Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

DGOO
Directie Digitale Overheid

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk
www.linkedin.com/company/ministerie-van-bzk

Kenmerk
2021-0000076463

Uw kenmerk

Datum	9 februari 2021
Betreft	Waardering motie Kröger c.s. over privacy by design en open source

In deze brief geef ik een appreciatie van de motie Kröger c.s.[1], aangehouden tijdens het debat van woensdag 3 februari over het privacylek in de systemen van de GGD.

Ik wil vooropstellen dat ik het belang van privacybescherming en informatieveiligheid volledig onderschrijf. De publieke en semi- publieke sector is en blijft zelf verantwoordelijk voor het naleven van wet- en regelgeving. Daarbij geldt dat semi-publieke organisaties (zoals de zorg, onderwijs en woningcorporaties) in gevallen gehouden zijn aan sectorspecifieke wet- en regelgeving, opgelegd via een verantwoordelijk ministerie.
Vanuit mijn verantwoordelijkheid voor overheidsdienstverlening beschouw ik het als mijn taak om de publieke sector te voorzien van concrete tooling en ondersteuningsmaterialen op het gebied van informatieveiligheid, privacy by design en open source. In deze brief licht ik de aspecten informatieveiligheid, privacy by design, opensourcetechnologie en aanbestedingen toe.

<u>Informatieveiligheid</u>
Op 16 oktober 2018 heb ik uw Kamer geïnformeerd over maatregelen die overheidsbreed zijn getroffen om de informatieveiligheid bij de overheid te verhogen.[2] De aangekondigde maatregelen zijn onderdeel van de actie-agenda informatieveiligheid, een belangrijk aspect van mijn interbestuurlijke agenda NL DIGIbeter. In het licht van de aangehouden motie wil ik uw Kamer nader toelichten hoe er overheidsbreed wordt gewerkt aan inkoopeisen op het terrein van cybersecurity.

Mijn ministerie heeft in samenwerking met het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) een zogeheten instrument Inkoopeisen Cybersecurity Overheid (ICO)[3] ontwikkeld. ICO is een online instrument en is sinds maart vorig jaar online beschikbaar als prototype. Een

[1] *Kamerstukken II* 2020/21, 27529 nr. 245.
[2] *Kamerstukken II* 2018/19, 26643, nr. 574.
[3] De ICO-wizard is te vinden op https://www.bio-overheid.nl/ico-wizard/

expertgroep met vertegenwoordigers vanuit het Rijk, provincies, gemeenten en waterschappen heeft bijgedragen aan het formuleren van cybersecurity inkoopeisen voor de verschillende onderkende inkoopsegmenten zoals clouddiensten en serverplatformen. Op dit moment zijn negen segmenten uitgewerkt. In de eerste maanden van 2021 komen nog twee[4] onderkende ICT-inkoopsegmenten beschikbaar. Op dit moment wordt het instrument in pilots getest bij verschillende overheidsorganisaties, waaronder bij ICTU en Logius. De pilots lopen door tot in 2021. Om een breed beeld te krijgen van de praktische uitwerking van de cybersecurity inkoopeisen wordt ingezet op het uitvoeren van pilots in alle overheidslagen. Zodra het ICO-instrument breed is getest bij alle overheidslagen, zal ik het gebruik van dit instrument stimuleren bij het Rijk, provincies, gemeenten en waterschappen.

Privacy by design

In de Algemene Verordening Gegevensbescherming (AVG) is privacy by design verplicht gesteld voor organisaties om als concept – bestaande uit zeven principes[5] - toe te passen wanneer zij persoonsgegevens verwerken. De overkoepelende gedachte achter het concept houdt in dat bij de bepaling van de verwerkingsmiddelen en bij de verwerking van persoonsgegevens zelf, passende technische en organisatorische maatregelen moeten worden genomen om de gegevensbeschermingsbeginselen uit te voeren. Het eerdergenoemde ICO-instrument bevat al veel privacybeschermende maatregelen. Mijn ministerie heeft het CIP gevraagd om de maatregelen verder aan te vullen vanuit de zeven principes. De verwachting is dat deze aanvulling in de loop van dit jaar is uitgewerkt en gereed wordt gemaakt voor pilots bij de overheid die uiterlijk starten in het vierde kwartaal van dit jaar.

Open source

Zoals in april 2020 aan uw Kamer is gemeld[6], is het uitgangspunt van het kabinet dat de overheid haar broncodes vrijgeeft ('open source'), tenzij er gegronde redenen zijn om dat niet te doen. Dit is bijvoorbeeld het geval indien het vrijgeven van broncodes strijdig is met de belangen van nationale of openbare veiligheid of indien de benodigde vertrouwelijke werkwijze van de overheid, denk aan opsporing en toezicht, wordt geschaad door het vrijgeven van broncodes. Met het vrijgeven van de broncode kunnen maatschappelijke doelen worden gerealiseerd waaronder betere informatiebeveiliging. Met het vrijgeven en transparant maken van de broncode kunnen kwetsbaarheden sneller worden ontdekt. Het is wel van belang om ervoor te zorgen dat die kwetsbaarheden snel opgepakt en gerepareerd worden. Dat moet goed worden georganiseerd.

---

[4] De onderkende inkoopsegmenten zijn: Applicatieontwikkeling algemeen, Clouddiensten, Communicatievoorzieningen, DiGiD applicaties, Huisvesting IV, Maatwerk of maatwerkpakket, Middleware, Mobiele Applicaties, Serverplatform, Softwarepakketten en Toegangsbeveiliging.

[5] De zeven principes zijn: 1) Voorkomen is beter dan genezen, 2) Privacy is de standaard, 3) Integreren van gegevensbescherming en beveiliging in het ontwerp, 4) Volledige functionaliteit, 5) End-to-end beveiliging, 6) Zichtbaarheid en transparantie, 7) Respect voor privacy van de betrokkene- de betrokkene staat centraal

[6] *Kamerstukken II* 2019/20, 26643, nr. 676.

Transparantie mag nooit ten koste gaan van de veiligheid en de mate waarin de burger daadwerkelijk beschermd wordt. De inzet van software en de keuze voor open of gesloten kan nooit een doel op zich zijn, maar is een middel om maatschappelijke doelen, in dit geval informatiebeveiliging, te bereiken. Open source biedt veel mogelijkheden, maar het kan er in sommige gevallen op neerkomen dat de inzet van open source niet in de rede ligt en dat (op onderdelen) voor closed source kan – en moet - worden gekozen omdat veiligheid met open source niet gegarandeerd kan worden.

Het verzoek aan het kabinet om het principe 'open source, tenzij' bij aanbestedingen te hanteren, ligt in lijn met de reeds ingezette beleidsinzet. In 2020 is in opdracht van mijn ministerie een overheidsbreed onderzoek uitgevoerd naar de rol van open source in de huidige aanbestedingspraktijk. Dit heeft geresulteerd in de publicatie van 'publieke software aanbesteden'.[7] Dit is bedoeld om professionals binnen de overheid meer inzicht in nut en noodzaak van open source software bij aanbesteden te bieden. Daarnaast zal mijn ministerie in 2021 de mogelijkheden verkennen om tot nadere kaders te komen om het principe 'open, tenzij' in de aanbestedingspraktijk verder te concretiseren.

Aanbestedingen

Opdrachtgevers hebben een cruciale rol in aanbestedingen. In december stuurde ik uw Kamer het geactualiseerde Afwegingskader ICT opdrachten voor de rijksoverheid.[8] Dit kader helpt opdrachtgevers en inkopers, die betrokken zijn bij een ICT aanbesteding, een keuze te maken voor het vormgeven van de dialoog met het bedrijfsleven en voor de wijze van aanbesteden. Tevens zijn daarin relevante ontwikkelingen benoemd binnen de ICT inkoop van de rijksoverheid en zijn verschillende instrumenten op een rij gezet, die door opdrachtgevers in projecten kunnen worden benut. Bijvoorbeeld economische veiligheid bij inkopen, inkoopeisen cybersecurity overheid en de inzet van open source. Vanuit het afwegingskader wordt overigens ook verwezen naar de Handleiding Privacy by Design van het CIP.[9] Zoals ik reeds heb aangegeven onder het kopje "privacy by design", wordt het ICO-instrument aangevuld vanuit de zeven principes die ten grondslag liggen aan Privacy by Design.

De keuze voor een bepaalde aanbestedingsprocedure en de afweging van inzet van bepaalde instrumenten gaat uit van de professionaliteit van de opdrachtgever en het multidisciplinaire inkoopteam. Uitgangspunt hierbij is dat een overheidsorganisatie een eigenstandige primaire verantwoordelijkheid heeft over het starten, uitvoeren en eventueel stopzetten van ICT-projecten.

[7] Het playbook publieke software aanbesteden is gepubliceerd op 5 januari 2021: https://www.rijksoverheid.nl/documenten/brochures/2021/01/05/playbook-publieke-software-aanbesteden
[8] *Kamerstukken II* 2020/21, 26643, nr.728
[9] Zie https://www.cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/privacy-bescherming/#handleiding-privacy-by-design

Tot slot

Het functioneren van de overheid is in sterke mate afhankelijk van een goede sturing op en gebruik van digitale voorzieningen en infrastructuur. Het goed regelen van privacybescherming en informatieveiligheid is hier onlosmakelijk mee verbonden.

Tot slot wil ik benadrukken, dat privacybescherming, veiligheid en betrouwbaarheid kernprincipes zijn die ten grondslag liggen aan het functioneren van de publieke sector. Met in achtneming van deze principes worden keuzes gemaakt. Daarbij gaat het er om de verwerking van persoonsgegevens – waar mogelijk met technische maatregelen – tot een minimum te beperken. Want hoe goed beschermende maatregelen ook worden getroffen in systemen, absolute veiligheid is nooit te garanderen. Daarom is het van essentieel belang om daarop voorbereid te zijn en hiermee rekening te houden. Gelet op het voorgaande beschouw ik de motie als ondersteuning van in gang gezet beleid en laat ik deze aan het oordeel van uw Kamer.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops