

Herziening regelgevend kader bescherming persoonsgegevens (uitgebreide samenvatting)

Inleiding

De Richtlijn bescherming persoonsgegevens van 1995 was een mijlpaal in de geschiedenis van de dataprotectie, maar deze richtlijn werd vastgesteld toen het Internet nog in de kinderschoenen stond. De Europese Commissie constateert daarom dat de huidige richtlijn, ondanks het feit dat haar algemene beginselen geldig blijven, verouderd is. De toen vastgestelde regels missen het vereiste niveau van harmonisatie en efficiency om het recht op bescherming van persoonsgegevens te waarborgen in de uitdagende digitale omgeving van vandaag. De Europese Commissie stelt daarom een nieuw regelgevend kader voor dat de rechten van individuen versterkt, de dimensie van de interne markt vergroot en administratieve lasten voor ondernemingen beperkt. Het nieuwe kader, gebaseerd op artikel 16 van het EU-Werkingsverdrag, bestaat uit:

- Een verordening, die Richtlijn 95/46/EG vervangt en een algemeen EU-kader bevat voor de bescherming van persoonsgegevens;
- Een richtlijn, die Kaderbesluit 2008/977/JBZ vervangt en regels bevat voor de bescherming van persoonsgegevens die worden verwerkt in het kader van politieke en justitiële activiteiten.

Controle van individuen over hun persoonsgegevens

Versterking van de rechten van individuen geschiedt door een reeks nieuwe maatregelen. De Europese Commissie streeft onder meer de verbetering na van de mogelijkheden voor individuen om de controle te houden over hun persoonsgegevens. Dit doet zij door:

- te verzekeren dat toestemming voor de verwerking van persoonsgegevens expliciet en vrijwillig wordt gegeven;
- introductie van een effectief *recht om vergeten te worden* in een online omgeving. Dit houdt in dat gebruikers een recht hebben op volledige verwijdering van hun persoonsgegevens indien zij hun toestemming intrekken en er geen andere legitieme redenen zijn om de data te bewaren;
- een gemakkelijke toegang tot de eigen persoonsgegevens te verzekeren, alsmede een recht op 'dataportabiliteit' (de vrijheid om data van de ene naar de andere dienstverlener mee te nemen);
- versterking van het recht op informatie over de wijze waarop persoonsgegevens (met name van kinderen) worden verwerkt.

Daarnaast zet de Europese Commissie in op verbetering van de mogelijkheden voor individuen om hun rechten uit te oefenen. Dit doet zij door:

- de onafhankelijkheid en bevoegdheden van nationale toezichthouders voor gegevensbescherming te versterken;

- de administratieve en juridische (rechts)middelen te verbeteren in gevallen van schending van gegevensbeschermingsrechten.

Ook het vergroten van de databeveiliging is een belangrijk streven van de Europese Commissie. Dit doet zij door:

- het gebruik van 'privacy enhancing' technologieën, van privacyvriendelijke standaardinstellingen en van programma's van privacycertificaten aan te moedigen;
- een algemene verplichting in te voeren om zogenaamde datalekken ongewild te melden bij de toezichthouder en bij de betrokken individuen.

Een ander belangrijk aspect van de Commissieplannen is vergroting van de verantwoordelijkheid van degenen die data verwerken. Dit geschiedt door:

- een verplichte functionaris voor gegevensbescherming (Data Protection Officer) in bepaalde grotere bedrijven of bedrijven die aan 'risky processing' doen;
- introductie van het 'privacy by design' principe;
- een verplichting voor bedrijven die betrokken zijn bij 'risky processing' om een *Data Protection Impact Assessment* uit te voeren.

Gegevensbeschermingsrecht geschikt voor de digitale interne markt

De huidige richtlijn uit 1995 is niet in staat eenzelfde niveau van gegevensbescherming in alle EU-lidstaten te verzekeren. Het feit dat er aanzienlijke verschillen tussen de lidstaten kunnen zijn, leidt tot rechtsonzekerheid, onnodige kosten en administratieve lasten. Ook de middelen en bevoegdheden van nationale toezichthouders zijn verre van geharmoniseerd. Om de dimensie van de interne markt te vergroten en administratieve lasten te verlichten, stelt de Europese Commissie de volgende maatregelen voor:

- De regels voor gegevensbescherming worden vastgelegd in een verordening in plaats van in een richtlijn (met uitzondering van de regels voor politie en justitie). Een verordening is rechtstreeks toepasselijk in alle lidstaten, wat een einde maakt aan verschillende nationale regimes voor gegevensbescherming;
- Een drastische inkrimping van de bestaande administratieve rompslomp en formaliteiten;
- De reeds genoemde versterking van de onafhankelijkheid en bevoegdheden van nationale toezichthouders voor gegevensbescherming. Deze moeten ook voldoende middelen krijgen om hun taken effectief uit te oefenen;
- Introductie van een 'one-stop-shop' systeem voor gegevensbescherming in de gehele Europese Unie. Dit houdt in dat bedrijven met vestigingen in meerdere lidstaten te maken hebben met slechts één toezichthouder, namelijk de toezichthouder van de lidstaat waar het bedrijf zijn hoofdkantoor heeft;
- Het creëren van de voorwaarden voor snelle en efficiënte samenwerking tussen toezichthouders voor gegevensbescherming;

- Het opzetten van een 'consistency mechanism' om te verzekeren dat beslissingen van toezichthouders voor gegevensbescherming met een bredere Europese impact kennisnemen van de gedachten van andere toezichthouders en volledig in overeenstemming zijn met EU-recht;
- Het upgraden van de Artikel 29 Werkgroep naar een onafhankelijke *European Data Protection Board*.

Politie en justitie

De verwerking van persoonsgegevens door politie en justitie wordt momenteel bestreken door Kaderbesluit 2008/977/JBZ. Dit kaderbesluit is niet op dezelfde wijze geïmplementeerd in alle lidstaten en is bovendien beperkt tot grensoverschrijdende verwerking van persoonsgegevens. Zuiver binnenlandse verwerking valt er dus niet onder. Om een hoog niveau van gegevensbescherming te verzekeren op het terrein van politie en justitie en om de uitwisseling van persoonsgegevens tussen de verschillende autoriteiten te vergemakkelijken doet de Europese Commissie een voorstel voor een richtlijn. Deze richtlijn past de algemene beginselen van gegevensbescherming toe op politieke en justitiële samenwerking in strafzaken, daarbij rekening houdend met de specifieke aard van deze terreinen.

Bescherming van persoonsgegevens en globalisatie

Het nieuwe regelgevende kader houdt tevens rekening met de uitdagingen van de globalisering en met wereldwijd opererende bedrijven. Het is het streven van de Europese Commissie tegen het einde van 2012 een akkoord te bereiken met het Europees Parlement en de Raad.

Voorstel voor een verordening bescherming persoonsgegevens

Het voorstel voor een verordening is als volgt opgebouwd:

- *Hoofdstuk 1* bevat algemene bepalingen. In dit hoofdstuk worden onder meer (**artikel 4**) definities gegevens van de begrippen die in de verordening worden gebruikt.
- *Hoofdstuk 2* gaat in op de beginselen van de verordening. Hier vinden we onder meer de criteria voor rechtmatige verwerking van persoonsgegevens (**artikel 6**) en een verbod op de verwerking van bepaalde categorieën persoonsgegevens (**artikel 9**).
- *Hoofdstuk 3* betreft de rechten van een 'data subject'. Hier wordt onder meer het recht van het individu om vergeten te worden vastgelegd (**artikel 17**), alsmede het recht op 'dataportabiliteit' (**artikel 18**). Ook vindt men hier het recht om niet onderworpen te worden aan maatregelen gebaseerd op 'profiling' (**artikel 20**).
- *Hoofdstuk 4* heeft betrekking op de verantwoordelijke voor en de bewerker van de persoonsgegevens. Het hoofdstuk ziet onder meer op de verplichting datalekken te melden (**artikel 31-32**), de verplichting om bij 'risky processing' een *Data Protec-*

tion Impact Assessment uit te voeren (**artikel 33**) en de verplichte functionaris voor gegevensbescherming (Data Protection Officer; **artikel 35**).

- *Hoofdstuk 5* betreft de overdracht van persoonsgegevens aan derde landen of internationale organisaties.
- *Hoofdstuk 6* waarborgt de aanwezigheid van onafhankelijke toezichthouders voor gegevensbescherming en regelt hun bevoegdheden. Wanneer een verantwoordelijke of een bewerker in verschillende lidstaten is gevestigd, geldt een 'one-stop-shop' systeem (**artikel 51**).
- *Hoofdstuk 7* gaat in op de samenwerking van de toezichthouders en de introductie van een 'consistency mechanism'. Ook de oprichting van de onafhankelijk *European Data Protection Board* wordt hier geregeld (**artikel 64 e.v.**). Dit bestaat uit de directeuren van de nationale toezichthouders en de European Data Protection Supervisor. De nieuwe instelling vervangt de Artikel 29 Werkgroep.
- *Hoofdstuk 8* betreft rechtsmiddelen, aansprakelijkheid en sancties.
- *Hoofdstuk 9* bevat bepalingen over bepaalde specifieke situaties van verwerking van persoonsgegevens, zoals verwerking van gezondheidsgegevens (**artikel 81**), verwerking in de context van werkgelegenheid (**artikel 82**) en verwerking voor historisch, statistisch en wetenschappelijk onderzoek (**artikel 83**).
- *Hoofdstuk 10* en *hoofdstuk 11* hebben betrekking op gedelegeerde regelgeving en op de slotbepalingen van de verordening.

Voorstel voor een richtlijn bescherming persoonsgegevens in de context van politie en justitie

De richtlijn bescherming persoonsgegevens uit 1995 is in de loop der jaren aangevuld door diverse instrumenten die specifieke regels bevatten voor de bescherming van persoonsgegevens op het terrein van politieke en justitiële samenwerking in strafzaken (de voormalige derde pijler). Een van de belangrijkste instrumenten is Kaderbesluit 2008/977/JBZ. Dit kaderbesluit heeft een beperkte reikwijdte, aangezien het alleen van toepassing is op grensoverschrijdende verwerking van persoonsgegevens en dus niet op puur binnenlandse aangelegenheden. Met het onderhavige voorstel trekt de Europese Commissie het kaderbesluit in en doet zij een voorstel voor een nieuwe richtlijn. Het voorstel is als volgt opgebouwd:

- *Hoofdstuk 1* bevat algemene bepalingen. In dit hoofdstuk is ook vastgelegd dat de reikwijdte van de richtlijn niet beperkt is tot grensoverschrijdende verwerking van persoonsgegevens, maar van toepassing is op iedere verwerking door een bevoegde (rechtshandavings)autoriteit (**artikel 2**).
- *Hoofdstuk 2* heeft betrekking op de algemene beginselen van de richtlijn. Hier wordt onder meer geregeld onder welke voorwaarden de verwerking van persoonsgegevens rechtmatig is (**artikel 7**).
- *Hoofdstuk 3* regelt de rechten van een 'data subject' en gaat onder meer in op het recht op toegang tot, rectificatie van en het wissen van persoonsgegevens.
- *Hoofdstuk 4* heeft betrekking op de verantwoordelijke voor en de bewerker van de persoonsgegevens.

- *Hoofdstuk 5* staat in het teken van de overdracht van persoonsgegevens aan derde landen of internationale organisaties en bepaalt de voorwaarden waaronder zo'n overdracht plaats kan vinden.
- *Hoofdstuk 6* waarborgt de aanwezigheid van onafhankelijke toezichthouders voor gegevensbescherming en regelt hun bevoegdheden.
- *Hoofdstuk 7* bevat regels over de samenwerking tussen de toezichthouders en over de taak van het, op grond van de verordening inzake de bescherming van persoonsgegevens ingestelde, *European Data Protection Board*.
- *Hoofdstuk 8* betreft rechtsmiddelen, aansprakelijkheid en sancties.
- *Hoofdstuk 9* en *hoofdstuk 10* hebben betrekking op gedelegeerde regelgeving en op de slotbepalingen van de richtlijn.