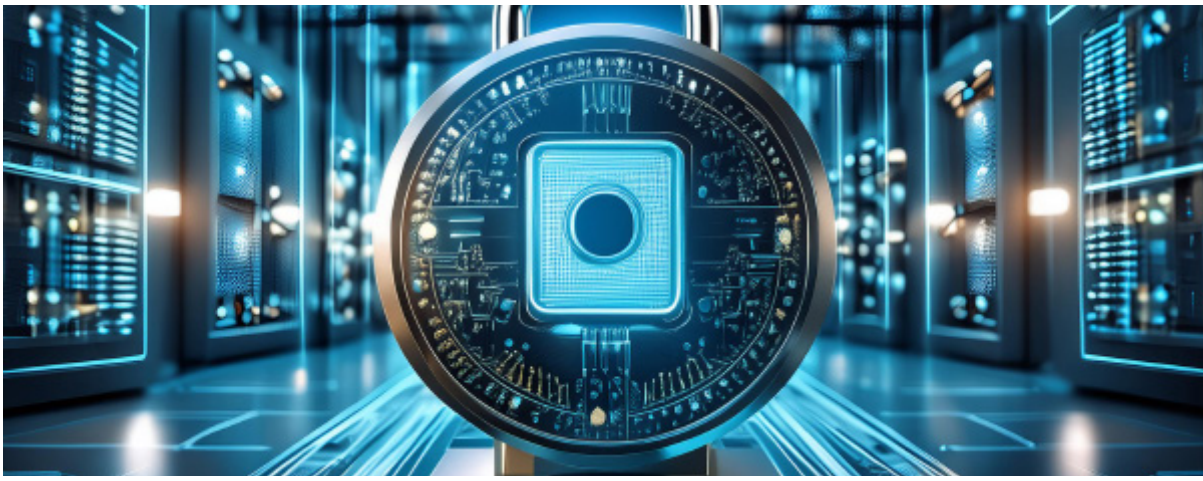
Juli 2024

Procurement letter

Integratie van de nieuwe cyber-beveiligingswet (NIS 2) in aanbestedingen:

Hoe wezenlijke wijziging bij de uitvoering van opdracht te voorkomen



Wat is een wezenlijke wijziging?

Een overeenkomst die na een aanbesteding is gesloten, mag niet wezenlijk worden gewijzigd gedurende de looptijd ervan. Dit principe is vastgelegd in de Aanbestedingswet 2012, hoofdstuk 2.5 "Wijziging van overheidsopdrachten". Wanneer er sprake is van een wezenlijke wijziging dan moet de opdracht in principe opnieuw worden aanbesteed.
Gelukkig zijn er manieren om ondanks onduidelijkheid over toekomstige wet- en regelgeving waaraan in de loop van de overeenkomst aan voldaan moet worden mee te nemen in de aanbesteding.

Artikel 2:163c Aw bepaalt dat wijzigingen alleen zijn toegestaan als deze duidelijk, nauwkeurig en ondubbelzinnig zijn vastgelegd in de oorspronkelijke aanbestedingsdocumenten. Dergelijke herzieningsclausules moeten:

- De omvang en aard van mogelijke wijzigingen of opties omschrijven;
- De voorwaarden waaronder deze kunnen worden gebruikt aangeven;
- Niet leiden tot wijzigingen die de algemene aard van de opdracht veranderen.

Het is dus belangrijk om na te gaan of dergelijke herzieningsclausules ook voor de nieuwe cyberbeveiligingswet meegenomen kunnen worden. Alvorens hier verder op in te gaan zullen eerst het doel, de scope en de belangrijkste verplichtingen van de cyberbeveiligingswet worden besproken.

Doel van de cyberbeveiligingswet

De cyberbeveiligingswet implementeert de NIS 2-richtlijn in Nederland en is van toepassing op entiteiten die bij uitval van diensten een ontwrichtende impact op de economie en samenleving kunnen hebben. De internetconsultatie van de conceptwet loopt tot 1 juli 2024. De wet richt zich op diverse sectoren zoals energie, vervoer, bankwezen, gezondheidszorg en digitale infrastructuur. Entiteiten die onder deze wet vallen worden opgedeeld in essentiële en belangrijke entiteiten. Voor de zorgplicht maakt deze indeling niet uit, maar wel voor het toezichtsregime. Essentiele entiteiten kunnen namelijk proactief worden gecontroleerd op het voldoen aan de cyberbeveiligingswet.
Belangrijke entiteiten kunnen achteraf worden gecontroleerd na een beveiligingsincident of zodra er een melding bij de toezichthouder wordt gedaan. Om te bepalen of een entiteit onder de wet valt, kan gebruik worden gemaakt van een zelfevaluatietool van de RDI[1].

1 NIS2 Zelfevaluatie NL (regelhulpenvoorbedrijven.nl)

De Procurement Letter is een uitgave van:

CORVERS
COMMERCIAL & LEGAL AFFAIRS

BARTELS
SUETERS
RASSA
AANBESTEDINGSADVOCATEN

Belangrijkste verplichtingen van de cyberbeveiligingswet

De conceptwettekst benoemt drie belangrijke verplichtingen: de zorgplicht, de meldplicht en de registratieplicht. In dit artikel focussen we op de zorgplicht en de meldplicht.

Zorgplicht

De zorgplicht houdt in dat entiteiten passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheren en incidenten zoveel mogelijk te voorkomen. Deze maatregelen moeten periodiek worden geëvalueerd en aangepast aan de stand van de techniek. Ook de aard en omvang van het risico en de uitvoeringskosten moeten worden meegenomen in het bepalen van de maatregelen.

De zorgplicht is uitgewerkt in artikel 23 van de cyberbeveiligingswet en omvat geen uitwerking van de maatregelen die wel staan opgenomen in artikel 21 NIS 2 voor wat betreft de zorgplicht[2]. Het gaat daarbij om maatregelen zoals:

- Beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- Incidentenbehandeling en bedrijfscontinuïteit;
- Beveiliging van de toeleveringsketen en gebruik van cryptografie;
- Beveiligingsaspecten ten aanzien van personeel en toegangsbeleid.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Het Nationale Cyber Security Centrum heeft een infosheet gemaakt die de zorgplicht nader toelicht[3].

Meldplicht

De meldplicht betreft het melden van significante incidenten. Een incident wordt als significant beschouwd als het een ernstige operationele verstoring of financiële verliezen veroorzaakt, of aanzienlijke materiële of immateriële schade aan andere entiteiten toebrengt[4]. De meldplicht lijkt sterk op de meldplicht voor datalekken onder de AVG. Ik verwacht dat via beleid er een nadere inkleuring zal worden gegeven van de term significante incidenten. De vraag die belangrijk is voorafgaand aan de aanbesteding is wie de melding mag doen.

Integratie van de cyberbeveiligingswet in aanbestedingen

Voldoen aan de zorgplicht

Voor overheidsorganisaties zoals het Rijk, gemeenten, waterschappen en provincies, geldt nu de Baseline Informatiebeveiliging Overheid (BIO) als normenkader voor informatiebeveiliging. Dit kader wordt momenteel aangepast aan de NIS 2-richtlijn. Voor deze partijen kan het dus voldoende zijn om aan te geven dat het aangeschafte systeem moet voldoen en blijven voldoen aan de eisen die daaraan worden gesteld vanuit de BIO ook wanneer deze is aangepast aan de implementatie van NIS 2.

Voor aanbestedende diensten die niet onder de BIO vallen maar wel moeten voldoen aan de NIS 2, is het belangrijk om herzieningsclausules op te nemen zoals gespecificeerd in artikel 2:163c Aw om zo aan de zorgplicht te kunnen voldoen. Aanbestedende diensten kunnen bijvoorbeeld aangeven dat enkele maanden voor de implementatie van de NIS 2-richtlijn een nieuwe risicoanalyse moet plaatsvinden, zodat de reeds bestaande informatiebeveiligingsmaatregelen hierop kunnen worden aangepast door opdrachtnemer zonder dat dit leidt tot een wezenlijke wijziging.

Belangrijk hierbij is wel om bijvoorbeeld afspraken te maken over eventuele hogere kosten die hieruit voort kunnen vloeien. Dit kan door hiervoor een budget voor af te spreken of bijvoorbeeld een uurtarief voor het aanpassen van de maatregelen voor zover deze redelijkerwijs niet in de afgenomen dienstverlening zijn

2 Richtlijn (EU) 2022/2555 van het Europese Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr 910/2014 en richtlijn 2018/1972 en tot intrekking van Richtlijn (EU)2016/1148 (NIS 2-richtlijn).

3 Infosheet NIS2 verplichtingen: Zorgplicht | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

4 Artikel 27 lid 2 concept cyberbeveiligingswet internetconsultatieversie.

opgenomen. Door het maken van dergelijke procesafspraken wordt eveneens een wezenlijke wijziging voorkomen en kan de aanbestedende dienst toch aan haar verplichtingen onder de cyberbeveiligingswet voldoen.

Voldoen aan de Meldplicht

Bij het voldoen aan de meldplicht is altijd de vraag wie de melding moet doen en hoe snel een melding gedaan moet worden. Hierbij kan aansluiting worden gezocht bij de keuzes die gemaakt zijn binnen de aanbestedende dienst voor het melden van een datalek. Vooruitlopend op de inwerkingtreding van de cyberbeveiligingswet kan in de aanbesteding nu al een eis worden meegenomen zoals:

"Opdrachtnemer meldt een significant incident binnen een x aantal uur aan opdrachtgever zodra dit wettelijk verplicht is."

Door een dergelijke eis op te nemen is er geen sprake van een wezenlijke wijziging zodra de cyberbeveiligingswet in werking treedt.

Conclusie

Door herzieningsclausules op te nemen in aanbestedingsdocumenten en tijdig risicoanalyses uit te voeren, kunnen aanbestedende diensten nu al rekening houden met de nieuwe cyberbeveiligingswet zonder dat sprake is van een wezenlijke wijziging. Dit zorgt ervoor dat aanbestedende diensten nu al in een aanbesteding voorbereid zijn op de invoering van de cyberbeveiligingswet en op het moment van inwerkingtreding van de cyberbeveiligingswet voldoen aan de aangescherpte eisen voor informatiebeveiliging die dan gaan gelden.

Auteur:

Mr. drs. Carolien Jobse
Privacy- en informatiebeveiligingsjurist
CHvV Associates

De Procurement *Letter*

De Procurement Letter is een nieuwsbrief met artikelen en nieuws rondom (Europees) aanbesteden. die 1 tot 2 maal per jaar wordt uitgegeven door Corvers Procurement Services en Bartels Sueters Rassa Aanbestedingsadvocaten.
Andere artikelen uit deze editie:

- Intrekken van een aanbesteding – waar op te letten?
- Fouten en herstel

Bekijk en/of download alle artikelen uit deze Procurement Letter hier.

Heeft u zich nog niet aangemeld voor de Procurement Letter, maar wilt u deze in de toekomst ook graag per mail ontvangen? Dan kunt u zich **aanmelden** via de aanmeldknop onderaan de site **www.aanbestedingsadvocaten.nl**

Redactie
073 - 614 8000

Stationsplein 91
5211 BM 's-Hertogenbosch

nieuwsbrief@aanbestedingsadvocaten.nl
www.aanbestedingsadvocaten.nl