

Vergaderjaar 2012–2013

**33 169**

## **EU-voorstel: Richtlijn bescherming persoonsgegevens bij gebruik door politieke en justitiële autoriteiten (COM(2012) 10) en EU-voorstel Verordening algemeen kader bescherming persoonsgegevens (COM(2012)11)**

**E**

### **VERSLAG VAN EEN SCHRIFTELIJK OVERLEG**

Vastgesteld 12 december 2012

De staatssecretaris van Veiligheid en Justitie heeft bij brief van 23 oktober 2012<sup>1</sup> de Eerste Kamer geïnformeerd over de onderhandelings-ronden die in juni, juli en september 2012 hebben plaatsgevonden over de algemene verordening gegevensbescherming<sup>2</sup> en de richtlijn gegevensbescherming opsporing en vervolging.<sup>3</sup> Naar aanleiding hiervan hebben de vaste commissies voor Immigratie & Asiel / JBZ-raad<sup>4</sup> en voor Veiligheid en Justitie<sup>5</sup> de staatssecretaris van Veiligheid en Justitie op 23 november 2012 een brief gestuurd.

De staatssecretaris heeft op 11 december 2012 gereageerd.

De commissies brengen bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier voor dit verslag,  
Kim van Dooren

<sup>1</sup> Kamerstukken I 2012/13, 33 169, D.

<sup>2</sup> COM(2012)11; dossier **E120003** op [www.europapoort.nl](http://www.europapoort.nl)

<sup>3</sup> COM(2012)10; dossier **E120004** op [www.europapoort.nl](http://www.europapoort.nl)

<sup>4</sup> Samenstelling Immigratie en Asiel / JBZ-Raad:

Holdijk (SGP), Broekers-Knol (VVD), Slagter-Roukema (SP), Franken (CDA), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), Duthler (VVD), Koffeman (PvdD), Kuiper (CU), Meurs (PvdA) (*voorzitter*), Quik-Schuijt (SP), Strik (GL), Lokin-Sassen (CDA), Scholten (D66), Th. de Graaf (D66), De Boer (GL), De Lange (OSF), Ter Horst (PvdA), Beuving (PvdA), Schrijver (PvdA), M. de Graaff (PVV) (*vice-voorzitter*), Reynaers (PVV), Popken (PVV), Huijbregt-Schiedon (VVD), Schouwenaar (VVD), Swagerman (VVD)

<sup>5</sup> Samenstelling Veiligheid en Justitie:  
Holdijk (SGP), Broekers-Knol (VVD) (*voorzitter*), Kneppers-Heijner (VVD), Kox (SP), Engels (D66), Franken (CDA), Thissen (GL), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA) (*vice-voorzitter*), Duthler (VVD), Koffeman (PvdD), Kuiper (CU), Quik-Schuijt (SP), Strik (GL), K.G. de Vries (PvdA), Knip (VVD), Hoekstra (CDA), Lokin-Sassen (CDA), Scholten (D66), De Boer (GL), De Lange (OSF), Ter Horst (PvdA), Beuving (PvdA), Kooie (PvdA), Schrijver (PvdA), Reynaers (PVV), Popken (PVV), Frijters-Klijnen (PVV), Swagerman (VVD)

## BRIEF AAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Den Haag, 23 november 2012

Bij brief van 23 oktober 2012<sup>1</sup> heeft de staatssecretaris van Veiligheid en Justitie de Eerste Kamer geïnformeerd over de onderhandelingsronden die in juni, juli en september 2012 hebben plaatsgevonden over de algemene verordening gegevensbescherming<sup>2</sup> en de richtlijn gegevensbescherming opsporing en vervolging.<sup>3</sup> Dit verslag geeft de commissies voor Immigratie & Asiel / JBZ-raad en voor Veiligheid en Justitie aanleiding om de volgende vragen te stellen.

1. Volgens de Nederlandse regering is artikel 11 van de ontwerpverordening zeer algemeen geformuleerd. Dit artikel bepaalt dat het privacybeleid en de uitoefening van de rechten van betrokkenen transparant en eenvoudig toegankelijk dienen te zijn. Het komt de commissies voor dat het juist onwenselijk is om de tekst meer specifiek te formuleren. Met een algemene formulering wordt immers ruimte gelaten om de invulling van deze bepaling te differentiëren naar aard en omvang van de activiteiten van een organisatie.

2. Artikel 20, tweede lid, van de ontwerpverordening regelt de voorwaarden waaronder profilering toegestaan wordt. Volgens de Nederlandse regering is deze bepaling te onbepaald en zij pleit daarom voor een gesloten lijst van profileringen. De commissies plaatsen hier vraagtekens bij. Het is immers niet op voorhand vast te stellen welke concrete profileringen in de toekomst mogelijk zullen zijn. Met de opstelling van de Nederlandse regering worden toekomstige profileringen die nu nog niet te voorzien zijn, maar wel nadere regulering behoeven, buiten bereik van dit artikel gehouden. De commissies achten dit onwenselijk.

3. De commissies onderstrepen het belang van het accountabilitybeginsel zoals dat in artikel 22 van de ontwerpverordening is verwoord. Het biedt helderheid aan verantwoordelijken en daarmee rechtszekerheid. Hoe stelt de Nederlandse regering zich een risicogerichte benadering concreet voor? De risicoverschillen tussen verwerkingen en de maatregelen die dienovereenkomstig getroffen zullen worden, zullen in het privacybeleid van een organisatie vanzelf tot uitdrukking komen. Daar is nu juist het privacybeleid voor bedoeld. De commissies zijn er wel voorstander van om eventuele uitzonderingen te maken voor kleine ondernemingen.

4. De commissies zijn het niet met de Nederlandse regering eens dat de inhoud van artikel 23 van de ontwerpverordening wordt afgedekt door de artikelen 14, 22 en 30. *Privacy by design en privacy by default* zijn weliswaar vormen van beveiliging, maar het treffen van passende technische en organisatorische maatregelen houdt niet altijd het toepassen van de principes *privacy by design en default* in. Door al in de ontwerpfase van een systeem rekening te houden met de eisen die privacywetgeving stelt (en de wet in het systeem te bouwen in plaats van de wet toe te passen op het systeem), wordt voorkomen dat systemen worden ontwikkeld die onvoldoende privacybescherming bieden. Het principe dat wat technisch afgedwongen kan worden, ook technisch afgedwongen moet worden, onderschrijven de commissies. Zij zijn dan ook een voorstander van het opnemen van de eisen van *privacy by design en default* in artikel 23 van de voorgestelde verordening. Zouden deze eisen niet expliciet in de verordening worden opgenomen, dan worden noch de industrie, noch de verantwoordelijken genoeg gestimuleerd om

---

<sup>1</sup> Kamerstukken I 2012/13, 33 169, D.

<sup>2</sup> COM(2012)11; dossier **E120003** op [www.europapoort.nl](http://www.europapoort.nl)

<sup>3</sup> COM(2012)10; dossier **E120004** op [www.europapoort.nl](http://www.europapoort.nl)

hun systemen zodanig te ontwikkelen en in te richten dat de privacybescherming van betrokkenen zo optimaal mogelijk is.

5. Nederland is er voorstander van de rechtsverhouding tussen verantwoordelijke en verwerker niet alleen op privaatrechtelijke grondslag te stellen, maar ook – met het oog op de publieke sector – in algemeen verbindende voorschriften te regelen. De commissies begrijpen deze opstelling niet. Wat is de meerwaarde hiervan? In welk opzicht schieten de bewerkersovereenkomsten die nu op grond van de geldende richtlijn en de Wet bescherming persoonsgegevens worden gesloten tekort?

6. Nederland heeft op 20 september 2012 een lijst van schriftelijke voorstellen aan het Raadssecretariaat gezonden, aldus de brief van 23 oktober. De commissies ontvangen graag een afschrift van deze lijst.

7. De commissies zijn het met de Nederlandse regering eens dat het wenselijk zou zijn om de verantwoordelijke te verplichten in contractvoorwaarden expliciete beveiligingsverplichtingen op te nemen. Ook onderschrijven zij het Nederlandse standpunt om de aanzetten voor een risicogerichte benadering van beveiligingsvraagstukken in artikel 30 beter uit te werken.

8. Nederland heeft bezwaar gemaakt tegen de verplichting een *privacy impact assessment* uit te voeren in geval van bewaking van openbaar toegankelijke ruimten met camera's. De commissies achten deze verplichting wel degelijk zinvol. Op deze manier kunnen aantoonbaar weloverwogen besluiten worden genomen om dergelijke camera's al of niet op te hangen en de beelden voor bepaalde doeleinden te gebruiken, te verwerken en te bewaren. De commissies ontvangen graag een reactie op dit standpunt.

9. Ten aanzien van de meldplicht datalekken, zoals vastgelegd in artikel 31 van de betreffende ontwerpverordening, hebben de commissies een tweetal vragen. Het eerste punt betreft de reikwijdte van de meldplicht. De commissies vernemen graag hoe de regering aankijkt tegen een algemene meldplicht versus een selectieve meldplicht waarbij objectieve criteria worden gehanteerd. Hoe voorkomt de regering een eventuele onredelijke toename van gepaard gaande administratieve lasten, in het bijzonder voor het bedrijfsleven? Graag willen de commissies hierbij de aantekening plaatsen dat het College Bescherming Persoonsgegevens (CBP) reeds heeft aangegeven geen capaciteit te hebben voor de verwerking van alle meldingen onder een algemene meldplicht.

De commissies constateren ten slotte nogmaals dat de beide voorstellen onderdeel zijn van één pakket dat strekt tot herziening van de regels voor de bescherming van persoonsgegevens binnen de Europese Unie. Ongeacht de vraag of het beter was om de beide voorstellen te integreren in één voorstel, hechten de commissies er grote waarde aan dat de bepalingen van beide voorstellen in ieder geval gelijktijdig in werking treden. Kan de regering toezeggen zich hiertoe tot het uiterste in te spannen? Zo nee, waarom niet? In de ogen van de commissies kan het ene voorstel zonder het andere onmogelijk volledig tot uiting komen. Hiervoor is de onderlinge samenhang te groot.

De commissies zien met belangstelling uit naar uw reactie op hun vragen en opmerkingen en ontvangen deze graag binnen **vier weken** na dagtekening van deze brief.

De voorzitter van de commissie voor Immigratie & Asiel / JBZ-raad,  
P.L. Meurs

De voorzitter van de commissie voor Veiligheid en Justitie,  
A. Broekers-Knol

## BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 11 december 2012

Bij brief van 23 november 2012, no. 151503.01u, hebben de Voorzitters van de Vaste Commissies voor Immigratie & Asiel/JBZ-raad en voor Veiligheid en Justitie enige vragen gesteld naar aanleiding van mijn brief van 23 oktober 2012 (Kamerstukken I 2012/13, 33 169, D) met betrekking tot de ontwerpverordening gegevensbescherming en de ontwerprichtlijn gegevensbescherming opsporing en vervolging. Ik dank de beide voorzitters voor deze vragen. Hieronder treft u de antwoorden aan.

1. Artikel 11 van ontwerpverordening bevat met name in het eerste lid enige zeer algemeen geformuleerde voorschriften met betrekking tot de openheid en de toegankelijkheid van het beleid dat de verantwoordelijke moet voeren bij de verwerking van persoonsgegevens en de wijze waarop hij inhoud geeft aan zijn beleid om de betrokkenen in staat te stellen hun rechten onder de verordening uit te oefenen. Met het achterliggende accountabilitybeginsel ben ik het graag eens. Maar de formulering van dit artikel is aanzienlijk algemener van aard dan de formulering van de kernbepalingen van richtlijn 95/46/EG, de bestaande privacyrichtlijn. Op die bepalingen bestaat vanwege het algemene karakter en het beweerdelijke gebrek aan houvast voor de uitvoeringspraktijk al veel kritiek. Artikel 11, eerste lid, is opgenomen in een ontwerpverordening en daarmee te zijner tijd een rechtstreeks werkende bepaling. De overtreding daarvan is krachtens artikel 79, vijfde lid, van de ontwerpverordening met een hoge bestuurlijke boete van maximaal € 500 000,= bedreigd. Uit artikel 7, eerste lid, van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) en artikel 49, eerste lid, van het Handvest voor de Grondrechten vloeit voort dat de sanctionering van overtredingen slechts dan gerechtvaardigd is wanneer de overtreden norm voldoende duidelijk is geformuleerd. Daarvan kan bij de desbetreffende bepaling moeilijk worden gesproken. Het is geheel aan de verantwoordelijke gelaten hoe hij daaraan – voor eigen rekening en risico – inhoud geeft. Ik ben er voorstander van dat de Europese wetgever meer moeite doet om de voorschriften van een verordening waarvan de niet-naleving ernstige consequenties kan hebben voor de bedrijfsvoering van de verantwoordelijke, duidelijker te formuleren. Ik ben ervan overtuigd dat dit ook zal bijdragen aan een betere acceptatie van deze normen door de samenleving.

2. Ik heb in mijn standpuntbepaling ten aanzien van artikel 20, dat een regeling over het profileren bevat, een vergelijking gemaakt tussen het voorstel van de Commissie en Resolutie CM/Rec (2010) 13 van het Comité van Ministers van de Raad van Europa over hetzelfde onderwerp. Ik heb dat gedaan omdat die resolutie gebaseerd is op een grondige analyse van het verschijnsel *profilen* en die resolutie ook goed weergeeft over welke aspecten van het *profilen* in Europa consensus heerst. Het is mij – niet in positieve zin – opgevallen dat noch in het Commissievoorstel, noch in de mondeling door de Commissie op artikel 20 gegeven toelichting, ook maar enige aandacht wordt gegeven aan de resolutie. De resolutie biedt een omschrijving van het begrip «*profilen*» die gesloten van karakter is. Artikel 20, eerste lid, van de verordening bevat een omschrijving die niet alleen aanzienlijk breder is dan die van resolutie, maar ook open van karakter is, door toevoeging van het element «*in particular*». Ik ben bereid open van gedachten te wisselen over de uitbreiding van de definitie in termen van beschreven eigenaardigheden die aanleiding geven voor een

vorm van profileren. Ik heb echter bezwaar tegen het in de ontwerpverordening veelvuldig hanteren van het element «*in particular*». Ik wijs erop dat artikel 79, zesde lid, van de ontwerpverordening overtreding van artikel 20 bedreigt met een bijzonder hoge bestuurlijke boete. Het maximum bedraagt € 1 000 000,-. Een dergelijke sanctie verplicht de Europese wetgever in de formulering van normen tot een zo groot mogelijke nauwkeurigheid. Een open formulering levert daaraan naar mijn oordeel geen bijdrage.

3. Het voorstel van de Europese Commissie biedt naar mijn mening, en die van vele andere lidstaten, onvoldoende mogelijkheden om de met de verordening gemoeide uitvoeringslasten goed toe te snijden op de risico's die met de concrete verwerkingen van persoonsgegevens zijn gemoeid. In een aantal bepalingen zoekt de Commissie haar toevlucht tot het criterium bedrijfsgrootte, waarbij de grootte van het bedrijf maatgevend is voor de gelding van die verplichtingen. Dit tegen de achtergrond van een vooronderstelde hogere draagkracht bij grote bedrijven.

Deze benadering is te eenzijdig. Waar het gaat om de bescherming van persoonsgegevens zijn bedrijven met een grote omvang, zeker in de industrie en de zakelijke dienstverlening, juist bedrijven met een verhoudingsgewijs gering aantal verwerkingen van persoonsgegevens met een betrekkelijk normaal risico. Kleine bedrijven die de verwerking van persoonsgegevens als hoofdactiviteit hebben, zoals bijvoorbeeld kleine webwinkels, zijn juist bedrijven die een hoger risico opleveren, maar niet altijd veel draagkracht bezitten voor de kosten van de nodige maatregelen. De ontwerpverordening laat de bedrijven enerzijds betrekkelijk vrij in de inrichting van hun interne systemen voor gegevensbescherming, zoals blijkt uit artikel 22, zonder die bedrijven veel houvast te bieden over het doel van de verplichtingen en de manier waarop zij die in concrete situaties moeten uitvoeren. Anderzijds verlangen de artikelen 28, 31, 32, 33, 34 en 35 nogal veel van bedrijven, overheden en individuele burgers die binnen de reikwijdte van die bepalingen vallen in termen van verplichtingen. Die reikwijdte is ook niet steeds consequent dezelfde voor elke verplichting. Ik acht die benadering niet overtuigend.

Nederland is van mening dat een *data protection impact assessment* een heel nuttig instrument is om de risico's van een verwerking in kaart te brengen. Daarbij kan het risico worden bepaald aan de hand van criteria als aantal en aard van betrokkenen, omvang van gegevensstromen, aard van de gegevens, en aantal en aard van de ontvangers van de gegevens. Er kan ook worden gedacht aan risico's als de mogelijkheid van identiteitsdiefstal, de mogelijk financiële nadelen voor de betrokkene en het bestaan van geheimhoudingsplichten en verschoningsrechten. Een inventarisatie van de risico's vormt dan de basis voor het gericht opleggen van verplichtingen voor de verantwoordelijke. Dit is zeker niet de enige denkbare risico-benadering. Andere lidstaten hebben ook voorstellen naar voren gebracht. Nederland zal de discussie daarover graag voortzetten.

4. Mijn kritiek op artikel 23 van de ontwerpverordening betreft de vormgeving, niet de inhoud. Met hetgeen de leden van de commissies uiteenzetten in hun brief ben ik het eens. Ten aanzien van *privacy by design* en *privacy by default* heb ik in mijn eerdergenoemde brief uiteengezet dat het eerste lid van artikel 23 inhoudelijk voldoende wordt afgedekt door de artikelen 14, 22 en 30 van de ontwerpverordening. De kern van de verplichting om *privacy by design* en *privacy by default* aan te bieden staat niet in artikel 23, eerste lid, maar in artikel 23, tweede lid. Daar kan ik mij in vinden, mits de uit die verplichting voortvloeiende afweging wordt uitgebreid met het rekening mogen houden met de stand van de techniek en de kosten van de tenuitvoerlegging.

5. In de wetgevingspraktijk komt zo nu en dan de vraag op of het voor verwerkingen die geheel of gedeeltelijk zijn gericht op de publieke sector niet de voorkeur verdient dat de wetgever of de Kroon regelend optreedt in de verhouding tussen verantwoordelijke en bewerker in specifieke gevallen. Er kunnen dan door de formele wetgever zelf of bij gedelegeerde regeling, onder ministeriële verantwoordelijkheid, regels worden gesteld met het oog op de behartiging van het publieke belang of een bijzonder belang bij de bescherming van de persoonsgegevens van Nederlandse burgers. Deze regels kunnen in plaats van of in aanvulling op bestaande bewerkerscontacten worden vastgesteld.

6. De door Nederland ingediende schriftelijke opmerkingen zijn niet meer dan de schriftelijke uitwerking van de mondeling uitgesproken bijdrage. Het betreft geen formele amendementen. U treft de opmerkingen<sup>1</sup> in schriftelijke vorm bijgaand aan.

7. Ik neem met genoeg kennis van de door de leden van de commissies uitgesproken ondersteuning op het punt van de beveiligingsvereisten.

8. Cameratoezicht op openbare of anderszins voor het publiek toegankelijke ruimten is naar mijn oordeel een maatregel die in brede lagen van de samenleving wordt aanvaard. In Nederland wordt algemeen beseft dat cameratoezicht op dergelijke plaatsen noodzakelijk is ten behoeve van van de bevordering van de veiligheid. Daarbij wordt ook beseft dat eenieder die zich op de openbare weg of op een andere voor eenieder toegankelijke plaats bevindt geen onbeperkte aanspraak op een absolute privacy heeft. Bij cameratoezicht gelden natuurlijk wel de gebruikelijke voorwaarden, zoals de omstandigheid dat dit toezicht openlijk kenbaar wordt gemaakt, dat beelden worden gebruikt voor het doel waarvoor ze worden verzameld en dat beelden niet onbeperkt bewaard blijven als ze geen aanleiding geven tot gericht vervolgonderzoek. Bovendien behoort wel een *privacy impact assessment* te worden gemaakt bij de voorbereiding van wetsvoorstellen tot regulering van cameratoezicht.

Voor zover dit cameratoezicht plaatsvindt op openbare plaatsen in de zin van de Gemeentewet, bevat de Gemeentewet al een regeling waarin de belangen van de veiligheid en de bescherming van de persoonlijke levenssfeer zorgvuldig tegen elkaar zijn afgewogen. Als die bevoegdheid in concrete gevallen toepassing vindt, is dat een verantwoordelijkheid van het desbetreffende bestuursorgaan. Over de uitoefening van die bevoegdheid vindt op democratische wijze verantwoording plaats. Dit systeem behoeft naar mijn oordeel geen verzwaring in de vorm van aanvullende eisen in de verordening.

Voor andere gevallen van cameratoezicht, zoals bijvoorbeeld privaats cameratoezicht op voor het publiek toegankelijke plaatsen, meen ik dat een *privacy impact assessment* wel een zinvolle maatregel kan zijn.

9. De twee vragen van de commissies met betrekking tot de meldplicht datalekken lijken mij samenhangend. Wat de reikwijdte van de meldplicht betreft, ben ik in algemene zin van oordeel dat deze gelijkelijk voor alle verantwoordelijken in de zin van de verordening moet gelden. Ik stel daarbij wel de voorwaarde dat de meldplicht op een zinvolle wijze wordt beperkt tot die gevallen waarin er sprake is van een aanmerkelijk risico op verlies of onrechtmatige verwerking van persoonsgegevens. Dat is tenminste het uitgangspunt van het wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens dat ik spoedig bij de Tweede Kamer zal indienen. In het kader van de onderhandelingen over de verordening gegevensbescherming en de richtlijn gegevensbescherming voor de opsporing en vervolging ben ik overigens bereid om ook naar andere zinvolle voorstellen te kijken om de reikwijdte van artikel 31 van de ontwerpverordening in te perken. Zo zou ook denkbaar zijn dat een vooraf

---

<sup>1</sup> Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. ....

gehouden *privacy impact assessment* waarin een gedegen risico-analyse is neergelegd aanleiding geeft te beslissen of oplegging van een meldplicht gerechtvaardigd is. Dergelijke maatregelen kunnen ook bijdragen aan een oplossing van de door de commissies terecht onder mijn aandacht gebracht zorgen over de administratieve lasten.

De voorgestelde reikwijdte is hoe dan ook te breed. Bij handhaving zal deze aanleiding geven tot ofwel een hausse aan meldingen, ofwel tot het negeren van de verplichting. In beide gevallen verliest de meldplicht zijn toegevoegde waarde.

Het College bescherming persoonsgegevens (Cbp) heeft ook aan mij te kennen gegeven onvoldoende mogelijkheid te zien om met de bestaande capaciteit de handhaving van de meldplicht op een aanvaardbaar niveau te brengen. In het kader van het wetsvoorstel heb ik het Cbp laten weten dat ik geïnteresseerd ben in een goede monitoring van aantal en aard van ontvangen meldingen na de inwerkingtreding van het wetsvoorstel. Op basis van de opgedane ervaringen kan ik zonodig nadere besluiten nemen. Naar aanleiding van de op 4 december 2012 door de Tweede Kamer aangenomen motie van het lid Schouw (Kamerstukken II 2012/13, 33 400 VI, nr. 48) ben ik voornemens de Tweede Kamer over dit onderwerp uiterlijk 1 maart 2013 nog afzonderlijk te informeren. Ik zal u die brief in afschrift toezenden.

Wat de verhouding tussen de ontwerpverordening en de ontwerprichtlijn betreft, heb ik er tijdens de JBZ Raad van oktober 2012 in Luxemburg op aangedrongen dat het werk aan beide instrumenten, dus ook aan de richtlijn, voortgang moet vinden. Ik meen dat het – zeker in dit stadium van behandeling van de ontwerprichtlijn – de voorkeur verdient mij te blijven richten op de voortgang in plaats van mij te richten op de inwerkingtreding, en wil mij daarvoor blijven inspannen.

De staatssecretaris van Veiligheid en Justitie,  
F. Teeven