EUROPESE COMMISSIE

Brussel, 25.1.2012
COM(2012) 9 final

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

Privacywaarborging in het online tijdperk
Een Europees gegevensbeschermingskader voor de 21e eeuw

(Voor de EER relevante tekst)

[…]

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

Privacywaarborging in het online tijdperk
Een Europees gegevensbeschermingskader voor de 21e eeuw

(Voor de EER relevante tekst)

1. ACTUELE UITDAGINGEN VOOR DE GEGEVENSBESCHERMING

Door de snelheid waarmee de technologie evolueert en de globalisering zich voltrekt, is de wijze waarop steeds meer persoonsgegevens worden verzameld, geraadpleegd, be- en verwerkt en verplaatst radicaal getransformeerd. Nieuwe manieren om informatie te delen via sociale netwerken en grote hoeveelheden gegevens op afstand op te slaan, zijn gemeengoed geworden voor een groot deel van de 250 miljoen Europese internetgebruikers. En voor heel wat bedrijven zijn persoonsgegevens een kostbaar goed geworden. Het verzamelen, koppelen en analyseren van gegevens van potentiële klanten is vaak een belangrijk onderdeel van hun bedrijvigheid[1].

In deze nieuwe digitale omgeving hebben **individuele personen recht op effectieve controle over hun persoonlijke gegevens**. Gegevensbescherming is in een Europa een grondrecht, dat is verankerd in artikel 8 van het Handvest van de grondrechten van de Europese Unie en in artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU), en dient dan ook een overeenkomstig niveau van bescherming te krijgen.

Een gebrek aan vertrouwen zal consumenten doen aarzelen om online aankopen te doen en nieuwe vormen van dienstverlening te accepteren. Daarom is een hoog niveau van gegevensbescherming ook essentieel om het vertrouwen in onlinediensten te vergroten en het potentieel van de digitale economie te ontsluiten ten gunste van **de economische groei en het concurrentievermogen van het bedrijfsleven in de EU**.

Er is behoefte aan moderne, coherente regels in de gehele EU om het mogelijk te maken dat gegevens vrij van de ene lidstaat naar de andere kunnen stromen. Het bedrijfsleven heeft behoefte aan duidelijke en uniforme regels die rechtszekerheid verschaffen en de administratieve lasten tot een minimum beperken. Voor het functioneren van de eengemaakte markt en het **bevorderen van economische groei, werkgelegenheid en innovatie** is dit essentieel[2]. Een meer op de interne markt

---

1 De markt voor het analyseren van zeer grote pakketten gegevens groeit wereldwijd met 40% per jaar: http://www.mckinsey.com/mgi/publications/big_data/.

2 Zie ook de conclusies van de Europese Raad van 23 oktober 2011, waarin de "sleutelrol" van de eengemaakte markt bij het "genereren van groei en werkgelegenheid" wordt benadrukt, alsook de behoefte aan het voltooien van de digitale eengemaakte markt tegen 2015.

toegesneden modernisering van de EU-privacyregels, die individuele personen een hoog niveau van gegevensbescherming biedt en de rechtszekerheid, duidelijkheid en coherentie ten goede komt, is derhalve een kernaspect van het Stockholm-actieplan van de Europese Commissie[3] en van de Digitale Agenda voor Europa[4], en draagt meer in het algemeen bij aan de Europa 2020-groeistrategie[5] van de EU.

De EU-richtlijn van 1995[6], de centrale wettekst voor de bescherming van persoonsgegevens in Europa, was een mijlpaal in de geschiedenis van de gegevensbescherming. De doelstellingen ervan – de werking van de eengemaakte markt en een effectieve bescherming van de fundamentele rechten en vrijheden van natuurlijke personen waarborgen – gelden nog steeds. De richtlijn dateert echter van 17 jaar terug, toen het internet nog in de kinderschoenen stond. In de nieuwe digitale omgeving met zijn talrijke uitdagingen bieden de bestaande regels niet de vereiste mate van harmonisatie, noch maken zij het mogelijk om het recht op bescherming van persoonsgegevens doeltreffend te waarborgen. Daarom stelt de Europese Commissie nu een fundamentele hervorming van het EU-kader voor gegevensbescherming voor.

Daarenboven is bij het Verdrag van Lissabon, en met name artikel 16 VWEU, een nieuwe rechtsgrondslag gelegd voor een moderne, integrale benadering van gegevensbescherming en het vrij verkeer van persoonsgegevens, onder andere op het gebied van politiële en justitiële samenwerking in strafzaken[7]. Deze benadering is uiteengezet in de mededelingen van de Europese Commissie over het Stockholm-programma en het Stockholm-actieplan[8], waarin wordt benadrukt dat de Unie "een integrale regeling voor de bescherming van persoonsgegevens [moet] ontwikkelen die geldt voor alle bevoegdheidsgebieden van de Unie" en "ervoor [moet] zorgen dat het grondrecht op bescherming van de persoonlijke levenssfeer consequent wordt toegepast".

Om de hervorming van het EU-kader voor gegevensbescherming op een transparante manier voor te bereiden, houdt de Commissie sinds 2009 openbare raadplegingen over gegevensbescherming[9] en onderhoudt zij een intensieve dialoog met belanghebbende partijen[10]. Op 4 november 2010 presenteerde de Commissie de mededeling "Een integrale aanpak van de bescherming van persoonsgegevens in de

---

3 COM(2010) 171 definitief.

4 COM(2010) 245 definitief.

5 COM(2010) 2020 definitief.

6 Richtlijn 95/46/EG 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.

7 Specifieke regels voor de verwerking door de lidstaten op het gebied van het gemeenschappelijk buitenlands en veiligheidsbeleid zullen worden vastgesteld in een besluit van de Raad op grond van artikel 39 VEU.

8 Zie respectievelijk COM(2009) 262 en COM(2010) 171.

9 Er zijn twee openbare raadplegingen over de hervorming geweest: een eerste van juli tot december 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) en een tweede van november 2010 tot januari 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 In 2010 vond doelgericht overleg plaats met de autoriteiten van de lidstaten en particuliere belanghebbenden. In november 2010 organiseerde vicevoorzitter Reding een rondetafelconferentie over de hervorming. Daarnaast werden gedurende 2011 ook workshops en seminars gehouden over specifieke vraagstukken (zoals meldingen van inbreuken met betrekking tot gegevens).

Europese Unie"[11], waarin de grote thema's van de hervorming werden belicht. Van september tot december 2011 voerde de Commissie diepgaande gesprekken met de Europese nationale gegevensbeschermingsautoriteiten en met de Europese Toezichthouder voor gegevensbescherming om opties te verkennen voor een consistentere toepassing van de EU-gegevensbeschermingsregels in alle lidstaten van de EU[12].

Uit die gesprekken kwam duidelijk naar voren dat zowel burgers als bedrijven willen dat de Europese Commissie de EU-regelgeving grondig hervormt. Na verschillende beleidsopties te hebben afgewogen[13], stelt de Europese Commissie nu een **stevig en coherent wettelijk kader voor dat voor alle beleidsterreinen geldt, de rechten van personen en de internemarktdimensie van gegevensbescherming versterkt en de formaliteiten voor bedrijven drastisch vermindert**[14]. Het Commissievoorstel voor het nieuwe kader bestaat uit:

– een **verordening** (in de plaats van Richtlijn 95/46/EG) tot vaststelling van een algemeen EU-kader voor gegevensbescherming[15];

– en een **richtlijn** (in de plaats van Kaderbesluit 2008/977/JBZ[16]) houdende regels inzake de bescherming van persoonsgegevens die worden verwerkt voor het **voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten en aanverwante justitiële activiteiten**.

De belangrijkste onderdelen van de hervorming van het EU-kader voor gegevensbescherming worden in onderhavige mededeling uiteengezet.

2. MENSEN ZELF LATEN BEPALEN WAT ER MET HUN PERSOONSGEGEVENS GEBEURT

De wijze waarop individuele personen hun recht op gegevensbescherming uit hoofde van Richtlijn 95/46/EG – momenteel het belangrijkste instrument van gegevensbescherming in het EU-recht – kunnen doen gelden, is onvoldoende EU-breed geharmoniseerd. Evenmin zijn de bevoegdheden van de nationale

---

11 COM(2010) 609.

12 Zie de brief van EU-commissaris voor Justitie Viviane Reding van 19 september 2011 aan de leden van de Groep artikel 29 op http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 Zie de effectbeoordeling (SEC(2012)72.

14 Dit zal in een later stadium leiden tot overeenkomstige aanpassingen van specifieke en sectorale instrumenten, zoals Verordening (EG) nr. 45/2001, PB L 8 van 12.1.2001, blz. 1.

15 De verordening brengt ook een beperkt aantal technische aanpassingen van de e-privacyrichtlijn mee (Richtlijn 2002/58/EG, laatstelijk gewijzigd bij Richtlijn 2009/136/EG – PB L 337 van 18.12.2009, blz. 11) die het gevolg zijn van de omzetting van Richtlijn 95/46/EG in een verordening. Welke inhoudelijke juridische gevolgen de nieuwe verordening en richtlijn zullen hebben voor de e-privacyrichtlijn, zal te zijner tijd door de Commissie worden bekeken, rekening houdende met de uitkomst van de onderhandelingen met het Europees Parlement en de Raad over de huidige voorstellen.

16 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. Een verslag over de toepassing van het kaderbesluit door de lidstaten (COM(2012)12) is aangenomen als onderdeel van het hervormingspakket gegevensbescherming.

autoriteiten op dit gebied voldoende geharmoniseerd om een consistente en effectieve toepassing van de regels te waarborgen. Dit betekent dat het in de ene lidstaat moeilijker is om dit recht uit te oefenen dan in andere, in het bijzonder met betrekking tot onlinetoepassingen.

Dit heeft ook te maken met de ontzaglijke hoeveelheid gegevens die elke dag worden verzameld en met de onwetendheid daaromtrent van gebruikers. Niettegenstaande dat heel wat Europeanen vinden dat het verstrekken van persoonsgegevens meer en meer deel uitmaakt van het leven van vandaag[17], is 72% van de internetgebruikers de mening toegedaan dat zij online om te veel persoonlijke informatie worden gevraagd[18]. Zij vinden dat hun gegevens aan hun controle ontsnappen. Zij worden niet behoorlijk geïnformeerd over wat er met hun persoonsgegevens gebeurt, en aan wie en voor welke doeleinden deze worden doorgegeven. Vaak weten zij niet hoe zij hun rechten online kunnen doen gelden.

"Het recht om te worden vergeten"

Een Europees student, aangesloten bij een sociaal netwerk op internet, vraagt inzage in alle persoonsgegevens die bij het netwerk over hem zijn opgeslagen. Hij stelt daarbij vast dat het netwerk veel meer gegevens verzamelt dan hij zich realiseerde en dat sommige gegevens waarvan hij dacht dat ze gewist waren, nog altijd waren opgeslagen.

Door de hervorming van de EU-regels inzake gegevensbescherming zal dit onmogelijk worden, dankzij:

- een uitdrukkelijke verplichting voor sociale netwerken op internet (en alle andere voor de verwerking verantwoordelijken) om de hoeveelheid persoonsgegevens van gebruikers die zij verzamelen en verwerken, tot een minimum te beperken;

- een verplichting om niet-openbaarmaking van gegevens als standaardinstelling te gebruiken;

- een uitdrukkelijke verplichting voor voor de verwerking verantwoordelijken om persoonsgegevens te wissen als de betrokkene daar uitdrukkelijk om verzoekt en er geen gegronde reden is om de gegevens te bewaren.

In dit concrete geval zou de aanbieder van het sociaal netwerk verplicht zijn om de gegevens van de student onmiddellijk en volledig te wissen.

Zoals in de Digitale Agenda voor Europa is aangegeven, houdt bezorgdheid omtrent hun privacy mensen heel vaak tegen om goederen en diensten online te kopen. Gelet op de bijdrage van de sector informatie- en communicatietechnologie (ICT-sector) aan de totale productiviteitsgroei in Europa – 20% direct van de sector en 30% van ict-investeringen[19] – is vertrouwen in dergelijke diensten van cruciaal belang om de groei van de economie en de concurrentiekracht van het bedrijfsleven in de EU aan te zwengelen.

Melding van gegevenslekken

[17] Zie speciale Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union, juni 2011, blz. 23.

[18] Ibidem, blz. 54.

[19] Zie Digitale Agenda voor Europa, blz. 4.

Een gamingsite die op spelers in de EU mikt, is het slachtoffer geworden van hackers. Het doelwit waren gegevensbestanden met persoonsgegevens (namen, adressen en creditcardgegevens) van tientallen miljoenen gebruikers wereldwijd. Het bedrijf meldde het lek pas een week na de ontdekking aan de betrokken gamers.

Door de hervorming van de EU-regels inzake gegevensbescherming zal dit onmogelijk worden. De nieuwe regels zullen bedrijven verplichten om:

- hun beveiligingsmaatregelen ter voorkoming van lekken te verscherpen;

-gegevenslekken waar mogelijk binnen 24 uur na de ontdekking te melden aan de nationale gegevensbeschermingsautoriteit en aan de betrokken personen.

De nieuwe wetgevingshandelingen die de Commissie voorstelt, hebben tot doel de rechtsbescherming te versterken, mensen de beschikking te geven over doeltreffende middelen om zich ervan te verzekeren dat zij volledig geïnformeerd worden over wat er met hun persoonsgegevens gebeurt en hen in staat te stellen hun rechten effectiever uit te oefenen.

De nieuwe regels die de Commissie voorstelt om de privacybescherming te versterken, zijn erop gericht:

Personen meer controle over hun gegevens te geven, door:

- ervoor te zorgen dat, wanneer hun **toestemming** wordt gevraagd, die **uitdrukkelijk** en uit vrije wil **wordt gegeven, hetzij op basis van een verklaring, hetzij door middel van een ondubbelzinnige, actieve handeling door de betrokken persoon**;

- internetgebruikers daadwerkelijk **het recht** te geven **om te worden vergeten** door onlinetoepassingen, d.w.z. het recht om te eisen dat hun gegevens worden verwijderd als zij hun toestemming intrekken en er voor het overige geen gegronde redenen zijn om de gegevens te bewaren;

- een **vlotte toegang tot de eigen gegevens** te waarborgen, evenals een **recht op gegevensoverdraagbaarheid**, d.w.z. een recht om van de voor de verwerking verantwoordelijke een kopie van de opgeslagen gegevens te krijgen en de vrijheid om deze zonder belemmering van een dienstverlener naar een andere over te dragen;

- het **recht op informatie** uit te breiden, zodat individuele personen volledig zicht hebben op wat er met hun persoonsgegevens gebeurt, in het bijzonder wanneer het gaat om **kinderen**.

Personen betere middelen geven om hun rechten uit te oefenen, door:

- de **nationale gegevensbeschermingsautoriteiten onafhankelijker te maken en meer bevoegdheden te geven** om klachten effectief te behandelen en onderzoeken in te stellen, bindende besluiten te nemen en daadwerkelijk afschrikkende sancties op te leggen;

- de **administratieve en rechtsmiddelen** waarover zij beschikken **bij schendingen** van hun privacyrechten, te versterken. In het bijzonder zullen

geautoriseerde groeperingen namens individuele personen naar de rechter kunnen stappen.

De gegevens beter te beveiligen, door:

- het gebruik te stimuleren van **privacybevorderende technologieën** (die de privacy beschermen door de opslag van persoonsgegevens tot een minimum te beperken), **privacyvriendelijke standaardinstellingen** en **privacycertificeringsprogramma's**;

- aan voor de verwerking verantwoordelijken een **algemene verplichting**[20] op te leggen om **gegevenslekken zo spoedig mogelijk** (binnen 24 uur waar zulks mogelijk is) **te melden** aan de betrokken personen en aan de gegevensbeschermingsautoriteiten.

De verwerkers van gegevens verantwoordelijker te maken, met name door:

- voor de verwerking verantwoordelijken te verplichten een gegevensbeschermingsfunctionaris (**Data Protection Officer**) aan te wijzen in bedrijven met meer dan 250 werknemers of bedrijven die zich bezighouden met verwerkingsactiviteiten die vanwege hun aard, hun omvang of hun doel specifieke risico's voor de rechten en vrijheden van individuele personen meebrengen ("gevoelige activiteiten");

- het **"Privacy by Design"-beginsel** te introduceren, waardoor reeds vanaf de ontwerpfase privacywaarborgen in procedures en systemen worden geïntegreerd;

- organisaties die gevoelige gegevens verwerken te verplichten een **privacyeffectbeoordeling** te maken.

3. GEGEVENSBESCHERMINGSREGELS DIE GESCHIKT ZIJN VOOR DE DIGITALE EENGEMAAKTE MARKT

Niettegenstaande dat de huidige richtlijn tot doel heeft een gelijkwaardig beschermingsniveau in de EU tot stand te brengen, lopen de regels nog altijd aanzienlijk uiteen van de ene lidstaat tot de andere. Daardoor moeten voor de verwerking verantwoordelijken in sommige gevallen rekening houden met 27 verschillende nationale wet- en regelgevingen. Het resultaat is een **gefragmenteerde juridische omgeving**, met **rechtsonzekerheid** en ongelijke bescherming van individuele personen als gevolg. Voor bedrijven betekent dit **vermijdbare extra kosten en administratieve lasten**, en het weerhoudt hen ervan om hun activiteiten op de eengemaakte markt over de grenzen heen uit te breiden.

Ook inzake de middelen en bevoegdheden van de nationale autoriteiten op het gebied van gegevensbescherming zijn er aanzienlijke verschillen tussen de lidstaten[21]. In

[20] Deze verplichting geldt momenteel alleen in de telecommunicatiesector en vloeit voort uit de e-privacyrichtlijn.

[21] Voor meer bijzonderheden over dit aspect, zie de effectbeoordeling bij de wetgevingsvoorstellen, SEC(2012)72.

sommige gevallen kunnen zij hun handhavingstaken niet naar behoren vervullen. De samenwerking tussen deze autoriteiten op Europees niveau, via het bestaande raadgevend orgaan (de Groep artikel 29)[22], leidt niet altijd tot een consequente handhaving en is voor verbetering vatbaar.

Consequente handhaving van privacyregels in heel Europa

Een multinational met verschillende vestigingen in de EU heeft een "online mapping"-systeem over geheel Europa ontplooid, waarbij beelden worden verzameld van alle particuliere en openbare gebouwen en ook toevallige voorbijgangers kunnen worden gefotografeerd. In één lidstaat werd de opneming van niet onscherp gemaakte beelden van personen die zich er niet bewust van waren dat zij waren gefotografeerd onwettig geacht; in andere lidstaten was er geen schending van de privacywetgeving. De nationale gegevensbeschermingsautoriteiten reageerden met andere woorden niet op dezelfde manier op het probleem.

Door de hervorming van de EU-regels inzake gegevensbescherming zal dit onmogelijk worden, omdat:

- de privacyvoorschriften en –waarborgen zullen worden neergelegd in een EU-verordening, die overal in de Unie rechtstreeks toepasselijk is;

- enkel de gegevensbeschermingsautoriteit van het land waar het bedrijf zijn belangrijkste vestiging heeft, zal oordelen of het bedrijf de wetgeving eerbiedigt;

- snelle en effectieve coördinatie van het optreden van de nationale gegevensbeschermingsautoriteiten, gesteld dat de dienstverlening tot individuele personen in verschillende lidstaten is gericht, zal waarborgen dat de nieuwe EU-privacyregels op een coherente manier worden toegepast en gehandhaafd in alle lidstaten.

De nationale autoriteiten moeten beter worden uitgerust en intensiever samenwerken om een consequente handhaving en, uiteindelijk, uniforme toepassing van de regels in de gehele EU te waarborgen.

Een sterk, duidelijk en uniform wettelijk EU-kader zal helpen om het potentieel van de digitale eengemaakte markt te ontsluiten en de economische groei, innovatie en werkgelegenheid stimuleren. Een verordening zal een einde maken aan de juridische fragmentatie en belemmeringen om de markt te betreden wegnemen, wat vooral voor zeer kleine, kleine en middelgrote ondernemingen van belang is.

De nieuwe regels zullen bedrijven uit de EU eveneens een internationaal concurrentievoordeel bezorgen. Dankzij het herziene kader zullen zij hun klanten kunnen verzekeren dat waardevolle persoonlijke informatie met de nodige zorgvuldigheid wordt behandeld. Vertrouwen in een EU-breed samenhangend juridisch kader is een sterke troef voor dienstenaanbieders en een stimulans voor investeerders, die zich bij hun keuze van een vestigingsplaats voor hun diensten laten leiden door de beste omstandigheden.

[22] De Groep artikel 29 is opgericht in 1996 (bij artikel 29 van Richtlijn 95/46/EG) en heeft een adviserende taak; de groep is samengesteld uit vertegenwoordigers van de nationale toezichthoudende autoriteiten inzake gegevensbescherming, de Europese Toezichthouder voor gegevensbescherming en de Commissie. Voor nadere informatie over zijn werkzaamheden, zie http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

Ter versterking van de **internemarktdimensie van de gegevensbescherming** stelt de Commissie voor:

- de regels inzake bescherming van persoonsgegevens op EU-niveau neer te leggen in een **verordening die direct van toepassing is in alle lidstaten**[23], waardoor er een einde komt aan de cumulatieve, parallelle toepassing van verschillende nationale wetgevingen. Voor het **bedrijfsleven** zou dit betekenen dat **op jaarbasis**, **aan administratieve formaliteiten alleen,** netto **circa 2,3 miljard euro minder moet worden uitgegeven**;

- **de regelgeving te vereenvoudigen en drastisch te snoeien in het aantal formaliteiten**, zoals algemene kennisgevingen (nettobesparing op jaarbasis: 130 miljoen euro door minder administratieve lasten alleen). Vanwege het belang voor het concurrentievermogen van de Europese economie wordt bijzondere aandacht geschonken aan de specifieke behoeften van zeer kleine, kleine en middelgrote ondernemingen;

- **de onafhankelijkheid van nationale gegevensbeschermingsautoriteiten te vergroten en hun meer bevoegdheden te geven** om onderzoeken in te stellen, bindende beslissingen te nemen en effectieve, afschrikkende sancties op te leggen, en de lidstaten te verplichten hun daartoe **voldoende middelen** te geven;

- **in de EU een "éénloketsysteem" inzake gegevensbescherming op te zetten:** voor de verwerking verantwoordelijken in de EU zullen met slechts één gegevensbeschermingsautoriteit zaken doen, namelijk de gegevensbeschermingsautoriteit van de lidstaat waar de hoofdzetel is gevestigd;

- de voorwaarden te creëren voor een **vlotte en efficiënte samenwerking tussen gegevensbeschermingsautoriteiten**, zoals de verplichting voor de ene gegevensbeschermingsautoriteit om op verzoek van een andere onderzoeken en inspecties te verrichten en mekaars beslissingen te erkennen;

- een **conformiteitstoetsing** op EU-niveau op te zetten die moet waarborgen dat beslissingen van een gegevensbeschermingsautoriteit, die een ruimere Europese reikwijdte hebben, genomen worden met volledige inachtneming van het standpunt van andere betrokken gegevensbeschermingsautoriteiten en van de wet- en regelgeving van de Unie;

- de Groep artikel 29 op te waarderen tot een **onafhankelijk Europees Comité voor gegevensbescherming**, dat een grotere bijdrage levert aan een consequente toepassing van de privacywetgeving en een solide basis vormt voor samenwerking tussen gegevensbeschermingsautoriteiten, waaronder de Europese Toezichthouder voor gegevensbescherming, en het secretariaat van de Europese instantie voor gegevensbescherming te laten verzorgen door de Europese Toezichthouder voor gegevensbescherming, omwille van de synergetische en pragmatische effecten.

[23] Voorgesteld wordt de toepasselijke regels inzake de politiële en justitiële samenwerking in strafzaken (zie afdeling 4 hierna) neer te leggen in een richtlijn, wat de lidstaten op dit specifieke terrein meer flexibiliteit laat.

De nieuwe EU-verordening moet een robuste bescherming van het fundamenteel recht op bescherming van de persoonsgegevens overal in de Europese Unie waarborgen en de werking van de eengemaakte markt versterken. Terzelfdertijd zal zij - omdat het recht op bescherming van persoonsgegevens, zoals het Hof van Justitie heeft benadrukt[24], geen absolute gelding heeft, maar in relatie tot de functie ervan in de samenleving moet worden beschouwd[25] en moet worden afgewogen tegen andere fundamentele rechten, overeenkomstig het evenredigheidsbeginsel[26] - uitdrukkelijke bepalingen bevatten ter waarborging van andere grondrechten, zoals de vrijheid van meningsuiting en van informatie, het recht op verdediging, het beroepsgeheim (bv. voor juridische beroepen), met eerbiediging van de status van kerken volgens het recht van de lidstaten.

4. HET GEBRUIK VAN PERSOONSGEGEVENS IN HET KADER VAN POLITIËLE EN JUSTITIËLE SAMENWERKING IN STRAFZAKEN

De inwerkingtreding van het Verdrag van Lissabon, en met name de invoering van een nieuwe rechtsgrond (artikel 16 VWEU), maakt het mogelijk een alomvattend kader voor de bescherming van gegevens te creëren dat een hoog niveau van bescherming van persoonsgegevens waarborgt en terzelfdertijd tegemoet komt aan de bijzondere eisen van de politiële en justitiële samenwerking in strafzaken. In het bijzonder biedt dit de mogelijkheid om met het herziene EU-beschermingskader zowel grensoverschrijdende als binnenlandse verwerking van persoonsgegevens te bestrijken, wat de verschillen tussen de wetgevingen van de lidstaten zou verkleinen en de bescherming van persoonsgegevens in het algemeen ten goede zou komen. Dit kan eveneens bevorderlijk zijn voor de uitwisseling van informatie tussen de politiële en justitiële autoriteiten van de lidstaten en zodoende voor de samenwerking in de strijd tegen zware criminaliteit in Europa. De verwerking van gegevens door de politiële en justitiële autoriteiten in strafzaken wordt momenteel hoofdzakelijk geregeld door Kaderbesluit 2008/977/JBZ, dat dateert van voor de inwerkingtreding van het Verdrag van Lissabon. Omdat het om een kaderbesluit gaat, is de Commissie niet bevoegd voor de handhaving ervan, wat tot een ongelijke toepassing heeft geleid. Daarenboven is de werking van het kaderbesluit beperkt tot grensoverschrijdende verwerkingsactiviteiten[27], wat betekent dat persoonsgegevens die niet het voorwerp van uitwisseling zijn, momenteel niet onder EU-regels vallen die de verwerking ervan beheersen en het fundamentele recht op gegevensbescherming waarborgen. Dat geeft aanleiding tot een praktisch probleem

---

24 Arrest van het Hof van Justitie van de EU van 9.11.2011 in gevoegde zaken C-92/09 en C-93/09, Volker und Markus Schecke en Eifert [2010], nog niet gepubliceerd.

25 Artikel 52, lid 1, van het Handvest van de grondrechten bepaalt dat beperkingen op de uitoefening van het recht op gegevensbescherming bij wet moeten worden gesteld en de wezenlijke inhoud van die rechten en vrijheden moeten eerbiedigen, en dat, met inachtneming van het evenredigheidsbeginsel slechts beperkingen kunnen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

26 Hof van Justitie van de EU, arrest van 6.11.2003 in zaak C-101/01, Lindqvist, Jurispr. 2003 blz. I-12971, punten 82-90; arrest van 16.12.2008, C-73/07, Satamedia, Jurispr. 2008 blz. I-9831, punten 50-62.

27 Om preciezer te zijn, is het kaderbesluit van toepassing op persoonsgegevens die worden of zijn verstrekt of beschikbaar gesteld tussen de lidstaten of die worden uitgewisseld tussen lidstaten en instellingen of instanties van de EU (zie artikel 1, lid 2).

voor de politie en andere instanties, omdat het niet altijd duidelijk is of de gegevensverwerking louter binnenlands is of grensoverschrijdend, en evenmin te voorzien is of "binnenlandse" gegevens achteraf toch over de grenzen heen zullen worden uitgewisseld[28].

Het beoogde doel van een hervormd EU-gegevensbeschermingskader is daarom een consequent, hoog niveau van bescherming te verzekeren, **om het wederzijds vertrouwen van de politiële en justitiële autoriteiten te versterken, en zodoende het vrij verkeer van gegevens en een effectieve samenwerking tussen die autoriteiten te bevorderen**.

Om een hoog niveau van bescherming van persoonsgegevens op het gebied van de politiële en justitiële samenwerking in strafzaken te waarborgen en de uitwisseling van die gegevens tussen de bevoegde nationale autoriteiten te vergemakkelijken, stelt de Commissie als onderdeel van het hervormingspakket een richtlijn voor die:

- **de grondbeginselen voor de gegevensbescherming** toepast op politiële samenwerking en de justitiële samenwerking in strafzaken, zonder het specifieke karakter van deze terreinen uit het oog te verliezen[29];

- **geharmoniseerde minimumcriteria en –voorwaarden** vaststelt voor mogelijke beperkingen op de algemene regels. Dit betreft in het bijzonder inperking van het recht van individuele personen om in kennis te worden gesteld van het gebruik of de raadpleging van hun gegevens door de politiële en justitiële autoriteiten. Dergelijke beperkingen zijn noodzakelijk om strafbare feiten effectief te kunnen voorkomen, onderzoeken, opsporen of vervolgen;

- **specifieke regels** vaststelt **om rekening te houden met de bijzondere aard van rechtshandhaving**, waarbij bijvoorbeeld **een onderscheid wordt gemaakt tussen verschillende categorieën betrokkenen** van wie de rechten kunnen verschillen (zoals getuigen en verdachten).

5. GEGEVENSBESCHERMING IN EEN GEGLOBALISEERDE WERELD

De rechten van individuele personen moeten gevrijwaard blijven wanneer persoonsgegevens vanuit de EU naar derde landen worden overgedragen en wanneer individuele personen in de lidstaten het doelwit zijn van dienstenaanbieders uit derde landen en hun gegevens worden gebruikt of geanalyseerd door deze dienstenaanbieders. De EU-privacynormen moeten bijgevolg gelden ongeacht waar een bedrijf of zijn verwerkingseenheid is gevestigd.

In de geglobaliseerde wereld waarin wij leven, worden persoonsgegevens in toenemende mate over virtuele en geografische grenzen heen verzonden en opgeslagen op servers in verschillende landen. Er zijn steeds meer bedrijven die

[28] Diverse lidstaten hebben zulks effectief vermeld in hun antwoord op de vragenlijst van de Commissie voor het verslag over de toepassing van het kaderbesluit (COM(2012) 12.

[29] Zie de Verklaring nr. 21 betreffende de bescherming van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en op het gebied van politiële samenwerking, gehecht aan de slotakte van de intergouvernementele conferentie die het Verdrag van Lissabon heeft aangenomen.

cloud computing-diensten aanbieden, dat zijn diensten waarbij klanten gegevens op afstand kunnen opslaan en raadplegen. Deze factoren nopen ertoe de huidige mechanismen voor de overdracht van gegevens naar derde landen aan te scherpen. Dit moet gebeuren door middel van adequaatheidsbesluiten, d.w.z. besluiten dat de gegevensbeschermingsstandaarden in derde landen van een "adequaat" niveau zijn, en van passende garanties zoals standaardcontractbepalingen of bindende bedrijfsvoorschriften[30], om een hoog niveau van gegevensbescherming bij internationale be- en verwerkingen te waarborgen en het grensoverschrijdend gegevensverkeer te vergemakkelijken.

Bindende bedrijfsvoorschriften

Een bedrijfsconcern moet regelmatig persoonsgegevens van zijn dochterondernemingen in de EU overdragen naar dochterondernemingen in derde landen. Het concern wil graag een stel bindende bedrijfsvoorschriften invoeren om aan de EU-regels te voldoen en terzelfdertijd de administratieve formaliteiten voor elke afzonderlijke overdracht te beperken. De bindende bedrijfsvoorschriften zorgen er in de praktijk voor dat binnen het concern één enkel stel voorschriften geldt, in plaats van verschillende interne contracten.

De huidige, binnen de Groep artikel 29 overeengekomen praktijk is, dat voor de erkenning van het adequate beschermingsniveau van bindende bedrijfsvoorschriften een grondige beoordeling door drie gegevensbeschermingsautoriteiten vereist is (één hoofdbeoordelaar en twee medebeoordelaars); andere gegevensbeschermingsautoriteiten mogen hun opmerkingen kenbaar maken. In heel wat lidstaten is overigens een additionele nationale erkenning nodig om overdrachten te doen op basis van bindende bedrijfsvoorschriften, wat de vaststelling van deze laatste omslachtig, duur, tijdrovend en ingewikkeld maakt.

Na de hervorming:

- zal dit proces eenvoudiger en gestroomlijnder zijn;

- zullen bindende bedrijfsvoorschriften gevalideerd kunnen worden door slechts één gegevensbeschermingsautoriteit en zullen er mechanismen zijn om andere belanghebbende gegevensbeschermingsautoriteiten daar snel bij te betrekken;

- zullen bindende bedrijfsvoorschriften, nadat zij door één autoriteit zijn goedgekeurd, geldig zijn in de gehele EU zonder dat additionele nationale erkenningen vereist zijn.

In het licht van **de globalisering en de risico's die deze meebrengt**, zijn – met name voor wereldwijd opererende bedrijven - flexibele instrumenten en procedures nodig, die individuele personen een bescherming zonder "mazen" bieden. De Commissie stelt in dat verband het volgende voor:

- **duidelijke regels** die bepalen **wanneer de EU-wetgeving van toepassing is op voor de verwerking verantwoordelijken die in derde landen zijn gevestigd**, in het bijzonder dat wanneer goederen en diensten aan individuele personen in de EU

[30] Bindende bedrijfsvoorschriften zijn gedragscodes die gebaseerd zijn op door ten minste één gegevensbeschermingsautoriteit goedgekeurde Europese normen inzake gegevensbescherming. Ze worden door multinationale organisaties vrijwillig opgesteld en nageleefd om passende waarborgen te bieden ten aanzien van categorieën van doorgiften van persoonsgegevens tussen ondernemingen die deel uitmaken van hetzelfde concern en die door die bedrijfsvoorschriften gebonden zijn. Ze worden niet uitdrukkelijk behandeld in Richtlijn 95/46/EG, maar zijn het praktische resultaat van de samenwerking tussen GBA's en genieten de steun van de Groep artikel 29.

worden aangeboden en in alle gevallen waarin hun gedragingen worden gevolgd, de **Europese regels van toepassing zijn**;

- alle **besluiten betreffende de adequaatheid** van de bescherming worden door de Europese Commissie genomen op basis van expliciet en duidelijk geformuleerde criteria, ook op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken;

- het geoorloofd gegevensverkeer met derde landen gemakkelijker te maken door aanscherping en vereenvoudiging van de **regels inzake internationale overdrachten** naar landen waarvoor geen adequaatheidsbesluit is genomen, in het bijzonder door het gebruik van instrumenten zoals **bindende bedrijfsvoorschriften** te stroomlijnen en uit te breiden, zodat deze ook kunnen worden toegepast door **gegevensverwerkers** en binnen **bedrijfsconcerns**, gezien het toenemende aantal bedrijven dat aan gegevensverwerking doet, vooral in het kader van cloud computing;

- de **dialoog** aangaan en eventueel **onderhandelingen** aanknopen met derde landen, in het bijzonder strategische partners van de EU en de landen van het Europees nabuurschapsbeleid, en betrokken internationale organisaties (zoals de Raad van Europa, de Organisatie voor Economische Samenwerking en Ontwikkeling, de Verenigde Naties) om **het gebruik van strenge, interoperabele gegevensbeschermingsnormen wereldwijd te bevorderen**.

6. SLOTOPMERKINGEN

Met de hervorming van de EU-gegevensbeschermingsregels wordt ernaar gestreefd een **modern, krachtig, consequent en alomvattend kader voor de Europese Unie** tot stand te brengen. Het fundamentele recht van individuele personen op bescherming van hun gegevens wordt versterkt. Andere grondrechten, zoals de vrijheid van meningsuiting en van informatie, de rechten van het kind, het recht op vrij ondernemerschap, het recht op een eerlijk proces, het beroepsgeheim (bv. voor juridische beroepen), en de status van kerken volgens het recht van de lidstaten worden geëerbiedigd.

De hervorming moet in de eerste plaats ten goede komen aan individuele personen, om hun rechten op bescherming uit te breiden en hun vertrouwen in de digitale omgeving te vergroten. Voorts moet zij het rechtskader voor het bedrijfsleven en de publieke sector aanzienlijk vereenvoudigen. Het is de bedoeling de ontwikkeling van de digitale economie op de eengemaakte EU-markt en daarbuiten te stimuleren, overeenkomstig de doelstellingen van de Europa 2020-strategie en de Digitale Agenda voor Europa. Tot slot moet de hervorming het wederzijdse vertrouwen van rechtshandhavingsautoriteiten versterken om de onderlinge uitwisseling van gegevens en de samenwerking in de strijd tegen zware criminaliteit te bevorderen, zonder het hoge beschermingsniveau voor individuele personen aan te tasten.

De Europese Commissie zal intensief met het Europees Parlement en de Raad samenwerken om tegen eind 2012 een akkoord over het nieuwe EU-kader voor gegevensbescherming te bereiken. Gedurende dit proces en daarna, vooral bij de tenuitvoerlegging van de nieuwe wetshandelingen, zal de Commissie **nauw en op**

een transparante manier een dialoog voeren met alle belanghebbenden, onder anderen vertegenwoordigers van de particuliere en publieke sectoren. Daarbij kan worden gedacht aan vertegenwoordigers van politie en justitie, regelgevende instanties op het gebied van elektronische communicatie, maatschappelijke organisaties, gegevensbeschermingsautoriteiten en academici, en vertegenwoordigers van gespecialiseerde EU-agentschappen zoals Eurojust, Europol, het Bureau voor de grondrechten en het Europees Agentschap voor netwerk- en informatiebeveiliging.

In een context waarin informatietechnologieën en maatschappelijke gedragingen voortdurend evolueren, is een dergelijke dialoog van het allergrootste belang om de vereiste input te krijgen voor een hoog beschermingsniveau van persoonsgegevens, de groei en het concurrentievermogen van het bedrijfsleven in de EU, het effectief functioneren van de overheid (o.a. politie en justitie) en een verlichting van de administratieve lasten.