Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

32 761 Verwerking en bescherming persoonsgegevens

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 282

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 juli 2023

Aanleiding

Met deze brief geef ik aan hoe invulling wordt gegeven aan de motie van het lid Verhoeven c.s. (Kamerstuk 27 529, nr. 239). In deze motie wordt de noodzaak benadrukt van het versterken van de chief privacy officers functie (CPO) binnen de overheid. Voorts licht ik het kabinetsstandpunt toe en informeer ik u over de opgestarte acties.

Kabinetsreactie

De afgelopen jaren zijn we ons steeds meer bewust van de potentiële risico's die voortkomen uit onvoldoende bescherming van persoonsgegevens. Er hebben zich verschillende situaties voorgedaan waarin de bescherming van persoonsgegevens door de (rijks-)overheid onvoldoende is gebleken of gegevens van burgers op onrechtmatige wijze worden verwerkt. De toeslagenaffaire, inclusief de voortdurende nasleep daarvan, laat zien hoe complex problemen kunnen worden en wat voor enorme impact deze problemen kunnen hebben.

De regering streeft naar meer centrale coördinatie op het gebied van informatievoorziening en privacy; dit zowel om een meer daadkrachtige overheid te stimuleren alsook een meer uniforme werkwijze voor de burger te bewerkstelligen. Onderwerpen als digitale weerbaarheid en privacy krijgen een steeds prominentere rol in de I-Strategie[1]. En in de hoofdlijnenbrief «beleid voor digitalisering» [2] staat ook benoemd dat naleving van de AVG een belangrijk onderwerp is.

Toch zien we in de praktijk dat de bescherming van persoonsgegevens vrijwel volledig decentraal is ingeregeld. Met het Besluit CIO-stelsel

[1] I-strategie Rijk I-strategie Rijk 2021–2025 – Digitale Overheid.
[2] Kamerstuk 26 643, nr. 842.

kst-32761-282
ISSN 0921 - 7371
's-Gravenhage 2023

Rijksdienst 2021[3] heeft de Rijkoverheid belangrijke stappen gezet rondom het versterken van de samenwerking tussen CIO's rijksbreed en het waarborgen van de veiligheid door de CISO's. De rijksbrede coördinerende rol voor privacy is in tegenstelling tot informatiebeveiliging (CISO-stelsel) nog niet ingevuld; in de huidige situatie maakt privacy geen onderdeel uit van het Besluit CIO-stelsel Rijksdienst 2021. Op het gebied van privacy bestaat er daarom onvoldoende mandaat om rijksbrede kaders te stellen die erop gericht zijn een interdepartementaal risicobeeld te vormen en deze risico's vervolgens te mitigeren. Deze constateringen zijn recent bevestigd in het WODC-rapport «Naleving van de AVG door overheden»[4] en de rijksbrede AVG-onderzoeken van de ADR (2021/2022)[5].

Het kabinet steunt de oproep in de motie van het lid Verhoeven c.s. om gegevensbescherming een stevigere positie te geven. Niet alleen bij grote uitvoeringsorganisaties, maar binnen de gehele Rijksoverheid. Hiermee wordt tegemoetgekomen aan de politieke en maatschappelijke wens om privacy hoger op de agenda te plaatsen en zorgt dit voor een meer integrale aanpak binnen de Rijksoverheid.

Naar aanleiding daarvan heeft CIO Rijk de opdracht gekregen te onderzoeken hoe privacygovernance het beste kan worden ingericht binnen het Rijk. Het onderzoek was primair gericht op de vraag hoe privacygovernance het beste kan worden ingebed binnen het huidige I-stelsel. Hierbij is het van belang te weten dat de Functionaris Gegevensbescherming (FG) primair de rol van toezichthouder heeft zoals beschreven in artikel 38 en 39 AVG, en dat de CPO een coördinerende/adviserende en monitorende rol vervult. De FG en CPO geven samen invulling aan de privacygovernance. Dit onderzoek richt zich op het versterken van de coördinerende/adviserende en monitorende rol binnen het Rijk. In het door Berenschot uitgevoerde onderzoek[6] zijn een vijftal scenario's onderzocht. In het onderzoek werd geconcludeerd dat de privacygovernance het beste kan worden versterkt door de Chief Privacy Officer (CPO) als aparte functie binnen het huidige I-stelsel toe te voegen. De inrichting van de CPO wordt naar analogie van het CISO-stelsel vormgegeven binnen het CIO-besluit. Dit betekent dat ieder departement een eigen CPO krijgt en dat er een CPO Rijk wordt benoemd die, in analogie van CISO Rijk, een rijksbrede coördinerende rol krijgt. Dit scenario komt het beste tegemoet aan de politieke en maatschappelijke wens om privacy hoger op de agenda te plaatsen, zorgt voor een meer integrale aanpak binnen de Rijksoverheid, en sluit het beste aan bij de visie en inrichting van privacygovernance binnen de ministeries.

Door het inrichten van het CPO-stelsel wordt privacy verankerd in het I-stelsel. Het integreren van de privacygovernance in de bestaande I-governance is voorwaardelijk om de wettelijke FG-taken te kunnen vervullen[7]. De aan te wijzen CPO zal in de uitvoering van zijn rol nauw samenwerken met andere functies binnen het CIO-office. De CPO Rijk zal, in analogie van de CISO Rijk, onder de CIO Rijk worden gepositioneerd waardoor de rijksbrede coördinerende rol van CIO Rijk wordt versterkt.

Dit advies is overgenomen door het CIO-Beraad en ook opgenomen in de werkagenda Waardengedreven digitaliseren[8]. Dit advies wordt ook gesteund door de Autoriteit Persoonsgegevens.

---

[3] Bijlage bij Kamerstuk 26 643, nr. 739.
[4] Bijlage bij Kamerstuk 32 761, nr. 261.
[5] Onderzoeksrapport Rijksbreed AVG onderzoek | Rapport | Rijksoverheid.nl.
[6] Inrichting rijksbrede privacy governance, dit onderzoek is toegevoegd als bijlage.
[7] FG-informatie | Autoriteit Persoonsgegevens.
[8] Kamerstuk 26 643, nr. 940.

Toelichting nieuwe I-stelsel

Het nieuwe I-stelsel wordt gebaseerd op het huidige besluit CIO-stelsel 2021. In het huidige I-stelsel zijn de taken van de CIO (Rijk) en CISO (Rijk) en de respectievelijke raden beschreven. In het nieuwe stelsel krijgt de CIO meer integrale I-verantwoordelijkheid; om dit te bereiken worden de Chief Privacy Officer (CPO), Chief Data Officer (CDO) en Chief Technical Officer (CTO) ook onderdeel van het I-stelsel.

Om de doelstelling te behalen is een programma opgesteld om deze uitbreiding in samenhang te realiseren.

Status & vervolgstappen

De scope van de vervolgopdracht is het uitwerken van het CPO-stelsel als onderdeel van het CIO- stelsel. De taken van de departementale CPO/CPO Rijk worden hiertoe uitgewerkt en de interdepartementale CPO-Raad zal worden ingericht. Het huidige stelsel voor informatiebeveiliging (CISO-stelsel) dient als voorbeeld voor de inrichting van het CPO-stelsel.

De hoofdtaken van een departementale CPO zijn het opstellen van een privacy strategie en governance voor het departement, het opstellen en monitoren van een Plan-Do-Check-Act (PDCA)-cyclus en het adviseren van het management.

De hoofdtaken van CPO Rijk zijn het zorgdragen voor rijksbreed privacy beleid en naleving, opstellen en actueel houden van het rijksbrede risicobeeld bescherming van persoonsgegevens en het coördineren van rijksbrede datalekken.

De CPO-Raad is een afspiegeling van het CIO-Beraad en zal als formeel voorportaal van het CIO-Beraad fungeren. Het kan hiertoe o.a. privacy-onderwerpen agenderen voor het CIO-Beraad, privacykaders/-beleid vaststellen en ter besluitvorming aanbieden aan het CIO-Beraad en Rijksbrede kennisdeling over privacy stimuleren.

Op dit moment zijn de taken van de CPO/CPO Rijk uitgewerkt en zijn de spelregels voor de CPO-Raad opgesteld. Dit wordt nu afgestemd met de FG's en aanpalende disciplines.

Vooruitlopend op de formele vaststelling van het CPO-stelsel zijn er al zes CPO's aangesteld. Het doel is dat in 2023 alle departementen een CPO hebben benoemd. De CPO-Raad i.o. is in maart 2023 geïnstalleerd en zal eind 2023 doorgroeien naar een formele CPO-Raad.

Het CPO-stelsel zal worden ondergebracht in het vernieuwde I-stelsel. Planning is dat het nieuwe I-stelsel eind 2023 gereed zal zijn.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen