Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
De staatssecretaris voor Digitalisering en Koninkrijkrelaties Dhr. F.Z. Szabó
Postbus 20901
2500 EX Den Haag

Datum
19 september 2024
Ons kenmerk
U202400439
Uw kenmerk
Consultatie BIO2
Telefoon
06-18575782
Bijlage(n)
-

Onderwerp: Betreft: consultatiereactie BIO2.

Geachte heer Szabó,

In de periode 8 mei tot 7 juni 2024 lag de tekst van de Baseline Informatiebeveiliging Overheid 2 (BIO2) ter consultatie[1]. Wij waarderen de transparante wijze waarop u de consultatietekst voor bewerking aanbood via de GitHub-omgeving en de verdere toelichtingen op de samenhang met NIS-2/Cyberbeveiligingswet.
Om een digitaal veilige en weerbare overheid te worden, is het van cruciaal belang dat gemeenten de nieuwe BIO2 als wet op lokaal niveau kunnen uitvoeren. Hierbij staan de haalbaarheid, betaalbaarheid en uitvoerbaarheid centraal.

Daarom brengen wij een aantal punten onder uw aandacht:

- Voor een goede implementatie is samenhang, een duidelijke invoeringstermijn en voldoende financiële middelen noodzakelijk
- Verduidelijk de positie van de Chief Information Security Officer (CISO)
- Versimpel en harmoniseer het toezichtstelsel en verlaag de auditlasten
- Houd rekening met verschillen tussen mede-overheden
- Vergroot transparantie en verlaag kosten door gezamenlijke aanpak inkoop en leveranciersmanagement
- Maak ook voor de BIO2 gebruik van overheidsbrede afstemming en vaststelling.

Voor een goede implementatie is samenhang, een duidelijke invoeringstermijn en voldoende financiële middelen noodzakelijk
De scope voor de invoering van de BIO2 is voor gemeenten fors en voor een groot deel nog onduidelijk, aangezien onder de cyberbeveiligingswet voor de primaire processen van de gemeenten tevens de nadere regelingen van de andere vakministers gaan gelden. Zoals

[1] https://www.digitaleoverheid.nl/nieuws/denk-mee-over-het-ontwerp-van-de-bio2/

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

beveiliging van aansturing van operationele technologie, (afval)water, (jeugd)zorg, Wmo, GGD en ook in de samenloop met de CER/Wet weerbarheid kritieke entiteiten. Dit bepaalt uiteindelijk de feitelijke scope van de BIO2 voor gemeenten. De verschillende richtlijnen maken bovendien geen onderscheid tussen grote of kleine gemeenten; zij moeten allen gelijktijdig aan dezelfde nieuwe eisen voldoen. Gemeenten hebben nu al onvoldoende middelen om te voldoen aan de eisen die de BIO1 stelt. Wij maken ons zorgen over de haalbaarheid, uitvoerbaarheid en betaalbaarheid van de BIO2 en de andere regelingen onder de cyberbeveiligingswet.

Voor de effectieve invoering en uitvoering van de BIO2 en de richtlijnen van de andere vakministers is het randvoorwaardelijk dat die nationale wetgeving tijdig, gebundeld, geïntegreerd en integraal afgewogen wordt aangeboden vanuit de verschillende ministeries, met een prioritering in de tijd. Wij vragen u om een passende invoeringstermijn en afspraken over een groeipad. Daarbij is het noodzakelijk dat dit voor gemeenten voorzien wordt van de benodigde structurele middelen.

Verduidelijk de positie van de Chief Information Security Officer (CISO)
In onze brief van 9 april 2024[2] vroegen wij om de rol van de CISO te versterken door een directe en duidelijke communicatielijn met de bestuurders te waarborgen, en deze positie te verankeren in de BIO2. De BIO2 zorgt voor deze versterking van de positionering van de CISO, door een onafhankelijke adviesrol naar zowel het bestuur als het lijnmanagement. Maar dit is nog niet voldoende. De waarborgen die noodzakelijk zijn om intern onafhankelijk te kunnen rapporteren aan het bestuur, vragen nog aandacht.

We vragen u om toe te werken naar een positionering van de CISO die zowel de onafhankelijkheid ten opzichte van het lijnmanagement en bestuur waarborgt, alsook een sterke verbinding met de ambtelijke organisatie behoudt, met de bijbehorende rechtsbescherming. In lijn met de uitwerking van de verantwoordelijkheidsverdeling ingevolge de cyberbeveiligingswet, zien we graag een nadere toelichting op de positie van de CISO in de nota van toelichting van de ministeriële regeling, waarin de BIO2 wordt verankerd.

Versimpel en harmoniseer het toezichtstelsel en verlaag de auditlasten
Gemeenten verantwoorden zich primair naar de gemeenteraad. Gemeenten gebruiken hier de ENSIA-systematiek voor, die zal worden uitgebreid om ook op de BIO2 verantwoording af te leggen. Het uitwerken van de BIO2 als basis voor informatieveiligheid bij de overheid biedt mogelijkheden tot harmoniseren van normenkaders van de andere wetten waar overheidsorganisaties aan moeten voldoen en waarin eisen aan informatieveiligheid zijn opgenomen. Wij zien in die harmonisering mogelijkheden om de wijze van audit en verantwoording te vereenvoudigen en daarmee de auditlasten en -kosten te verlagen en vragen u dit te concretiseren in het uit te werken verantwoordings- en toezichtstelsel.

Houd rekening met verschillen tussen mede-overheden
De BIO2 sluit aan op de internationale ISO-aanpak waarmee informatiebeveiliging procesmatig en risico-gebaseerd ingericht wordt, gericht op het borgen van digitale weerbaarheid en passend bij de eigen organisatie. Gemeenten zijn in grote mate afhankelijk van ketenpartners en ICT-dienstverleners om de doelstellingen uit de NIS-2 en de BIO2 te kunnen realiseren.
We werken graag samen toe naar een gezamenlijk niveau voor veilige gegevensuitwisseling in de keten en naar een moment dat het stellen van specifieke eisen aan de samenwerking in overheidsketens tot een minimum beperkt kan worden. We vragen u hierbij rekening te houden met de forse verschillen die er tussen de mede-overheden zitten.

[2] https://vng.nl/sites/default/files/2024-04/reactie_nis2.pdf

Vergroot transparantie en verlaag kosten door gezamenlijke aanpak inkoop en leveranciersmanagement
In de concept BIO2 is de toepassing van de set aan Inkoopeisen Cybersecurity Overheid (ICO)[3] opgenomen. Met uw voornemen om de BIO2 in de Cyberbeveiligingswet te verankeren wordt de toepassing van die ICO-eisenset ook wettelijk verplicht.

Gemeenten onderschrijven het belang van eenduidigheid voor inkoopeisen cybersecurity voor de hele overheid. Een aantal van de Inkoopeisen Cybersecurity Overheid (ICO) is opgenomen in de Gemeentelijke Inkoopvoorwaarden bij IT-Toolbox (GIBIT)4. In de bovenliggende principes voor de digitale samenleving5 leggen gemeenten de basis om technologie veilig, inclusief en verantwoord in te zetten. Ook zijn de principes van informatiebeveiliging en privacybescherming by-design hierin opgenomen. Deze principes zijn verder uitgewerkt in de GIBIT die gemeenten bij inkoop en aanbesteding toepassen.

Wij zien mogelijkheden om eenduidige en samenhangende kaders te stellen aan de inkoop en gedurende de looptijd van het contract, zodat gezamenlijk de digitale veiligheid van overheidsdiensten wordt versterkt. Hiertoe stellen ministeries echter verschillende handreikingen6 en eisensets7 op.

Een belangrijke ontwikkeling is de Cyber Resillience Act (CRA) waarmee de minister van Economische Zaken, mede namens de EU, cybersecurityeisen stelt aan de fabrikanten en leveranciers voor een keurmerk op veilige hard- en software, voordat zij een ICT-product of dienst op de Europese markt mogen brengen. Tevens dienen zij gedurende de levensduur van producten gratis veiligheidsupdates te leveren en digitale kwetsbaarheden en incidenten te melden. Hierop wordt toezicht ingericht. Daarmee komt er een verantwoordelijkheid bij de leveranciers en producenten, om veilige hardware, software en diensten aan te bieden en te onderhouden. Het stellen van nadere inkoopeisen door aanbestedende diensten zal daardoor ook veranderen. Het goede gesprek gedurende de periode dat het contract loopt heel belangrijk blijft om tussentijdse dreigingen/kwetsbaarheden op te vangen en samen aan te pakken.

Wij verzoeken u om voorafgaand aan de wettelijke invoering van de BIO2 interbestuurlijk de governance en het proces in te richten voor het opstellen, bijstellen en vaststellen van één eenduidige set aan inkoopeisen cybersecurity waar de hele overheid aan zou moeten voldoen, in lijn met de verantwoordelijkheden die op de leveranciers en fabrikanten komen te rusten onder de CRA. Wij verzoeken u aan te sluiten op het interbestuurlijke besluitvormingsproces voor de BIO2.
In samenwerking met leveranciers en fabrikanten kan de overheid er zo voor zorgen dat bij de toepassing van ICT-diensten en -producten de digitale veiligheid voorop staat en dat de dienstverlening gedurende de looptijd van de contracten voldoet aan de Europese en nationale (inkoop)eisen voor cybersecurity[8].

Maak ook voor de BIO2 gebruik van overheidsbrede afstemming en vaststelling
De BIO1 kent een verplichtende zelfregulering. Dit is in het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), zo afgesproken en in de ministerraad in december 2018 vastgesteld. Het is van belang dat wanneer de BIO via de Cyberbeveiligingswet wordt verankerd, er zorgvuldig en juridisch onderzocht moet worden of hier sprake is van medebewind om te verzekeren dat alle betrokken

[3] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/inkoopeisen-cybersecurity-overheid/
[4] https://vng.nl/projecten/gibit
[5] https://vng.nl/sites/default/files/2022-12/Principes-voor-de-Digitale-Samenleving.pdf
[6] https://www.nctv.nl/onderwerpen/economische-veiligheid/toolbox-veilig-inkopen
[7] https://www.rijksoverheid.nl/actueel/nieuws/2023/12/01/europees-akkoord-veiligheidseisen-en-standaarden-voor-alle-digitale-producten
[8] https://vng.nl/nieuws/regels-nodig-voor-inkoop-risicovolle-soft-en-hardware

bestuurslagen hun verantwoordelijkheden en bevoegdheden op een passende wijze kunnen blijven uitoefenen. Wij vragen u om ook voor deze BIO2 en volgende iteraties en de onderliggende aanpak voor inkoopeisen en leveranciersmanagement dezelfde overheidsbrede afstemming en vaststellingsroute volgen. Voorts vragen wij u om de BIO2 ook in een bestuurlijk overleg te bekrachtigen, dan wel via een voorhangprocedure voor te leggen, zodat de gemeenten en andere medeoverheden in de interbestuurlijke besluitvorming voldoende worden gekend.

Namens alle gemeenten vertrouwen wij erop dat u onze punten meeneemt in de definitieve versie van de BIO2 en de bijbehorende Nota van Toelichting. Waar verdere toelichting nodig is zullen we deze uiteraard verstrekken.

Afgelopen jaren werkten wij samen met uw ambtenaren om tot een goede implementatie van de NIS2- richtlijn en BIO2 voor lokale overheden te komen. Wij zetten deze samenwerking graag voort om zo tot een digitaal veilige en weerbare overheid te komen.

Met vriendelijke groet,

Vereniging van Nederlandse Gemeenten

mr. L.K. Geluk
Algemeen directeur