Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2011–2012

33 169 EU-voorstel: Richtlijn bescherming persoonsgegevens bij gebruik door politiële en justitiële autoriteiten (COM(2012) 10) en EU-voorstel Verordening algemeen kader bescherming persoonsgegevens (COM(2012)11)

B

BRIEF AAN DE VICE-VOORZITTER VAN DE EUROPESE COMMISSIE

Den Haag, 21 mei 2012

De vaste commissies voor Immigratie & Asiel/JBZ-raad en voor Veiligheid en Justitie hebben met belangstelling kennisgenomen van het voorstel van de Europese Commissie voor een algemene verordening gegevensbescherming[1], alsmede van het voorstel voor een richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens.[2] De commissies leggen graag enige vragen en opmerkingen over deze beide voorstellen aan u voor.

Vragen over de algemene privacyverordening

1. De commissies staan positief tegenover de introductie van de verplichting tot het uitvoeren van een privacyeffectbeoordeling voor die verwerkingen die genoemd staan in het voorgestelde artikel 33. Wel vinden zij het opmerkelijk dat overheidsinstanties of -organen in bepaalde gevallen uitgezonderd worden van deze verplichting. De commissies achten het juist wel gewenst dat ook zij vooraf een privacyeffectbeoordeling uitvoeren. De commissies verzoeken de Europese Commissie deze uitzondering te laten vervallen.

2. Bijzonder is dat in artikel 35 overheidsinstanties of -organen verplicht worden een functionaris voor gegevensbescherming (fg) aan te wijzen. De commissies kunnen zich dat voorstellen vanwege de voorbeeldfunctie die deze instanties hebben. Zij vragen zich wel af welke voorstelling de Europese Commissie heeft bij de concrete invulling van deze functie. In lid 6 van artikel 35 wordt bepaald dat de verantwoordelijke en de bewerker ervoor zorgen dat alle andere beroepswerkzaamheden van de fg verenigbaar zijn met zijn taken en verplichtingen als fg. Is dit geen verantwoordelijkheid van in eerste instantie de fg zelf? En hoe verhoudt zich dat tot het bepaalde in lid 3 van het voorgestelde artikel 36? Daarin

[1] COM(2012)11; zie E120003 op www.europapoort.nl
[2] COM(2012)10; zie E120004 op www.europapoort.nl

kst-33169-B
ISSN 0921 - 7371
's-Gravenhage 2012

wordt verondersteld dat de fg beschikt over personeel, kantoren, uitrusting en alle andere middelen die nodig zijn om zijn functie goed in te kunnen vullen. Daarmee wordt de indruk gewekt dat het dus om een meer dan fulltime functie gaat. Met andere woorden, hoe verhouden deze bepalingen zich tot elkaar? En welke criteria moeten worden gehanteerd om van een overheidsinstantie of -orgaan te spreken? Vallen private instellingen met een publieke taak, semipublieke organisaties, zelfstandige bestuursorganen ook onder deze begrippen?

3. De bestaande meldingsplicht wordt met dit voorstel afgeschaft, de informatieplicht wordt in het voorgestelde artikel 14 sterk uitgebreid alsook de verzoeken tot inzage, correctie en vernietiging. De verantwoordelijke moet behalve het doel van de verwerking en zijn identiteit de betrokkenen nu ook informeren over onder meer de vertegenwoordiger van de verantwoordelijke en van de functionaris voor gegevensbescherming, de bewaartermijn van de persoonsgegevens, het bestaan van zijn recht om inzage, correctie en vernietiging van de gegevens te verlangen of om bezwaar te maken, het recht om een klacht in te dienen bij – in Nederland – het College Bescherming Persoonsgegevens (CBP), de ontvangers of categorieën ontvangers van zijn persoonsgegevens, in voorkomend geval het voornemen van de doorgifte van zijn persoonsgegevens naar een derde land of een internationale organisatie en het door dat derde land geboden beschermingsniveau onder verwijzing naar een besluit van de Commissie waarbij het beschermingsniveau passend wordt verklaard en alle verdere informatie die nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen. Nu lijkt het heel mooi dat de meldingsplicht wordt afgeschaft, want de indruk wordt gewekt dat daarmee een hoop administratieve rompslomp wordt afgeschaft. Met de uitbreiding van de informatieplicht en de rechten van betrokkenen zal de verantwoordelijke toch weer bijna precies dezelfde gegevens moeten vastleggen. Verschil is dat deze nu niet in een meldingsformulier worden vastgesteld dat naar de nationale toezichthouder moet worden gestuurd, maar dat deze in een uitgebreide brief aan de betrokkene rechtstreeks moet worden gemeld. Hoe kijkt de Europese Commissie hiertegen aan? Was dit inderdaad de bedoeling van de Commissie? En brengen deze verplichtingen niet onnodig veel administratieve lasten met zich mee?

4. De documentatieplicht van artikel 28 is niet van toepassing op ondernemingen of organisaties met minder dan 250 werknemers die persoonsgegevens slechts als nevenactiviteit verwerken. Het criterium van 250 personen lijkt nogal willekeurig. De grootte van de organisatie zou niet doorslaggevend moeten zijn, maar de doeleinden van de gegevensverwerkingen, de aard van de persoonsgegevens, de hoeveelheid persoonsgegevens en de ontvangers van persoonsgegevens. Bovendien is het voldoen aan de documentatieplicht geen grote moeite, gelet op de verplichtingen van de artikelen 11 tot en met 15. De commissies verzoeken de Europese Commissie de uitzondering van artikel 28 lid 4 sub b te laten vervallen.

5. In artikel 23 worden verantwoordelijken voor verwerkingen van gegevens verplicht de principes van «privacy by design» en «privacy by default» toe te passen. In het tweede lid van dit artikel wordt bepaald dat de verantwoordelijke mechanismen moet instellen om ervoor te zorgen dat alleen de persoonsgegevens worden verwerkt die voor elk specifiek doeleinde van de verwerking nodig zijn en dat het verzamelen of het bewaren van die gegevens zich – zowel wat betreft de hoeveelheid gegevens als de periode van opslag daarvan – beperkt tot dat wat voor die doeleinden strikt noodzakelijk is. Deze mechanismen moeten er met name voor zorgen dat persoonsgegevens in beginsel niet voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt. Deze laatste zin

ziet op het instellen van autorisatieschema's en mechanismen die de vertrouwelijkheid moeten waarborgen. Deze mechanismen zorgen er dan nog niet voor dat de gegevensverwerking alleen plaatsvindt als dat voor de doeleinden nodig is en dat de gegevens niet langer worden bewaard dan voor die doeleinden strikt noodzakelijk is. Het is niet duidelijk of de Europese Commissie ook mechanismen verplicht wil maken om de doelbindings- en proportionaliteitsbeginselen systeemtechnisch af te kunnen laten dwingen. Kan de Europese Commissie dat nader toelichten?

6. In artikel 24 van de voorgestelde privacyrichtlijn worden de lidstaten verplicht erop toe te zien dat een registratie wordt bijgehouden van ten minste de verzameling, wijziging, raadpleging, verstrekking, combinatie of wissing van gegevens. Bij de registratie van raadpleging en verstrekking dienen tenminste het doel, de datum en het tijdstip van die handeling te worden aangegeven en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of verstrekt. Wat is de reden dat deze bepaling wel in deze voorgestelde richtlijn staat, maar niet in de voorgestelde privacyverordening?

7. Artikel 51 lid 2 bepaalt dat de toezichthouder van de lidstaat waar de hoofdvestiging van de verantwoordelijke zich bevindt, bevoegd is om toezicht uit te oefenen op de verwerkingen van de verantwoordelijke in alle lidstaten. Nu is het in de praktijk niet altijd duidelijk welke vestiging de hoofdvestiging is. Dit betekent dat de criteria op basis waarvan vast komt te staan welke toezichthouder bevoegd is en hoe de onderlinge besluitvorming plaatsvindt, duidelijker moeten worden geformuleerd. Zo zou bepaald kunnen worden dat als niet kan worden vastgesteld waar de hoofdvestiging zich bevindt, de Europese toezichthouder – de European Data Protection Board – de bevoegdheid krijgt om te bepalen welke nationale toezichthouder de leiding neemt en hoe de onderlinge rolverdeling met andere nationale toezichthouders is. Hoe denkt de Europese Commissie hierover?

8. De commissies staan positief tegenover de introductie van een meldplicht van inbreuken in verband met persoonsgegevens. Een verantwoordelijke moet zonder onnodige vertraging en binnen 24 uur nadat hij er kennis van heeft gekregen de melding doen. De bewerker moet de verantwoordelijke onmiddellijk waarschuwen en informeren nadat hij een inbreuk heeft vastgesteld. Is het juist dat deze meldplicht verder gaat dan de verplichting tot het melden van datalekken en dat elke doorbreking van technische en organisatorische maatregelen die een passend beveiligingsniveau moeten waarborgen, moet worden gemeld? En is het praktisch gezien haalbaar dat de bewerker conform artikel 31 lid 3 onmiddellijk bij de melding van de inbreuk mededeling doet van de in sub a tot en met e genoemde zaken? Zou het niet logischer zijn dat de bewerker de inbreuk wel onmiddellijk meldt, maar dat hij zo spoedig als mogelijk is de verantwoordelijke over de overige zaken informeert?

Vragen over de specifieke privacyrichtlijn voor strafzaken

1. De voorgestelde privacyrichtlijn is van toepassing op alle verwerkingsactiviteiten die bevoegde autoriteiten voor de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen uitvoeren. Het begrip «voorkoming» van strafbare feiten is een ruim en rekbaar begrip. Kan de Europese Commissie aangeven hoe dit begrip geïnterpreteerd moet worden?

2. Het begrip «bevoegde autoriteiten» staat in de voorgestelde privacyrichtlijn in artikel 3 sub 14 omschreven als «elke overheidsinstantie die bevoegd is ten aanzien van de voorkoming, het onderzoek, de opsporing

of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen». Met name de overheidsinstanties die bevoegd zijn ten aanzien van de voorkoming van strafbare feiten kunnen een ruime categorie omvatten. Kan de Europese Commissie tenminste voorbeelden geven van deze instanties? Aan bevoegde autoriteiten die belast zijn met de voorkoming van strafbare feiten worden doorgaans andere eisen gesteld ten aanzien van hun competenties en hun bevoegdheden kennen doorgaans geen wettelijke grondslag. Waarom is dit onderscheid niet vertaald naar de rechten en verplichtingen die bevoegde autoriteiten op grond van dit voorstel krijgen?

3. Hoe moet de samenhang tussen de voorgestelde specifieke privacyrichtlijn voor strafzaken en de voorgestelde algemene privacyverordening worden gezien? Als gegevens worden verwerkt door samenwerkingsverbanden die zijn opgericht om criminaliteit tegen te gaan, is dan de onderhavige voorgestelde richtlijn van toepassing of de algemene privacyverordening? Voor samenwerkingsverbanden geldt in Nederland op dit moment dat op hun gegevensverwerkingen de algemene Wet bescherming persoonsgegevens van toepassing is en niet de sectorspecifieke Wet politiegegevens. Dat komt omdat ook bijvoorbeeld gemeenten participeren in de samenwerkingsverbanden, die niet onder de Wet politiegegevens vallen. Hoe zit dat als de algemene privacyverordening van kracht is en de specifieke privacyrichtlijn voor strafzaken is geïmplementeerd in nationale wetgeving en van kracht is geworden?

4. Volgens artikel 4 sub a van de voorgestelde privacyrichtlijn moeten de lidstaten bepalen dat persoonsgegevens eerlijk en rechtmatig worden verwerkt. Wat wordt verstaan onder «eerlijk»?

5. Volgens artikel 4 sub f moeten de lidstaten bepalen dat persoonsgegevens moeten worden verwerkt onder de verantwoordelijkheid en aansprakelijkheid van de voor de verwerking verantwoordelijke. Welke betekenis heeft «aansprakelijkheid» hier? De voor de verwerking verantwoordelijken zullen doorgaans politiële en justitiële autoriteiten zijn. Kennen juist zij – zoals dat in Nederland het geval is – geen immuniteit als het gaat om aansprakelijkheid? Hoe moet de term «aansprakelijkheid» in dit kader dan uitgelegd worden?

6. Artikel 19 heeft als kop «privacy by design» en «by default». Uit de tekst van artikel 19 blijkt niet duidelijk wat onder «privacy by default» moet worden verstaan. Betekent het dat de ICT-systemen waarmee persoonsgegevens worden verwerkt te allen tijde zodanig moeten zijn ontworpen en ingericht dat de bescherming van persoonsgegevens met de systemen kan worden afgedwongen? Kan de Europese Commissie dat uitleggen en nader toelichten?

7. De commissies verzoeken de Europese Commissie tot slot de samenhang tussen de algemene verordening en de specifieke richtlijn te verbeteren. Dat kan door algemene beginselen en definities in beide voorstellen op te nemen en gelijk te schakelen. Ook zou de samenhang worden verbeterd als de verplichtingen die van toepassing zijn op de verantwoordelijke en de bewerker gelijkgeschakeld worden, zoals de verplichting tot het uitvoeren van privacy impact assessments en het toepassen van «privacy by design».

Rappel

De commissies maken ten slotte graag van de gelegenheid gebruik de Europese Commissie erop te wijzen dat twee vanuit de Eerste Kamer verzonden brieven nog niet door de Europese Commissie zijn beant-

woord. Het betreft de volgende brieven, waarvan de door de Europese Commissie voor haarzelf vastgestelde reactietermijn van drie maanden reeds is verstreken:

– brief van 8 november 2011 inzake het Noodmechanisme herinvoering binnengrenstoezicht Schengen (COM(2011)560), kenmerk 149443.01u;
– brief van 11 november 2011, inzake de Richtlijn inzake het gebruik van passagiersgegevens voor wethandhavingsdoeleinden (COM(2011)32), kenmerk 147341.06u;

De commissies verzoeken u genoemde brieven zo spoedig mogelijk te beantwoorden. Zij zien voorts met belangstelling uit naar uw reactie op deze brief.

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

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