Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1116

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 januari 2024

In het commissiedebat Informatiebeveiliging bij de overheid van de vaste commissie voor Digitale Zaken van 5 april jl. (Kamerstuk 26 643, nr. 1016) is toegezegd de Kamer een brief te sturen naar aanleiding van de vraag van het lid Slootweg (CDA) over (extra) waarborgen in de aanbestedingsregels ten behoeve van mensen die de overheid informatie toevertrouwen.

Allereerst is het belangrijk om voorop te stellen dat het waarborgen van privacy en informatiebeveiliging altijd om maatwerk vraagt, en daarbij een onderscheid te maken in de verschillende fases van een inkooptraject. Deze verschillende fases kennen verschillende mogelijkheden om invulling te geven aan de eisen rondom privacy en informatiebeveiliging. De eerste fase is de aanbestedingsfase, wanneer het betreffende product of dienst wordt ingekocht. Daarna volgt de fase dat er een contract of overeenkomst wordt gesloten, en tot slot de uitvoeringsfase van de overeenkomst.

Aanbestedingsfase

Het inkoopproces start met de aanbestedingsfase. De aanbestedingsregels hebben op de aanbestedingsprocedure zelf betrekking, dus op het proces van (het inrichten van) de aanbesteding, en niet op de concrete opdracht. De aanbestedingswet- en regelgeving zelf is daarmee ook niet de plek waar inhoudelijke waarborgen omtrent privacy en informatiebeveiliging vastgelegd zijn en/of worden[1], maar biedt wel de ruimte om ten aanzien van een concrete opdracht specifieke eisen en criteria op te nemen in de aanbestedingsdocumenten.

[1] De algemene verplichting om opdrachtspecifieke afspraken te maken als sprake is van de verwerking en bescherming van persoonsgegevens, is reeds in de AVG vastgelegd.

kst-26643-1116
ISSN 0921 - 7371
's-Gravenhage 2024

In de aanbestedingsfase wordt in kaart gebracht welke eisen en wensen noodzakelijk zijn om het project succesvol te laten zijn. Dit heeft ook betrekking op eisen en wensen op het gebied van privacy en informatiebeveiliging, die noodzakelijk zijn om een adequaat niveau van privacy en informatiebeveiliging te kunnen waarborgen.[2] Deze eisen en wensen moeten vervolgens in de aanbestedingsdocumenten worden opgenomen. Als er sprake is van het verwerken van persoonsgegevens is ook het sluiten van een verwerkersovereenkomst verplicht.

Sluiten van het contract

Na de aanbestedingsprocedure volgt het sluiten van de overeenkomst met de betreffende marktpartij. De Rijksoverheid contracteert op basis van de Algemene Rijksvoorwaarden en de daarbij behorende modelovereenkomsten. Hierin zijn reeds verschillende bepalingen over geheimhouding, informatiebeveiliging, privacy, toezicht en audits opgenomen.

Gebruik van de Algemene Rijksvoorwaarden in combinatie met de modelovereenkomsten is dan ook het uitgangspunt. Het vereist maatwerk om de concrete noodzakelijke waarborgen af te spreken met de betreffende marktpartij, en deze nadere maatwerkafspraken in de overeenkomst op te nemen.

Zoals hierboven al kort aangegeven moet als er sprake is van het verwerken van persoonsgegevens er ingevolge de AVG daarnaast ook nog een verwerkersovereenkomst worden gesloten met de betreffende marktpartij, waarbij moet worden aangegeven hoe door de betreffende partij voldaan wordt aan de normen en passende technische en organisatorische maatregelen uit het Programma van Eisen of de offerteaanvraag in het kader van de beveiliging van persoonsgegevens. Daarnaast wordt afgesproken hoe er wordt omgegaan met inbreuken in verband met persoonsgegevens, waaronder datalekken.
Op deze wijze bieden de bestaande regels en instrumenten genoeg ruimte om waarborgen te stellen op het gebied van privacy en informatiebeveiliging.

Contractuitvoeringsfase

Na het sluiten van de overeenkomst, start de uitvoeringsfase van het contract. Tijdens deze fase moet er via contractmanagement op gestuurd worden dat de partijen ook de afspraken rondom informatiebeveiliging en privacy nakomen. Dit wordt onder meer gedaan door het uitvoeren van toezicht en audits indien concrete omstandigheden daartoe aanleiding geven. Indien blijkt dat de afspraken niet goed worden nagekomen, wordt dit met passende prioriteit via de reguliere managementcyclus opgelost. In het kader van ketenrisico's moet er in deze fase ook aandacht zijn voor het leveranciersmanagement, inclusief de inzet van subleveranciers.

Om toezicht te houden is het best practice om te eisen dat de leverancier op basis van oordelen van onafhankelijke derden[3] aantoont te voldoen aan de informatiebeveiligings- en privacyeisen. Op basis van de Algemene Rijksvoorwaarden in combinatie met de modelovereenkomsten kan indien concrete omstandigheden daartoe aanleiding geven een audit uitgevoerd worden waaraan de leverancier of opdrachtnemer moet

[2] De eisen omtrent informatiebeveiliging en privacy zijn o.a. geregeld in de Algemene Verordening Gegevensbescherming (AVG), de Wet beveiliging netwerk- en informatiesystemen en de Baseline Informatiebeveiliging Overheid (BIO).
[3] Voorbeelden hiervan zijn auditverklaringen, certificeringsrapporten, pentestrapport, SOC2 type 2 verklaringen, ISAE 3402-2 verklaringen en FEDRAMP-rapporten.

meewerken. Een dergelijk onderzoek kan betrekking hebben op uiteenlopende contractuele en wettelijke verplichtingen, zoals naleving van de AVG of eisen aan informatieveiligheid. Ook kunnen in de overeenkomst nog nadere concrete afspraken gemaakt over bijvoorbeeld de aard of het aantal tijdens de contractduur uit te voeren audits.
Daarnaast zijn er nog wettelijke toezichthouders, zoals de Autoriteit Persoonsgegevens (AP) voor (toezicht op naleving van) de AVG.

Zoals hierboven aangegeven zijn er meerdere mogelijkheden en instrumenten om waarborgen omtrent privacy en informatiebeveiliging in verschillende fases in het inkoopproces in te bouwen, en daarmee het risico op inbreuken en datalekken in kaart te brengen en zoveel mogelijk te mitigeren. Het is belangrijk dit gehele bestaande instrumentarium nog beter te benutten en aandacht aan te blijven besteden.

Baseline Informatiebeveiliging Overheid (BIO) & Inkoopeisen Cybersecurity Overheid (ICO)

De overheid hanteert de Baseline Informatiebeveiliging Overheid (BIO) als standaard om zich te weren tegen dreigingen gericht tegen de informatievoorziening van de overheid. Daarnaast worden standaarden gehanteerd zoals de ISO & NEN-standaarden, of van het NIST, CIS en OWASP.

Door in een concrete aanbesteding specifieke beveiligingseisen te stellen en te specificeren, kan de scope afgebakend worden en ingegaan worden op de verantwoordelijkheden van de betrokken partijen, wat tevens bijdraagt aan een efficiënt en effectief inkoopproces. In een aanbesteding wordt informatiebeveiliging primair geborgd via concrete en voor de opdracht passende beveiligingseisen in het Programma van Eisen. Daarvoor biedt onder andere de BIO handvatten. De BIO schrijft het basisniveau voor informatiebeveiliging voor binnen de overheid. Regelmatig zijn echter aanvullende maatregelen op het gebied van informatiebeveiliging noodzakelijk, hetgeen maatwerk vereist. Tijdens de aanbestedingsfase worden verkorte risicoanalyses uitgevoerd. Op basis daarvan worden aanvullende eisen risicogebaseerd gesteld die toegesneden zijn op de exacte scope en aard van de aanbesteding.

Ook voor de BIO geldt dat omtrent toezicht het best practice is om te eisen dat de leverancier op basis van oordelen van onafhankelijke derden aantoont te voldoen aan de BIO, en hetgeen hierboven bij de contractuitvoeringsfase uiteengezet is met betrekking tot het (laten) uitvoeren van audits.

Voor de vertaling naar meer specifieke eisen per in te kopen dienst of product zijn eisen ten aanzien van cybersecurity ontwikkeld. Deze eisen komen samen in een online-instrument welke beschikbaar is voor iedereen, met de naam «Inkoopeisen Cybersecurity Overheid (ICO)». De hedendaagse dreigingen vergen echter een meer specifiek eisenpakket per dienst of product, daarom worden aanvullende instrumenten ontwikkeld om dit eisenpakket aan te scherpen.

Deze cybersecurity-eisen kunnen als basis dienen om het programma van eisen op te stellen voor aanbestedingen en deze vervolgens op te nemen in af te sluiten contracten. Dit draagt tevens bij aan de eisen die overheid stelt aan haar leveranciers. Onlangs is dit aan uw Kamer gemeld in de Nederlandse Cybersecurity strategie[4] en in de Werkagenda Waardengedreven Digitaliseren die 4 november jl. aan uw Kamer is aangeboden.[5] In

[4] *Kamerstukken II* 2022/23, 26 643, nr. 925.
[5] *Kamerstukken II* 2022/23, 26 643, nr. 940.

de Werkagenda is aangegeven dat uiterlijk eind 2025 via wetgeving is geborgd dat de normensets voor veilig inkopen van ICT-producten en -diensten verplicht worden toegepast door overheden.

Het ICO-instrument is sinds 2021 beschikbaar via de site BIO-overheid.nl[6] voor alle overheidsorganisaties en ook voor leveranciers van ICT-producten en -diensten. Er loopt een meerjarig programma om overheidsorganisaties te helpen bij het gebruik van het ICO-instrument.

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

[6] Zie onder meer www.bio-overheid.nl/ico-wizard/.