Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2013–2014

31 051 Evaluatie Wet bescherming persoonsgegevens

G

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 24 oktober 2013

De leden van de commissie voor Veiligheid en Justitie[1] hebben kennisgenomen van de brief d.d. 22 juni 2013 inzake het toetsmodel Privacy Impact Assessment (PIA) Rijksdienst. Dit toetsmodel vormt een nadere invulling en uitvoering van het regeerakkoord, de motie van het lid Franken c.s. (EK 31 051, D), de toezegging tot doorontwikkeling van een PIA (T01516) alsmede de in de iStrategie aangekondigde maatregelen om aandacht voor privacy te versterken bij grote ICT-projecten. Naar aanleiding hiervan hebben de leden van de commissie op 9 juli 2013 een brief gestuurd aan de minister voor Wonen en Rijksdienst en de staatssecretaris van Veiligheid en Justitie.

De minister voor Wonen en Rijksdienst en de staatssecretaris van Veiligheid en Justitie hebben op 4 oktober 2013 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Dooren

[1] Samenstelling: Holdijk (SGP), Kneppers-Heijnert (VVD), Kox (SP), Engels (D66), Franken (CDA), Thissen (GL), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), (vice-voorzitter), Duthler (VVD), (voorzitter), Koffeman (PvdD), Kuiper (CU), Quik-Schuijt (SP), Strik (GL), K.G. de Vries (PvdA), Knip (VVD), Hoekstra (CDA), Lokin-Sassen (CDA), Scholten (D66), Schouwenaar (VVD), De Boer (GL), De Lange (OSF), Ter Horst (PvdA), Beuving (PvdA), Koole (PvdA), Schrijver (PvdA), Reynaers (PVV), Popken (PVV), Frijters-Klijnen (PVV) en Swagerman (VVD).

kst-31051-G
ISSN 0921 - 7371
's-Gravenhage 2013

BRIEF AAN DE MINISTER VOOR WONEN EN RIJKSDIENST

Den Haag, 9 juli 2013

De leden van de commissie voor Veiligheid en Justitie (V&J) hebben met belangstelling kennisgenomen van de brief d.d. 22 juni 2013 inzake het toetsmodel Privacy Impact Assessment (PIA) Rijksdienst[2]. Dit toetsmodel vormt een nadere invulling en uitvoering van het regeerakkoord, de motie van het lid Franken c.s. (EK 31 051, D), de toezegging tot doorontwikkeling van een PIA (T01516) alsmede de in de iStrategie aangekondigde maatregelen om aandacht voor privacy te versterken bij grote ICT-projecten. De leden van de commissie hebben nog enkele vragen.

Deze leden merken op dat met het toetsmodel alleen het risico-identificerende gedeelte van een PIA wordt doorlopen en de risico's in kaart worden gebracht. Dit is een goede en relevante stap, maar een volledige PIA gaat verder. Ook de voorgestelde Europese privacyverordening gaat uit van een volledige PIA.[3] Kan de regering aangeven hoe zij de relatie van het toetsmodel PIA Rijksdienst ziet met de privacyeffectbeoordeling van artikel 33 van de voorgestelde Europese privacyverordening? In het derde lid van het voorgestelde artikel 33 wordt vereist dat de beoordeling naast een algemene beschrijving van de verwerkingen, minstens bevat een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen, de maatregelen die worden beoogd om de risico's te beperken, en de waarborgen, beveiligingsmaatregelen en mechanismes die de bescherming van persoonsgegevens verzekeren en aantonen dat aan deze verordening is voldaan. Deze vereisten worden niet automatisch afgedekt met het invullen van het toetsmodel. Deze leden ontvangen graag een reactie van de regering op dit punt.

Sowieso is het toetsmodel voornamelijk gebaseerd op de Wet bescherming persoonsgegevens (Wbp) en zijn nieuwe elementen uit de voorgestelde Europese privacyverordening niet opgenomen, zoals het vereiste tot het toepassen van principes van «privacy by design» en «privacy by default». Weliswaar is de tekst van de voorgestelde Europese privacyverordening nog niet definitief, de verwachting is gerechtvaardigd dat een dergelijke verplichte toepassing van deze principes ook in de definitieve tekst zal zijn opgenomen. Wat is de reden voor de regering geweest om dergelijke verplichtingen niet te verwerken in het toetsmodel en is de regering bereid om dat alsnog te doen?

Verder vragen de leden van deze commissie zich af of de regering bij het opstellen van de vragenlijst voor de toets voldoende heeft stilgestaan bij de gevolgen van beantwoording van een vraag. Het is lang niet in alle gevallen duidelijk welke gevolgen een bepaald antwoord heeft. Om een voorbeeld te geven: De eerste vraag van onderdeel II.1 luidt: «Heeft u het /de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld?» Dit is een belangrijke vraag. Echter, wat een «nee-antwoord» betekent, wordt in het midden gelaten en er wordt geen consequentie aan verbonden. Betekent dit dan slechts een geconstateerd risico en wat zijn de consequenties daar dan van? De toetsvragen lijken eerder op vragen bedoeld voor het kunnen toepassen van de Wbp op geïnventariseerde verwerkingen, dan voor het in kaart brengen van risico's die voorgenomen verwerkingen hebben voor de privacybe-

---

[2] Kamerstuk EK 31 051, F.

[3] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), COM(2012)11 final, E120003 op www.europapoort.nl.

scherming van betrokkenen. Hoe kijkt de regering hier tegen aan? Is de regering bereid om een volgende versie van het toetsmodel meer in overeenstemming te brengen van de werkelijke bedoeling van een PIA alsook met de eisen die de te verwachten Europese privacyverordening met zich mee brengt?

De leden van de commissie V&J zien uw antwoorden op deze vragen met belangstelling tegemoet en hopen uw reactie binnen vier weken te mogen ontvangen. Een gelijkluidende brief is gestuurd aan de staatssecretaris van Veiligheid en Justitie.

De Vice-Voorzitter van de vaste commissie voor Veiligheid en Justitie,
Van Bijsterveld

BRIEF VAN DE MINISTER VOOR WONEN EN RIJKSDIENST EN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 4 oktober 2013

De regering heeft met belangstelling kennis genomen van de wat kritisch getoonzette vragen van 9 juli jl. van de leden van de commissie voor Veiligheid en Justitie over het Toetsmodel Privacy Impact Assessment Rijksdienst.

In algemene zin hecht de regering eraan erop te wijzen dat Nederland een van de eerste landen in Europa is dat een dergelijk model vaststelt en interne toepassing ervan verplicht stelt voor de overheidssector. Verder verdient nadruk dat het toetsmodel wordt ingepast in een veel breder, al bestaand instrumentarium om privacyaspecten van beleid- en wetgeving te toetsen. Dat kader blijft onverkort van kracht. De verschillende onderdelen van dit kader maken slechts in samenhang een beoordeling mogelijk van de volledige «privacy impact» van voornemens en voorstellen. Het nieuwe toetsmodel vult dit al bestaande kader op twee aspecten aan, zoals ook blijkt uit de toelichting bij het toetsmodel dat er een integraal onderdeel van vormt. Ten eerste door het vertalen van al geldende juridische normen naar feitelijke vragen die in het beginstadium van beleidsvorming vaak spelen, alsmede het boven tafel krijgen van andere feitelijke informatie die voor het maken van welafgewogen besluitvorming noodzakelijk is. Ten tweede door het (beter) verbinden van de verschillende al bestaande toetsinstrumenten en betrokken actoren, zoals functionarissen gegevensbescherming en Chief Information Officers. Met deze gerichte maatregel wordt bevorderd dat voor beleidsmatige en technische afwegingen relevante informatie in een vroegtijdig stadium beschikbaar komt en dat in dit stadium nog aanpassingen meegenomen kunnen worden. Daarnaast wordt hiermee het bewustzijn van inhoudelijke vereisten en procedures met betrekking tot privacy binnen de Rijksoverheid vergroot.

Met betrekking tot de specifieke vragen willen de leden allereerst nadere duiding van de regering over de relatie tussen het vastgestelde PIA toetsmodel Rijksdienst en artikel 33 van de voorgestelde Europese privacyverordening. In formele zin is deze verhouding duidelijk. Artikel 33, lid 5 van het genoemde Commissievoorstel zondert de overheid expliciet uit van de verplichting om risicovolle bewerkingen te beoordelen door middel van het uitvoeren van PIA. Deze uitzondering hangt samen met het feit dat van overheden bij ontwikkeling van wetgeving en beleid wordt verwacht al waarborgen te hanteren die privacyaspecten structureel toetsen. In deze zin legt de regering dus een hogere standaard aan voor de Nederlandse Rijksoverheid dan de concept-Europese privacyverordening voorstelt. Wel heeft het feit dat er al uiteenlopende toetsmodellen en procedures voor het staven van privacy bestaan gevolgen gehad voor de formulering en inkleding van het PIA toetsmodel Rijksdienst. Enkele van die keuzen liggen ten grondslag aan elementen waarover de leden de twee overige vragen hebben gesteld.

De leden informeren in het tweede deel van hun tweede vraag naar de overwegingen van de regering om noties als «privacy by design» en «privacy by default», die al wel in de voorstellen voor een Europese privacyverordening staan vermeld, nog niet te verwerken in het toetsmodel. Aan deze keuze ligt ten grondslag dat een privacy impact assessment als hulpmiddel, en privacy by design en privacy by default als technische oplossingen weliswaar in elkaars verlengde liggen maar in een

andere context spelen. Dit blijkt allereerst uit de concept-verordening zelf. Privacy by design en privacy by default als technische mogelijkheden worden daar in het verband van waarborging van een passend beveiligingsniveau (artikel 30) opgevoerd, en niet in het verband van vroegtijdige risico-analyse door middel van de privacy impact assessment (artikel 33). Ook uit de Cbp richtsnoeren beveiliging van persoonsgegevens (p. 17), waar in de PIA Toetsmodel Rijksdienst-vragen over beveiliging (IV.1-3) naar wordt verwezen, blijkt dat de PIA resultaten onder andere hun vertaling moeten vinden in de vorm van definitieve technische ontwerpbeslissingen. De drijfveer om tot privacyvriendelijke systeemontwerpen te komen door hiermee in de ontwerpfase al rekening te houden (privacy by design) en zelfs bepaalde specifiek door privacy-overwegingen ingegeven ontwerpkeuzen te maken (privacy by default) ligt kortom ten grondslag aan de opzet van de PIA-vragenlijst. Om echter verwarring over het verband tussen de PIA en privacy by design en privacy by default te voorkomen is er voor gekozen om deze termen niet als zodanig in de vragenlijst op te nemen. Dat wil overigens geenszins zeggen dat de Rijksoverheid geen rekening houdt met privacy by design en privacy by default. Ook bij nieuwe bouw of aanpassing van overheidssystemen zullen de PIA-resultaten als input dienen. Door de verplichting om de resultaten van een uitgevoerde PIA standaard naar Chief Information Officers te sturen, zoals verwoord in de toelichting (onderdeel 5.3), wordt verankerd dat dit bij besluitvorming over beveiligingsmaatregelen ook kan worden meegenomen. Ten slotte is in de Baseline Informatiebeveiliging Rijksdienst (BIR) vastgelegd dat de bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen

In het eerste deel van de tweede vraag en de derde vraag informeren de leden naar de mate van verwijzing naar de Wet bescherming persoonsgegevens en meer in het algemeen naar de wijze van formulering van de vragen in het PIA toetsmodel Rijksdienst. Zoals hierboven aangegeven is de onderliggende gedachte van het toetsmodel het aanvullen, en met elkaar in verband brengen van bestaande toetsinstrumenten zoals bijvoorbeeld de Leidraad afstemming op de Wet bescherming persoonsgegevens (Wbp). Tegen die achtergrond zijn de vaak als abstract ervaren normen uit de Wbp in meer feitelijke vragen vertaald. Ook zijn ze op een volgorde gezet zoals die over het algemeen bij eerste beleidsvorming aan bod zullen komen. In de toelichting bij het PIA toetsmodel (onderdeel 1), is duidelijk aangegeven dat vragen waarop nog geen antwoord kan worden geformuleerd moeten worden gezien als uitnodiging om die te formuleren. In die zin is het toetsmodel richtinggevend van aard (onderdeel 1.4 toelichting). Het toetsmodel is daarnaast ook sturend en corrigerend in de zin dat het vaak zal voorkomen dat eerder geformuleerde antwoorden opnieuw tegen het licht zullen worden gehouden tijdens het beantwoordingproces omdat eerdere oplossingsrichtingen bij nadere beschouwing niet goed genoeg kunnen worden onderbouwd. De regering heeft om meerdere redenen expliciet voor deze werkwijze gekozen. Het voorkomt allereerst overlap met meer juridisch en technisch getinte toetsinstrumenten. Bij de toepassing van deze instrumenten zullen de resultaten van een PIA juist als input moeten dienen. Daarnaast sluit het richtinggevende en corrigerende karakter van de formulering van de PIA-vragen aan bij de basisdoelstelling van het toetsmodel: het vergroten van het bewustzijn van de verschillende aspecten van privacy binnen de Rijksoverheid. De regering ziet dus vooralsnog geen aanleiding om deze aanpak te veranderen.

Tenslotte wijst de regering er nog op dat is aangekondigd om het gebruik van het PIA toetsmodel Rijksdienst binnen twee jaar na 1 september 2013 te evalueren. Onderdeel van deze evaluatie zal zijn of het toetsmodel qua

invulling en formulering voldoende aansluit bij de specifiek voor de overheid geldende vereisten om privacyaspecten te toetsen in het vroege stadium van beleidsontwikkeling.

De Minister voor Wonen en Rijksdienst,
S.A. Blok

De Staatssecretaris van Veiligheid en Justitie,
F. Teeven