics, juli 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), blz. 14.

gebruikt. Ook overheidsinstanties gebruiken meer en meer persoonsgegevens voor uiteenlopende doeleinden, bv. voor het opsporen van personen bij de uitbraak van een besmettelijke ziekte, om terrorisme en criminaliteit doeltreffender te voorkomen en te bestrijden, om socialezekerheidssstelsels te beheren, voor belastingdoeleinden, in het kader van hun e-overheidstoepassingen enz.

Dit alles doet de vraag rijzen of de bestaande EU-wetgeving inzake gegevensbescherming deze uitdagingen nog ten volle en doeltreffend aankan.

Om die vraag te beantwoorden heeft de Commissie een evaluatie van het bestaande wettelijke kader op touw gezet, met eerst een conferentie op hoog niveau in mei 2009, gevolgd door een openbare raadpleging tot eind 2009[3]. Er werd ook opdracht gegeven voor een aantal studies [4].

De conclusie was dat de kernbeginselen van de richtlijn overeind blijven en dat het technologieneutrale karakter ervan moet worden gehandhaafd. Er wordt echter gewezen op verscheidene knelpunten, die specifieke problemen meebrengen, zoals:

- *Omgaan met de gevolgen van nieuwe technologieën*

In het kader van de raadpleging hebben zowel individuele personen als organisaties bevestigd dat moet worden verduidelijkt en gespecificeerd hoe de beginselen inzake gegevensbescherming moeten worden toegepast op nieuwe technologieën. Een en ander moet garanderen dat eenieders persoonsgegevens werkelijk doeltreffend worden beschermd, wat ook de voor de verwerking van die gegevens gebruikte technologie is, en dat de voor gegevensverwerking verantwoordelijken zich ten volle bewust zijn van de effecten van nieuwe technologieën op de gegevensbescherming. Dit aspect is gedeeltelijk geregeld door Richtlijn 2002/58/EG (de zogeheten "e-privacy"-richtlijn)[5], die een nadere uitwerking van en aanvulling op de algemene richtlijn gegevensbescherming vormt voor de sector van de elektronische communicatie[6].

---

3 Voor de antwoorden op de openbare raadpleging van de Commissie, zie: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Een meer gerichte bevraging van belanghebbenden vond plaats in de loop van 2010. Onder voorzitterschap van vicevoorzitter Viviane Reding vond op 5 oktober 2010 in Brussel ook een bijeenkomst op hoog niveau met belanghebbenden plaats. De Commissie raadpleegde voorts de Groep artikel 29, die een omvangrijke bijdrage leverde aan de raadpleging van 2009 (WP 168) en in juli 2010 een specifiek advies goedkeurde over het begrip verantwoordingsplicht (WP 173).

4 Naast de reeds in voetnoot 2 aangehaalde *Study on the economic benefits of privacy enhancing technologies bijvoorbeeld ook de Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, januari 2010, (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Voorts wordt gewerkt aan een studie ten behoeve van een effectbeoordeling voor de toekomst van het wettelijke kader van de EU inzake bescherming van persoonsgegevens

5 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

6 Richtlijn 95/46/EG inzake gegevensbescherming legt de normen op het gebied van gegevensbescherming vast voor alle wetgevende besluiten van de EU, waaronder de Richtlijn 2002/58/EG inzake e-privacy (gewijzigd bij Richtlijn 2009/136/EG, PB L 337 van 18.12.2009, blz. 11). De e-privacy-richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken. Ze vertaalt de principes van de gegevensbeschermingsrichtlijn in specifieke voorschriften voor de sector

- *Verder uitwerken van de internemarktdimensie van gegevensbescherming*

Een van de belangrijkste punten waarover belanghebbenden, met name multinationale ondernemingen, zich blijvend zorgen maken, is dat de wetgeving van de lidstaten inzake gegevensbescherming, in weerwil van een gemeenschappelijk wettelijk kader op EU-niveau, onvoldoende geharmoniseerd is. Zij wijzen op de noodzaak van een grotere rechtszekerheid, minder administratieve lasten en gelijke mededingingsvoorwaarden voor ondernemingen en andere voor gegevensverwerking verantwoordelijken.

- *Omgaan met de globalisering en verbeteren van internationale gegevensdoorgifte*

Verscheidene belanghebbenden wijzen op het feit dat de verwerking steeds vaker wordt uitbesteed, dikwijls buiten de EU, wat leidt tot diverse problemen in verband met het op de verwerking toepasselijke recht en de toewijzing van de daarmee samenhangende verantwoordelijkheid. Op het gebied van internationale gegevensdoorgiften zijn nogal wat organisaties van mening dat de bestaande regelingen niet geheel bevredigend zijn en moeten worden herzien en geharmoniseerd om dergelijke doorgiften eenvoudiger en minder omslachtig te maken.

- *Een betere institutionele regeling tot stand brengen voor een effectieve handhaving van de voorschriften inzake gegevensbescherming*

De belanghebbenden zijn het erover eens dat de rol van de gegevensbeschermingsautoriteiten met het oog op een betere handhaving van de regels inzake gegevensbescherming moet worden uitgebreid. Sommige organisaties vragen ook om meer transparantie in de werkzaamheden van de Groep artikel 29 (*zie punt 2.5*) en een verduidelijking van de taken en bevoegdheden van die Groep.

- *Verbeteren van de samenhang in het wettelijke kader voor gegevensbescherming*

Alle belanghebbenden hebben in het kader van de openbare raadpleging gewezen op de behoefte aan een overkoepelend instrument dat van toepassing is op gegevensverwerking in alle sectoren en beleidsterreinen van de Unie en dat borg staat voor zowel een geïntegreerde aanpak als een naadloze, coherente en effectieve bescherming[7].

Met het oog op de hierboven beschreven uitdagingen **moet de EU een integrale en coherente aanpak ontwikkelen** die waarborgt dat **het fundamentele recht van individuen op gegevensbescherming binnen de EU en daarbuiten onverkort wordt geëerbiedigd**. Het Verdrag van Lissabon heeft ervoor gezorgd dat de EU over extra middelen beschikt om dat te bereiken: het EU-Handvest van de grondrechten – waarvan artikel 8 een zelfstandig recht op de bescherming van persoonsgegevens erkent – is in rechte bindend geworden en er is een nieuwe rechtsgrondslag[8] ingevoerd voor de vaststelling van integrale en coherente EU-wetgeving betreffende de bescherming van individuen ten aanzien van de verwerking van hun persoonsgegevens en het vrije verkeer van die gegevens. In het bijzonder stelt de nieuwe

---

van de elektronische communicatie. Richtlijn 95/46/EG is onder meer van toepassing op niet-openbare communicatiediensten.

7 In afzonderlijke bijdragen na het einde van de openbare raadpleging hebben Europol en Eurojust ervoor gepleit toch rekening te houden met de bijzondere kenmerken van hun werkzaamheden op het gebied van de coördinatie van de rechtshandhaving en de misdaadpreventie.

8 Zie artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU).

rechtsgrondslag de EU in staat om in één rechtsinstrument de gegevensbescherming te regelen, ook op het gebied van zowel politiële samenwerking als justitiële samenwerking in strafzaken. Het gemeenschappelijke buitenlandse en veiligheidsbeleid valt slechts partieel onder artikel 16 VWEU, aangezien op dit gebied specifieke voorschriften inzake gegevensverwerking door lidstaten moeten worden vastgesteld bij een besluit van de Raad dat een andere rechtsgrondslag heeft[9].

Op grond van deze nieuwe wettelijke mogelijkheden zal de Commissie de hoogste prioriteit geven aan het toezicht op de naleving van het fundamentele recht op gegevensbescherming in de hele Unie en op al haar beleidsterreinen, maar terzelfder tijd zal zij de internemarktdimensie verder uitwerken en het vrije verkeer van persoonsgegevens vergemakkelijken. Bij het waarborgen van het fundamentele recht op bescherming van persoonsgegevens moet ten volle rekening worden gehouden met andere relevante grondrechten die in het handvest zijn neergelegd, en met andere doelstellingen van de Verdragen.

Met deze mededeling wordt beoogd de aanpak uiteen te zetten die de Commissie zal volgen met het oog op de modernisering van de wettelijke regeling van de EU voor de bescherming van persoonsgegevens op alle werkterreinen van de Unie, waarbij met name rekening wordt gehouden met de uitdagingen die voortvloeien uit de globalisering en de nieuwe technologieën, zodat blijvend een hoog niveau van bescherming van individuen ten aanzien van de verwerking van persoonsgegevens op alle werkterreinen van de EU wordt gewaarborgd. Zo zal de EU een toonaangevende rol kunnen blijven spelen om wereldwijd hoge normen inzake gegevensbescherming te promoten.

2. HOOFDDOELSTELLINGEN VAN DE INTEGRALE AANPAK VAN GEGEVENSBESCHERMING

2.1. Versterking van de rechten van individuen

2.1.1. In alle omstandigheden individuen een passende bescherming verzekeren

De in de bestaande EU-instrumenten op het gebied van gegevensbescherming neergelegde regels hebben tot doel **de grondrechten van natuurlijke personen, in het bijzonder van hun recht op bescherming van persoonsgegevens te beschermen**, conform het EU-Handvest van de grondrechten[10].

Het begrip "persoonsgegevens" is een van de centrale begrippen in het kader van de bescherming die individuen ontlenen aan de bestaande EU-instrumenten op het gebied van gegevensbescherming, en bepaalt of de verwerkers van gegevens en voor de verwerking verantwoordelijken bepaalde verplichtingen moeten nakomen[11]. Daarbij worden

---

9 Zie artikel 16, lid 2, laatste alinea, VWEU en artikel 39 van het Verdrag betreffende de Europese Unie (VEU).

10 Zie arresten van het Europees Hof van Justitie in zaak C-101/01, Bodil Linqvist, Jurispr. 2003, blz. I-1297, punten 96-97, en zaak C-275/06, Productores de Música de España (Promusicae) tegen Telefónica de España SAU, Jurispr. 2008, blz. I-271. Zie ook de rechtspraak van het Europees Hof voor de rechten van de mens, bv. de zaken: S. en Marper/Verenigd Koninkrijk, 4.12.2008 (verzoekschriften nrs. 30562/04 en 30566/04) en Rotaru/Roemenië, 4.5.2000 (nr. 28341/95, § 55, ECHR 2000-V).

11 Zie de definities van "voor de verwerking verantwoordelijke" en "verwerker" in artikel 2, onder d) en e), van Richtlijn 95/46/EG.

"persoonsgegevens" zo gedefinieerd dat iedere (directe of indirecte) informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon eronder valt. Om te bepalen of een persoon identificeerbaar is, dienen alle middelen in aanmerking te worden genomen waarvan redelijkerwijs te verwachten valt dat zij door degene die voor de verwerking verantwoordelijk is, of door ieder ander worden gebruikt om de eerstgenoemde persoon te identificeren[12]. Deze door de wetgever gekozen, doordachte definitie heeft het voordeel van soepelheid, want zij kan worden toegepast op uiteenlopende situaties en ontwikkelingen die van invloed zijn op de grondrechten, ook die welke niet voorzienbaar waren toen de richtlijn werd vastgesteld. Een gevolg van die ruime en soepele benadering is evenwel dat het bij de toepassing van de richtlijn in vele gevallen niet erg duidelijk is hoe de zaak moet worden beoordeeld, of de betrokkenen aanspraak kunnen maken op gegevensbescherming en of de voor de verwerking verantwoordelijken moeten voldoen aan de door de richtlijn opgelegde verplichtingen[13].

Er zijn situaties waarin specifieke informatie wordt verwerkt, waarvoor op grond van het EU-recht extra beschermende maatregelen vereist zijn. Dergelijke maatregelen bestaan reeds in bepaalde gevallen. Zo is bijvoorbeeld het opslaan van gegevens in eindapparatuur (bv. mobiele telefoons) alleen toegestaan als de betrokkene zijn toestemming daarvoor heeft gegeven. Dit punt moet wellicht ook op EU-niveau worden geregeld met betrekking tot bv. versleutelde gegevens, gps-gegevens, "datamining"-technologie die het mogelijk maakt gegevens uit verschillende bronnen te combineren, of gevallen waarin de vertrouwelijkheid en integriteit in informatietechnologiesystemen[14] moet worden verzekerd.

Alle bovenstaande kwesties moeten derhalve zorgvuldig worden bestudeerd.

De Commissie zal nagaan **hoe een coherente toepassing van de regels inzake gegevensbescherming kan worden verzekerd, rekening houdend met de impact van nieuwe technologieën op de rechten en vrijheden van individuen en met inachtneming van het doel het vrije verkeer van persoonsgegevens binnen de interne markt te waarborgen**.

2.1.2. Grotere transparantie voor de betrokkenen

Transparantie is een basisvoorwaarde, willen individuen controle kunnen uitoefenen over hun eigen gegevens en zich van een effectieve bescherming van hun persoonsgegevens kunnen verzekeren. Daarom is het van wezenlijk belang dat individuen door degenen die voor de verwerking verantwoordelijk zijn **goed en duidelijk, op een transparante wijze, worden geïnformeerd** over hoe en door wie hun gegevens worden verzameld en verwerkt, voor welke doeleinden, gedurende welke periode en in hoeverre zij het recht hebben hun gegevens in te zien, te corrigeren of te wissen. De bestaande bepalingen betreffende de aan de betrokkene te verstrekken informatie[15] zijn niet toereikend.

Transparantie vereist in essentie dat de **informatie vlot toegankelijk en gemakkelijk te begrijpen is en dat duidelijke en eenvoudige taal wordt gebruikt**. Dit is in het bijzonder relevant in een online-omgeving, waarin privacyverklaringen vaak onduidelijk, moeilijk te

---

12 Zie overweging 26 van Richtlijn 95/46/EG.

13 Zie bijvoorbeeld het geval van IP-adressen, dat is besproken in advies 4/2007 van de Groep artikel 29 over het begrip persoonsgegeven (WP 136).

14 Zie bijvoorbeeld het arrest van het Duitse grondwettelijke hof (Bundesverfassungsgericht) van 27 februari 2008, 1 BvR 370/07.

15 Zie de artikelen 10 en 11 van Richtlijn 95/46/EG

vinden, ondoorzichtig[16] en niet steeds conform de bestaande voorschriften zijn. Waar dit met name het geval zou kunnen zijn, is bij online "behavioural advertising" (gerichte reclame op basis van het surfgedrag). Zowel het grote aantal spelers dat zich ermee bezighoudt als de technologische complexiteit van deze praktijk maken dat het voor een individu moeilijk is te weten en te begrijpen of, door wie en met welk doel persoonsgegevens worden verzameld.

Kinderen verdienen in deze context extra bescherming, aangezien zij zich allicht minder bewust zijn van de risico's, gevolgen, beschermingsmaatregelen en rechten in verband met de verwerking van persoonsgegevens[17].

De Commissie zal overwegen:

- in het wettelijke kader van een **algemeen beginsel van transparante verwerking** van persoonsgegevens op te nemen;

- **specifieke verplichtingen** in te voeren voor de voor verwerking verantwoordelijken met betrekking tot het soort informatie dat mag worden verstrekt en de **voorwaarden waaronder** die wordt verstrekt, inzonderheid ten aanzien van **kinderen**;

- een of meer **EU-standaardformulieren** ("**privacyverklaringen**") op te stellen die door de voor de verwerking van gegevens verantwoordelijken moeten worden gebruikt.

Het is voor een persoon ook belangrijk te worden geïnformeerd wanneer zijn gegevens per ongeluk of op onrechtmatige wijze worden vernietigd, zoek raken, worden gewijzigd, of worden ingezien door dan wel medegedeeld aan onbevoegde personen. Bij de recente herziening van de e-privacyrichtlijn werd een **verplichte kennisgeving bij een inbreuk in verband met persoonsgegevens** ingevoerd, die echter alleen voor de telecommunicatiesector geldt. Daar het risico op gegevensinbreuken ook bestaat in andere sectoren (bv. de financiële sector), zal de Commissie onderzoeken hoe de meldingsplicht voor inbreuken op persoonsgegevens kan worden uitgebreid tot andere sectoren, overeenkomstig de verklaring over de melding van gegevensinbreuken die de Commissie in 2009 voor het Europees Parlement heeft afgelegd in het kader van het regelgevingskader voor elektronische communicatie[18]. Dit onderzoek doet geen afbreuk aan de bepalingen van de e-privacyrichtlijn,

---

16 Uit een in 2009 uitgevoerde Eurobarometer-enquête bleek dat bijna de helft van de respondenten privacyverklaringen op websites "zeer onduidelijk" of "vrij onduidelijk" vonden (zie Flash Eurobarometer nr. 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Zie het kwalitatieve onderzoek "Veiliger internet voor kinderen", dat is uitgevoerd bij kinderen in de leeftijdsgroepen 9-10 jaar en 12-14 jaar, waaruit is gebleken dat kinderen de neiging hebben om de aan het gebruik van internet verbonden risico's te onderschatten en de gevolgen van hun risicogedrag te minimaliseren (te vinden op: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 "De Commissie neemt kennis van de wens van het Europees Parlement om de meldingsplicht bij inbreuken met betrekking tot persoonsgegevens niet te beperken tot de elektronische-communicatiesector, maar ook op te leggen aan andere entiteiten, bijvoorbeeld aanbieders van diensten van de informatiemaatschappij […]. De Commissie zal derhalve onverwijld beginnen met de voorbereidende werkzaamheden, met inbegrip van een raadpleging van de belanghebbenden, opdat zij uiterlijk tegen eind 2011 zo nodig met passende voorstellen op dit gebied kan komen […]", te vinden op http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN. Zie ook overweging 59 van Richtlijn 2009/136/EG tot wijziging van de e-pricacy-richtlijn 2002/58/EG: "Het algemene belang van gebruikers om te worden ingelicht is duidelijk niet beperkt tot de sector elektronische communicatie, en bijgevolg moeten op Gemeenschapsniveau prioritair expliciete, verplichte meldingseisen worden ingevoerd die voor alle sectoren gelden".

die tegen 25 mei 2011 in nationaal recht moeten worden omgezet[19]. Er moet op dit gebied een consequente en coherente aanpak komen.

De Commissie zal:

- onderzoeken onder welke voorwaarden in het algemene wettelijke kader een **algemene meldingsplicht voor inbreuken met betrekking tot persoonsgegevens** kan worden ingevoerd, en met name aan wie dergelijke kennisgevingen moeten gebeuren en op basis van welke criteria de meldingsplicht ontstaat.

2.1.3. Grotere zeggenschap over de eigen gegevens

Twee belangrijke voorwaarden om individuen een hoog niveau van gegevensbescherming te kunnen bieden zijn dat de **verwerking door de voor de verwerking verantwoordelijken wordt beperkt tot wat voor het beoogde doel noodzakelijk is (beginsel van minimalisering van de gegevensverwerking)** en dat de betrokkenen **daadwerkelijk zeggenschap behouden over hun eigen gegevens**. Artikel 8, lid 2, van het Handvest stelt dat eenieder recht heeft "op toegang tot de over hem verzamelde gegevens en op correctie daarvan". Personen moeten te allen tijde hun gegevens kunnen inzien, corrigeren, wissen of afschermen, tenzij rechtmatige redenen waarin de wet voorziet hieraan in de weg staan. Deze rechten bestaan reeds in het huidige wettelijke kader. De wijze waarop ze kunnen worden uitgeoefend is echter niet geharmoniseerd, en bijgevolg is de uitoefening ervan in de ene lidstaat al gemakkelijker dan in de andere. Dit is daarenboven bijzonder prangend geworden in de onlineomgeving, waarin gegevens vaak worden bewaard zonder dat de betrokkene wordt geïnformeerd en/of daarvoor zijn toestemming heeft gegeven.

Online sociale netwerken zijn in dit verband een sprekend voorbeeld, aangezien zich daar bijzondere problemen voordoen met betrekking tot de daadwerkelijke zeggenschap van het individu over zijn eigen persoonsgegevens. De Commissie heeft diverse vragen ontvangen van personen die er niet in waren geslaagd hun persoonsgegevens, bijvoorbeeld hun foto's, terug te vinden bij online dienstverleners en die daardoor werden belemmerd in de uitoefening van hun recht op inzage, correctie en wissing van hun gegevens.

Die rechten moeten derhalve worden geëxpliciteerd, verduidelijkt en mogelijk versterkt.

[19] Artikel 4 van Richtlijn 2009/136/EG.

De Commissie zal daarom de mogelijkheden onderzoeken om:

- het **beginsel van minimalisering van gegevensverwerking** te versterken;

- de **praktische regelingen** voor de feitelijke **uitoefening van het recht op inzage, correctie, wissing of afscherming van gegevens te verbeteren** (bv. door termijnen in te voeren waarbinnen op verzoeken van individuen moet worden geantwoord, door de uitoefening van rechten via elektronische weg mogelijk te maken of door te bepalen dat het recht op inzage in beginsel kosteloos moet zijn);

- het zogeheten "**recht om te worden vergeten**" duidelijker te omschrijven, d.w.z. het recht van een persoon om te verkrijgen dat zijn gegevens niet meer worden verwerkt en worden gewist wanneer ze niet langer nodig zijn voor rechtmatige doeleinden. Dat is bijvoorbeeld het geval wanneer de verwerking gebaseerd is op de toestemming van de betrokkene en hij die toestemming intrekt of wanneer de bewaartermijn is verstreken;

- de rechten van de betrokkenen uit te breiden door "**gegevensportabiliteit**" te waarborgen, d.w.z. door uitdrukkelijk te voorzien in eenieders recht om zijn eigen gegevens (bv. foto's of een lijst van vrienden) uit een applicatie of dienst terug te trekken en, voor zover dit technisch mogelijk is, naar een andere applicatie of dienst over te dragen zonder inmenging van de voor de verwerking verantwoordelijken.

2.1.4. Bewustmaking

Transparantie is absoluut noodzakelijk, maar tegelijk is het nodig het grote publiek, en vooral jongeren, meer bewust te maken van de risico's die aan de verwerking van persoonsgegevens verbonden zijn, en van hun rechten. Uit een in 2008 uitgevoerde Eurobarometer-enquête bleek dat de meeste mensen in de EU-lidstaten van mening zijn dat slechts weinigen weten hoe persoonsgegevens in hun eigen land worden beschermd[20]. Bewustmakingsacties verdienen dus aanmoediging en zoveel mogelijk partners moeten zich er achter scharen, zowel autoriteiten van de lidstaten – met name gegevensbeschermingsautoriteiten en onderwijsinstanties – als verantwoordelijken voor gegevensverwerking en middenveldorganisaties. Het moet dan onder meer gaan om niet-wetgevende maatregelen zoals bewustmakingscampagnes in de gedrukte en elektronische media en het verstrekken van duidelijke informatie via websites, waarbij de rechten van de betrokkenen en de verantwoordelijkheden van de voor de verwerking verantwoordelijken op begrijpelijke wijze worden uitgelegd.

De Commissie zal nagaan:

- of **medefinanciering van bewustmakingsacties op het gebied van gegevensbescherming** via de EU-begroting mogelijk is;

- of het nodig en wenselijk is in het wettelijke kader een **verplichting tot het opzetten van bewustmakingsacties** op dit gebied op te nemen.

2.1.5. Zorgen voor geïnformeerde en vrije toestemming

Wanneer een geïnformeerde toestemming verlangd wordt, schrijven de huidige regels voor dat de toestemming van de betrokkene voor de verwerking van zijn persoonsgegevens een

[20] Zie Flash Eurobarometer nr. 225 – Gegevensbescherming in de Europese Unie: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

"vrije, specifieke en op informatie berustende wilsuiting" moet zijn waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt[21]. Die voorwaarden worden momenteel in de lidstaten echter verschillend geïnterpreteerd, variërend van een algemene eis dat schriftelijk toestemming wordt verleend tot de aanvaarding van een stilzwijgende instemming.

Daarenboven is het voor individuen in een online omgeving – gelet op het in veel gevallen onduidelijke privacybeleid – vaak moeilijker te weten wat hun rechten zijn en een geïnformeerde toestemming te geven. Het wordt er niet eenvoudiger op doordat in sommige gevallen zelfs niet duidelijk is wat als een vrije, specifieke en op informatie berustende toestemming tot gegevensverwerking kan worden beschouwd, bijvoorbeeld in het geval van "behavioural advertising", waarbij bepaalde instellingen van de internetbrowser door sommigen wel en door anderen niet als toestemming van de gebruiker worden aangezien.

Er moet derhalve meer duidelijkheid komen over de voorwaarden waaraan de toestemming van de betrokkene moet voldoen om in alle gevallen te garanderen dat geïnformeerde toestemming is gegeven en dat de betrokkene zich er ten volle van bewust is dat hij een toestemming geeft en voor welke gegevensverwerking hij dat doet, overeenkomstig artikel 8 van het EU-Handvest van de grondrechten. Duidelijkheid omtrent de kernbegrippen kan ook bevorderlijk zijn voor de ontwikkeling van zelfregulerende initiatieven om praktische oplossingen uit te werken die stroken met het EU-recht.

De Commissie zal onderzoeken hoe de **regels inzake het verlenen van toestemming kunnen worden verduidelijkt en verbeterd**.

2.1.6. Bescherming van gevoelige gegevens

De verwerking van gevoelige gegevens, d.w.z. gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksleven betreffen, is in de regel thans reeds verboden, met beperkte uitzonderingen wanneer bepaalde voorwaarden en garanties in acht zijn genomen[22]. In het licht van de technologische en maatschappelijke ontwikkelingen moet de bestaande regeling voor gevoelige gegevens evenwel opnieuw worden bekeken, moet worden nagegaan of er geen andere gegevenscategorieën aan moeten worden toegevoegd en moet nader worden verduidelijkt onder welke voorwaarden verwerking mogelijk is. Het kan bijvoorbeeld gaan om genetische gegevens, die momenteel niet uitdrukkelijk worden vermeld als categorie van gevoelige gegevens.

De Commissie zal overwegen:

- of andere categorieën van gegevens, bijvoorbeeld **genetische** gegevens, als "**gevoelige gegevens**" dienen te worden aangemerkt;

- of een verdere verduidelijking en **harmonisatie van de voorwaarden** voor de verwerking van gevoelige gegevens gewenst is.

[21] Zie artikel 2, onder h), van Richtlijn 95/46/EG.

[22] Zie artikel 8 van Richtlijn 95/46/EG.

2.1.7. Corrigerende maatregelen en sancties doeltreffender maken

Met het oog op de handhaving van de regels inzake gegevensbescherming is het van wezenlijk belang dat is voorzien in **doeltreffende corrigerende maatregelen en sancties**. Wanneer een individu wordt geschaad door een inbreuk op de voorschriften inzake gegevensbescherming, raakt dit vaak ook een groot aantal anderen die in dezelfde situatie verkeren.

De Commissie zal daarom nagaan:

- of het mogelijk is de **bevoegdheid om een zaak aanhangig te maken bij de nationale rechter** uit te breiden tot gegevensbeschermingsautoriteiten en middenveldorganisaties, alsook tot **andere verenigingen die de belangen van de betrokkenen behartigen**;

- of het nodig is de **bestaande sanctieregeling aan te scherpen**, bijvoorbeeld door uitdrukkelijk te voorzien in strafsancties voor ernstige inbreuken op de gegevensbescherming, teneinde de handhaving doeltreffender te maken.

2.2. Verder uitwerken van de internemarktdimensie

2.2.1. Vergroten van de rechtszekerheid en scheppen van gelijke voorwaarden voor verantwoordelijken voor gegevensverwerking

Gegevensbescherming heeft in de EU **een sterke internemarktdimensie**. Dat wil zeggen dat binnen de interne markt het vrije verkeer van persoonsgegevens tussen de lidstaten moet worden gewaarborgd. Bijgevolg blijft de harmonisatie van de nationale wettelijke regelingen inzake gegevensbescherming waarin de richtlijn voorziet, niet beperkt tot een minimumharmonisatie, maar gaat het in beginsel om een volledige harmonisatie[23].

Terzelfder tijd kent de richtlijn de lidstaten op bepaalde gebieden een manoeuvreerruimte toe en machtigt ze hen bijzondere regelingen voor specifieke situaties te handhaven of in te voeren[24]. Dit heeft, samen met het feit dat de richtlijn door de lidstaten soms foutief is toegepast, geleid tot **verschillen tussen de nationale wettelijke regelingen tot omzetting van de richtlijn, hetgeen in strijd is met een van de hoofddoelstellingen ervan, namelijk het verzekeren van het vrije verkeer van persoonsgegevens binnen de interne markt**. Die verschillen doen zich voor in een groot aantal sectoren en situaties, bv. bij de verwerking van persoonsgegevens in de context van arbeidsvoorziening of voor gezondheidsdoeleinden. Het ontbreken van harmonisatie is een van de blijvende grote punten van bezorgdheid van particuliere belanghebbenden, zoals ondernemingen, aangezien het voor hen extra kosten en administratieve lasten meebrengt. Dit is met name het geval voor verantwoordelijken voor gegevensverwerking die in verscheidene lidstaten vestigingen hebben en verplicht zijn zich in elk van die landen aan de voorschriften en gangbare praktijken te conformeren. De verschillen in de omzetting van de richtlijn door de lidstaten scheppen bovendien rechtsonzekerheid, niet alleen voor de voor gegevensverwerking verantwoordelijken maar ook voor de betrokkenen zelf, en dreigen afbreuk te doen aan het gelijkwaardige beschermingsniveau dat de richtlijn geacht wordt te bewerkstelligen en te verzekeren.

---

23 Europees Hof van Justitie, zaak C-101/01, Bodil Linqvist, Jurispr. 2003, blz. I-1297, punten 96-97.

24 *Ibidem*, punt 97: Zie ook overweging 9 van Richtlijn 95/46/EG.

De Commissie zal onderzoeken hoe een **verdere harmonisatie van de regels inzake gegevensbescherming op EU-niveau** kan worden bereikt.

2.2.2. De administratieve belasting verminderen

Door het scheppen van gelijke voorwaarden zal niet meer aan uiteenlopende nationale voorschriften moeten worden voldaan en zal de administratieve belasting voor de voor verwerking verantwoordelijken derhalve aanmerkelijk lichter worden. Een andere concrete maatregel ter vermindering van de administratieve belasting en de kosten voor verantwoordelijken voor gegevensverwerking zou kunnen bestaan in een **herziening en vereenvoudiging van het bestaande aanmeldingssysteem**[25]. Onder verantwoordelijken voor gegevensverwerking bestaat er eensgezindheid over dat de huidige algemene verplichting om alle verwerkingen bij de gegevensbeschermingsautoriteiten aan te melden een vrij tijdrovende verplichting is die op zichzelf geen echte meerwaarde oplevert voor de bescherming van de persoonsgegevens van de betrokkenen. Dit is daarenboven een van de gevallen waarin de richtlijn een zekere manoeuvreerruimte geeft aan de lidstaten, die vrij kunnen beslissen over eventuele uitzonderingen of vereenvoudigingen en over de te volgen procedures.

Een geharmoniseerd en vereenvoudigd systeem zou zowel de kosten als de administratieve belasting verminderen, in het bijzonder voor multinationale ondernemingen die in verschillende lidstaten vestigingen hebben.

De Commissie zal verschillende mogelijkheden onderzoeken om **het bestaande aanmeldingssysteem te vereenvoudigen en te harmoniseren**, onder meer het opstellen van een **eenvormig registratieformulier dat voor de hele EU zou kunnen gelden**.

2.2.3. Verduidelijken van de regels met betrekking tot het toepasselijke recht en de verantwoordelijkheid van de lidstaten

In het eerste verslag van de Commissie over de toepassing van de richtlijn gegevensbescherming werd er reeds in 2003[26] nadrukkelijk op gewezen dat de bepalingen betreffende het toepasselijke recht[27] "in diverse gevallen gebrekkig [waren] met als resultaat dat het soort wetsconflicten die dit artikel tracht te vermijden, kan ontstaan". De situatie is er sindsdien niet beter op geworden, waardoor het voor de voor gegevensverwerking verantwoordelijken en voor de gegevensbeschermingsautoriteiten niet altijd duidelijk is welke lidstaat verantwoordelijk is en welk recht moet worden toegepast wanneer er meerdere lidstaten betrokken zijn. Dit is met name het geval wanneer een voor de verwerking verantwoordelijke aan verschillende eisen van verschillende lidstaten moet voldoen, wanneer een multinationale onderneming vestigingen heeft in meerdere lidstaten of wanneer de voor de verwerking verantwoordelijke niet in de EU gevestigd is maar wel diensten verleent aan EU-inwoners.

De complexiteit neemt ook toe ten gevolge van de globalisering en de technologische ontwikkelingen: de voor gegevensverwerking verantwoordelijken zijn steeds vaker actief in meerdere lidstaten en rechtsgebieden, waarbij zij dag en nacht diensten en bijstand verlenen. Het internet maakt het voor verantwoordelijken die buiten de Europese Economische Ruimte

---

25 Zie artikel 18 van Richtlijn 95/46/EG.

26 Verslag van de Commissie - Eerste verslag over de toepassing van de richtlijn gegevensbescherming (95/46/EG) - COM(2003) 265.

27 Zie artikel 4 van Richtlijn 95/46/EG.

(EER)[28] gevestigd zijn veel gemakkelijker op afstand diensten te verlenen en persoonsgegevens in de online omgeving te verwerken. Vaak is het ook moeilijk te bepalen waar persoonsgegevens en de gebruikte apparatuur zich op een bepaald tijdstip bevinden (bv. bij applicaties en diensten die "in the cloud" werken).

De Commissie is evenwel van oordeel dat het feit dat de verwerking van persoonsgegevens wordt verricht door een verantwoordelijke die in een derde land is gevestigd, niet ten gevolge mag hebben dat individuen de bescherming verliezen waarop zij krachtens het EU-Handvest van de grondrechten en de EU-wetgeving inzake gegevensbescherming recht hebben.

De Commissie zal onderzoeken hoe te komen tot een **herziening en verduidelijking van de bestaande regels betreffende het toepasselijke recht**, inclusief de aanknopingspunten, om zo de rechtszekerheid te vergroten, de verantwoordelijkheid van de lidstaten voor de toepassing van de regels inzake gegevensbescherming duidelijker te omschrijven en uiteindelijk EU-betrokkenen eenzelfde beschermingsniveau te bieden ongeacht waar de voor de gegevensverwerking verantwoordelijke zich bevindt.

2.2.4. Uitbreiden van de verantwoordelijkheid van de voor de verwerking verantwoordelijke

Administratieve vereenvoudiging mag er **niet toe leiden dat de verantwoordelijkheid van de voor gegevensverwerking verantwoordelijken om een doeltreffende gegevensbescherming te bieden per saldo vermindert**, wel integendeel. De Commissie is van oordeel dat hun verplichtingen juist duidelijker moeten worden omschreven in het wettelijke kader, ook wat betreft interne controlemechanismen en samenwerking met de gegevensbeschermingsautoriteiten. Daarenboven moet ervoor worden gezorgd dat die verantwoordelijkheid ook geldt voor verantwoordelijken die gebonden zijn aan een beroepsgeheim (bv. advocaten) en in de steeds vaker voorkomende gevallen waarin de voor de verwerking verantwoordelijken de gegevensverwerking delegeren aan andere entiteiten (bv. verwerkers).

De Commissie zal daarom nagaan hoe het best kan worden **verzekerd dat de voor gegevensverwerking verantwoordelijken de facto een beleid voeren en mechanismen instellen om te bereiken dat de regels inzake gegevensbescherming worden nageleefd**. Daarbij zal zij rekening houden met het aan de gang zijnde debat over de mogelijke invoering van een accountability-beginsel[29]. Het is niet de bedoeling de voor de verwerking verantwoordelijken een extra administratieve belasting op te leggen, aangezien deze maatregelen eerder gericht zijn op het invoeren van beschermingsmaatregelen en mechanismen die het afdwingen van gegevensbescherming doeltreffender maken en tegelijk bepaalde administratieve formaliteiten, bijvoorbeeld aanmeldingen (*zie punt 2.2.2*), verminderen en vereenvoudigen.

Het aanmoedigen van privacybevorderende technologieën (PET's – Privacy Enhancing Technologies) – zoals reeds aangegeven in de mededeling van de Commissie van 2007 over

[28] Van de Europese Economische Ruimte maken ook Noorwegen, Liechtenstein en IJsland deel uit.

[29] Zie met name advies 3/2010 van de Groep artikel 29 van 13 juli 2010.

dit onderwerp – en het beginsel van "ingebouwde privacy" zouden in dit opzicht een belangrijke rol kunnen spelen, ook met het oog op dataveiligheid[30].

De Commissie zal de volgende punten onderzoeken om de verantwoordelijkheid van de voor de verwerking verantwoordelijken aan te scherpen:

– het verplicht maken van de aanstelling van een onafhankelijke **functionaris voor gegevensbescherming** en het harmoniseren van diens taken en bevoegdheden[31], waarbij de Commissie echter ook zal nadenken over een passende drempel om onnodige administratieve lasten, met name voor kleine en micro-ondernemingen, te vermijden;

– het opnemen in het wettelijke kader van een verplichting voor verantwoordelijken voor gegevensverwerking om in bepaalde gevallen een **effectbeoordeling uit een oogpunt van gegevensbescherming** uit te voeren, bijvoorbeeld bij de verwerking van gevoelige gegevens of wanneer het soort verwerking anderszins specifieke risico's meebrengt, met name bij het gebruik van bijzondere technologieën, mechanismen of procedures, waaronder profiling en videobewaking;

– de blijvende aanmoediging van het gebruik van PET's en van de mogelijkheden om concrete invulling te geven aan het begrip "**ingebouwde privacy**".

2.2.5. Aanmoediging van zelfregulering en onderzoek naar EU-certificeringsregelingen

De Commissie blijft van mening dat **zelfregulerende initiatieven** van de voor gegevensverwerking verantwoordelijken kunnen **bijdragen tot een betere handhaving van de regels inzake gegevensbescherming**. Van de bestaande bepalingen over zelfregulering in de gegevensbeschermingsrichtlijn, meer bepaald de mogelijkheid tot het opstellen van gedragscodes[32], is tot dusver zeer weinig gebruikt gemaakt. Particuliere belanghebbenden vinden ze onbevredigend.

Voorts zal de Commissie nagaan of EU-**certificeringsregelingen (bv. "privacyzegels")** kunnen worden ingevoerd voor processen, technologieën, producten en diensten die aan de privacyregels voldoen[33]. Die zouden niet alleen een aanwijzing vormen voor gebruikers van de betrokken technologieën, producten en diensten, maar ook relevant zijn voor de verantwoordelijkheid van de voor gegevensverwerking verantwoordelijken: door te kiezen voor gecertificeerde technologieën, producten of diensten kan de voor verwerking verantwoordelijke allicht gemakkelijker aantonen dat hij zijn verplichtingen is nagekomen (*zie punt 2.2.4*). Uiteraard is het daarbij van wezenlijk belang de **betrouwbaarheid van die**

30 Inzake PET's zie: mededeling van de Commissie aan het Europees Parlement en de Raad inzake de verbetering van de gegevensbescherming door technologieën ter bevordering van de persoonlijke levenssfeer, COM(2007) 228. Het beginsel van "ingebouwde privacy" houdt in dat de bescherming van de particuliere levenssfeer en van gegevens in acht wordt genomen gedurende de volledige levenscyclus van een technologie, vanaf de fase waarin deze wordt ontworpen tot en met de fase waarin ze wordt geïnstalleerd, gebruikt en uiteindelijk verwijderd. Dit beginsel wordt onder meer vermeld in de mededeling van de Commissie over "Een digitale agenda voor Europa" - COM(2010) 245.

31 Van de reeds bestaande mogelijkheid om een functionaris voor gegevensbescherming aan te stellen die op onafhankelijke wijze toeziet op de naleving van de nationale en EU-voorschriften inzake gegevensbescherming en individuele betrokkenen bijstaat, is in verscheidene lidstaten reeds gebruik gemaakt (zie bv. de "Beauftragter für den Datenschutz" in Duitsland en de "correspondant informatique et libertés (CIL)" in Frankrijk).

32 Zie artikel 27 van Richtlijn 95/46/EG.

33 Zie in dit verband de reeds in voetnoot 30 aangehaalde mededeling over PET's.

privacyzegels te garanderen en ervoor te zorgen dat ze in overeenstemming zijn met de wettelijke verplichtingen en internationale technische normen.

De Commissie zal:

- zoeken naar middelen om **zelfregulering verder aan te moedigen**, onder meer door het gebruik van gedragscodes actief te promoten;

- de haalbaarheid onderzoeken van de invoering van **EU-certificeringsregelingen** op het gebied van privacy- en gegevensbescherming.

2.3. Herziening van de voorschriften inzake gegevensbescherming in het kader van de politiële en justitiële samenwerking in strafzaken

De gegevensbeschermingsrichtlijn is van toepassing op elk verwerking van persoonsgegevens in de lidstaten in zowel de publieke als de particuliere sector. Ze is evenwel niet van toepassing op de verwerking van persoonsgegevens met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten, zoals de activiteiten op het gebied van de politiële en justitiële samenwerking in strafzaken[34]. Het Verdrag van Lissabon heeft de vroegere "pijlerstructuur" van de EU afgeschaft en een nieuwe, algemene rechtsgrondslag ingevoerd voor de bescherming van persoonsgegevens in alle onderdelen van het EU-beleid[35]. Tegen die achtergrond en gelet op het EU-Handvest van de grondrechten werd er in de mededelingen van de Commissie over het programma van Stockholm en het actieplan van Stockholm[36] grote nadruk op gelegd dat er een "integrale beschermingsregeling" moet komen en dat "het standpunt van de EU over de bescherming van persoonsgegevens van individuen in het kader van alle EU-beleid moet worden versterkt, ook op het gebied van rechtshandhaving en criminaliteitspreventie".

Het EU-instrument voor de bescherming van persoonsgegevens in het kader van de politiële en justitiële samenwerking in strafzaken is **Kaderbesluit 2008/977/JBZ**[37]. Het kaderbesluit vormt een belangrijke stap vooruit op een terrein waar gemeenschappelijke normen voor gegevensbescherming ten zeerste noodzakelijk waren. Er moet echter nog meer gebeuren.

Het kaderbesluit heeft uitsluitend betrekking op de grensoverschrijdende uitwisseling van persoonsgegevens binnen de EU en niet op de binnenlandse verwerking van gegevens in de lidstaten. Dit onderscheid is in de praktijk moeilijk te maken en kan de daadwerkelijke uitvoering en toepassing van het kaderbesluit bemoeilijken[38].

---

34 Zie artikel 3, lid 2, eerste streepje, van Richtlijn 95/46/EG.

35 Zie artikel 16 VWEU.

36 Zie COM(2009) 262 van 10.6.2009 en COM(2010) 171 van 20.4.2010.

37 Kaderbesluit 2008/977/JBZ van de Raad van 27.11.2008 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. Het kaderbesluit voorziet slechts in een minimale harmonisatie van de normen inzake gegevensbescherming.

38 Dit onderscheid wordt niet gemaakt in de relevante instrumenten van de Raad van Europa, zoals: het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (CETS nr. 108), het aanvullend protocol daarbij aangaande toezichthoudende autoriteiten en grensoverschrijdende datastromen (ETS nr. 181) en de op 17 september 1987 aangenomen Aanbeveling R(87)15 van het Comité van ministers aan de lidstaten tot regeling van het gebruik van persoonsgegevens op politieel gebied.

Voorts **voorziet het kaderbesluit in een al te ruime uitzondering op het doelbindingsbeginsel**. Een andere tekortkoming is het ontbreken van een bepaling dat een onderscheid moet worden gemaakt volgens de graad van nauwkeurigheid en betrouwbaarheid van de verschillende categorieën gegevens, dat gegevens die gebaseerd zijn op feiten moeten worden onderscheiden van gegevens die gebaseerd zijn op meningen of persoonlijke inschattingen[39] en dat er een onderscheid moet worden gemaakt tussen verschillende categorieën betrokkenen (criminelen, slachtoffers, getuigen enz.), waarbij bijzondere garanties worden vastgelegd voor gegevens betreffende personen die geen verdachte zijn[40].

Overigens **komt het kaderbesluit niet in de plaats van de diverse sectorspecifieke wetgevingsinstrumenten voor politiële en justitiële samenwerking in strafzaken die op EU-niveau zijn vastgesteld**[41], onder meer die betreffende de werking van Europol, Eurojust, het Schengen-informatiesysteem (SIS) en het douane-informatiesysteem (DIS)[42], die voorzien in bijzondere gegevensbeschermingsregelingen en/of gewoonlijk verwijzen naar de gegevensbeschermingsinstrumenten van de Raad van Europa. Voor activiteiten op het gebied van de politiële en justitiële samenwerking hebben alle lidstaten Aanbeveling nr. R(87)15 van de Raad van Europa onderschreven, waarin de beginselen van Verdrag nr. 108 voor de politiesector wordt uitgewerkt. Dit is echter geen in rechte bindend instrument.

Dit kan directe gevolgen hebben voor de mogelijkheid van individuen om in deze context hun recht op gegevensbescherming uit te oefenen (d.w.z. te weten welke persoonsgegevens over hen worden verwerkt en uitgewisseld, door wie en met welk doel, en hoe zij hun rechten – bv. het recht om hun gegevens in te zien – kunnen uitoefenen).

Het streven om een alomvattend en coherent systeem in de EU en ten opzichte van derde landen op te zetten, maakt het **noodzakelijk een herziening te overwegen van de bestaande regels inzake gegevensbescherming in het kader van de politiële en justitiële samenwerking in strafzaken**. De Commissie wijst erop dat een integrale gegevensbeschermingsregeling niet uitsluit dat er binnen dat algemene kader specifieke voorschriften gelden voor gegevensbescherming in de sector politie en justitie, die rekening houden met de specifieke aard van die werkterreinen, zoals aangegeven in verklaring 21 bij het Verdrag van Lissabon. Dit brengt onder meer mee dat moet worden nagegaan in welke mate de uitoefening van bepaalde rechten inzake gegevensbescherming door een individu de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van strafsancties in een bepaald geval in gevaar zou kunnen brengen.

---

39 Zoals voorgeschreven door principe 3.2 van Aanbeveling nr. R(87)15.

40 In strijd met beginsel 2 van Aanbeveling nr. R(87)15 en de evaluatieverslagen erover.

41 Voor een overzicht van die instrumenten, zie de mededeling van de Commissie "Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht" – COM(2010) 385.

42 Naast de algemene bevoegdheden van de Europese Toezichthouder voor gegevensbescherming inzake toezicht op de instellingen, organen, bureaus en agentschappen van de Unie, die gebaseerd zijn op Verordening (EG) nr. 45/2001, zijn door de betrokken instrumenten gemeenschappelijke toezichthoudende autoriteiten ingesteld om de gegevensbescherming te controleren.

De Commissie zal met name:

- de **uitbreiding van de toepassing van de algemene regels inzake gegevensbescherming tot de politiële en justitiële samenwerking in strafzaken** onderzoeken, ook bij verwerking in het binnenland, met dien verstande dat waar nodig wordt voorzien in geharmoniseerde **beperkingen** op bepaalde rechten van individuen inzake gegevensbescherming, bv. het recht van inzage of het tranparantiebeginsel;

- onderzoeken of **specifieke, geharmoniseerde bepalingen** moeten worden ingevoerd in het nieuwe algemene gegevensbeschermingskader, bijvoorbeeld in verband met de verwerking van **genetische gegevens** in het kader van strafvervolging of om onderscheid te maken tussen de verschillende categorieën betrokkenen (getuigen, verdachten enz.) in het kader van de politiële en justitiële samenwerking in strafzaken;

- in 2011 een **raadpleging** van alle belanghebbenden houden over de beste manier om de **huidige toezichtregelingen op het gebied van de politiële en justitiële samenwerking in strafzaken te herzien**, teneinde een uit een oogpunt van gegevensbescherming doeltreffend en coherent toezicht op alle instellingen, organen, bureaus en agentschappen van de Unie te waarborgen;

- evalueren of het op lange termijn noodzakelijk is de **diverse bestaande sectorspecifieke voorschriften die op EU-niveau met het oog op de politiële en justitiële samenwerking in strafzaken in specifieke instrumenten zijn opgenomen te harmoniseren** met het nieuwe algemene wettelijke kader voor gegevensbescherming.

2.4. De wereldwijde dimensie van gegevensbescherming

2.4.1. De regels voor internationale doorgifte van gegevens verduidelijken en vereenvoudigen

Een van de middelen om de doorgifte van persoonsgegevens buiten de EU en de EER-zone mogelijk te maken is de zogeheten "**adequaatheidstoetsing**" van de geboden bescherming. Thans kan de adequaatheid van de bescherming in een derde land – d.w.z. of een derde land een beschermingsniveau waarborgt dat de EU als passend beschouwt – worden vastgesteld door de Commissie en door de lidstaten.

Als de Commissie een beschermingsniveau passend bevindt, betekent dit dat persoonsgegevens vanuit de 27 EU-lidstaten en de drie EER-landen vrij kunnen worden doorgegeven naar het betrokken derde land, zonder enige verdere beschermingsmaatregel. De exacte eisen voor de erkenning van een passend beschermingsniveau door de Commissie zijn momenteel echter niet voldoende gedetailleerd omschreven in de gegevensbeschermingsrichtlijn. Bovendien voorziet het kaderbesluit niet in een dergelijk besluit van de Commissie.

In sommige lidstaten wordt de adequaatheid van de bescherming in eerste instantie beoordeeld door de voor de verwerking verantwoordelijke die zelf persoonsgegevens doorgeeft naar een derde land, soms met toezicht achteraf door de toezichthoudende gegevensbeschermingsautoriteit. Dit kan ertoe leiden dat bij de beoordeling van het beschermingsniveau dat derde landen of internationale organisaties bieden uiteenlopende benaderingen worden gevolgd, en **brengt het risico mee dat het beschermingsniveau dat een bepaald derde land voor de betrokkenen biedt in de ene lidstaat anders wordt beoordeeld dan in de andere**. In de bestaande rechtsinstrumenten zijn evenmin nauwkeurige, geharmoniseerde bepalingen opgenomen over de vraag welke doorgiften als rechtmatig

kunnen worden beschouwd. Daardoor verschilt de wijze waarop hiermee wordt omgegaan van lidstaat tot lidstaat.

Wat overigens doorgiften van gegevens betreft aan derde landen die geen passend beschermingsniveau bieden, zijn de huidige standaardbepalingen van de Commissie betreffende de doorgifte van persoonsgegevens aan voor de verwerking verantwoordelijken[43] en aan verwerkers[44] niet afgestemd op niet-contractuele situaties en kunnen ze bijvoorbeeld niet worden gebruikt voor doorgiften tussen overheidsdiensten onderling.

Daarenboven moeten in internationale overeenkomsten die door de EU of haar lidstaten worden gesloten, vaak beginselen en specifieke bepalingen inzake gegevensbescherming worden opgenomen. Het kan darbij voorkomen dat verschillende teksten met onderling afwijkende bepalingen en rechten worden gebruikt, wat aanleiding kan geven tot uiteenlopende interpretaties, ten nadele van de betrokkenen. Daarom heeft de Commissie aangekondigd dat zij een aantal vaste onderdelen zou uitwerken om de bescherming van persoonsgegevens te regelen in overeenkomsten die de Unie voor rechtshandhavingsdoeleinden sluit met derde landen[45].

Andere middelen die als een vorm van zelfregulering zijn ontwikkeld, bijvoorbeeld interne gedragscodes van concerns, bekend als “bindende bedrijfsvoorschriften” (Binding Corporate Rules – BCR's)[46], kunnen eveneens een nuttig instrument zijn om op rechtmatige wijze persoonsgegevens uit te wisselen tussen ondernemingen van hetzelfde concern. Belanghebbenden hebben evenwel opgemerkt dat dit mechanisme nog kan worden verbeterd en dat de toepassing ervan kan worden vereenvoudigd.

Om de beschreven problemen aan te pakken is het **over de hele lijn noodzakelijk de bestaande mechanismen voor internationale doorgiften van persoonsgegevens te verbeteren**, met dien verstande dat persoonsgegevens op passende wijze moeten worden beschermd wanneer zij buiten de EU en de EER worden doorgegeven en verwerkt.

---

43 Beschikking 2001/497/EG van de Commissie van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG, PB L 181 van 4.7.2001. blz. 19; Beschikking 2002/16/EG van de Commissie van 27 december 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG, PB L 6 van 10.1.2002. blz. 52; Beschikking 2004/915/EG van de Commissie van 27 december 2004 tot wijziging van Beschikking 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen, PB L 385 van 29.12.2004, blz. 74.

44 Besluit van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, PB L 39 van 12.2.2010, blz. 5.

45 Zie het reeds in voetnoot 36 aangehaalde actieplan van Stockholm.

46 Bindende bedrijfsvoorschriften zijn gedragscodes die gebaseerd zijn op de Europese normen inzake gegevensbescherming. Ze worden door multinationale organisaties opgesteld en vrijwillig nageleefd om passende waarborgen te bieden ten aanzien van de doorgifte of categorieën van doorgiften van persoonsgegevens tussen ondernemingen die deel uitmaken van hetzelfde concern en die door die bedrijfsvoorschriften gebonden zijn. Zie: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

De Commissie zal onderzoeken hoe het mogelijk is om:

- **de bestaande procedures** voor de internationale doorgifte van gegevens **te verbeteren en te harmoniseren**, zowel wettelijke instrumenten als bindende bedrijfsvoorschriften, om te komen tot een **meer eenvormige en coherente EU-aanpak** ten opzichte van derde landen en internationale organisaties;

- de **procedure voor adequaatheidstoetsing door de Commissie te verduidelijken** en beter de **criteria en eisen** te omschrijven die worden gehanteerd bij de beoordeling van het beschermingsniveau in een derde land of bij een internationale organisatie;

- **vaste onderdelen voor de gegevensbescherming door de EU** vast te stellen die kunnen worden gebruikt voor alle soorten internationale overeenkomsten.

2.4.2. Bevordering van universele beginselen

Gegevensverwerking geschiedt wereldwijd en dus is er behoefte aan de ontwikkeling van universele beginselen voor de bescherming van individuen met betrekking tot de verwerking van hun persoonsgegevens.

Het wettelijke kader van de EU inzake gegevensbescherming is vaak gebruikt als **ijkpunt voor derde landen bij het vaststellen van regels inzake gegevensbescherming**. Het effect en de invloed ervan zijn zowel binnen als buiten de Unie steeds zeer groot geweest. De **Europese Unie moet derhalve een stuwende kracht blijven achter de ontwikkeling en de bevordering van internationale wettelijke en technische normen voor de bescherming van persoonsgegevens**, uitgaande van de relevante EU- en andere Europese instrumenten op het gebied van gegevensbescherming. Dit is vooral belangrijk in het kader van het uitbreidingsbeleid van de EU.

Wat de door normalisatie-instellingen uitgewerkte internationale technische normen betreft, is de Commissie van oordeel dat coherentie tussen het toekomstige wettelijke kader en die normen van zeer groot belang is om zich van een consistente en praktische toepassing van de voorschriften inzake gegevensbescherming door de voor gegevensverwerking verantwoordelijken te verzekeren.

De Commissie zal:

- in derde landen en op internationaal niveau de **ontwikkeling van strenge wettelijke en technische normen inzake gegevensbescherming blijven promoten**;

- ervoor ijveren het **beginsel van wederkerigheid van de bescherming bij elk internationaal optreden van de Unie** te doen aanvaarden, in het bijzonder in het geval van personen van wie de gegevens uit de EU worden uitgevoerd naar derde landen;

- **met het oog daarop intensiever gaan samenwerken met derde landen en internationale organisaties** zoals de OESO, de Raad van Europa, de Verenigde Naties en andere regionale organisaties;

- **van nabij de ontwikkeling volgen van internationale technische normen door normalisatie-instellingen** zoals CEN en ISO, om erop toe te zien dat ze een nuttige aanvulling vormen op de wettelijke regels en ervoor te zorgen dat de belangrijkste eisen inzake gegevensbescherming daadwerkelijk en doeltreffend worden toegepast.

2.5. Een betere institutionele regeling voor handhaving van de voorschriften inzake gegevensbescherming

De tenuitvoerlegging en handhaving van de beginselen en regels op het gebied van gegevensbescherming is een wezenlijk aspect van het waarborgen van de naleving van de rechten van het individu.

In dit verband is voor **de gegevensbeschermingsautoriteiten een cruciale rol** weggelegd. Zij zijn de onafhankelijke hoeders van de fundamentele rechten en vrijheden op het gebied van de bescherming van persoonsgegevens, en mensen rekenen op hen om de bescherming van hun persoonsgegevens en de wettigheid van de verwerking van gegevens te waarborgen. Daarom is de Commissie van oordeel dat hun rol moet worden uitgebreid, met name gelet op de recente jurisprudentie van het Europees Hof van Justitie over hun onafhankelijkheid[47], en dat hen de nodige bevoegdheden en middelen moeten worden toegekend om hun taken, zowel op nationaal niveau als in hun onderlinge samenwerking, naar behoren te kunnen uitoefenen.

De Commissie is er echter tevens van overtuigd dat de **gegevensbeschermingsautoriteiten nauwer moeten samenwerken en hun werkzaamheden beter moeten coördineren**, met name bij de behandeling van problemen die vanwege hun aard een grensoverschrijdende dimensie hebben. Dit is meer bepaald het geval wanneer multinationale ondernemingen vestigingen hebben in verscheidene lidstaten en hun werkzaamheden in elk van die landen verrichten, of wanneer gecoördineerd toezicht met de Europese Toezichthouder voor gegevensbescherming vereist is[48].

Daarbij kan de **Groep artikel 29 een belangrijke rol spelen**[49]. Die heeft immers, naast zijn adviserende rol[50], ook reeds tot taak bij te dragen tot de eenvormige toepassing van de EU-voorschriften inzake gegevensbescherming op nationaal niveau. Wegens de blijvende verschillen in de toepassing en interpretatie van de EU-regels door gegevensbeschermingsautoriteiten – in weerwil van het feit dat de problemen op het stuk van gegevensbescherming dezelfde zijn in de hele EU – is het echter wenselijk de taak van de Groep inzake coördinatie van de standpunten van de gegevensbeschermingsautoriteiten uit te breiden.

---

47 Zie het arrest van 9.3.2010, Commissie tegen Duitsland, Zaak C-518/07.

48 Dat is momenteel het geval voor grote IT-systemen, bv. SIS II (zie artikel 46 van Verordening (EG) nr. 1987/2006 – PB L 318 van 28.12.2006, blz. 4) en VIS (zie artikel 43 van Verordening (EG) nr. 767/2008 – PB L 218 van 13.8.2008, blz. 60).

49 De Groep artikel 29 is een adviesorgaan bestaande uit één vertegenwoordiger per lidstaat, gegevensbeschermingsautoriteiten, de Europese Toezichthouder voor gegevensbescherming en de Commissie (zonder stemrecht). Deze laatste verzorgt tevens het secretariaat. Zie: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 De Groep artikel 29 heeft tot taak de Commissie te adviseren over het beschermingsniveau in de EU en in derde landen en over elke andere maatregel in verband met de verwerking van persoonsgegevens.

De Commissie zal onderzoeken:

- hoe **de rechtspositie en de bevoegdheid van de nationale gegevensbeschermingsautoriteiten** in het nieuwe wettelijke kader kan worden **verbeterd, verduidelijkt en geharmoniseerd**, waarbij onder meer het begrip "volledige onafhankelijkheid" ten volle wordt waargemaakt[51];

- hoe de **samenwerking en coördinatie tussen gegevensbeschermingsautoriteiten kan worden verbeterd**;

- hoe kan worden gezorgd voor een meer eenvormige toepassing in de hele interne markt van de EU-regels inzake gegevensbescherming. Daarbij kan worden gedacht aan **een uitbreiding van de rol van de nationale toezichthouders voor gegevensbescherming, een betere coördinatie van hun werkzaamheden door de Groep artikel 29 (die een meer transparant orgaan moet worden) en/of de invoering van een mechanisme dat onder het gezag van de Europese Commissie de eenvormigheid binnen de interne markt moet bewaken**.

3. CONCLUSIE: DE WEG VOORUIT

Net als de technologie, is de wijze waarop onze persoonsgegevens in onze maatschappij worden gebruikt en gedeeld voortdurend aan verandering onderhevig. Dit stelt wetgevers voor de uitdaging een wetgevingskader uit te werken dat de tand des tijds kan doorstaan. Aan het einde van het hervormingsproces moeten de Europese regels inzake gegevensbescherming nog steeds een hoog beschermingsniveau garanderen en aan meerdere generaties individuele personen, overheidsdiensten en ondernemingen binnen de interne markt rechtszekerheid bieden. Ongeacht hoe complex de situatie of hoe geavanceerd de technologie ook is, er moet duidelijkheid zijn over de regels en normen die de nationale autoriteiten moeten handhaven en die ondernemingen en technologieontwikkelaars in acht moeten nemen. Individuele personen moeten ook duidelijk weten welke rechten zij hebben.

De **integrale aanpak van de Commissie** om de problemen op te lossen en de in deze mededeling beschreven hoofddoelstellingen te bereiken, zal het uitgangspunt vormen voor verdere besprekingen met de overige Europese instellingen en andere belanghebbenden en zal later worden vertaald in concrete voorstellen en maatregelen van zowel wetgevende als niet-wetgevende aard. Met het oog daarop ontvangt de Commissie graag feedback over de vraagstukken die in deze mededeling zijn behandeld.

Na een effectbeoordeling en rekening houdend met het EU-Handvest van de grondrechten zal de Commissie **in 2011 wetgevingsvoorstellen doen** met het oog op de herziening van het wettelijke kader voor gegevensbescherming, teneinde de positie van de EU te versterken met betrekking tot de bescherming van de persoonsgegevens van het individu in het kader van alle onderdelen van het EU-beleid, met inbegrip van rechtshandhaving en misdaadpreventie, een en ander met inachtneming van de eigen kenmerken van deze werkterreinen. Terzelfder tijd wordt werk gemaakt van niet-wetgevende maatregelen, zoals het aanmoedigen van zelfregulering en het onderzoeken van de haalbaarheid van EU-privacyzegels.

[51] Zie het arrest van het Europees Hof van Justitie van 9.3.2010, Commissie tegen Duitsland, Zaak C-518/07.

In een tweede fase zal de Commissie **afwegen of andere wettelijke instrumenten moeten worden aangepast** aan het nieuwe algemene gegevensbeschermingskader. Daarbij gaat het allereerst om Verordening (EG) nr. 45/2001, waarvan de bepalingen aan het nieuwe algemene wettelijke kader zullen moeten worden aangepast. Het effect op andere sectorale instrumenten zal in een later stadium eveneens zorgvuldig moeten worden onderzocht.

De Commissie zal voorts blijven zorgen voor een adequaat toezicht op de correcte naleving van het EU-recht ter zake door het voeren van een **actief inbreukbeleid** wanneer de EU-voorschriften inzake gegevensbescherming niet correct worden uitgevoerd of toegepast. De huidige herziening van de instrumenten op het gebied van gegevensbescherming doet immers geenszins afbreuk aan de verplichting van de lidstaten om de bestaande wettelijke instrumenten inzake de bescherming van persoonsgegevens ten uitvoer te leggen en op de correcte toepassing ervan toe te zien[52].

Een hoog en eenvormig niveau van gegevensbescherming in de EU aanhouden is de beste manier om de normen die de EU op dat gebied voorstaat wereldwijd te bevorderen.

[52] Dit geldt ook voor Kaderbesluit 200/977/JBZ van de Raad. De lidstaten moeten de nodige maatregelen treffen om vóór 27 november 2010 aan dit kaderbesluit te voldoen.