Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 490

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 september 2017

Hierbij bied ik u, mede namens de Staatssecretaris van Veiligheid en Justitie, het nieuwe model voor gegevensbeschermingseffectbeoordelingen, ook wel Privacy Impact Assessment genoemd (hierna: PIA) aan[1], dat zal worden gebruikt binnen de rijksdienst. Het model, dat is vastgesteld in de ministerraad, volgt het toetsmodel Privacy Impact Assessment Rijksdienst uit 2013 op, zoals ik heb toegezegd bij brief van 6 juli 2016 en bevestigd bij brief van 16 maart 2017.[2] Bij de ontwikkeling van het model is het advies van de Autoriteit persoonsgegevens op een eerder concept van waarde geweest.

Aanleiding voor het nieuwe model is het onderzoeksrapport Evaluatie Toetsmodel PIA Rijksdienst dat in mei 2016 is opgeleverd door Privacy Management Partners, dat bij de eerder genoemde brief is aangeboden aan de Kamers.[3] In dit evaluatierapport zijn negen aanbevelingen geformuleerd om het PIA-toetsmodel en het bijbehorende proces te verbeteren. Het nieuwe model is bovendien toegesneden op de nieuwe Europese privacyregels die zullen gelden per 25 mei 2018, zoals die zijn

[1] Raadpleegbaar via www.tweedekamer.nl
[2] Kamerstuk 26 643, nr. 416 en nr. 453.
[3] Bijlage bij Kamerstuk 26 643, nr. 416. Het evaluatierapport is ook te vinden op https://www.rijksoverheid.nl/documenten/rapporten/2016/05/20/rapport-evaluatie-toetsmodel-pia-rijksdienst

kst-26643-490
ISSN 0921 - 7371
's-Gravenhage 2017

vervat in de Algemene verordening gegevensbescherming (AVG)[4] en de Richtlijn gegevensbescherming politie en justitie (Richtlijn).[5]

Om recht te doen aan de aanbevelingen is gekozen voor een opdeling van het model in drie delen. Het nieuwe model bestaat uit een proceskader (deel I) waarin onder meer staat wanneer een PIA moet worden gedaan en wie daarvoor verantwoordelijk is, het model om een PIA uit te voeren aan de hand van 17 punten (deel II) en een toelichting op de punten met daarin achtergronden en voorbeelden (deel III).

Door in het proceskader duidelijk uiteen te zetten wanneer het uitvoeren van een PIA verplicht is en tevens het uitvoeren van PIA's breder verplicht te stellen dan de AVG en de Richtlijn vereisen, wordt mede uitvoering gegeven aan de aanbevelingen van de evaluatie die zich richten op het bevorderen van het uitvoeren van PIA's op tijd en altijd wanneer dat nodig is en in het verlengde daarvan het bevorderen van het privacybewustzijn binnen de rijksoverheid (aanbevelingen 1 en 2). In dat kader kan nog worden opgemerkt dat het proceskader inzet op het zo vroeg mogelijk in het proces uitvoeren van een PIA zodat de resultaten van een PIA in de ontwerpfase een rol spelen. Om dit te bevorderen zijn uiterlijke momenten in het proces vastgesteld voor het uitvoeren van een PIA.

Een PIA moet volgens het model worden uitgevoerd bij (1) de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien en (2) bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen. Het kabinetsbeleid gaat hiermee verder dan waartoe de Europese privacyregels verplichten, omdat daarin niet is voorzien in een verplichting tot het verrichten van een PIA ten aanzien van regelgeving (categorie 1). Hiermee wordt het kabinetsbeleid dat in 2013 is ingezet bij de uitvoering van de motie Franken voortgezet.[6] De AVG en de Richtlijn verplichten bij voorgenomen verwerkingen met een hoog risico voor de rechten en vrijheden van betrokkenen een PIA. Dit model integreert die eis door daar een op een bij aan te sluiten (categorie 2). In de praktijk is dit model dus leidend voor de vraag wanneer een PIA wordt uitgevoerd binnen de rijksdienst.

De 17 punten van het model zijn geschikt en relevant voor het uitvoeren van zowel PIA's voor beleid en regelgeving als voor overheidsverwerkingen. Bij de invulling van die punten kunnen er wel accentverschillen zijn. Daarop is ingespeeld in het proceskader en de toelichting, door waar nodig nader aandacht te schenken aan specifieke aspecten die spelen bij PIA's voor beleid en regelgeving en PIA's voor overheidsverwerkingen. Hoewel dus niet is gekozen voor het opstellen van twee verschillende modellen, is op deze wijze tegemoet gekomen aan de aanbeveling die vraagt om een onderscheid tussen beide PIA's (aanbeveling 3).

---

[4] Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

[5] Richtlijn (EU) 2016/680 van het Europees parlement en de Raad van 27 april 2016 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 en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

[6] Kamerstuk 26 643, nr. 282, herdruk 1 (brief van 21 juni 2013, aanbieding toetsmodel PIA Rijksdienst aan Tweede Kamer). Zie ook Kamerstuk 31 051, D en Kamerstuk 33 410, nr. 15.

Het proceskader vormt tevens de uitwerking van de aanbeveling die ziet op het verhelderen en uitwerken van het proces van een PIA (aanbeveling 5). In onderdeel 7 van het proceskader zijn de processtappen van een PIA vastgelegd. Daarmee wordt bewerkstelligd dat opstellers van een PIA door stap voor stap door het proces geleid (aanbeveling 8). Ook bij de volgorde van de 17 punten is hiermee rekening gehouden. Tevens wordt in het proceskader antwoord gegeven op de vragen in welke gevallen een PIA verplicht is (aanbeveling 4), wie verantwoordelijk is voor het uitvoeren van een PIA en hoe de uitkomsten van een PIA verantwoord moeten worden.

De 17 punten uit het model om een PIA uit te voeren zijn ontleend aan artikel 35 AVG en verdeeld over vier onderdelen: een beschrijving van de voorgenomen gegevensverwerkingen en verwerkingsdoeleinden (onderdeel A), de beoordeling van de onder A verzamelde informatie aan het juridische kader (onderdeel B), de risico's voor betrokkenen (onderdeel C) en de beoogde maatregelen om die risico's aan te pakken (onderdeel D). Met deze indeling is gehoor gegeven aan de aanbevelingen die vragen om een model-vragenlijst c.q. model-opzet van een PIA-rapport (aanbeveling 5), het inruimen van voldoende ruimte voor het beoordelen van de proportionaliteit (aanbeveling 6) en voor de privacy risico's en voor het vaststellen van de benodigde maatregelen (aanbeveling 7). Met de heldere systematiek van de vier onderdelen kan diepgaand inzicht worden gekregen in verwerkingen van persoonsgegevens zoals een gegevensbeschermingseffectbeoordeling vereist, maar de systematiek is ook goed bruikbaar voor verwerkingen met beperkte privacyrisico's.

Het 17 punten model wordt verplicht voorgeschreven opdat er één standaard is in de gehele rijksdienst. Dit bevordert de eenduidigheid, vergelijkbaarheid en kwaliteit van de PIA's. Het staat organisaties vrij om het model zelf aan te vullen met organisatiespecifieke onderdelenvragen, waardoor het instrument beter bruikbaar wordt. Dit alles maakt het model gebruiksvriendelijker (aanbeveling 9).

Het doel van dit model is om, conform de eisen van de Europese privacyregels en de aanbevelingen uit het evaluatierapport, de bescherming van persoonsgegevens op een gestructureerde manier onderdeel te laten zijn van de belangenafweging en besluitvorming over voorgenomen gegevensverwerkingen binnen de Rijksdienst.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk