PELS RIJCKEN

Juridische analyse sturingsmechanismen mensenrechtenschendingen in aanbestedingen van camarasystemen door gemeenten

Versie 11 januari 2024



1 Achtergrond

1.1 De VNG heeft ons gevraagd om te adviseren over de juridische mogelijkheden om bij de inkoop van camera's door Nederlandse gemeenten risico's in termen van mensenrechtenschendingen en cyberveiligheid zoveel als mogelijk te mitigeren.

1.2 De afgelopen maanden hebben wij in overleg met de VNG diverse interviews gevoerd. Uit die interviews hebben wij begrepen dat de risico's op het gebied van cyberveiligheid grotendeels kunnen worden weggenomen door het treffen van technische maatregelen (bijvoorbeeld door het toepassen van goede netwerksegmentatie). Een restrisico blijft.

1.3 Bij het stellen van de adviesvraag door de VNG is tot uitgangspunt genomen dat gemeenten camera's inkopen die reeds ontwikkeld zijn en dus "commercial off-the-shelf" beschikbaar zijn. Deze analyse ziet niet op de ontwikkeling van camera's in opdracht van een gemeente.

1.4 Naar wij van de geïnterviewde experts begrepen, zijn de camera's die in de regel door de gemeenten worden ingekocht afkomstig van zes fabrikanten. De camera's van twee van deze fabrikanten worden vervaardigd in China. Eén camera in Zuid-Korea en één in Taiwan. De overige twee camera's worden grotendeels in Europa vervaardigd.

1.5 Deze fabrikanten zijn in de regel zelf geen inschrijvers op de aanbestedingen van Nederlandse gemeenten. Over het algemeen doen aan aanbestedingen van Nederlandse gemeenten systemintegrators mee die camera's aanbieden van één van deze zes fabrikanten.

1.6 Van belang is dat bij het opstellen van deze analyse tot uitgangspunt is genomen dat gemeenten in de aanbesteding geen specifieke partijen op voorhand uitsluiten.

1.7 Deze analyse richt zich wel op de mogelijkheden die gemeenten hebben om bij de inkoop van camerasystemen in Europese aanbestedingen zo veel als mogelijk:

- inschrijvers te weren die zijn gevestigd in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen. Blijkens het AIVD jaarverslag 2022 zijn vorenbedoelde landen thans Rusland, Iran, Noord-Korea en China;
- camerasystemen te weren die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen.

1.8 Naar inschatting van de VNG worden met de onder punt 1.7 dezes genoemde maatregelen ook zoveel als mogelijk camera's geweerd van partijen die de mogelijkheid tot culturele genocide of etnisch profileren buiten Europa faciliteren of hebben gefaciliteerd.

1.9 Waar de VNG onderkent dat thans nog geen camera's beschikbaar zijn die volledig in Europa zijn ontwikkeld/gefabriceerd, wenst de VNG de markt ook nog te prikkelen op Europees grondgebied gefabriceerde camera's aan te bieden die zo min mogelijk onderdelen bevatten die zijn ontwikkeld en/of gefabriceerd in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen. Inschrijvers kunnen in de aanbesteding punten scoren afhankelijk van het aantal onderdelen dat is ontwikkeld en/of gefabriceerd in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen. Hoe minder camera onderdelen uit landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen hoe beter.

1.10 Ook wenst de VNG bij inschrijving een plan van aanpak uit te vragen waarin inschrijvers de cyberveiligheidsrisico's met het aangeboden camerasysteem inzichtelijk dienen te maken, alsook de beheersmaatregelen die zij zullen treffen teneinde die risico's zoveel als mogelijk te mitigeren. Hoe effectiever de aangeboden beheersmaatregelen, hoe beter. Een dergelijk plan van aanpak kan ook worden uitgevraagd wat betreft mensenrechtenschendingen (culturele genocide en etnisch profileren).

1.11 U verzocht ons na te gaan in hoeverre de onder punten 1.7 – 1.10 dezes genoemde maatregelen/sturingsmechanismen vanuit aanbestedingsrechtelijk perspectief toelaatbaar zijn. Daarnaast verzocht u ons na te gaan of ook nog andere aanbestedingsrechtelijke sturingsmechanismen kunnen worden toegepast in Europese aanbestedingen teneinde risico's in termen van mensenrechtenschendingen (culturele genocide en etnisch profileren buiten Europa) en cyberveiligheid zoveel als mogelijk te mitigeren. Ook verzocht u ons na te gaan welke mogelijkheden gemeenten hebben op basis van (toekomstige) Europese richtlijnen inzake mensenrechten, alsook op basis van het wetsvoorstel Wet verantwoord en duurzaam internationaal ondernemen. Dat doen wij vanzelfsprekend graag.

Zoals besproken, ziet onze advisering niet op het mitigeren van eventuele mensenrechtenschendingen op "de werkvloer"/"in de mijnen" met uitzondering van de contractvoorwaarden Mensenrechten in hoofdstuk 4 dezes.

Evenmin zijn wij nagegaan in hoeverre met toepassing van ISO-standaarden of "Zero Trust Architecture" uitgangspunten/cyberveiligheidseisen kan worden bewerkstelligd dat camera's uit specifieke landen kunnen worden geweerd.

Uit de interviews is overigens gebleken dat in sommige gemeenten ook de politie de gemeentecamera's uitleest. Niet is gebleken dat bij de inkoop van die camera's gerubriceerde gegevens een rol spelen (zie ook hierna onder punt 3.22 dezes).

1.12 Graag merken wij ook nog het volgende op. Indien de VNG/gemeenten beslissen om actief maatregelen te treffen om producten uit derde landen uit te sluiten, achten wij het raadzaam om die maatregelen op voorhand af te stemmen met het ministerie van EZK om te voorkomen dat dit onverhoopt negatieve (geopolitieke) implicaties heeft.

1.13 Zoals wij hierna nader uiteen zullen zetten, achten wij de volgende sturingsmechanismen een optie teneinde risico's in termen van mensenrechtenschendingen en cyberveiligheid zoveel als mogelijk te mitigeren:

Sturingsmechanisme	**Wetsartikel**	**Randnummer**	**Optie? Ja/Nee**
Uitvoerings voorwaarden	Art. 2.80 Aw 2012	2.2.7 e.v.	Ja, mits verenigbaar met het EU-recht
Gunningscriterium plan van aanpak met contractuele voorwaarde	Art. 2.113a Aw 2012	2.4 e.v.	Ja, mits proportioneel en controleerbaar
Contractvoorwaarden Mensenrechten		4 e.v.	Ja, mits proportioneel

1.14 Voor de goede orde merken wij nog op dat het uiteindelijk aan iedere individuele gemeente is uit dit pallet aan voorwaarden te kiezen.

2 Voorgestelde sturingsmechanismen VNG

2.1 Weren inschrijvers gevestigd in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen

2.1.1 De vraag in hoeverre inschrijvers uit derde landen al dan niet van een aanbesteding kunnen worden uitgesloten dient op basis van een "case-by-case assessment" te worden bepaald. Met sommige "derde landen" heeft de Europese Unie ("EU") via multi- of bilaterale verdragen afspraken gemaakt over de toegang tot de Europese aanbestedingsmarkt. Aanbestedende diensten moeten die regels volgen.

2.1.2 Het belangrijkste verdrag tussen de EU en derde landen is de Government Procurement Agreement (hierna: "GPA"). Wanneer de GPA van toepassing is, mogen leveranciers uit derde landen conform artikel 1.23 Aanbestedingswet geen minder gunstige behandeling krijgen dan ondernemers uit de EU.

2.1.3 Nu Volksrepubliek China (op dit moment) geen partij is bij de GPA en evenmin sprake is van een bilaterale handelsovereenkomst met China, staat het gemeenten vrij om Chinese bedrijven – categorisch, op voorhand – uit te sluiten bij aanbestedingen.

2.1.4 Overigens wijzen wij volledigheidshalve op de conclusie van Advocaat-Generaal Rantos van 11 mei 2023 in de zaak C-266/22 consortium CRRC Qingdao Sifang CO LTD/Astra

Vagoane tegen de autoriteit spoorweghervormingen te Roemenië waarin de vraag speelt of een in de Volksrepubliek China gevestigde ondernemer kan worden uitgesloten van een aanbestedingsprocedure gelet op de definitie van het begrip "ondernemer" in de Aanbestedingsrichtlijn. De Advocaat-Generaal is van mening dat in derde landen gevestigde ondernemers in beginsel niet onder de Aanbestedingsrichtlijn vallen met uitzondering van ondernemers die zijn gevestigd in derde landen waarmee multi- of bilaterale verdragen afspraken zijn gemaakt. Dat betekent wat betreft de Advocaat Generaal dat die ondernemers geen aanspraak kunnen maken op een bevoorrechte toegang tot overheidsopdrachten van de Europese Unie. Wanneer de uitspraak van het Hof van Justitie volgt is ons niet bekend.

NB: Of bedrijven uit Rusland, Iran en Noord-Korea kunnen worden geweerd laten wij in deze analyse in het midden nu in die landen voor zover wij hebben begrepen geen camera's worden vervaardigd die door gemeenten worden ingekocht. Voor Rusland gelden overigens sanctiemaatregelen.

2.1.5 Inschrijvingen blijken echter naar wij begrepen veelal plaats te vinden door in Nederland (of elders in Europa) gevestigde systemintegrators, zodat uitsluiting op deze grond in de praktijk naar verwachting weinig effectief zal zijn. Dat brengt ons tot de volgende door u voorgenomen maatregel, te weten het weren van camera's die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen.

Voor de goede orde merken wij op dat indien gemeenten niettegenstaande het voorgaande inschrijvers uit derde landen wensen te weren, in de aanbestedingsdocumentatie de volgende zin kan worden opgenomen: "Inschrijvers gevestigd in [land in te vullen door gemeente] worden van deze aanbesteding uitgesloten". Als hiervoor opgemerkt, dient de vraag in hoeverre inschrijvers uit derde landen al dan niet van een aanbesteding kunnen worden uitgesloten op basis van een "case-by-case assessment" te worden bepaald.

2.2 Weren camera's die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen toelaatbaar?

<u>Specifieke aanbestedingsregels inschrijvingen met producten uit derde landen</u>

2.2.1 De reguliere Aanbestedingsrichtlijn (2014/24 EU) bevat geen bijzonder kader voor de behandeling van inschrijvingen met producten of diensten uit derde landen.

2.2.2 De enige specifieke regels op dit punt zijn opgenomen in de artikelen 85 en 86 van de Nutssectorenrichtlijn (2014/25 EU) waarvan artikel 85 is geïmplementeerd in artikel 3.76 Aanbestedingswet. Inschrijvingen met meer dan 50% producten uit derde landen

kunnen worden geweigerd, ook wanneer die producten worden aangeboden door een onderneming die gevestigd is in een EU-lidstaat of een ander niet-derde land. Indien een gelijkwaardige inschrijving is ontvangen met minder dan 50% producten uit derde landen, dan moet het speciale sectorbedrijf met meer dan 50% producten uit derde landen afwijzen tenzij – kort gezegd – sprake is van een technische noodzaak om de inschrijving met meer dan 50% producten uit derde landen toch te accepteren.

2.2.3 Artikel 3.76 Aanbestedingswet lijkt in de praktijk niet gebruikt te worden. In literatuur wordt wel gesuggereerd dat de oorzaak hiervan ligt in de lastige praktische toepasbaarheid. Zo moet de oorsprong van de producten bijvoorbeeld worden vastgesteld overeenkomstig Verordening (EU) 952/2013 tot vaststelling van het douanewetboek van de Unie.

2.2.4 Er is ons geen rechtspraak over artikel 3.76 Aanbestedingswet bekend en evenmin over artikel 85 van de Nutssectorenrichtlijn.

2.2.5 Uit de toelichting van de Europese Commissie bij haar voorstellen voor de Initial legislative proposals (2012 en 2016) blijkt dat de Europese Commissie van oordeel is dat bovenstaande regeling uitsluitend van toepassing is op nutssectoren (speciale sectoropdrachten).

2.2.6 Gelet daarop zijn wij van mening dat artikel 3:76 Aanbestedingswet zich niet leent voor analoge toepassing voor "reguliere" overheidsopdrachten onder de Aanbestedingswet zoals de inkoop van camera's door gemeenten. Artikel 3:76 Aanbestedingswet biedt daarmee geen soelaas voor het weren van camera's die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen.

<u>Uitvoeringsvoorwaarde</u>

2.2.7 Nu de wet geen soelaas biedt rijst de vraag of binnen een Europese aanbesteding het gewenste effect kan worden bereikt door middel van een aanvullende bijzondere uitvoeringsvoorwaarde in de aanbestedingsdocumentatie. Daarover het volgende.

2.2.8 De betreffende uitvoeringsvoorwaarde zou betreffen het in een "bijzondere voorwaarde" verbieden van camerasystemen die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen. Via deze weg zouden partijen op straffe van ongeldigheid dergelijke camera's niet mogen aanbieden.

2.2.9 Krachtens artikel 2.80 Aanbestedingswet kunnen aanbestedende diensten voorwaarden verbinden aan de uitvoering van een overheidsopdracht, mits dergelijke voorwaarden verband houden met het voorwerp van de opdracht en in de aankondiging of de aanbestedingsstukken zijn vermeld.

2.2.10 Het begrip "aanvullende bijzondere voorwaarde" is geïntroduceerd in de zaak Beentjes van 1988. Het Hof van Justitie EU oordeelde in dat verband dat het lidstaten is toegestaan aanvullende bijzondere voorwaarden te stellen mits zij "alle relevante bepalingen van het gemeenschapsrecht eerbiedigen en met name de verboden die voortvloeien uit de in het Verdrag neergelegde beginselen inzake het recht van vestiging en het vrij verrichten van diensten".

2.2.11 Ook in overweging 104 bij de Aanbestedingsrichtlijn is benadrukt dat (bijzondere) voorwaarden niet direct of indirect discriminerend mogen zijn:

"104 (…) Contractvoorwaarden moeten met de richtlijn verenigbaar zijn indien zij niet direct of indirect discriminerend zijn en verband houden met het voorwerp van de opdracht, dat alle factoren omvat die te maken hebben met het specifieke proces van productie, verrichting of verkoop. Daartoe behoren de voorwaarden betreffende het uitvoeringsproces van de opdracht, maar niet de eisen met betrekking tot algemeen ondernemingsbeleid".

2.2.12 In lijn daarmee is ook in de memorie van toelichting bij artikel 2.80 Aanbestedingswet aangegeven dat bijzondere voorwaarden in overeenstemming dienen te zijn met het Unierecht:

- Kamerstukken II 2015/16, 34 329, 3, p. 62:

"(…) Evenals gunningscriteria, moeten bijzondere voorwaarden verband houden met het voorwerp van de opdracht in de zin van artikel 2.115, derde lid, en dienen zij in overeenstemming te zijn met het gemeenschapsrecht (…)".

2.2.13 In dit verband zijn (onder meer) de fundamentele vrijheden zoals die gelden binnen de EU van belang.[1] Meer concreet is in deze situatie het vrij verkeer van goederen relevant, zoals neergelegd in artikel 28 VWEU e.v. Beperkingen op het vrij verkeer van goederen zijn slechts toegestaan als aan een aantal voorwaarden is voldaan.

2.2.14 De reikwijdte van de fundamentele vrijheden beperkt zich tot de EU. De regels van het vrij verkeer zijn ook van toepassing op bijzondere voorwaarden voor producten uit derde landen die zich in de lidstaten in het vrije verkeer bevinden.[2] Op die manier kan de maatregel die inhoudt dat producten uit een land met een offensieve cyberagenda

[1] Zoals beschreven in het Verdrag betreffende Werking van de Europese Unie ("VWEU"), zie artikelen 34-37 en 45-66 VWEU.

[2] Zie artikel 29 VWEU luidt: "*Als zich bevindend in het vrije verkeer in een lidstaat worden beschouwd: de producten uit derde landen waarvoor in genoemde staat de invoerformaliteiten zijn verricht en de verschuldigde douanerechten en heffingen van gelijke werking zijn voldaan en waarvoor geen gehele of gedeeltelijke teruggave van die rechten en heffingen is verleend.*'

worden geweerd kwalificeren als een beperking op het vrij verkeer van goederen (als maatregel van gelijke werking in de zin van artikel 34 VWEU[3]).

2.2.15 Een beperking van het vrij verkeer van goederen is geoorloofd indien de beperking gerechtvaardigd kan worden door (één van) de uitzonderingsgronden zoals genoemd in artikel 36 VWEU, te weten: openbare zedelijkheid, openbare orde, openbare veiligheid, de gezondheid en leven van personen, dieren of planten, het nationaal artistiek historisch en archeologisch bezit of het industriële of commerciële eigendom, of door (één van) de (niet-uitputtende lijst van) redenen die door het Hof van Justitie zijn erkend als "dwingende vereisten van algemeen belang", zoals milieubescherming, consumentenbescherming of bescherming van de grondrechten.[4] Ook de bescherming van de menselijke waardigheid is in de rechtspraak van het Hof van Justitie erkend als dwingende reden van algemeen belang.[5]

2.2.16 Hierbij moet de bijzondere voorwaarde voldoen aan de volgende voorwaarden:

(i) de voorwaarde moet geschikt zijn om de verwezenlijking van het nagestreefde doel (de rechtvaardigingsgrond) te waarborgen (geschiktheidstoets);
(ii) de voorwaarde mag niet verder gaan dan noodzakelijk is om dat doel te bereiken, en het doel kan niet met een minder ingrijpende of minder beperkende maatregel worden bereikt (noodzakelijkheidstoets); en
(iii) de voorwaarde moet in verhouding staan tot het nagestreefde doel (evenredigheidstoets).

2.2.17 Er dient aldus rekening te worden gehouden met de mogelijkheid dat in een procedure één van de inschrijvende partijen die camera's wil aanbieden uit landen met een offensieve cyberagenda of de producent daarvan, zich beroept op de regels van het vrij verkeer en stelt dat de bijzondere voorwaarde een (verboden) beperking is op het vrij verkeer van goederen.[6] In dat geval zal moeten worden aangetoond dat sprake is van een rechtvaardigingsgrond voor de beperking en dat is voldaan aan de geschiktheids-, noodzakelijkheids-, en evenredigheidstoets. Het is dus niet voldoende om te stellen dat er (mogelijke) risico's zijn; het is aan de partij die zich op een bepaalde rechtvaardiging beroept om de belangen, doelen en risico's voldoende te onderbouwen en te motiveren hoe de beperking bijdraagt aan de bescherming van die belangen en doelen.

2.2.18 Zoals genoemd, bestaan er verschillende rechtvaardigingsgronden. Bij de inkoop van camera's kan de rechtvaardigingsgrond gebaseerd op "openbare veiligheid" (artikel 36

[3] Een maatregel van gelijke werking is "iedere regeling die de intracommunautaire handel al dan niet rechtstreeks, daadwerkelijk of potentieel kan belemmeren", zie HvJEU 11 juli 1974, zaak 8-74, ECLI:EY:C:1974:82 (*Dassonville*), punt 5.
[4] Zie ook HvJEU 20 februari 1979, zaak 120/78 (*Cassis de Dijon*), ECLI:EU:C:1979:42, r.o. 8.
[5] HvJEU C-36/02 14 oktober 2004, (*Omega Spielhallen*), ECLI:EU:C:2004:614.
[6] Mogelijk kunnen ook de vrijheid van vestiging (artikel 49 VWEU) of het vrij verkeer van diensten (artikel 56 VWEU) in het geding zijn. Daarvoor geldt echter dezelfde toets.

VWEU) relevant zijn. Deze rechtvaardigingsgrond kan zowel betrekking hebben op interne als externe veiligheid van een lidstaat. Uit de rechtspraak van het Hof van Justitie volgt evenwel dat een rechtvaardiging op grond van de openbare veiligheid niet snel wordt aangenomen, met name omdat niet wordt voldaan aan de noodzakelijkheidstoets. In de rechtspraak waarin deze rechtvaardigingsgrond wel is aangenomen ging het doorgaans om situaties waarin er sprake was van een bedreiging van een fundamenteel publiek belang, bijvoorbeeld het beschermen van de zekerheid van de energievoorziening. [7] Voor zover ons bekend is er geen voorbeeld in de rechtspraak van het Hof van Justitie waarbij een rechtvaardiging op grond van de openbare veiligheid voortkwam uit cybersecurityrisico's.

2.2.19 Wel verwijzen wij in dit kader naar een uitspraak van de Belgische Raad van State.[8] De zaak ging over een onderhandelingsprocedure van de Belgische Staat voor het leveren van scanapparaten voor de Belgische douane, bestemd voor controles van de inhoud van voertuigen en containers. Door de Belgische Staat werd een beroep gedaan op een uitzonderingsbepaling waardoor niet behoefde te worden aanbesteed.[9] Voor de onderhandelingsprocedure waren maar twee geselecteerde partijen uitgenodigd. Een partij die producten aanbood van een bepaald Chinees bedrijf (Nuctech) werd niet uitgenodigd voor de procedure. De Belgische rechter oordeelde dat de Belgische staat een gerechtvaardigd beroep had gedaan op de uitzondering omdat er sprake was van essentiële veiligheidsbelangen[10], die in het gedrang konden komen (punt 27-30). Verzoeker, de partij die niet was uitgenodigd, zijnde de Poolse vestiging Nuctech, voerde onder andere aan dat sprake was van schending van het vrij verkeer van goederen. De rechter oordeelde dat, hoewel sprake was van een beperking van het vrij verkeer, die beperking gerechtvaardigd kon worden uit hoofde van bescherming van de openbare veiligheid, zoals bedoeld in artikel 36 VWEU.

2.2.20 Gemeenten zouden zich bij de inkoop van camera's mogelijk ook kunnen beroepen op een andere rechtvaardigingsgrond, bijvoorbeeld gebaseerd op gegevensbescherming, bescherming van consumenten of bescherming van de grondrechten, waaronder ook de menselijke waardigheid. Zo is voorstelbaar dat een rechtvaardiging voor een beperking van het vrij verkeer kan liggen in de bescherming van (gegevens van) bepaalde mensen in Nederland (zoals Oeigoeren die nu in Nederland wonen) die (mogelijk) bespioneerd worden door een buitenlandse overheid, of bescherming van (gegevens van) bepaalde belangrijke personen – zoals bewindslieden – die met de camera's gefilmd worden.

[7] Er is geen uitputtende lijst van belangen. Zie bijvoorbeeld HvJEU 10 juli 1984, zaak 72/83, (*Campus Oil*) ECLI:EU:C:1984:256, r.o. 34.

[8] Belgische Raad van State 21 mei 2023, zaak A.238.967/XII-9366, te raadplegen via: http://www.raadvst-consetat.be/Arresten/256000/600/256645.pdf.

[9] De uitzondering is gebaseerd op artikel 15, lid 2 en 3 van Richtlijn 2014/24/EU.

[10] Namelijk: bescherming van (persoons)gegevens; bescherming van alle andere gegevens die door de (scan)apparatuur verwerkt worden; de bescherming van België tegen kennisvergaring door buitenlandse inlichtingendiensten of cyberaanvallen; het vermijden dat kritieke sectoren, de strijd tegen de internationale drugssmokkel, de georganiseerde misdaad en de schade aan bedrijven in het havengebied en de bescherming van de volksgezondheid, in hoge mate afhankelijk zouden worden van een buitenlands regime dat economische dossiers gebruikt voor (geo)politieke doeleinden, zie punt 29.

2.2.21 Met betrekking tot de vraag in hoeverre de door de VNG beoogde bijzondere voorwaarde verband houdt met de opdracht merken wij op dat alhoewel de voorwaarde strikt genomen niet inherent is aan de opdracht zelf (te weten het leveren en implementeren van camera's) ons inziens kan worden betoogd dat de voorwaarde de uitvoering ervan wel kan beïnvloeden. De systemintegrators zullen gegeven die voorwaarde immers geen camera's inkopen die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen. De voorwaarden houden bovendien verband met cybersecurity en mensenrechten overwegingen van aanbestedende diensten. Of de bijzondere voorwaarde in rechte daadwerkelijk stand zal houden, is op voorhand echter lastig in te schatten; een precedent is niet voorhanden. Aanbestedende diensten hebben bij toepassing van de bijzondere voorwaarde dan ook rekening te houden met de mogelijkheid van ecartering van de voorwaarde en in het verlengde daarvan met een eventuele heraanbesteding.

2.2.22 Overigens zal ook per aanbesteding moeten worden nagegaan in hoeverre de bijzondere voorwaarde proportioneel is. Aanbesteder zal in dat verband moeten beoordelen of de omvang van de opdracht en de aard daarvan zich leent voor het stellen van de eis dat camera's die zijn ontwikkeld en/of gefabriceerd door partijen die gevestigd zijn in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen niet mogen worden aangeboden.

2.2.23 Volledigheidshalve merken wij op dat voor zover de bijzondere uitvoeringsvoorwaarde als technische specificatie in de zin van artikel 2.75/2.76 Aanbestedingswet kwalificeert de voorwaarde/specificatie net zo min tot ongerechtvaardigde belemmeringen mag leiden in de openstelling van overheidsopdrachten voor mededinging. Op grond van artikel 2.76 lid 3 Aanbestedingswet is het verwijzen naar een bepaalde oorsprong verboden tenzij dit door het voorwerp van de opdracht gerechtvaardigd is.

Als **Bijlage A** bij deze analyse hebben wij een model uitvoeringsvoorwaarde gevoegd.

2.3 Gunningscriterium "hoe minder camera onderdelen die zijn ontwikkeld en/of gefabriceerd in landen met een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen, hoe beter" toelaatbaar?

2.3.1 Ook gunningscriteria dienen in overeenstemming te zijn met het Unierecht. Gelet op het voorgaande achten wij dit gunningscriterium niet goed verenigbaar met het VWEU. Waar bij een bijzondere voorwaarde/knock out-eis mogelijk kan worden betoogd dat de beperking van het vrije verkeer gerechtvaardigd is vanwege bijvoorbeeld de (potentiële) afbreuk van de openbare veiligheid, kan dat bij een gunningscriterium

niet. Een gunningscriterium betreft immers geen binair criterium zodat bij toepassing daarvan een potentieel veiligheidsrisico gradueel voor lief wordt genomen. Dit nog daargelaten de controleerbaarheid van een dergelijk criterium.

2.4 Gunningscriterium Plan van Aanpak toelaatbaar?

2.4.1 Als hiervoor uiteengezet, heeft de VNG ook als mogelijkheid benoemd dat gemeenten een plan van aanpak uitvragen waarin inschrijvers de risico's in termen van mensenrechtenschendingen (culturele genocide en etnisch profileren) en/of cyberveiligheid met het aangeboden camerasysteem inzichtelijk dienen te maken, alsook de beheersmaatregelen die zij zullen treffen teneinde die risico's zoveel als mogelijk te mitigeren. Hoe effectiever de aangeboden beheersmaatregelen, hoe beter.

2.4.2 Een dergelijk gunningscriterium achten wij in principe toelaatbaar. Wel merken wij op dat gunningscriteria controleerbaar en proportioneel dienen te zijn. Eén en ander zal per aanbesteding door gemeenten moeten worden beoordeeld. Ook zal per aanbesteding duidelijk moeten worden gemaakt wat onder "cyberveiligheid" dient te worden verstaan (achterdeurtjes waarmee data kan worden doorgegeven aan vreemde mogendheden? Of breder?).

> Als **Bijlage B** en **Bijlage C** zijn bij deze analyse model gunningscriteria gevoegd op het gebied van het mitigeren van het risico op het faciliteren culturele genocide of etnisch profileren en op het gebied van het mitigeren van het cyberveiligheidsrisico.

2.4.3 Om gunningscriteria met betrekking tot het mitigeren van mensenrechtenschendingen in termen van culturele genocide en etnisch profileren effectief te laten zijn zullen in het contract ter zake duidelijke afdwingbare afspraken moeten worden opgenomen. Worden de aangeboden beheersmaatregelen daadwerkelijk toegepast en hoe effectief zijn die? Ook het formuleren van escalatiemogelijkheden is van belang.

> Als **Bijlage D** zijn bij deze analyse model contractsvoorwaaren opgenomen die aansluiten op de gunningscriteria geformuleerd in Bjilage B en Bijlage C.

2.4.4 Voorts kunnen in de contractvoorwaarden bepalingen worden opgenomen met betrekking tot het inschakelen van onderaannemers/de voorwaarden waaronder opdrachtgever daarvoor al dan niet toestemming verleend.

> In Bijlage D is eveneens een artikel opgenomen over de toevoeging of wijziging van onderaannemers tijdens de looptijd van en overeenkomst.

2.4.5 Overigens werkt het Rijk aan het ontwikkelen van beveiligingseisen voor aanbestedingen van de rijksoverheid en de Nationale Politie die de nationale veiligheid raken: de Algemene beveiligingseisen rijksoverheid Opdrachten ("ABRO"). Mogelijk

kunnen gemeenten daar te zijner tijd op aanhaken teneinde risico’s in termen van cyberveiligheid/mensenrechtenschendingen zoveel als mogelijk te mitigeren.

3 Andere beschikbare Aanbestedingsrechtelijke sturingsmechanismen

3.1 Conform uw verzoek beoordelen wij ook of andere aanbestedingsrechtelijke sturingsmechanismen zoals geschiktheidseisen, selectiecriteria en uitsluitingsgronden kunnen worden toegepast om risico's op het gebied van mensenrechtenschendingen en cyberveiligheid zoveel als mogelijk te mitigeren.

Geschiktheidseisen en selectiecriteria

3.2 Voor het hanteren van geschiktheidseisen en selectiecriteria als sturingsmechanisme zien wij vooralsnog weinig aanknopingspunten: inschrijvers zijn naar wij begrepen hoofdzakelijk systemintegrators die naar verwachting prima in staat zullen zijn referenties over te leggen waaruit blijkt dat zij in de afgelopen jaren camera's hebben geleverd.

Uitsluitingsgronden

3.3 In het aanbestedingsrecht wordt gebruik gemaakt van uitsluitingsgronden om niet-integere, onbetrouwbare of onbekwame ondernemingen uit te sluiten van een aanbestedingsprocedure. De uitsluitingsgronden zijn van toepassing op de inschrijver en op ondernemers waarop een inschrijver een beroep doet om aan de geschiktheidseisen te kunnen voldoen.

3.4 Uitsluitingsgronden zijn in de Aanbestedingswet limitatief opgesomd. Daarbij wordt een onderscheid gemaakt tussen dwingende en facultatieve uitsluitingsgronden.

3.5 "Facultatief" betekent dat een aanbestedende dienst bij de start van de aanbestedingsprocedure de keuze heeft om deze gronden op de aanbesteding van toepassing te verklaren. Dat geeft de aanbestedende dienst aan in het Uniform Europees Aanbestedingsdocument. Indien de aanbestedende dienst daartoe eenmaal heeft gekozen, is hij verplicht de uitsluitingsgrond ook toe te passen.

3.6 De facultatieve uitsluitingsgrond "Ernstige Fout" van artikel 2.87 lid 1 onderdeel c Aanbestedingswet ziet op een ernstige fout in de uitoefening van het beroep die ertoe leidt dat de integriteit van de inschrijver of gegadigde in twijfel kan worden getrokken.

3.7 Dit begrip is in de Aanbestedingsrichtlijn en de Aanbestedingswet niet geëxpliciteerd. Uitgangspunt is dat aanbestedende diensten in de aanbestedingsdocumentatie invulling dienen te geven aan de uitsluitingsgrond "Ernstige fout".

3.8 Van belang is overigens dat het Hof van Justitie EU het begrip "ernstige fout" heeft uitgelegd in het "Forposta" arrest van 13 december 2012 (C-465/11). Het Hof van Justitie heeft in dat verband overwogen dat sprake zal moeten zijn van kwade opzet of nalatigheid van een zekere ernst van de ondernemer:

> "Niettemin moet worden aangenomen dat het begrip „ernstige fout" gewoonlijk ziet op gedrag van de betrokken marktdeelnemer dat wijst op kwaad opzet of nalatigheid van een zekere ernst van deze marktdeelnemer. Elke onjuiste, onnauwkeurige of gebrekkige uitvoering van een overeenkomst of een deel ervan kan derhalve eventueel wijzen op een beperkte vakbekwaamheid van de betrokken marktdeelnemer, maar staat niet automatisch gelijk met een ernstige fout".

3.9 De vaststelling van een "ernstige fout" vergt derhalve een concrete en individuele beoordeling van het gedrag van de betrokken marktdeelnemer.

3.10 Voor de vaststelling van een "ernstige fout" is niet vereist dat sprake is van een onherroepelijk vonnis. Voor de vaststelling van een ernstige fout volstaat dat de aanbestedende dienst die voldoende aannemelijk kan maken.

3.11 Voor de uitsluitingsgrond "Ernstige fout" geldt een terugkijktermijn van 3 jaar.

3.12 Als hoofdregel geldt dat een aanbestedende dienst, indien een dwingende of facultatieve uitsluitingsgrond van toepassing is, de ondernemer in de gelegenheid dient te stellen te bewijzen dat hij voldoende maatregelen heeft genomen om zijn betrouwbaarheid aan te tonen. Indien de aanbestedende dienst het bewijs toereikend acht, ziet hij af van uitsluiting.

3.13 Het kwalificeren van het hebben van een offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland/Nederlandse belangen als "ernstige fout" is naar uw verwachting weinig effectief. Systemintegrators zullen immers geen offensieve cyberagenda/offensief inlichtingenprogramma gericht op Nederland/Nederlandse belangen hebben. Het kwalificeren van het faciliteren van de mogelijkheid tot culturele genocide of etnisch profileren buiten Europa/niet- derde landen door inschrijver als "ernstige fout" ligt om die reden evenmin voor de hand. Het ligt immers niet in de verwachting dat systemintegrators van kwade opzet of nalatigheid van een zekere ernst kunnen worden beticht met betrekking tot het faciliteren van de mogelijkheid tot culturele genocide of etnisch profileren buiten Europa/niet- derde landen. Daargelaten dat het toepassen van een dergelijke uitsluitingsgrond tot complexe (uitleg)vraagstukken/procedures kan leiden in de aanbesteding. Al dan niet naar aanleiding van klachten van inschrijvers over elkaar. Mocht uw verwachting ten aanzien van systemintegrators genuanceerder komen te liggen dan dient deze optie in die zin heroverwogen te worden.

3.14 Voor de goede orde merken wij wel op dat het uitsluitend aansturen op het mitigeren van mensenrechtenschendingen buiten Europa/niet-derde landen (politiek) niet goed uit te leggen valt. Is een ondernemer die de mogelijkheid tot culturele genocide/etnisch profileren in Europa/een niet-derde land faciliteert wat betreft de VNG/de aanbestedende dienst wel integer? Indien de "Ernstige fout" wordt ingevuld

raden wij dan ook aan het faciliteren van de mogelijkheid tot culturele genocide/etnisch profileren in zijn algemeenheid uit te sluiten.

Mogelijkheden ADV?

3.15 De Aanbestedingswet op defensie-en veiligheidsgebied (hierna: "de ADV") dient ter implementatie van de Defensierichtlijn (2009/81/EG) die tot doel heeft een open en transparante Europese markt voor defensie- en veiligheidsmateriaal te verwezenlijken met meer concurrentie en gelijke concurrentievoorwaarden.

3.16 Conform artikel 2.1 van de ADV is de ADV onder meer van toepassing op de levering van gevoelig materiaal.

3.17 Blijkens artikel 1.1 van de ADV dient onder "gevoelig materiaal" te worden verstaan materiaal bestemd voor veiligheidsdoeleinden dat op gerubriceerde gegevens betrekking heeft, dat gerubriceerde gegevens noodzakelijk maakt of dat zelf gerubriceerde gegevens bevat. Om de opdracht te kwalificeren als "gevoelig" moet het dus gaan om opdrachten die bestemd zijn voor veiligheidsdoeleinden en waar gerubriceerde gegevens een rol spelen.

3.18 Veiligheidsdoeleinden zijn blijkens de Memorie van Toelichting bij de ADV bijvoorbeeld bestrijding van terrorisme en georganiseerde misdaad, grensbewaking en crisisbeheersing.

3.19 Blijkens de Memorie van Toelichting is het begrip gerubriceerde gegevens opgebouwd uit verschillende bestanddelen. Het dient te gaan om gegevens of materiaal waarvan de integriteit, exclusiviteit en beschikbaarheid beschermd dient te worden in het belang van de nationale veiligheid. Gegevens die omwille van andere belangen bescherming nodig hebben, zoals op grond van de Wet bescherming persoonsgegevens of om de enkele reden dat het bedrijfs- of fabricagegegevens zijn, zijn geen gerubriceerde gegevens. Verder dient aan de gegevens of het materiaal een bepaald niveau van veiligheidsclassificatie of een beveiligingsniveau te zijn toegekend en dient de benodigde bescherming te zijn vastgelegd in wettelijke voorschriften, bindende aanwijzingen gegeven vanwege het Rijk of in bestuursrechtelijke besluiten. De kwalificatie als gerubriceerde gegevens dient daardoor telkens in overeenstemming te zijn met of gebaseerd op geldende regels.

3.20 Ook onder de ADV dient in uitgangspunt Europees te worden aanbesteed. De Defensierichtlijn/ADV beogen nu eenmaal een open en transparante Europese markt voor defensie- en veiligheidsmateriaal.

3.21 Wel is in artikel 2.77 lid 1 van de ADV een "extra" facultatieve uitsluitingsgrond opgenomen ten opzichte van de Aanbestedingswet: een aanbestedende dienst kan een inschrijver uitsluiten indien is vastgesteld dat hij niet over de betrouwbaarheid beschikt die nodig is om risico's voor de nationale veiligheid uit te sluiten. In

rechtsoverweging 65 van Richtlijn 2009/81 voor opdrachten op defensie- en veiligheidsgebied wordt overwogen dat "deze risico's het gevolg kunnen zijn van bepaalde kenmerken van de producten die door de gegadigde worden geleverd of van de aandeelhoudersstructuur van de gegadigde".

3.22 Voor zover wij dat in de gesprekken met de VNG en de interviews hebben kunnen nagaan, spelen bij de inkoop van camera's gegevens waarvan de integriteit, exclusiviteit en beschikbaarheid beschermd dienen te worden in het belang van de nationale veiligheid in principe geen rol. Eventuele persoonsgegevens op de camera's die bescherming nodig hebben, kwalificeren niet als gerubriceerde gegevens. Dat maakt dat de ADV in principe niet van toepassing is bij de inkoop van camera's. Indien bij de inkoop van camera's gerubriceerde gegevens toch een rol spelen, is dat mogelijk anders.

Onderhandse gunning buiten aanbesteding – bescherming wezenlijke belangen Nederland

3.23 Volledigheidshalve merken wij ook op dat op basis van artikel 2.23 sub e Aanbestedingswet overheidsopdrachten van aanbesteding zijn uitgezonderd die geheim zijn verklaard of waarvan de uitvoering overeenkomstig de geldende wettelijke en bestuursrechtelijke bepalingen met bijzondere veiligheidsmaatregelen gepaard moet gaan dan wel indien de bescherming van wezenlijke belangen van Nederland zulks vereist en deze niet met minder ingrijpende maatregelen kan worden geborgd.

3.24 Dit artikel betreft een uitwerking van artikel 15 lid 3 van de Richtlijn 2014/24/EU. Uit dat artikel volgt dat de uitzondering uitsluitend van toepassing is indien de lidstaat heeft besloten dat essentiële belangen niet kunnen worden gewaarborgd met minder ingrijpende maatregelen.

3.25 Het is vaste Europese jurisprudentie dat deze uitzondering restrictief moet worden uitgelegd. Het is aan de aanbestedende dienst die zich er op beroept om het bewijs te leveren dat daarmee de grenzen van deze uitzondering niet worden overschreden, en (gegeven de Richtlijn) de essentiële belangen van Nederland niet met minder vergaande middelen kunnen worden geborgd.

3.26 Voor de goede orde merken wij nog op dat de algemene bepalingen van afdeling 1.2.1 van de Aanbestedingswet onverkort gelden. Dat betekent dat de aanbestedende dienst conform artikel 1.4 van de Aanbestedingswet op basis van objectieve criteria de keuze voor de procedure en de daarvoor uit te nodigen ondernemer(s) dient te bepalen. Als objectieve criteria op basis waarvan een aanbestedende dienst zijn keuze voor (een) ondernemer(s) kan maken noemt de parlementaire geschiedenis onder andere de ervaring in de betreffende sector, de omvang en infrastructuur van de onderneming of andere elementen.

3.27 Of bij de inkoop van camera's van dit artikel gebruik kan worden gemaakt, zal op basis van een "case-by-case assessment" moeten worden bepaald. Op voorhand schatten wij echter in dat van een gerechtvaardigd beroep op van artikel 2.23 sub e Aanbestedingswet niet snel sprake zal zijn: van verspreiding van gevoelige informatie bij aanbesteding zal voor zover wij dat hebben kunnen nagaan in de interviews bijvoorbeeld geen sprake zijn. Daarbij kunnen ter voorkoming van openbaarmaking van gevoelige informatie (in de aanbesteding) ook (contractuele) vertrouwelijkheids- en veiligheidsmaatregelen worden getroffen. In het verlengde daarvan valt ons inziens op voorhand niet goed uit te leggen waarom de inkoop van camera's niet zou kunnen worden aanbesteed.

Screening

3.28 Blijkens artikel 2 sub g en artikel 4 sub b van de Regeling Naslag Wet op de inlichtingen- en veiligheidsdiensten 2017 kan de Minister van Justitie dan wel de Minister die het aangaat een schriftelijk verzoek richten aan de Minister van Binnenlandse zaken respectievelijk de Minister van Defensie voor het doen van naslag met betrekking tot bedrijven of organisaties die door levering van producten aan de Nederlandse overheid in een positie kunnen komen waarin zij de nationale veiligheid schade kunnen toebrengen. Bij een verzoek tot naslag worden door de AIVD of de MIVD verwerkte gegevens geraadpleegd om na te gaan of er ten aanzien van een bepaalde instantie relevante gegevens beschikbaar zijn. Overigens bestaat voor de inlichtingendiensten geen plicht desgevraagd een naslag uit te voeren.

3.29 Nu gemeenten niet bevoegd zijn een verzoek om naslag te doen, ligt het ons inziens niet voor de hand voor te schrijven dat inschrijvers en hun eventuele onderaannemers een screening door de AIVD/MIVD succesvol dienen te doorlopen alvorens voor gunning in aanmerking te komen. Gemeenten kunnen die eis immers niet effectueren/controleren. Daargelaten de lange doorlooptijd van een eventuele screening door de inlichtingendiensten (vaak enkele maanden).

4 Europese richtlijnen inzake mensenrechten/wetsvoorstel Wet verantwoord en duurzaam internationaal ondernemen

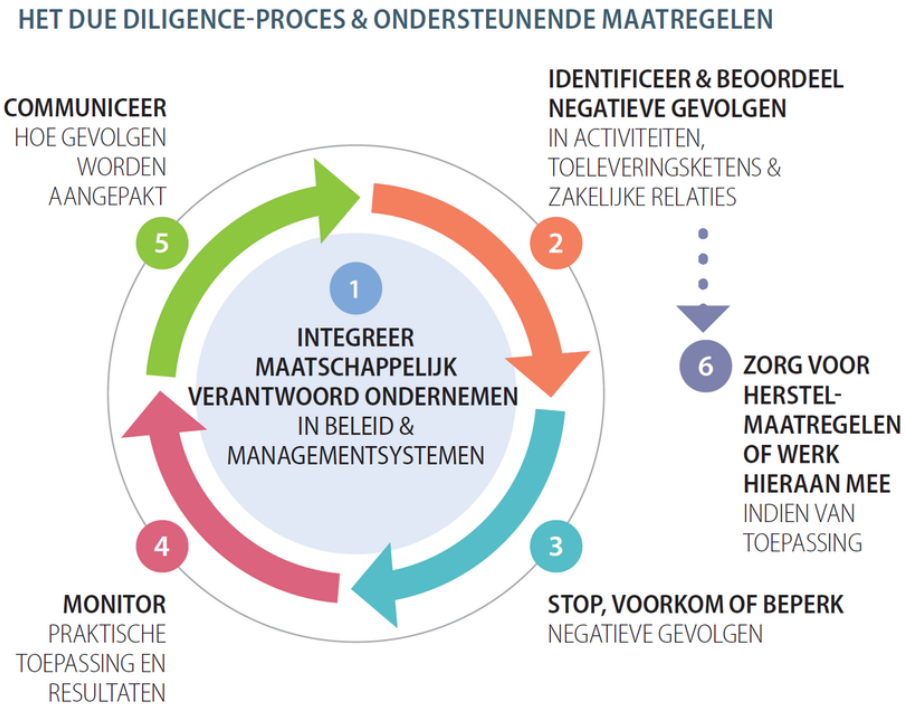
4.1 Als hiervoor aangegeven, verzocht u ons na te gaan welke mogelijkheden gemeenten hebben op basis van (toekomstige) Europese richtlijnen inzake mensenrechten, alsook op basis van het wetsvoorstel Wet verantwoord en duurzaam internationaal ondernemen. In dat verband het volgende.

4.2 Dat op het terrein van mensenrechtenschendingen eisen worden gesteld, is voor bepaalde risicocategoriën binnen de Rijksoverheid, zoals de ICT-sector, conform Rijksbeleid verplicht in Europese aanbestedingen. De Internationale Sociale Voorwaarden (hierna: ISV) zijn een veelgebruikt voorbeeld van dergelijke voorwaarden.11 Buiten die risicocategoriën (en door andere overheden) is het ook niet ongebruikelijk om dergelijke eisen te stellen en wordt dit ook aanbevolen.[12] De mate waarin op dit terrein eisen worden gesteld en de strengheid van die eisen verschilt echter. Veelal worden ook niet alle zes stappen van het gepaste zorgvuldigheidsproces, zoals die in de OESO Richtlijnen voor Multinationale Ondernemingen over Verantwoord Ondernemen zijn vastgelegd, voorgeschreven. Die zes stappen zijn kort weergegeven in het volgende schema:[13]

11 Zie voor die ISV ook de website van PIANOO, te raadplegen via https://www.pianoo.nl/nl/themas/maatschappelijk-verantwoord-inkopen/ketenverantwoordelijkheid-internationale-sociale.

12 Zie bijvoorbeeld van Voorlichten naar Verplichten, Ministerie van Buitenlandse Zaken 2020, p. 21 en 27, te raadplegen op https://open.overheid.nl/documenten/ronl-1a58c4b1-ab68-41e2-93f2-405c385984f5/pdf. Vergelijk ook het recent toegevoegde art. 3.2.7 aan het voorstel voor de Wet verantwoord en duurzaam internationaal ondernemen en de toelichting daarop, Kamerstukken II 2022/23, 35 761, nr. 17, p. 15.

13 Zie voor deze richtlijnen https://www.oecd-ilibrary.org/finance-and-investment/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en en zie voor het schema OECD Due Diligence Guidance for Responsible Business Conduct, p. 21, te raadplegen via http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf. Het origineel is in het Engels. Zie ook Kamerstukken II 2022/23, 35 761, nr. 10, onder 1.1.



4.3 De Rijksoverheid verwacht van alle ondernemingen in Nederland dat zij zich aan dit gepaste zorgvuldigheidsproces in de OESO richtlijnen houden.[14] Wel laten de richtlijnen toe dat het gepaste zorgvuldigheidsproces afhangt van de grootte van de onderneming en het risico op mensenrechtenschendingen (in waardeketens). Zo kan van een grote onderneming in een sector met bekende grote mensenrechtenrisico's meer worden verwacht dan van een eenmanszaak in een sector waarin deze risico's zeer beperkt zijn. Het proces hoeft dus niet steeds op dezelfde wijze te worden uitgevoerd. Inmiddels is ook steeds meer wetgeving in de maak die dergelijke gepaste zorgvuldigheid voor grotere ondernemingen verplicht gaat stellen. Uitgangspunt van die wetgeving is ook dat (grotere) ondernemingen het hiervoor beschreven gepaste zorgvuldigheidsproces doorlopen. In het bijzonder valt te wijzen op de passende zorgvuldigheid op basis van de richtlijn inzake "passende zorgvuldigheid in het bedrijfsleven op het gebied van duurzaamheid' van de Europese Unie[15] die naar verwachting begin 2024 zal worden vastgesteld en het Nederlandse initiatiefvoorstel voor de Wet verantwoord en duurzaam internationaal ondernemen,[16] waarvan nog niet duidelijk is of en wanneer die zal worden aangenomen. Als **Bijlage E** hebben wij een set met contractsvoorwaarden opgesteld waarin wij op die wettelijke verplichtingen vooruitlopen, met de gedachte dat (grotere) ondernemingen daar op termijn toch aan moeten gaan voldoen. De contractuele voorwaarden gaan dus uit van de noodzaak om dit hele proces te doorlopen en ook om herstel te bieden wanneer dat van toepassing

14 Zie bijvoorbeeld van Voorlichten naar Verplichten, Ministerie van Buitenlandse Zaken 2020, p. 21 en 27.

15 COM (2022) 71 final. Het voorstel van de Europese Commissie daarvoor is te raadplegen op https://eur-lex.europa.eu/resource.html?uri=cellar:bc4dcea4-9584-11ec-b4e4-01aa75ed71a1.0004.02/DOC_1&format=PDF.

16 Kamerstukken II 2022/23, 35 761, waarvan de nota van wijzigingen is verschenen, zie nr. 17.

is (indien de onderneming een mensenrechtenschending heeft veroorzaakt of daaraan heeft bijgedragen).

4.4 Ook voor deze voorwaarden geldt dat deze proportioneel dienen te zijn. Eén en ander zal per aanbesteding door gemeenten moeten worden beoordeeld.

5 Overzicht sturingsmechanismen

5.1 Gelet op onze voorgaande analyse komen wij tot het volgende overzicht waarin de verschillende sturingsmechanismen inzichtelijk zijn gemaakt als ook of die sturingsmechanismen ons inziens al dan niet een optie zijn:

Sturingsmechanisme	**Wetsartikel**	**Randnummer**	**Optie? Ja/Nee**
Weren inschrijvers gevestigd in derde landen	Art. 1.23 Aw 2012	2.1 e.v.	Ja, in theorie, naar verwachting weinig effectief, inschrijvers zijn veelal Europese systemintegrators
Weren inschrijving met >50% producten uit derde landen op grond van artikel 3.76 Aanbestedingswet	Art. 85 en 86 Ver. 2014/25/EU en art. 3.76 Aw 2012	2.2.1 e.v.	Nee, geen analoge toepassing op "reguliere" overheidsopdrachten zoals de inkoop van camera's door gemeenten
Uitvoerings voorwaarden (Bijlage A)	Art. 2.80 Aw 2012	2.2.7 e.v.	Ja, mits verenigbaar met het EU-recht
Gunningscriterium zo min mogelijk camera-onderdelen uit landen met offensieve cyberagenda	Art. 2.113a Aw 2012	2.3 e.v.	Nee, wij raden dit gunningscriterium af
Gunningscriterium plan van aanpak met contractuele voorwaarde (Bijlagen B, C en D)	Art. 2.113a Aw 2012	2.4 e.v.	Ja, mits proportioneel en controleerbaar
Geschiktheidseis	Art. 2.90 Aw 2012	3.2 e.v.	Nee, wij zien hier geen aanknopingspunten
Uitsluitingsgrond "Ernstige fout"	Art. 2.87 lid 1 onderdeel c Aw 2012	3.3 e.v.	Ja, in theorie, naar verwachting weinig effectief terwijl het toepassen van de uitsluitingsgrond tot complexe (uitleg)vraagstukken/procedures in de aanbesteding kan leiden
Toepassing ADV	Art. 2.1 ADV	3.15 e.v.	Nee, voor zover wij hebben kunnen nagaan, is geen sprake van gerubriceerde gegevens
Uitzondering bescherming wezenlijke belangen van Nederland	Art. 2.23 sub e Aw 2012	3.23 e.v.	Restrictieve toepassing, case-by-case assessment, toepassing lijkt op voorhand niet aan de orde

Screening	Artikel 2 Regeling Naslag Wiv 2017	3.28 e.v.	Nee, gemeenten zijn niet bevoegd een verzoek om naslag te doen. Daargelaten dat er geen plicht bestaat voor inlichtingendiensten om naslag te verrichten
Contractvoorwaarden Mensenrechten (Bijlage E)		4 e.v.	Mits proportioneel