AUTORITE DES SERVICES ET MARCHES FINANCIERS

[C − 2023/43804]

Autorisation de fusion entre sociétés de gestion d'organismes de placement collectif (alternatifs) ou entre de telles sociétés et d'autres institutions financières (articles 214 et 215 de la loi du 3 aout 2012 relative aux organismes de placement collectif qui répondent aux conditions de la Directive 2009/65/CE et les articles 327 et 328 de la loi du 19 avril relative aux organismes de placement collectif alternatifs et à leurs gestionnaires)

En application de l'article 214 de la loi du 3 aout 2012 relative aux organismes de placement collectif qui répondent aux conditions de la Directive 2009/65/CE et l'article 327 de la loi du 19 avril 2014 relative aux organismes de placement collectif alternatifs et à leurs gestionnaires, le comité de direction de l'Autorité des services et marchés financiers (FSMA) a autorisé la fusion par absorption entre la société de gestion d'organismes de placement collectif (alternatifs) de droit belge KBC Asset Management NV, dont le siège social est établi à 1080 Bruxelles, Avenue du Port 2, Belgique, et la société de gestion d'organismes de placement collectif de droit bulgare KBC Investment Management EAD, dont le siège social est établi à 55, Nikola Vaptsarov Blvd., Expo 2000, Lozenets District, Sofia 1407, Bulgaria, comme exposé dans le projet de fusion du 31 mars 2023, rédigé conformément à l'article 12:112 du Code des sociétés et des associations. L'autorisation est réputée acquise à la date du 13 juin 2023.

Conformément à l'article 215 de la loi du 3 aout 2012 et l'article 328 de la loi du 19 avril 2014, toute cession totale ou partielle entre sociétés de gestion d'organismes de placement collectif (alternatifs) ou entre de telles sociétés et d'autres institutions financières des droits et obligations résultant des opérations des sociétés ou institutions concernées, et autorisée conformément à l'article 214 de la loi du 3 aout 2012 et l'article 327 de la loi du 19 avril 2014, est opposable aux tiers dès la publication au *Moniteur belge* de l'autorisation de la FSMA.

Bruxelles, le 12 juillet 2023.

A. ROMBOUTS

AUTORITEIT VOOR FINANCIELE DIENSTEN EN MARKTEN

[C − 2023/43804]

Toestemming voor fusie tussen beheervennootschappen van (alternatieve) instellingen voor collectieve belegging of van dergelijke vennootschappen en andere in de financiële sector bedrijvige instellingen (artikelen 214 en 215 van de wet van 3 augustus 2012 betreffende de instellingen voor collectieve belegging die voldoen aan de voorwaarden van Richtlijn 2009/65/EG en de artikelen 327 en 328 van de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders)

Met toepassing van artikel 214 van de wet van 3 augustus 2012 betreffende de instellingen voor collectieve belegging die voldoen aan de voorwaarden van richtlijn 2009/65/EG en artikel 327 van de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders, heeft het directiecomité van de Autoriteit voor financiële diensten en markten (FSMA) haar toestemming verleend voor de fusie door opslorping tussen de Belgische beheervennootschap van (A)ICB's KBC Asset Management NV, met maatschappelijke zetel te 1080 Brussel, Havenlaan 2, België, en de Bulgaarse beheervennootschap van ICB's KBC Investment Management EAD, met maatschappelijke zetel te 55, Nikola Vaptsarov Blvd., Expo 2000, Lozenets District, Sofia 1407, Bulgaria, zoals uiteengezet in het fusievoorstel van 31 maart 2023, opgesteld overeenkomstig artikel 12:112 van het Wetboek van vennootschappen en verenigingen. De toestemming wordt geacht te zijn verleend op 13 juni 2023.

Ingevolge artikel 215 van de wet van 3 augustus 2012 en artikel 328 van de wet van 19 april 2014 is iedere overdracht tussen beheervennootschappen van (alternatieve) instellingen voor collectieve belegging of tussen dergelijke vennootschappen en andere in de financiële sector bedrijvige instellingen, van rechten en verplichtingen die voortkomen uit verrichtingen van de betrokken vennootschappen of instellingen, waarvoor toestemming is verleend overeenkomstig artikel 214 van de wet van 3 augustus 2012 en artikel 327 van de wet van 19 april 2014 aan derden tegenstelbaar zodra de toestemming van de FSMA is bekendgemaakt in het *Belgisch Staatsblad*.

Brussel, 12 juli 2023.

A. ROMBOUTS

SERVICE PUBLIC FEDERAL CHANCELLERIE DU PREMIER MINISTRE

[C − 2023/46030]

11 SEPTEMBRE 2023. — Circulaire. — Réduction des risques de sécurité dans le cadre des marchés publics. — Fuite d'informations sensibles. — Espionnage

Aux pouvoirs adjudicateurs fédéraux visés à l'article 1er, 6°, de l'arrêté royal du 3 avril 2013 relatif à l'intervention du Conseil des Ministres, aux délégations de pouvoir et aux habilitations en matière de passation et d'exécution des marchés publics, des concours de projets et des concessions de travaux publics au niveau fédéral. La présente circulaire s'applique aux marchés publics relevant du titre 2 de la loi du 17 juin 2016 relative aux marchés publics.

Madame, Monsieur le Ministre/Secrétaire d'Etat,

Mesdames, Messieurs,

Lors de sa réunion du 20 juillet 2023, le Conseil des ministres a décidé que les pouvoirs adjudicateurs fédéraux doivent respecter et utiliser comme cadre d'interprétation la boîte à outils, jointe en annexe I, visant à réduire les risques de sécurité dans le cadre des marchés publics. Ils doivent également procéder au quick scan visé à l'annexe II pour tous les marchés publics susceptibles d'avoir un impact sur la sécurité nationale.

Les pouvoirs adjudicateurs fédéraux doivent remplir une fonction d'exemple.

La présente circulaire entre en vigueur le jour de sa publication au *Moniteur belge*.

Bruxelles, le 11 septembre 2023.

Le Premier Ministre,
A. DE CROO

Le Ministre de la Justice,
V. VAN QUICKENBORNE

La Ministre de la Défense,
L. DEDONDER

FEDERALE OVERHEIDSDIENST KANSELARIJ VAN DE EERSTE MINISTER

[C − 2023/46030]

11 SEPTEMBER 2023. — Omzendbrief. — Reduceren van veiligheidsrisico's in het kader van overheidsopdrachten. — Lekken van gevoelige informatie. — Spionage

Aan de federale aanbestedende overheden als bedoeld in artikel 1, 6°, van het koninklijk besluit van 3 april 2013 betreffende de tussenkomst van de Ministerraad, de overdracht van bevoegdheid en de machtigingen inzake de plaatsing en de uitvoering van overheidsopdrachten, ontwerpenwedstrijden en concessies voor openbare werken op federaal niveau. De onderhavige omzendbrief is van toepassing op de overheidsopdrachten die onder het toepassingsgebied van titel 2 van de wet van 17 juni 2016 inzake overheidsopdrachten vallen.

Mevrouw, Mijnheer de Minister/Staatssecretaris,

Mevrouwen, Mijne Heren,

Tijdens zijn zitting van 20 juli 2023 heeft de Ministerraad beslist dat de federale aanbestedende overheden de Toolbox voor het reduceren van veiligheidsrisico's in het kader van overheidsopdrachten die in bijlage I wordt gevoegd moeten naleven en hanteren als interpretatiekader. Zij moeten eveneens de in bijlage II bedoelde quickscan uitvoeren voor alle overheidsopdrachten waar er een impact kan zijn op de nationale veiligheid.

De federale aanbestedende overheden moeten terzake een voorbeeldfunctie vervullen.

De onderhavige omzendbrief treedt in werking op dag waarop ze in het *Belgisch Staatsblad* wordt bekend gemaakt.

Brussel, 11 september 2023.

De Eerste Minister,
A. DE CROO

De Minister van Justitie,
V. VAN QUICKENBORNE

De Minister van Defensie,
L. DEDONDER

ANNEXE I - BOÎTE À OUTILS DESTINÉE À LA RÉDUCTION DES RISQUES DE SÉCURITÉ DANS LE CADRE DES MARCHÉS PUBLICS

INTRODUCTION

Certains marchés publics sont susceptibles d'avoir un impact sur la sécurité nationale de notre pays. Il peut notamment s'agir d'un accès à des données sensibles, d'un risque d'espionnage ou de créer une dépendance stratégique à l'égard d'infrastructures critiques ou vitales vis-à-vis de pays tiers poursuivant des intérêts géopolitiques différents de ceux de notre pays. Dans ce contexte, nous voulons éviter que la passation de marchés publics entraîne des situations dangereuses en matière de continuité du service, fasse naître des dépendances stratégiques indésirables, provoque des fuites d'informations sensibles ou de l'espionnage.

La législation relative aux marchés publics prévoit plusieurs possibilités pour réduire ces risques. Ainsi, il convient tout d'abord de déterminer si la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité (ci-après abrégée loi « défense et sécurité ») doit être appliquée. Le champ d'application de cette loi est strictement limité aux équipements militaires (lire armement) et à tout ce qui a trait aux données classifiées. Cette loi apporte cependant un cadre juridique mieux adapté permettant de prendre en compte les risques susmentionnés. Elle ne peut toutefois pas être utilisée pour tous les marchés présentant un risque important pour la sécurité nationale de notre pays. Par ailleurs, pour les marchés publics dans les secteurs classiques et spéciaux, les adjudicateurs disposent également d'un certain nombre d'outils pour réduire les risques susmentionnés. Souvent, un certain nombre de risques peuvent déjà être efficacement évités par diverses interventions dans la conception générale du marché public. Il existe en outre un certain nombre d'outils juridiques qui, selon le cas, peuvent aider à maîtriser ces risques.

Un outil important est fourni par l'article 33 de la loi relative aux marchés publics du 17 juin 2016. Cette disposition permet, sous conditions, de déroger à l'application des règles de passation normalement applicables, et plus précisément si cela s'avère nécessaire pour la protection des intérêts essentiels en matière de sécurité. Ces possibilités sont insuffisamment connues et doivent donc être mieux encadrées, notamment à la

BIJLAGE I - TOOLBOX VOOR HET REDUCEREN VAN VEILIGHEIDSRISICO'S IN HET KADER VAN OVERHEIDSOPDRACHTEN

INLEIDING

Sommige overheidsopdrachten kunnen een impact hebben op de nationale veiligheid van ons land. Dit kan onder meer het geval zijn indien ze toegang tot gevoelige gegevens behelzen, er een risico bestaat op spionage of een strategische afhankelijkheid riskeert te ontstaan met betrekking tot kritieke of vitale infrastructuur ten aanzien van derde landen die andere geopolitieke belangen nastreven dan ons land. Voor dergelijke opdrachten willen we vermijden dat overheidsopdrachten tot onveilige situaties op het vlak van continuïteit van de dienstverlening leiden, dat er ongewenste strategische afhankelijkheden ontstaan, dat er gevoelige informatie weglekt of dat spionage plaatsvindt.

De wetgeving inzake overheidsopdrachten bevat diverse mogelijkheden om deze risico's te reduceren. Zo moet vooreerst worden nagegaan of de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied (hierna de wet 'defensie en veiligheid' genoemd) moet worden toegepast. Het toepassingsgebied van deze wet is echter strikt afgebakend tot militair materiaal (lees bewapening) en al wat te maken heeft met geclassificeerde gegevens. Deze wet biedt wel een rechtskader dat beter aangepast is om rekening te houden met de voormelde risico's. Deze wet mag echter niet voor alle opdrachten met een aanzienlijk risico voor de nationale veiligheid van ons land aangewend worden. De aanbesteders beschikken ook voor de overheidsopdrachten in de klassieke en speciale sectoren dan weer wel over een aantal handvaten om de voormelde risico's te verminderen. Een aantal risico's kunnen vaak reeds doeltreffend worden ondervangen door diverse ingrepen in het algemeen opzet van de overheidsopdracht. Daarnaast bestaan er een aantal juridische tools die er, afhankelijk van het geval, toe kunnen bijdragen om de voormelde risico's onder controle te houden.

Een belangrijke tool wordt geboden door artikel 33 van de wet van 17 juni 2016 inzake overheidsopdrachten. Deze bepaling laat onder voorwaarden afwijkingen toe op de toepassing van de normaal geldende plaatsingsregels, meer bepaald indien dit nodig is voor de bescherming van de essentiële veiligheidsbelangen. Deze mogelijkheden zijn onvoldoende gekend en moeten dan ook nader worden gekaderd, met name in het licht van de rechtspraak van het Hof van Justitie waarin de

lumière de la jurisprudence de la Cour de Justice qui précise les conditions d'une telle approche.

Le présent guide vise à expliquer la « boîte à outils » contenant les mesures pouvant être utilisées selon les cas, et ce afin de vous permettre d'y recourir plus facilement en tant qu'adjudicateur. Cependant, beaucoup d'éléments dépendront du risque spécifique qui se présente. Il est important d'examiner très attentivement le risque d'espionnage et d'ingérence non autorisée à la lumière des intérêts essentiels en matière de sécurité. Ce n'est que lorsque cet examen aura été scrupuleusement effectué qu'une stratégie appropriée pourra être élaborée, au cas par cas, pour atténuer le risque, dans la mesure où cela serait nécessaire et de manière proportionnée. Ce faisant, ce guide fournit un certain nombre de clauses qui peuvent être utiles dans certains cas. Dans certains cas, il est possible de limiter les risques sans toucher au marché, par exemple avec des mesures d'organisation comme le contrôle d'accès.

Le « quick scan » sera utilisé à des fins d'évaluation des risques (annexe II). Ce quick scan offre une méthodologie qui permet à l'adjudicateur de réaliser une analyse préliminaire des risques. La réalisation d'une telle analyse des risques est cruciale et devient donc obligatoire pour le gouvernement fédéral.

Cette boîte à outils présente un intérêt particulier pour les adjudicateurs qui identifient un risque ayant un impact sur la sécurité nationale. Les adjudicateurs dont la tâche principale n'est pas de protéger les intérêts relatifs à la sécurité peuvent également rencontrer ce type de problème. Le présent guide leur est principalement destiné. Pour cette raison, les outils applicables aux marchés des secteurs classiques et spéciaux seront expliqués en détails.

Ce guide fait partie des directives dont les pouvoirs adjudicateurs fédéraux doivent tenir compte (pour une description de ce champ d'application matériel, voir la circulaire du 11 septembre 2023 - réduction des risques de sécurité dans le cadre des marchés publics - fuites d'informations sensibles - espionnage). Il peut toutefois également inspirer d'autres adjudicateurs.

Ce guide est divisé en quatre chapitres.

Le **premier chapitre** se concentrera sur le cadre juridique applicable. La question centrale de ce chapitre est de savoir comment déterminer la loi applicable : la loi « défense et sécurité » du 13 août 2011 ou la loi relative aux marchés publics du 17 juin 2016. Ce chapitre porte

voorwaarden voor een dergelijke benadering werden toegelicht.

De onderhavige gids is erop gericht de 'toolbox' van maatregelen die, afhankelijk van het geval, aangewend kunnen worden, toe te lichten, zodat u er als aanbesteder vlotter gebruik van kunt maken. Veel zal echter afhangen van het concrete risico dat zich aandient. Het is van belang dat het risico op spionage en ongeoorloofde inmenging in het licht van essentiële veiligheidsbelangen op zorgvuldige wijze wordt geëvalueerd. Pas als dit op zorgvuldige wijze gebeurd is, kan, geval per geval, een passende strategie worden ontwikkeld om het risico te mitigeren, voor zover dit nodig zou zijn en op proportionele wijze. In deze gids worden daarbij een aantal clausules aangereikt die in sommige gevallen van nut kunnen zijn. Soms is het ook mogelijk om de risico's te beperken zonder aan de opdracht te raken, bijvoorbeeld met organisatorische maatregelen zoals bijvoorbeeld toegangscontrole.

Om de risico's te screenen zal gebruik gemaakt worden van de 'quickscan'" (bijlage II). In deze quickscan wordt een methodologie aangeboden die de aanbesteder in staat stelt de voorafgaande risicoanalyse door te voeren. Het uitvoeren van een dergelijke risicoanalyse is van cruciaal belang en wordt dan ook verplicht voor de federale overheid.

De onderhavige toolbox is vooral interessant voor aanbesteders die vaststellen dat zich een risico voordoet met een impact op de nationale veiligheid. Ook aanbesteders wiens hoofdtaak er niet in bestaat veiligheidsbelangen te beschermen, kunnen in aanraking komen met de problematiek. De onderhavige gids is vooral voor hen bedoeld. Om die reden zullen met name tools worden toegelicht die van toepassing zijn voor de opdrachten in de klassieke en speciale sectoren.

De onderhavige gids maakt deel uit van de richtsnoeren waarmee de federale aanbestedende overheden rekening moeten houden (zie, voor een omschrijving van dit materieel toepassingsgebied, omzendbrief van 11 september 2023 - reduceren van veiligheidsrisico's in het kader van overheidsopdrachten – lekken van gevoelige informatie – spionage). Ook andere aanbesteders kunnen zich er echter door laten inspireren.

Deze gids wordt onderverdeeld in vier hoofdstukken.

In het **eerste hoofdstuk** wordt belicht welk rechtskader van toepassing is. De centrale vraag in dit hoofdstuk bestaat erin hoe uitgemaakt kan worden of de wet 'defensie en veiligheid' van 13 augustus 2011 van toepassing is, dan wel de wet van 17 juni 2016 inzake

également sur les options spécifiques disponibles dans la loi « défense et sécurité » pour tenir compte des besoins de sécurité.

Le **deuxième chapitre** abordera un certain nombre d'outils qui sont à votre disposition en tant qu'adjudicateurs, sans avoir à rédiger de motivation spéciale liée aux intérêts de sécurité, et que vous pouvez utiliser, si nécessaire, dans une procédure concrète de passation selon le cas. Plusieurs de ces outils dépendent de certaines conditions. Ces outils sont par nature destinés à réduire les risques de sécurité, mais dans certains cas, ils ne préviennent pas le risque de manière suffisante. Un préjudice ou un risque important reste parfois associé à une approche utilisant uniquement les outils décrits dans ce chapitre. Dans ce cas, vous disposez d'autres options pour vous assurer de la prise en compte des intérêts de sécurité. Le **troisième chapitre** traitera donc d'un certain nombre d'outils permettant de déroger aux règles de passation normalement applicables dans le but de protéger les intérêts essentiels de sécurité. Il faut cependant toujours motiver une telle dérogation.

Enfin, **le quatrième chapitre** se concentrera sur plusieurs initiatives législatives qui peuvent, dans certains cas, avoir un impact positif sur les problématiques abordées dans ce guide, mais en adoptant un angle différent de celui de la lutte contre l'espionnage et l'ingérence dans le contexte des marchés publics. Cette législation « d'accompagnement » peut toutefois également contribuer à la réduction des risques. Ce chapitre abordera notamment le Règlement européen relatif aux subventions étrangères, l'instrument relatifs aux marchés publics internationaux, les mesures qui peuvent être prises par le Conseil européen (comme ce fut récemment le cas à l'égard de la Russie) et le Règlement général sur la protection des données. Étant donné que ces mesures ne contribuent qu'indirectement à réduire les problèmes de sécurité, elles ne sont pas considérées dans le présent guide comme étant des « outils » à la disposition de l'adjudicateur. Il est néanmoins important de comprendre les mécanismes de fonctionnement sous-jacents, ne serait-ce que pour évaluer correctement les risques en matière de sécurité.

Sauf indication contraire, les chapitres 2 à 4 ne développeront que les marchés des secteurs classiques.

Chapitre 1 – Cadre juridique et possibilité de dérogation

overheidsopdrachten en welke specifieke mogelijkheden in de wet 'defensie en veiligheid' ter beschikking staan om rekening te kunnen houden met de veiligheidsnoden.

In het **tweede hoofdstuk** worden een aantal tools besproken die u als aanbesteder ter beschikking staan, zonder dat u een bijzondere motivering die verband houdt met veiligheidsbelangen hoeft op te maken, en die u desgevallend kan inzetten in een concrete plaatsingsprocedure, afhankelijk van het geval. Sommige van deze tools zijn wel afhankelijk van bepaalde voorwaarden. Deze tools zijn van aard om het veiligheidsrisico te doen dalen, maar nemen in een aantal gevallen het risico niet op voldoende wijze weg. Soms blijft een aanzienlijk nadeel of risico verbonden aan een aanpak waarbij uitsluitend gebruik wordt gemaakt van de in dit hoofdstuk beschreven tools. In dat geval beschikt u over andere mogelijkheden om ervoor te zorgen dat de veiligheidsbelangen worden behartigd. In het **derde hoofdstuk** worden daarom een aantal tools behandeld waarbij een afwijking wordt ingeroepen op de normaal van toepassing zijnde plaatsingsregels, omwille van de bescherming van essentiële veiligheidsbelangen. Een dergelijke afwijking moet echter steeds gemotiveerd kunnen worden.

Tot slot wordt in het **vierde hoofdstuk** ingezoomd op een aantal wetgevende initiatieven die in sommige gevallen een positief effect kunnen hebben op de problematiek die in deze gids besproken wordt, maar waarbij een andere invalshoek wordt gehanteerd dan de strijd tegen spionage en inmenging in het kader van overheidsopdrachten. Ook deze "flankerende" wetgeving kan er echter toe bijdragen dat de risico's verkleinen. Er wordt met name uitleg verschaft omtrent de Europese verordening rond buitenlandse subsidies, het Instrument voor internationale overheidsopdrachten, de maatregelen die door de Europese Raad getroffen kunnen worden (zoals momenteel het geval is ten aanzien van Rusland) en de algemene verordening inzake gegevensbescherming. Aangezien deze maatregelen slechts op onrechtstreekse wijze bijdragen aan het reduceren van de veiligheidsbelangen, worden ze in de onderhavige gids niet beschouwd als een "tool" die ter beschikking staat aan de aanbesteder. Niettemin is het van belang om inzicht te verwerven in de achterliggende werkingsmechanismen, al was het maar om de veiligheidsrisico's goed te kunnen inschatten.

Tenzij anders aangegeven, zal in de hoofstukken 2 tot 4 enkel uitgeweid worden over de opdrachten in de klassieke sectoren.

Hoofdstuk 1 – Rechtskader en afwijkingsmogelijkheid

En fonction de votre domaine d'activité, des fournitures, des services ou des travaux envisagés, votre marché public peut tomber soit sous le champ d'application de la loi du 17 juin 2016 relative aux marchés publics, soit sous le champ d'application de la loi du 13 août 2011 « défense et sécurité ».

Pour déterminer la base législative applicable, veuillez-vous référer aux exclusions établies aux articles 33 et 34 de la loi du 17 juin 2016 et au champ d'application prévu aux articles 13 et 15 de la loi du 13 août 2011.

1.1. Recours à la loi du 13 août 2011 « défense et sécurité »

Si vous êtes un pouvoir adjudicateur ou une entreprise publique (pour les marchés qui ont trait à vos tâches de service public)[1], vous êtes susceptible d'utiliser la loi « défense et sécurité ». Pour pouvoir utiliser cette loi, votre marché doit toutefois être passé dans les domaines de la défense et de la sécurité et avoir pour objet:

- la fourniture d'équipements militaires OU sensibles ;
- des travaux, des fournitures et des services directement liés à un équipement militaire OU sensible pour tout ou partie de son cycle de vie;
- des travaux et des services destinés à des fins spécifiquement militaires ou sensibles.

Qu'entend-on par équipement militaire ?

Il s'agit de l'équipement spécifiquement conçu ou adapté à des fins militaires, destiné à être utilisé comme arme, munitions ou matériel de guerre.

Qu'entend-on par équipement sensible, travaux sensibles et services sensibles ?

Il s'agit des équipements, travaux et services destinés à des fins de sécurité qui font intervenir, nécessitent et/ou comportent des informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Afhankelijk van uw werkdomein en van de beoogde leveringen, diensten of werken, kan uw overheidsopdracht hetzij onder het toepassingsgebied vallen van de wet van 17 juni 2016 inzake overheidsopdrachten, hetzij onder dat van de wet 'defensie en veiligheid' van 13 augustus 2011.

Om te bepalen welke rechtsgrondslag van toepassing is, kan worden verwezen naar de uitsluitingen vermeld in de artikelen 33 en 34 van de wet van 17 juni 2016 en naar het toepassingsgebied voorzien in de artikelen 13 en 15 van de wet van 13 augustus 2011.

1.1. Een beroep doen op de wet 'defensie en veiligheid' van 13 augustus 2011

Als u een aanbestedende overheid of een overheidsbedrijf bent (voor opdrachten die betrekking hebben op uw taken van openbare dienst)[2], zal u zich waarschijnlijk beroepen op de wet 'defensie en veiligheid'. Om gebruik te kunnen maken van deze wet, moet uw overheidsopdracht echter geplaatst worden op defensie- en veiligheidsgebied en betrekking hebben op:

- de levering van militair OF gevoelig materiaal;
- werken, leveringen en diensten die rechtstreeks verband houden met militair OF gevoelig materiaal voor alle fasen of voor een deel van de levenscyclus ervan;
- werken en diensten voor specifieke militaire of gevoelige doeleinden.

Wat moet men verstaan onder militair materiaal?

Het gaat om materiaal dat specifiek ontworpen of aangepast is voor militaire doeleinden en bedoeld is om te worden gebruikt als wapen, munitie of oorlogsmaterieel.

Wat verstaat men onder gevoelig materiaal, gevoelige werken en gevoelige diensten?

Het gaat om materiaal, werken en diensten die veiligheidsdoeleinden dienen en die betrekking hebben op informatie die geclassificeerd is in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, of die dergelijke informatie noodzakelijk maken of bevatten.

[1] Sont également visés les personnes bénéficiant de droits spéciaux et exclusifs visés à l'article 94, 2°, b, et les entreprises publiques et les pouvoirs adjudicateurs visés respectivement à l'article 94, 2°, a, et c, de la loi du 17 juin 2016 relative aux marchés publics.

[2] Dit geldt ook voor personen die bijzondere of exclusieve rechten genieten uit hoofde van artikel 94, 2°, b, en de overheidsbedrijven en aanbestedende overheden die respectievelijk vermeld worden in artikel 94, 2°, a, en c, van de wet van 17 juni 2016 inzake overheidsopdrachten.

A noter que des dérogations existent également concernant les marchés relevant de l'application de l'article 346 du Traité sur le fonctionnement de l'Union européenne ou ayant trait aux intérêts essentiels de sécurité du Royaume.

1.2. Recours à la loi du 17 juin 2016 relative aux marchés publics

Si votre marché public n'entre pas dans le champ d'application de la loi « défense et sécurité », vous devez utiliser la loi du 17 juin 2016 relative aux marchés publics (en gardant à l'esprit que ladite loi comporte un certain nombre d'exclusions). A titre d'exemple, un pouvoir adjudicateur du secteur classique, comme le Ministère de la Défense, la Police fédérale ou une zone de police, appliquera le régime prévu par la loi du 17 juin 2016 pour des marchés de fournitures de véhicules civils ou de matériel de bureau, tandis que ses achats d'armements militaires ou d'équipements sensibles relèveront de la loi « défense et sécurité ».

1.3. Marchés mixtes

Certains marchés peuvent être « mixtes » et relever pour partie de l'une et de l'autre loi. Dans ce cas particulier, il est important de vous référer aux dispositions relatives aux marchés mixtes afin de déterminer la législation à appliquer (cf. art. 23 et 24 ou 106 et 107 de la loi du 17 juin 2016).

Il convient de différencier les situations en fonction du caractère objectivement séparable du marché :

- lorsque les différentes parties de votre marché sont objectivement **inséparables,** vous pouvez passer votre marché conformément à la loi « défense et sécurité » ;
- lorsque les différentes parties de votre marché sont objectivement **séparables**, vous pouvez, au choix, décider de passer des marchés distincts pour les différentes parties de votre marché ou décider de passer un **marché unique**. Lorsque vous décidez de passer des **marchés distincts**, la décision concernant le régime juridique applicable à chacun des marchés distincts est adoptée sur la base des caractéristiques des différentes parties.

Merk op dat er ook afwijkingen bestaan met betrekking tot opdrachten die binnen de werkingssfeer vallen van artikel 346 van het Verdrag betreffende de werking van de Europese Unie of die verband houden met de wezenlijke veiligheidsbelangen van het Koninkrijk.

1.2. Een beroep doen op de wet van 17 juni 2016 inzake overheidsopdrachten

1.3.

Indien uw overheidsopdracht niet binnen het toepassingsgebied van de wet 'defensie en veiligheid' valt, moet u zich beroepen op de wet van 17 juni 2016 inzake overheidsopdrachten (rekening houdend met het feit dat deze wet een aantal uitsluitingen bevat). Zo zal een aanbestedende overheid in de klassieke sector, zoals het ministerie van Defensie, de Federale Politie of een politiezone, de regeling in de wet van 17 juni 2016 toepassen voor opdrachten bestaande uit de levering van civiele voertuigen of van kantoormateriaal, terwijl hun aankopen van militaire wapenuitrusting of gevoelig materiaal vallen onder de wet 'defensie en veiligheid'.

1.4. Gemengde opdrachten

Sommige opdrachten kunnen "gemengd" zijn en gedeeltelijk onder de ene en onder de andere wet vallen. In dit bijzondere geval is het belangrijk om terug te grijpen naar de bepalingen inzake gemengde opdrachten om te kunnen bepalen welke wetgeving moet worden toegepast (cf. art. 23 en 24 of 106 en 107 van de wet van 17 juni 2016).

Er moet een onderscheid worden gemaakt tussen situaties op basis van de objectief deelbare aard van de opdracht:

- wanneer de verschillende onderdelen van uw opdracht objectief gezien **niet deelbaar** zijn, kunt u uw opdracht plaatsen overeenkomstig de wet 'defensie en veiligheid';
- wanneer de verschillende onderdelen van uw opdracht objectief gezien **deelbaar** zijn, kunt u ervoor kiezen om voor de afzonderlijke delen van uw opdracht afzonderlijke opdrachten te plaatsen of om **één enkele opdracht** te plaatsen. Indien u ervoor kiest om **afzonderlijke opdrachten** te plaatsen, wordt de beslissing over het juridische kader dat voor elk van de afzonderlijke opdrachten moet

gelden, genomen op grond van de kenmerken van de afzonderlijke onderdelen.

1.4. Comparaison entre la loi « défense et sécurité » et la loi marchés publics

La loi « défense et sécurité » présente bel et bien des spécificités. Elles ne sont toutefois pas listées de manière exhaustive.

Citons notamment que :

- La loi « défense et sécurité » prévoit des motifs d'exclusion spécifiques mieux adaptés pour préserver la sécurité. Notons par exemple la possibilité d'exclure du marché le candidat ou le soumissionnaire au sujet duquel il est établi qu'il ne possède pas la fiabilité nécessaire pour éviter des atteintes à la sécurité de l'Etat[3] ou la possibilité d'exclure du marché le candidat ou le soumissionnaire qui a fait l'objet d'un jugement ayant force de chose jugée et constatant un délit affectant sa moralité professionnelle, notamment la violation de la législation en matière d'exportation d'équipements de défense et/ou de sécurité. En outre, le non-respect des obligations en matière de sécurité des données est explicitement mentionné dans le motif d'exclusion « faute professionnelle » ;

- La loi « défense et sécurité » comporte des dispositions particulières concernant l'accès des opérateurs économiques originaires de pays tiers (Art 21 loi DS).

- Le pouvoir adjudicateur a la possibilité de préciser dans les documents du marché des exigences en matière de sécurité d'approvisionnement. Cela pourrait par exemple impliquer de limiter géographiquement (à l'Espace économique européen le lieu de production, de réparation ou d'entretien afin de pas exposer l'adjudicateur à une possible rupture

1.5. Vergelijking tussen de wet 'defensie en veiligheid' en de wet overheidsopdrachten

1.5.

De wet 'defensie en veiligheid' bevat toch wel enkele bijzonderheden. Deze worden hier echter niet op exhaustieve wijze opgesomd.

Bij wijze van voorbeeld kan worden vermeld dat:

- de wet 'defensie en veiligheid' specifieke uitsluitingsgronden bevat die meer geschikt zijn om de veiligheid te beschermen. Er is bijvoorbeeld de mogelijkheid om een kandidaat of inschrijver uit te sluiten van de opdracht wanneer werd vastgesteld dat deze niet over de nodige betrouwbaarheid beschikt om risico's voor de veiligheid van de Staat[4] te vermijden of de mogelijkheid om een kandidaat of inschrijver uit te sluiten van de opdracht als deze het voorwerp heeft uitgemaakt van een rechterlijke beslissing met kracht van gewijsde, waarbij een delict is vastgesteld dat in strijd is met zijn beroepsgedragsregels, namelijk de schending van de wetgeving inzake de uitvoer van defensie- en/of veiligheidsmateriaal. Daarnaast wordt de niet-nakoming van de verplichtingen inzake gegevensbeveiliging uitdrukkelijk vermeld bij de uitsluitingsgrond "beroepsfout";

- de wet 'defensie en veiligheid' specifieke bepalingen bevat inzake de toegang van ondernemers uit derde landen (art 21 Wet DV);

- de aanbestedende overheid de mogelijkheid heeft om in de opdrachtdocumenten eisen op te nemen inzake de bevoorradingszekerheid. Dit zou bijvoorbeeld kunnen inhouden dat de geografische locatie van de productie, de reparatie of het onderhoud wordt beperkt tot de Europese Economische Ruimte, zodat de aanbestedende overheid niet wordt blootgesteld aan een mogelijke onderbreking

[3] Voir point 9 de la Guidance note on Security of Information de la Commission Européenne du 12 février 2016 concernant ce motif d'exclusion.

[4] Zie punt 9 van de Guidance note on Security of Information van de Europese Commissie van 12 februari 2016 omtrent deze uitsluitingsgrond.

d'approvisionnement[5]. Il pourrait également être demandé à un soumissionnaire de mettre en place et/ou de maintenir les capacités nécessaires pour faire face à une éventuelle augmentation des besoins du pouvoir adjudicateur par suite d'une situation de crise.

- Le pouvoir adjudicateur peut également demander que l'offre comporte des informations suffisantes au sujet des sous-traitants déjà identifiés afin de les préapprouver. Cela peut en effet permettre au pouvoir adjudicateur de déterminer si chacun d'entre eux possède les capacités requises pour préserver de manière appropriée la confidentialité des informations classifiées auxquelles il a accès ou qu'il sera amené à produire dans le cadre de la réalisation de ses activités de sous-traitance.

van de bevoorrading[6]. Van een inschrijver kan ook worden verlangd dat hij de nodige capaciteit opbouwt en/of in stand houdt om een eventuele toename van de behoeften van de aanbestedende overheid als gevolg van een crisissituatie op te vangen;

- de aanbesteder ook kan vragen dat de offerte voldoende informatie bevat over de reeds geïdentificeerde onderaannemers, zodat deze vooraf kunnen worden goedgekeurd. Dit om de aanbesteder in staat te stellen om voor elk van hen te bepalen of ze over de nodige capaciteiten beschikken om het vertrouwelijke karakter van de geclassificeerde informatie waartoe ze toegang hebben of die ze bij de uitvoering van hun onderaannemingsactiviteiten moeten produceren, op gepaste wijze te beschermen.

Loi défense et sécurité	**Loi marchés publics**
Exclusion obligatoire (art. 63, §1er - A.R. passation 23/01/2012)	**Exclusion obligatoire (Art. 67 loi marchés publics)**
Participation à une organisation criminelle	Participation à une organisation criminelle
Corruption	Corruption
Fraude	Fraude
infraction terroriste, liée à une activité terroriste ou complicité à une telle infraction	infraction terroriste, liée à une activité terroriste ou complicité à une telle infraction
blanchiment de capitaux	blanchiment de capitaux ou financement du terrorisme
	travail des enfants ou traite des êtres humains
	occupation de ressortissants étrangers en séjour illégal
nb: dérogation possible à l'obligation d'exclusion pour motif d'intérêt général (art. 63, § 1er, al. 3 - A.R. passation 23/01/2012).	nb: dérogation possible à l'obligation d'exclusion pour motif d'intérêt général (art. 67, § 1er, al. 4 - Loi MP).
Motifs d'exclusion facultative (art. 63, §2 - A.R. passation 23/01/2012)	**Motifs d'exclusion facultative (Art. 69 loi marchés publics)**

Wet defensie en veiligheid	**Wet overheidsopdrachten**
Verplichte uitsluiting (art. 63, §1 – KB plaatsing 23/01/2012)	**Verplichte uitsluitingsgronden (art. 67 - Wet overheidsopdrachten)**
Deelname aan een criminele organisatie	Deelname aan een criminele organisatie
Corruptie	Corruptie
Fraude	Fraude
Terroristisch misdrijf, strafbaar feit in verband met een terroristische activiteit, of medeplichtigheid aan een dergelijk misdrijf	Terroristisch misdrijf, strafbaar feit in verband met een terroristische activiteit, of medeplichtigheid aan een dergelijk misdrijf
Witwassen van geld	Witwassen van geld of financiering van terrorisme
	Kinderarbeid of mensenhandel
	Tewerkstellen van illegaal verblijvende onderdanen van derde landen
NB: mogelijkheid tot afwijking van verplichting tot uitsluiting op grond van een algemeen belang (art. 63, §1, lid 3 – KB plaatsing 23/01/2012).	NB: mogelijkheid tot afwijking van verplichting tot uitsluiting op grond van een algemeen belang (art. 67, §1, lid 4 – Wet overheidsopdrachten).
Facultatieve uitsluitingsgronden (art. 63, §2 - KB plaatsing 23/11/2012)	**Facultatieve uitsluitingsgronden (art. 69 - Wet overheidsopdrachten)**

[5] Le principe de proportionnalité devra être respecté. Il semblerait en effet difficile de limiter la provenance géographique à l'Union européenne pour l'ensemble des composants de certains produits technologiques.

[6] Het proportionaliteitsbeginsel moet in acht worden genomen. Het zal immers moeilijk blijken om de geografische oorsprong voor alle onderdelen van bepaalde technologische producten te beperken tot de Europese Unie.

	(constat prouvé par tout moyen) non-respect du droit environnemental, social et du travail
état ou aveu de faillite, liquidation, cessation ou réorganisation judiciaire	état ou aveu de faillite, liquidation, cessation ou réorganisation judiciaire
(force de chose jugée) délit affectant la moralité professionnelle dont la violation de la législation en matière d'exportation d'équipements de défense ou sécurité	(constat prouvé par tout moyen) faute professionnelle grave remettant en cause son intégrité
(constat prouvé par tout moyen) faute grave dont la violation des obligations en matière de sécurité de l'information, ou de sécurité d'approvisionnement	
	(constat prouvé par tout moyen) ententes dans le but de fausser la concurrence
(constat prouvé par tout moyen) fiabilité insuffisante pour éviter les atteintes à la sécurité de l'État	
	Existence d'un conflit d'intérêts
Avantage qui fausse les conditions normales de la concurrence suite à la participation du soumissionnaire à l'élaboration du marché (art. 66 - A.R. passation 23/01/2012)	Distorsion de la concurrence résultant de la participation préalable de l'opérateur économique à la préparation de la procédure de passation
	Défaillances importantes et persistantes du soumissionnaire constatées lors de l'exécution de marchés antérieurs
(constat prouvé par tout moyen) coupable de fausses déclarations en fournissant les renseignements exigibles pour soumissionner	Coupable de fausse déclaration dans le cadre de la procédure de passation
	Tentative d'influer indûment sur le processus décisionnel du pouvoir adjudicateur

	(Vaststelling aangetoond met elk passend middel) schending van milieu-, sociaal en arbeidsrecht
Staat of aangifte van faillissement, vereffening, staking van werkzaamheden of gerechtelijke reorganisatie	Staat of aangifte van faillissement, vereffening, staking van werkzaamheden of gerechtelijke reorganisatie
(Kracht van gewijsde) delict dat in strijd is met de beroepsmoraliteit, waaronder de schending van de wetgeving inzake de uitvoer van defensie- of veiligheidsmateriaal	(Vaststelling aangetoond met elk passend middel) ernstige fout waardoor de integriteit in twijfel kan worden getrokken
(Vaststelling aangetoond met elk passend middel) ernstige fout waaronder de schending van de verplichtingen inzake gegevensbeveiliging of bevoorradingszekerheid	
	(Vaststelling aangetoond met elk passend middel) overeenkomsten gericht op vervalsing van de mededinging
(Vaststelling aangetoond met elk passend middel) onvoldoende betrouwbaar om risico's voor de veiligheid van de Staat uit te sluiten	
	Bestaan van een belangenconflict
Voordeel dat leidt tot een vertekening van de normale mededingingsvoorwaarden ten gevolge van de deelname van de inschrijver aan de uitwerking van de opdracht (art. 66 – KB plaatsing 23/01/2012)	Vervalsing van de mededinging ten gevolge van de eerdere betrokkenheid van de ondernemer bij de voorbereiding van de plaatsingsprocedure
	Inschrijver heeft blijk gegeven van aanzienlijke of voortdurende tekortkomingen tijdens de uitvoering van eerdere overheidsopdrachten
(Vaststelling aangetoond met elk passend middel) schuldig aan valse verklaringen bij het verstrekken van de informatie die nodig is om in te schrijven	Schuldig aan valse verklaringen in het kader van de plaatsingsprocedure van de opdracht
	Poging tot het beïnvloeden van het besluitvormingsproces van de aanbestedende overheid

Chapitre 2 – Outils ne nécessitant pas de motivation spéciale en raison d'intérêts essentiels de sécurité

Hoofdstuk 2 – Tools waarvoor geen bijzondere motivering in verband met essentiële veiligheidsbelangen vereist is

2.1. Accès non garanti aux opérateurs économiques des pays tiers

2.1. Geen gegarandeerde toegang voor ondernemers uit derde landen

Sur la base de l'article 4 de la loi relative aux marchés publics, il est possible d'exclure les opérateurs économiques des pays avec lesquels aucun accord multilatéral ou bilatéral ne s'applique en termes d'accès aux marchés publics.

> *[…] Les adjudicateurs traitent les opérateurs économiques sur un pied d'égalité et sans discrimination et agissent d'une manière transparente et proportionnée.*
>
> *Dans la mesure où les annexes 1, 2, 4 et 5 et les notes générales relatives à l'Union européenne de l'appendice I de l'Accord sur les Marchés Publics du 15 avril 1994 ainsi que d'autres conventions internationales liant l'Union européenne le prévoient, les adjudicateurs accordent aux travaux, aux fournitures, aux services et aux opérateurs économiques des signataires de ces conventions un traitement qui n'est pas moins favorable que celui accordé aux travaux, aux fournitures, aux services et aux opérateurs économiques de l'Union européenne. […]*

En principe, les opérateurs économiques des pays membres de « l'Accord sur les marchés publics (AMP)[7] » de l'Organisation mondiale du commerce (OMC)[8] disposent de droits d'accès automatiques et incontestables aux marchés publics des États membres de l'UE.

Ainsi, dans les cas où il n'existe aucun accord international ou qu'aucun accord ne s'applique dans le cas en question, aucun accès garanti ne peut être prévu. L'accès n'est pas non plus automatiquement interdit. Il appartient aux adjudicateurs de décider d'exclure ou non un tel opérateur économique. Il est préférable de le mentionner dans la publication, particulièrement en cas de procédure ouverte.

La Commission européenne a publié dernièrement, le 24 juillet 2019, des lignes directrices sur la participation des soumissionnaires et des produits de pays tiers aux marchés publics de l'UE. Vous pouvez prendre connaissance de celles-ci via ce lien[11]. De plus amples informations sont disponibles sur les sites web de la Commission européenne et de l'AMP. Il est également possible de savoir si un tel accord international peut s'appliquer ou non.

Op basis van artikel 4 van de wet inzake overheidsopdrachten is het mogelijk om ondernemingen uit landen waarmee geen multilateraal of bilateraal akkoord van toepassing is op het vlak van toegang tot overheidsopdrachtenmarkt, uit te sluiten.

> *[…] De aanbesteders behandelen de ondernemers op gelijke en niet-discriminerende wijze en handelen op een transparante en proportionele wijze.*
>
> *Voor zover de bijlagen 1, 2, 4 en 5 en de algemene opmerkingen bij aanhangsel I van de Europese Unie bij de Overeenkomst inzake overheidsopdrachten van 15 april 1994 en de andere internationale overeenkomsten waardoor de Europese Unie gebonden is van toepassing zijn, geven aanbesteders aan werken, leveringen, diensten en ondernemers van de ondertekenende partijen van deze overeenkomsten geen minder gunstige behandeling dan die welke zij aan werken, leveringen, diensten en ondernemers van de Europese Unie geven. […]*

In principe hebben de ondernemingen uit landen die lid zijn van de 'Government Procurement Agreement (GPA)[9]' binnen de World Trade Organization (WTO)[10] automatisch en onbetwistbaar toegangsrecht tot de overheidsopdrachten van de EU-lidstaten.

In gevallen waarbij er geen dergelijke internationale overeenkomst bestaat of waarbij een dergelijke overeenkomst in het concrete geval niet van toepassing is, wordt er zodoende geen gegarandeerde toegang verschaft. De toegang wordt ook niet automatisch verboden. Het komt aan de aanbesteders toe te beslissen om een dergelijke ondernemer al dan niet uit te sluiten. Dit wordt best bij de bekendmaking vermeld, zeker bij een openbare procedure.

De Europese Commissie heeft op 24 juli 2019 richtsnoeren uitgevaardigd voor de deelname van inschrijvers en goederen uit derde landen aan de aanbestedingsmarkt van de EU. Via deze link[12] kan u kennis nemen van deze richtsnoeren. Op de website van de Europese Commissie en van de GPA is meer informatie voorhanden en kan uitgezocht worden of al dan niet een dergelijke internationale overeenkomst van toepassing kan zijn.

[7] l'Accord sur les marchés publics (AMP).
[8] l'Organisation Mondiale sur le Commerce (OMC).
[9] NL: de Overeenkomst inzake overheidsopdrachten
[10] NL: de Wereldhandelsorganisatie (WHO)
[11] https://commission.europa.eu/funding-tenders/tools-public-buyers/public-procurement-and-non-eu-participation_fr
[12] https://ec.europa.eu/info/policies/public-procurement/tools-public-buyers/public-procurement-and-non-eu-participation_nl

Remarque

L'AMP et les chapitres relatifs aux marchés publics des accords de libre-échange ne s'appliquent pas automatiquement à TOUS les marchés publics. L'AMP et les accords de libre-échange se composent généralement de deux (2) parties :

1. un texte juridique contenant des règles sur les principes et les procédures, et

3. le schéma de couverture de chaque partie.

Les listes déterminent les autorités publiques devant se conformer aux règles convenues et dans quelle mesure leurs marchés de biens et de services sont ouverts à la participation d'opérateurs économiques (et de leurs biens et services) des autres parties de l'AMP ou des pays partenaires de l'accord de libre-échange.

Seules les offres dépassant les seuils fixés dans les listes relatives au champ d'application de chaque partie sont couvertes.

→ Principe : L'AMP ne peut être appelé que pour les marchés > au seuil de l'UE

Les listes du marché de l'UE sont établies dans les annexes de l'appendice I de l'AMP et dans les annexes correspondantes des accords de libre-échange respectifs.[13] En vérifiant ces sources, l'adjudicateur peut déterminer si un soumissionnaire (ou ses biens et services) dispose d'un accès garanti à son marché public.

Attention

Nonobstant le fait que ces mesures permettent au pouvoir adjudicateur de restreindre l'accès, cela n'implique pas nécessairement que les pays concernés ne soient pas en mesure de continuer à proposer leurs produits et/ou services par l'intermédiaire d'un opérateur économique établi dans l'UE/EEE. Pour atténuer au mieux les risques de sécurité, les mesures de restriction d'accès devront être complétées par d'autres mesures, telles qu'expliquées dans cette boîte à outils.

Il est possible qu'au cours de la procédure de passation, le statut d'un pays tiers change, soit par la conclusion de nouveaux traités bilatéraux ou multilatéraux, soit par leur rupture ou leur suspension (par exemple, comme mesure

Opmerking

De GPA en de hoofdstukken inzake overheidsopdrachten van de vrijhandelsovereenkomsten zijn niet automatisch van toepassing op ALLE overheidsopdrachten. De GPA en de vrijhandelsovereenkomsten bestaan doorgaans uit twee (2) delen:

2. een wettekst met regels voor beginselen en procedures;

4. de dekkingsschema's van elke partij.

De dekkingsschema's bepalen welke overheidsinstanties moeten voldoen aan de overeengekomen regels en in welke mate hun aanbesteding van goederen en diensten opengesteld is voor deelname van ondernemers (en hun goederen en diensten) van de andere partijen van de Overeenkomst inzake overheidsopdrachten of de partnerlanden van een vrijhandelsovereenkomst.

Enkel aanbestedingen die de in de dekkingsschema's van elke partij vastgelegde drempelwaarden overstijgen, zijn gedekt.

→ Principe: GPA enkel inroepbaar voor opdrachten > EU-drempel

De dekkingsschema's van de EU-markt zijn vastgelegd in de bijlagen bij aanhangsel I van de GPA en in de relevante bijlagen bij de respectieve vrijhandelsovereenkomsten.[14] Door deze bronnen te checken kan de aankoper bepalen of een inschrijver (of zijn goederen en diensten) gewaarborgde toegang heeft tot zijn overheidsopdracht.

Opgelet

Niettegenstaande dat dergelijke maatregelen de aanbestedende overheid toelaten de toegang te beperken, impliceert dit niet noodzakelijk dat desbetreffende landen niet in de mogelijkheid verkeren om alsnog hun producten en/of diensten aan te bieden via een economische operator die gevestigd is binnen de EU/EER. Om eventuele veiligheidsrisico's zo goed mogelijk te mitigeren, zullen de maatregelen inzake toegangsbeperking moeten worden aangevuld met andere maatregelen, zoals toegelicht in deze toolbox.

Het is mogelijk dat in de loop van de plaatsingsprocedure het statuut van een derde land wijzigt, door het sluiten van nieuwe bilaterale of multilaterale verdragen of door het verbreken of schorsen ervan (bijvoorbeeld als

[13] Vous pouvez prendre connaissance de celles-ci via ce lien : https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm

[14] Hieronder kan u kennis nemen van een link naar deze dekkingsschema's : https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm

de représailles de l'UE pour un accès inégal aux marchés publics ou en raison de sanctions internationales). Dans le cas d'un nouveau traité qui accorde explicitement l'accès aux marchés publics aux entreprises d'un pays tiers, la date de référence pour décider si l'entreprise doit être admise ou non est la date à laquelle la candidature ou, dans le cas des procédures ouvertes, l'offre a été présentée. Si un traité arrive à expiration ou est suspendu pendant la procédure de passation, le statut du candidat ou du soumissionnaire change également (de même que celui du soumissionnaire qui cesse de satisfaire aux motifs d'exclusion ou aux critères de sélection au cours de la procédure). Toutefois, une fois le marché clôturé, il existe un contrat entre le soumissionnaire et l'adjudicateur, qui ne peut être annulé sans conséquences juridiques.

2.2. Choix de la procédure de passation

Une fois votre base légale déterminée, vous saurez quelles procédures de passation s'offre à vous. C'est alors le moment de déployer différentes stratégies pour se prémunir des situations à risque.

a) Recours à une procédure en 2 phases

Le choix d'une procédure en 2 phases vous permet d'effectuer la passation du marché en deux étapes. D'abord, vous effectuez une sélection de candidats qui seront ensuite les seuls invités à remettre offre. Il s'agit d'une bonne façon de limiter l'accès aux documents sensibles15 du marché aux seuls opérateurs économiques qui ont préalablement prouvé satisfaire vos critères de sélection. Vous pouvez également vous assurer que ces opérateurs économiques traitent ces documents de façon sécurisée en imposant une procédure spécifique (voir infra).

La loi relative aux marchés publics (art. 64, § 1er) nous oblige à donner accès aux documents du marché dès la publication (sauf exceptions bien définies) ou lors de l'invitation à confirmer l'intérêt. On peut néanmoins réserver certaines informations sensibles (dans le sens large du mot) aux candidats sélectionnés ou même à l'adjudicataire, pour autant que les informations publiées permettent aux opérateurs économiques de décider s'ils se sentent aptes à exécuter le marché, si les conditions (timing, lieux, conditions spécifiques liées à l'exécution) les arrangent et s'ils peuvent apporter une réponse adéquate aux spécifications techniques.

represaillemaatregel van de EU omwille van ongelijke toegang tot overheidsopdrachten of door internationale sancties). In het geval van een nieuw verdrag dat ondernemingen uit een derde land expliciet toegang verleent tot overheidsopdrachten, geldt de datum waarop de kandidatuur moest gesteld zijn of, bij openbare procedures, de offerte moest ingediend zijn als referentiedatum om te beslissen of de onderneming al dan niet moet toegelaten worden. Indien een verdrag vervalt of geschorst wordt tijdens de plaatsingsprocedure, wijzigt het statuut van de kandidaat of inschrijver mee (net zoals van de inschrijver die in de loop van de procedure niet meer voldoet in het kader van de uitsluitingsgronden of selectiecriteria). Eens de opdracht gesloten is, bestaat er echter een contract tussen de aanbesteder en de opdrachtnemer, dat niet meer zonder juridische gevolgen kan teniet gedaan worden.

2.2. Keuze van de plaatsingsprocedure

Zodra u uw rechtsgrondslag heeft bepaald, weet u welke plaatsingsprocedures voor u beschikbaar zijn. Vervolgens kunt u verschillende strategieën inzetten om uzelf te beschermen tegen risicovolle situaties.

b) Gebruik van de tweestapsprocedure

Door te kiezen voor een tweestapsprocedure kunt u de plaatsing van de opdracht in twee fasen uitvoeren. Eerst maakt u een selectie van kandidaten die vervolgens als enige worden uitgenodigd om een offerte in te dienen. Dit is een goede manier om de toegang tot gevoelige opdrachtdocumenten[16] te beperken tot de ondernemers die vooraf hebben bewezen dat zij aan uw selectiecriteria voldoen. U kunt er ook voor zorgen dat deze ondernemers deze documenten veilig behandelen door een specifieke procedure op te leggen (zie onder).

De wet op de overheidsopdrachten (art. 64, § 1) verplicht ons om van bij de bekendmaking (behalve in welbepaalde gevallen) of bij de uitnodiging tot bevestiging van de belangstelling toegang te verlenen tot de opdrachtdocumenten. Niettemin kan bepaalde gevoelige informatie (in ruime zin) worden voorbehouden aan de geselecteerde kandidaten of zelfs aan de opdrachtnemer, op voorwaarde dat de bekendgemaakte informatie de ondernemers in staat stelt te beslissen of zij zich geschikt achten om de opdracht uit te voeren, of de voorwaarden (tijdschema, plaats, specifieke uitvoeringsvoorwaarden)

[15] Attention, vous ne pouvez pas vous abstenir de publier l'entièreté du contenu du cahier spécial des charges. Le candidat doit disposer de suffisamment d'informations pour déterminer s'il peut remettre offre !

[16] Let op: u kunt niet afzien van de publicatie van de volledige inhoud van het bestek. De kandidaat moet over voldoende informatie beschikken om te bepalen of hij in kan schrijven!

Parmi les procédures en 2 phases, on peut citer notamment :

Procédure restreinte (Art 37 loi marchés publics)	Pas de négociation
Procédure concurrentielle avec négociation (Art 38 loi marchés publics)	Négociation possible

b) Recours à la procédure négociée sans publication préalable

Lorsque le recours à la procédure négociée sans publication préalable est possible, vous pouvez inviter les opérateurs économiques de votre choix à soumettre une offre. De cette façon vous pouvez opérer votre propre sélection et évitez les opérateurs économiques présentant une risque potentiel ou avéré. L'adjudicateur doit, dans la mesure du possible, consulter plusieurs soumissionnaires (au moins 3). En d'autres termes, il doit, dans la mesure du possible, organiser lui-même la mise en concurrence.

La procédure négociée sans publication préalable ne peut être utilisée qu'à titre exceptionnel, notamment dans les cas suivants :

- si la dépense à approuver est inférieure au montant maximum visé à l'article 90 de l'A.R. relatif à la passation des marchés publics dans les secteurs classiques ;
- en cas d'urgence impérieuse résultant d'évènements imprévisibles pour le pouvoir adjudicateur. Cette possibilité ne peut être utilisée, dans la mesure strictement nécessaire, que si les délais de la procédure ouverte, restreinte ou concurrentielle avec négociation ne peuvent être respectés en raison de l'urgence résultant d'évènements imprévisibles pour le pouvoir adjudicateur ;
- dans le cas où aucune demande de participation ou offre appropriée n'a été présentée dans le cadre d'une procédure ouverte ou restreinte, pour autant que les

hun schikken en of ze op gepaste wijze kunnen beantwoorden aan de technische vereisten.

Voorbeelden van tweestapsprocedures zijn:

Niet-openbare procedure (art. 37 wet overheidsopdrachten)	Geen onderhandeling
Mededingingsprocedure met onderhandeling (art. 38 wet overheidsopdrachten)	Onderhandeling mogelijk

c) Gebruik van de onderhandelingsprocedure zonder voorafgaande bekendmaking

Wanneer een onderhandelingsprocedure zonder voorafgaande bekenmaking mogelijk is, kunt u kiezen welke ondernemers u uitnodigt om een offerte in te dienen. Zo kunt u zelf uw selectie maken en ondernemers die een mogelijk of bewezen risico vormen, vermijden. De aanbesteder moet, indien mogelijk, meerdere inschrijvers consulteren (minstens drie). Met andere woorden moet hij, waar mogelijk, de mededinging zelf organiseren.

Er kan slechts uitzonderlijk gebruik worden gemaakt van de onderhandelingsprocedure zonder voorafgaande bekendmaking, meer bepaald in onderstaande gevallen:

- als de goed te keuren uitgave lager is dan het in artikel 90 van het KB plaatsing klassieke sectoren bedoelde maximumbedrag;
- in geval van dwingende spoed die niet te wijten is aan de aankoper zelf. Van deze mogelijkheid mag slechts gebruik worden gemaakt, voor zover dit strikt noodzakelijk is, indien de termijnen voor de openbare of niet-openbare procedure of de mededingingsprocedure met onderhandeling wegens deze dwingende spoed die moet voortvloeien uit onvoorzienbare gebeurtenissen voor de aanbesteder, niet in acht kunnen worden genomen;
- in het geval waarbij er geen geschikte aanvraag tot deelneming of offerte werd ingediend ingevolge een openbare of niet-openbare procedure, mits de

conditions initiales du marché ne soient pas substantiellement modifiées ;

- si un monopole existe pour une raison spécifique (pour des raisons artistiques, des droits exclusifs, des raisons techniques), qui doit être précisément motivée dans chaque cas.
- dans le cas d'un marché public de travaux ou de services, lorsqu'il s'agit de nouveaux travaux ou services consistant en la répétition de travaux ou services similaires, attribués à l'adjudicataire du marché initial par le même pouvoir adjudicateur, à condition que ces travaux ou services correspondent à un projet de base et que ce projet ait fait l'objet d'un marché initial passé selon une procédure visée à l'article 35, premier alinéa, de la loi du 17 juin 2016 ;
- dans le cas d'un marché public de fournitures, lorsqu'il s'agit de produits fabriqués exclusivement à des fins de recherche, d'expérimentation, d'étude ou de développement ;
- des fournitures complémentaires doivent être effectuées par le fournisseur initial, soit pour le renouvellement partiel de fournitures ou d'installations, soit pour l'extension de fournitures ou d'installations existantes, lorsqu'un changement de fournisseur obligerait le pouvoir adjudicateur à acquérir des fournitures ayant des caractéristiques techniques différentes, de sorte qu'il en résulterait une incompatibilité ou des difficultés techniques disproportionnées d'utilisation et d'entretien ;

Les possibilités susmentionnées doivent toujours être interprétées de manière restrictive. Pour connaître les conditions exactes dans lesquelles le recours à cette procédure est possible, veuillez-vous référer à l'article 42 de la loi du 17 juin 2016.

2.3 Application des motifs d'exclusion

a) Motifs d'exclusion obligatoire

Le pouvoir adjudicateur ne dispose pas de pouvoir d'appréciation dans le cadre des motifs d'exclusion obligatoire. Il est par conséquent obligé d'exclure le candidat/soumissionnaire s'il a été condamné, par une

oorspronkelijke voorwaarden van de opdracht niet wezenlijk worden gewijzigd;

- als er om een specifieke reden een monopolie bestaat (omwille van artistieke redenen, alleenrechten, technische redenen), hetgeen telkenmale zorgvuldig gemotiveerd moet worden;
- in geval van een overheidsopdracht voor werken of diensten wanneer het gaat om nieuwe werken of diensten bestaande uit een herhaling van soortgelijke werken of diensten, die aan de opdrachtnemer van de oorspronkelijke opdracht worden gegund door dezelfde aanbesteder, op voorwaarde dat deze werken of diensten overeenstemmen met een basisproject en dit project het voorwerp uitmaakte van een oorspronkelijke opdracht die geplaatst werd bij een procedure zoals bedoeld in artikel 35, eerste lid, van de wet van 17 juni 2016;
- in geval van een overheidsopdracht voor leveringen wanneer het producten betreft die uitsluitend voor onderzoek, proefneming, studie of ontwikkeling worden vervaardigd;
- aanvullende leveringen moeten worden verricht door de oorspronkelijke leverancier, die ofwel bestemd zijn voor de gedeeltelijke vernieuwing van leveringen of installaties, ofwel voor de uitbreiding van bestaande leveringen of installaties, wanneer een verandering van leverancier de aanbestedende overheid ertoe zou verplichten leveringen te verwerven met andere technische eigenschappen, zodat onverenigbaarheid zou ontstaan of zich bij het gebruik en het onderhoud onevenredige technische moeilijkheden zouden voordoen.

De voormelde mogelijkheden moeten steeds op restrictieve wijze geïnterpreteerd worden. Voor de precieze voorwaarden waaronder gebruik gemaakt mag worden van deze procedure, wordt verwezen naar artikel 42 van de wet van 17 juni 2016.

2.3 Toepassing van de uitsluitingsgronden

b) Verplichte uitsluitingsgronden

In het kader van de verplichte uitsluitingsgronden beschikt de aanbestedende overheid niet over appreciatiebevoegdheid en is hij verplicht de kandidaat/inschrijver uit te sluiten, indien deze, bij een

décision de justice passée en force de chose jugée[17], notamment en cas de participation à une organisation criminelle, corruption, fraude, infractions terroristes, etc. Cette exclusion vaut pour une période de cinq ans à compter de la date de la condamnation.[18] Toute décision est considérée comme étant passée en force de chose jugée dès lors qu'elle n'est plus susceptible d'opposition ou d'appel, sous réserve des exceptions prévues par la loi et sans préjudice des effets des recours extraordinaires.

Attention : pas d'exclusion si le candidat/soumissionnaire peut démontrer, conformément à l'art. 70 de la loi relative aux marchés publics, qu'il a pris des mesures adéquates (correctrices) attestant de sa fiabilité.

Moyen de preuve = un **extrait du casier judiciaire** ou un document équivalent délivré par une autorité judiciaire ou publique du pays d'origine ou de provenance et montrant que les conditions requises sont remplies (art. 72, § 2, 1°, de l'A.R. relatif à la passation des marchés publics dans les secteurs classiques). Lorsqu'un tel extrait ou document n'est pas délivré dans le pays concerné ou ne contient pas toutes les informations requises, il peut être remplacé par une déclaration sous serment ou, dans les pays où cette modalité n'est pas prévue, par une déclaration solennelle faite par l'intéressé devant une autorité judiciaire ou publique, un notaire ou un organisme professionnel compétent dans le pays d'origine ou de provenance.

Remarque : Une déclaration sous serment (caractère formel) se distingue d'une déclaration sur l'honneur explicite/implicite de la part du candidat ou du soumissionnaire, selon laquelle il n'est pas concerné par le motif d'exclusion allégué. Ces dernières ne doivent pas être assimilées à un moyen de preuve et, le cas échéant, leur authenticité doit être vérifiée par le pouvoir adjudicateur.

b) Motifs d'exclusion facultative

Le pouvoir adjudicateur dispose, dans le cadre des motifs d'exclusion facultative, d'un certain pouvoir d'appréciation pour exclure ou non le candidat/soumissionnaire[21] :

rechterlijke beslissing met kracht van gewijsde[19], veroordeeld werd voor bv. deelname aan een criminele organisatie, omkoping, fraude, terroristische misdrijven enz. Deze uitsluiting geldt voor een periode van vijf jaar vanaf de datum van de veroordeling.[20] Iedere beslissing gaat in kracht van gewijsde zodra zij niet meer voor verzet of hoger beroep vatbaar is, behoudens de uitzonderingen die de wet bepaalt en onverminderd de gevolgen van de buitengewone rechtsmiddelen.

Opgelet: geen uitsluiting indien de kandidaat/inschrijver kan aantonen, overeenkomstig art. 70 van de wet overheidsopdrachten, toereikende (corrigerende) maatregelen te hebben getroffen die alsnog zijn betrouwbaarheid bevestigen.

Bewijsmiddel = **uittreksel uit het strafregister** of een gelijkwaardig document uitgereikt door een gerechtelijke of overheidsinstantie van het land van oorsprong of herkomst en waaruit blijkt dat aan de gestelde eisen is voldaan (Art 72, §2, 1°, van het KB inzake plaatsing overheidsopdrachten in de klassieke sectoren). Wanneer een dergelijk uittreksel of document niet wordt uitgereikt in het betrokken land of daarin niet alle gevraagde informatie wordt vermeld, kan het worden vervangen door een verklaring onder ede of, in landen waar niet in een eed is voorzien, door een plechtige verklaring van de betrokkene voor een gerechtelijke of overheidsinstantie, een notaris of een bevoegde beroepsorganisatie van het land van oorsprong of herkomst.

Opmerking: Een verklaring onder ede (formeel karakter) verschilt van een expliciete/impliciete verklaring op erewoord vanwege de kandidaat of inschrijver dat hij zich niet in de gestelde uitsluitingsgrond bevindt. Dit laatste mag niet worden gelijkgesteld met een bewijsmiddel en dient in voorkomend geval naar echtheid te worden gecontroleerd door de aanbestedende overheid.

c) Facultatieve uitsluitingsgronden

Wat de facultatieve uitsluitingsgronden betreft beschikt de aanbestedende overheid wel over enige

[17] Toutefois, en ce qui concerne l'emploi de ressortissants de pays tiers en séjour illégal, le pouvoir adjudicateur doit déjà les exclure dès que l'infraction est constatée par une décision administrative ou judiciaire.

[18] Cinq ans à compter de la fin de l'infraction pour l'emploi de ressortissants de pays tiers en séjour illégal.

[19] Wat het tewerkstellen van illegaal verblijvende onderdanen van derde landen betreft moet de aanbestedende overheid echter reeds tot uitsluiting overgaan zodra de inbreuk is vastgesteld door middel van een administratieve of rechterlijke beslissing.

[20] Vijf jaar vanaf de beëindiging van de inbreuk voor het tewerkstellen van illegaal verblijvende onderdanen van derde landen

[21] Cela signifie que même si le motif d'exclusion facultative est applicable et que le soumissionnaire pourrait être exclu en raison de l'existence de ce motif dans son chef, le pouvoir adjudicateur peut décider de ne pas exclure le soumissionnaire. Bien que le pouvoir adjudicateur dispose d'un certain pouvoir discrétionnaire, ce pouvoir sera quelque peu limité en raison du respect du devoir de diligence et de prudence dans le chef du pouvoir adjudicateur. Ces principes de bonne administration impliquent généralement qu'un pouvoir adjudicateur ne s'engage pas avec des candidats ou soumissionnaires pour lesquels s'applique un motif d'exclusion facultative. Que le pouvoir adjudicateur choisisse d'exclure ou de ne pas exclure, dans les deux cas, il devra

- si le pouvoir adjudicateur prouve par tout moyen approprié que le candidat ou le soumissionnaire a violé les **obligations applicables en matière de droit environnemental, social et du travail** ;

- lorsque le pouvoir adjudicateur peut prouver, par tout moyen approprié, que le candidat ou le soumissionnaire a commis une **faute professionnelle grave** mettant en cause son intégrité ;

  Par ex. une enquête pénale en cours sans prononcé final ou condamnation.

  La faute en matière professionnelle est ici qualifiée de « *tout comportement fautif [...] qui a une incidence sur la crédibilité professionnelle de l'opérateur en cause* » (voir Cour de Justice, C-465/11 du 13 décembre 2012), ce qui a également été confirmé par la jurisprudence du Conseil d'État (voir par ex. Conseil d'État, n° 237.912 du 7 avril 2017).

  De plus, cette erreur doit être de nature « grave », ce qui est décrit par la CJ comme un comportement de l'opérateur économique en cause « *qui dénote une intention fautive ou une négligence d'une certaine gravité de sa part* » et est défini par la doctrine comme « une faute qu'un professionnel

appreciatiebevoegdheid om de kandidaat/inschrijver al dan niet uit te sluiten[22]:

- indien de aanbestedende overheid met elk passend middel aantoont dat de kandidaat of inschrijver de toepasselijke **verplichtingen op het vlak van het milieu-, sociaal en arbeidsrecht, heeft geschonden**;

- wanneer de aanbestedende overheid kan aantonen, met elk passend middel, dat de kandidaat of inschrijver in de uitoefening van zijn **beroep een ernstige fout** heeft begaan, waardoor zijn integriteit in twijfel kan worden getrokken;

  Bv. lopend strafonderzoek zonder dat er sprake is van een definitieve uitspraak of veroordeling.

  Een fout in de uitoefening van zijn beroep wordt hierbij beschreven als "*elk onrechtmatig gedrag […] dat invloed heeft op de professionele geloofwaardigheid van de betrokken marktdeelnemer*" (zie het arrest C-465/11 van het hof van Justitie 13 december 2012), wat ook bevestigd werd door de rechtspraak van de Raad van State (zie bijvoorbeeld het arrest nr. 237.912 van 7 april 2017).

  Deze fout dient bovendien een 'ernstig' karakter te hebben, wat door het HvJ beschreven wordt als een gedraging die "*wijst op kwaad opzet of nalatigheid van een zekere ernst van deze marktdeelnemer*" en door de rechtsleer wordt omschreven als een fout die een normaal

motiver sa décision. La marge d'appréciation du pouvoir adjudicateur doit donc être utilisée avec prudence. Le pouvoir adjudicateur devra s'assurer que les principes d'égalité et de proportionnalité sont bien respectés. Et, dans tous les cas, il devra formellement motiver sa décision. En ce qui concerne plus spécifiquement le champ d'application du motif d'exclusion relatif à la collusion (article 69, alinéa 1er, 4°, de la loi du 17 juin 2016), il est renvoyé dans son intégralité au titre 5.3 « la compétence des pouvoirs adjudicateurs en matière d'application du motif d'exclusion: leur large marge d'appréciation et les limites de leur pouvoir d'appréciation » de la communication C(2021)1631 de la Commission européenne publiée le 18 mars 2021 sur les outils de lutte contre la collusion dans les marchés publics et orientations sur la manière d'appliquer le motif d'exclusion y relatif.

[22] Zelfs indien de facultatieve uitsluitingsgrond van toepassing is en de inschrijver op deze grond kan worden uitgesloten, kan de aanbestedende overheid dus beslissen om de inschrijver niet uit te sluiten. Hoewel de aanbestedende overheid over enige mate van discretionaire beslissingsruimte beschikt, zal deze beslissingsruimte enigszins beperkt worden ingevolge de naleving van de zorgvuldigheids- en voorzichtigheidsplicht in hoofde van de aanbestedende overheid. Deze beginselen van behoorlijk bestuur zullen doorgaans inhouden dat een aanbestedende overheid zich niet met kandidaten of inschrijvers inlaat waarvoor een facultatieve uitsluitingsgrond van toepassing is. Of de aanbestedende overheid nu beslist om uit te sluiten of niet uit te sluiten, hij zal zijn beslissing in beide gevallen moeten motiveren. De beoordelingsmarge van de aanbestedende overheid moet dus met de nodige omzichtigheid worden gehanteerd. De aanbestedende overheid moet zich ervan vergewissen dat het gelijkheids- en evenredigheidsbeginsel in acht wordt genomen. Bovendien moet zij in ieder geval haar beslissing formeel motiveren. Wat meer specifiek de beslissingsruimte aangaande de uitsluitingsgrond inzake collusie betreft (artikel 69, eerste lid, 4°, van de wet van 17 juni 2016) wordt integraal verwezen naar titel 5.3 "Bevoegdheid van aanbestedende diensten om de uitsluitingsgrond toe te passen: ruime beoordelingsmarge en grenzen aan hun beoordelingsvrijheid" van de op 18 maart 2021 bekend gemaakte Mededeling de Europese Commissie C(2021)1631 over instrumenten ter bestrijding van collusie bij overheidsopdrachten en over richtsnoeren voor de toepassing van de desbetreffende uitsluitingsgrond.

.

normalement diligent et gardien des règles de la profession ne commettrait pas et qui ébranle la confiance de l'autorité. »

Ainsi, pour qu'un pouvoir adjudicateur puisse invoquer une telle « faute grave » pour exclure un candidat/soumissionnaire, cette exclusion doit être fondée sur une évaluation minutieuse et concrète de chaque cas, la « marge d'appréciation » étant limitée par les principes généraux de bonne gouvernance (obligation de motivation, principe du caractère raisonnable, principe de proportionnalité, etc.)

Toutefois, une faute professionnelle grave peut être prouvée par « tout moyen approprié ». Cela n'exige pas que le pouvoir adjudicateur soit en mesure de présenter des preuves « incontestables » ou que le comportement dénoncé puisse être punissable (voir à cet effet Conseil d'État n° 252.479 du 20 décembre 2021).

Par ex. un procès-verbal, (voir Conseil d'État n° 237.029 du 12 janvier 2012), un rapport d'expertise (voir Conseil d'État n° 217.306 du 18 janvier 2012), l'examen d'un dossier pénal (voir Conseil d'État n° 188.712 du 11 décembre 2008) ou une proposition de transaction (voir Conseil d'État n° 237.912 du 7 avril 2017) dont il ressort que le manquement est imputable au soumissionnaire.

toegewijde beroepsbewaker van de regels van het vak niet zal begaan en waardoor het vertrouwen van het bestuur wordt ondermijnd.

Wil een aanbestedende overheid een dergelijke 'ernstige fout' inroepen om een kandidaat/inschrijver uit te sluiten, dient deze uitsluiting dus te berusten op een zorgvuldige en concrete beoordeling van elk individueel geval op zich, waarbij de 'appreciatieruimte' wordt begrensd door de algemene beginselen van behoorlijk bestuur (motiveringsplicht, redelijkheidsbeginsel, proportionaliteitsbeginsel, enz.).

De ernstige beroepsfout kan evenwel worden aangetoond aan de hand van "elk passend middel". Hierbij is het niet vereist dat de aanbestedende overheid een "onomstotelijk" bewijs kan voorleggen of dat het gelaakte gedrag strafbaar kan worden gesteld (zie hiervoor arrest Raad van State nr. 252.479 van 20 december 2021).

Bv. een proces-verbaal (zie RvS nr. 237.029 van 12 januari 2012), een deskundigenverslag (zie RvS nr. 217.306 van 18 januari 2012), inzage in het strafdossier (zie RvS nr. 188.712 van 11 december 2008) of een minnelijke schikking (zie RvS nr. 237.912 van 7 april 2017) waaruit de tekortkoming in hoofde van de inschrijver blijkt.

- lorsque le pouvoir adjudicateur dispose d'indices suffisamment plausibles pour conclure que le candidat ou le soumissionnaire aurait commis des actes, accords ou ententes, **visant à fausser la concurrence** ;

- si le candidat ou soumissionnaire a échoué à satisfaire, de manière grave ou persistante, **aux obligations fondamentales qui lui incombaient dans le cadre de l'exécution d'un ou de plusieurs marchés publics antérieurs, d'un marché antérieur conclu avec le pouvoir adjudicateur ou d'un autre contrat de concession** et si cela a conduit à prendre des mesures d'office, à imposer des réparations ou d'autres sanctions similaires ;

- si le candidat ou soumissionnaire s'est rendu gravement coupable de **fausses déclarations** en fournissant les informations nécessaires au contrôle de l'absence de motifs d'exclusion ou du

- wanneer de aanbestedende overheid over voldoende plausibele aanwijzingen beschikt om te besluiten dat de kandidaat of inschrijver handelingen zou hebben gesteld, overeenkomsten zou hebben gesloten of afspraken zou hebben gemaakt, die gericht zijn op **vervalsing van de mededinging**;

- wanneer de kandidaat of inschrijver blijk heeft gegeven van **aanzienlijke of voortdurende tekortkomingen bij de uitvoering van een wezenlijk voorschrift tijdens een eerdere overheidsopdracht** en dit geleid heeft tot het nemen van ambtshalve maatregelen, schadevergoedingen of andere vergelijkbare sancties;

- wanneer de kandidaat of inschrijver zich in ernstige mate schuldig heeft gemaakt aan **valse verklaringen** bij het verstrekken van de informatie die nodig is voor de controle op het ontbreken van

respect des critères de sélection, s'il a retenu des informations ou s'il n'a pas pu fournir les pièces justificatives requises en vertu de l'article 73 de la loi ;

- si le candidat ou soumissionnaire a tenté d'influencer illégalement le processus décisionnel du pouvoir adjudicateur.

uitsluitingsgronden of de naleving van de selectiecriteria, of hij informatie heeft achtergehouden;

- wanneer de kandidaat of inschrijver heeft getracht om het besluitvormingsproces van de aanbestedende overheid onrechtmatig te beïnvloeden

Ces motifs d'exclusion facultative entraînent une exclusion pour une période de trois ans à compter de la date de l'événement en question ou de la fin du manquement, lorsque celui-ci est continu. Toutefois, si le comportement relevant du motif d'exclusion visé à l'article 69, alinéa 1er, 1°, 3°, 4°, 8° ou 9°, de la loi a été sanctionné par une décision d'une autorité administrative ou judiciaire compétente constatant la violation d'une règle de droit, dans le cadre d'une procédure régie par le droit de l'Union ou le droit national, le délai de trois ans est calculé à partir de la date de cette décision[23].

Deze facultatieve uitsluitingsgronden leiden tot uitsluiting voor een periode van drie jaar vanaf de datum van de betrokken gebeurtenis of vanaf de beëindiging van de inbreuk, wanneer het een voortdurende inbreuk betreft. Indien de gedraging die valt onder de in het artikel 69, eerste lid, 1°, 3°, 4°, 8° of 9°, van de wet bedoelde uitsluitingsgrond echter bestraft werd door middel van een besluit van een bevoegde administratieve of gerechtelijke autoriteit houdende vaststelling van een inbreuk op een rechtsregel, in het kader van een door het Unierecht of het nationale recht geregelde procedure wordt, de termijn van drie jaar berekend vanaf de datum van dit besluit.[24]

Attention : pas d'exclusion si le candidat/soumissionnaire peut démontrer, conformément à l'art. 70 de la loi relative aux marchés publics, qu'il a pris des mesures adéquates (correctrices) attestant de sa fiabilité.

Opgelet: geen uitsluiting indien de kandidaat/inschrijver kan aantonen, overeenkomstig art 70. van de wet overheidsopdrachten, toereikende (corrigerende) maatregelen te hebben getroffen die alsnog zijn betrouwbaarheid bevestigen.

Note explicative concernant les mesures correctrices

Toelichting inzake corrigerende maatregelen

Suite à la loi du 18 mai 2022 modifiant la loi du 17 juin 2016 relative aux marchés publics et la loi du 17 juin 2016 relative aux contrats de concession (M.B. 30 mai 2022), plusieurs amendements ont été apportés à la réglementation en matière de « mesures correctrices » en conséquence de l'arrêt de la Cour de Justice du 14 janvier 2021 dans l'affaire C-387/19.

Ingevolge de wet van 18 mei 2022 tot wijziging van de wet van 17 juni 2016 inzake overheidsopdrachten en de wet van 17 juni 2016 betreffende de concessieovereenkomsten (B.S. 30 mei 2022 werden een aantal wijzigingen aangebracht aan de regeling omtrent 'corrigerende maatregelen', als gevolg van het arrest van het Hof van Justitie van 14 januari 2021 in de zaak C-387/19.

Ainsi, il est clarifié que le candidat/soumissionnaire ne doit plus dans tous les cas soumettre les mesures correctrices de sa propre initiative dès le début de la procédure de passation :

Aldus wordt verduidelijkt dat de kandidaat/inschrijver niet meer in alle gevallen op eigen initiatief de corrigerende maatregelen moet voorleggen van bij aanvang van de plaatsingsprocedure:

⇨ Motifs d'exclusion obligatoire : les preuves des mesures correctrices doivent être apportées de la propre initiative du candidat/soumissionnaire. Toutefois, les documents du marché doivent faire référence à cette obligation. Plus précisément, une référence à l'art. 70,

⇨ Verplichte uitsluitingsgronden: de bewijzen inzake corrigerende maatregelen dienen op eigen initiatief van de kandidaat/inschrijver te worden voorgelegd. In de opdrachtdocumenten moet wel verwezen worden naar deze verplichting. Meer bepaald moet een verwijzing

[23] Toutefois, le pouvoir adjudicateur peut prendre une décision d'exclusion avant la décision de l'autorité compétente, pour autant que toutes les conditions soient réunies.

[24] De aanbestedende overheid kan echter een beslissing tot uitsluiting nemen voorafgaand aan de beslissing van de bevoegde autoriteit, voor zover alle voorwaarden daartoe vervuld zijn

§ 2, deuxième alinéa de la loi relative aux marchés publics doit être incluse.

⇨ Motifs d'exclusion facultative : les preuve des mesures correctrices ne doit plus être soumise de la propre initiative du candidat/soumissionnaire. Avant d'exclure un candidat/soumissionnaire, le pouvoir adjudicateur doit en principe encore donner au candidat/soumissionnaire la possibilité de présenter des mesures correctrices.

Le pouvoir adjudicateur peut toutefois déroger à ce mécanisme par le biais d'une disposition à cet effet dans les documents du marché. Cela est cependant soumis à différentes conditions. Pour plus d'explications à ce sujet, veuillez-vous référer à l'art. 70, § 3, de la loi relative aux marchés publics et au commentaire de la disposition correspondante dans l'exposé des motifs (à savoir le commentaire de l'article 5 du projet de loi).

2.4. Points d'attention lors de l'élaboration des spécifications techniques et les conditions d'exécution particulières

Les spécifications techniques et les conditions d'exécutions particulières varient évidemment en fonction de la nature du matériau et de l'usage auquel il est destiné. Souvent, les acheteurs ne disposent pas de l'expertise nécessaire pour évaluer les risques de sécurité liés à une utilisation particulière d'un type de matériau donné.

Souvent, dans la configuration générale des spécifications techniques élaborées, certains problèmes peuvent être évités.

Dans les clauses techniques du marché l'adjudicataire fixe les exigences ayant trait à la sécurité. Celles-ci portent sur les caractéristiques intrinsèques aux fourniture ou aux services à acquérir.

Quant aux caractéristiques intrinsèques des fournitures ou services, il est souvent utile de recourir à des certifications de sécurité officielles. Citons par exemple le **rapport de conformité (SOC)2** sur la protection des données clients et l'efficacité des mesures de contrôle. Cette norme est utile pour tout achat de solution logicielle traitant des données privées, par exemple une suite bureautique disponible dans le *cloud*.

worden opgenomen naar art. 70, §2, tweede lid van de wet overheidsopdrachten.

⇨

⇨ Facultatieve uitsluitingsgronden: de bewijzen inzake corrigerende maatregelen dienen niet meer op eigen initiatief van de kandidaat/inschrijver te worden voorgelegd. Alvorens een kandidaat/inschrijver uit te sluiten, moet de aanbestedende overheid de kandidaat/inschrijver in principe nog de mogelijkheid bieden om corrigerende maatregelen voor te leggen.

De aanbestedende overheid kan echter van dit mechanisme afwijken door middel van een bepaling in die zin in de opdrachtdocumenten. Hiervoor gelden wel verschillende voorwaarden. Voor nadere toelichting hieromtrent wordt verwezen naar art. 70, § 3 van de wet overheidsopdrachten en naar de commentaar bij de overeenkomstige bepaling in de Memorie van Toelichting (namelijk de toelichting bij artikel 5 van het wetsontwerp).

2.4. Aandachtspunten bij het uitwerken van technische specificaties en bijzondere uitvoeringsvoorwaarden

De technische specificaties en bijzondere uitvoeringsvoorwaarden zijn uiteraard verschillend naar gelang de aard van het materiaal en het beoogde gebruik. Vaak ontbreekt het aankopers aan expertise om de veiligheidsrisico's die verbonden zijn aan een bepaald gebruik van een bepaald soort materiaal in te schatten.

Vaak kunnen ingevolge het algemeen opzet bij de uitgewerkte technische specificaties bepaalde problemen voorkomen worden.

In de technische clausules van de opdracht legt de aanbesteder de eisen op het vlak van veiligheid vast. Deze hebben betrekking op de intrinsieke kenmerken van de aan te besteden leveringen of diensten.

Wat de intrinsieke kenmerken van leveringen of diensten betreft, is het vaak nuttig een beroep te doen op officiële veiligheidscertificaten. Een voorbeeld daarvan is het **conformiteitsverslag (SOC)2** over de bescherming van klantengegevens en de doeltreffendheid van de controlemaatregelen. Deze norm is nuttig voor elke aankoop van een softwaretoepassing waarin persoonlijke gegevens verwerkt worden, zoals een kantoorpakket dat beschikbaar is in de *cloud*.

Pour les services, nous pouvons citer les normes internationales très populaires **ISO27001** relative à la sécurité de l'information ou **ISO31000** concernant la gestion des risques. Celles-ci ne peuvent être imposées en tant que spécifications techniques que s'il existe également un lien suffisant avec le produit ou le service.

Il est important de noter que l'adjudicateur pourrait également mobiliser de telles certifications comme critère de sélection[25] du marché plutôt que comme exigence de régularité. Dans le cas où, trop peu de prestataires pourraient justifier disposer de certifications probantes, leur détention pourrait être utilisé dans le cadre des critères d'attribution (e.g. « mesure dans laquelle les garanties de sécurité sont disponibles et efficaces »).

Voici deux sources d'informations essentielles afin de se renseigner sur les normes de sécurité disponibles pour les fournitures ou services :

a) Le Bureau de Normalisation[27] ;

a) Le National Cybersecurity Certification Authority (NCCA)[29] .

Quant aux conditions d'exécution du marché, il est courant de prévoir les mesures suivantes (dont des clauses post-contractuelles[31]) afin de garantir la sécurité de l'information :

a) Exiger une habilitation ou une vérification de sécurité pour l'exécution du marché ;

   Si vous n'êtes pas certain que suffisamment d'opérateurs économiques disposent d'une habilitation de sécurité pour soumissionner à votre marché (critère de sélection), vous pouvez l'exiger pour l'exécution du marché. Soyez néanmoins conscient que la délivrance d'une habilitation de sécurité nécessite 6 à 12 mois. Il s'agit donc

Voor diensten kan verwezen worden naar de internationaal gekende **ISO27001**-normen voor wat de veiligheid van informatie betreft of **ISO31000** voor risicobeheer. Deze kunnen enkel als technische eis worden opgelegd als er ook voldoende verband is met het product of de dienst.

Het zij opgemerkt dat de aanbesteder dergelijke certificeringen niet enkel als regelmatigheidsvereiste, maar ook als selectiecriterium[26] voor de opdracht zou kunnen gebruiken. Indien te weinig dienstverleners kunnen aantonen dat ze over overtuigende certificaten beschikken, zou het bezit ervan als in het kader van de gunningscriteria gebruikt kunnen worden (bv. 'mate waarin veiligheidsgaranties aanwezig en doeltreffend zijn').

Hier zijn twee belangrijke bronnen van informatie over de beschikbare veiligheidsnormen voor leveringen of diensten:

b) het Bureau voor Normalisatie[28];

b) de National Cybersecurity Certification Authority (NCCA)[30].

Wat de uitvoeringsvoorwaarden van de opdracht betreft, is het gebruikelijk de volgende maatregelen te nemen (inclusief postcontractuele clausules[32]) om de veiligheid van de informatie te vrijwaren:

b) een veiligheidsmachtiging of -verificatie eisen voor de uitvoering van het contract:

   Indien u niet zeker bent of voldoende ondernemers over een veiligheidsmachtiging beschikken om op uw opdracht in te schrijven (selectiecriterium), kunt u een machtiging eisen voor de uitvoering van het contract. Houd er rekening mee dat de aflevering van een veiligheidsmachtiging tussen de 6 en de 12 maanden in beslag neemt. De opdracht

[25] Il est important que le pouvoir adjudicateur indique clairement si une certaine exigence doit être considérée comme un critère de sélection, une exigence technique minimale et/ou une condition particulière d'exécution. Si cela n'est pas suffisamment clair, le pouvoir adjudicateur risque qu'un juge décide que seule l'exigence en question doit être satisfaite au moment de l'exécution (conditions particulières d'exécution ; voir l'arrêt 247.455 du Conseil d'État du 28 avril 2022), ce qui, du point de vue de la sécurité, peut s'avérer risqué, selon le cas.

[26] Het is wel van belang dat de aanbestedende overheid duidelijk aangeeft of een bepaalde eis aanzien moet worden als een selectiecriterium, als een minimale technische eis en/of als een bijzondere uitvoeringsvoorwaarde. Als dit niet voldoende duidelijk is riskeert de aanbestedende overheid dat geoordeeld wordt dat alleen aan de betreffende eis voldaan moet zijn op het ogenblik van de uitvoering (bijzondere uitvoeringsvoorwaarden; zie het arrest 247.455 van de Raad van State 28 april 2022), terwijl dit vanuit veiligheidsoogpunt risico's met zich kan zijn, afhankelijk van het geval.

[27] https://www.nbn.be/fr

[28] https://www.nbn.be/nl

[29] https://ccb.belgium.be/fr/service-certification-ccb-certification

[30] https://ccb.belgium.be/nl/dienst-certificering-ccb-certification

[31] Cf. article 13, § 3, de la loi du 17 juin 2016 relative aux marchés publics.

[32] Cf. artikel 13, § 3, van de wet van 17 juni 2016 inzake overheidsopdrachten.

d'attribuer son marché avec suffisamment d'avance par rapport à la période d'exécution. Quand bien même il n'est pas question de disposer d'une habilitation de sécurité, vous pouvez toujours imposer à l'adjudicataire de se soumettre à une vérification de l'Autorité Nationale de Sécurité à quelque moment que ce soit durant l'exécution du marché[33].

moet met andere woorden ruim voor de uitvoeringstermijn gegund worden. Zelfs indien een veiligheidsmachtiging niet nodig is, kunt u de opdrachtnemer steeds opleggen om zich te onderwerpen aan een verificatie door de Nationale Veiligheidsoverheid op gelijk welk moment tijdens de uitvoering van de opdracht[34].

a) dans un contrat de traitement de données dans le cadre du RGPD :

b) een verwerkingsovereenkomst tussen de aanbesteder en de opdrachtnemer in het kader van de GDPR:

Les pouvoirs adjudicateurs européens sont en principe soumis au **Règlement Général sur la Protection des Données (RGPD)**, si leur marché vise le traitement des données à caractère personnel [35]. Il est toujours nécessaire de préciser l'application du Règlement et de prévoir une résiliation unilatérale du marché en cas de non-respect de ce dernier. Les entreprises étrangères (hors de l'Europe) travaillant dans un contexte législatif différent sont souvent légalement obligées de partager leurs données avec les autorités de leur pays d'origine, avec moins de garanties juridiques quant à la protection de la vie privée. Dans certains cas, vous serez peut-être uniquement capables de satisfaire aux exigences du RGPD si vous prenez des mesures additionnelles de protection des données. Ces mesures sont à déterminer au cas par cas, en fonction des catégories des données à caractère personnel traitées et en collaboration avec les opérateurs économiques internationaux.

Europese aanbestedende overheden zijn in beginsel onderworpen aan de **Algemene Verordening Gegevensbescherming (AVG of GDPR)**, indien hun opdracht de verwerking van persoonsgegevens omvat[36]. Het is steeds noodzakelijk om de toepassing van de Verordening te verduidelijken en te voorzien in een eenzijdige beëindiging van de opdracht in geval van niet-naleving ervan. Buitenlandse (niet-Europese) bedrijven die in een andere wetgevingscontext opereren, zijn vaak wettelijk verplicht hun gegevens te delen met de autoriteiten in hun land van herkomst, met minder juridische garanties wat betreft de bescherming van de privacy. In sommige gevallen kunt u alleen aan de vereisten van de GDPR voldoen als u aanvullende gegevensbeschermingsmaatregelen neemt. Deze maatregelen moeten per geval worden vastgesteld, afhankelijk van de categorieën van verwerkte persoonsgegevens en in samenwerking met internationale ondernemers.

Toutefois, il peut également s'agir d'une condition important dans le cadre de la vérification de la régularité et donc distincte des conditions d'exécution.

Dit kan echter ook een voorwaarde vormen die van belang is in het kader van het regelmatigheidsonderzoek en dat dus los staat van de uitvoeringsvoorwaarden.

c) Prévoir la signature d'une déclaration de confidentialité (NDA – *Non Disclosure Agreement*)

d) Voorzien in de ondertekening van een geheimhoudingsverklaring (NDA – *Non Disclosure Agreement*);

c) Imposer l'utilisation de moyens de communication sécurité (e.g. cryptage des données).

d) het gebruik van veilige communicatiemiddelen opleggen (bv. gegevensversleuteling).

Puisqu'il n'est pas toujours aisé d'identifier les risques de sécurité inhérent à l'objet particulier d'un marché, il est parfois utile de recourir à de la consultance externe. Au sein des pouvoirs adjudicateurs fédéraux, une offre de conseil est disponible via les marchés de consultance stratégique

Aangezien het niet altijd makkelijk is om de veiligheidsrisico's die inherent zijn aan het specifieke voorwerp van een opdracht te identificeren, is het soms nuttig om een beroep te doen op extern advies. Binnen de federale aanbestedende overheden dit advies beschikbaar

[33] https://www.nvoans.be/fr

[34] https://www.nvoans.be/nl

[35] En Belgique, une exclusion est prévue pour certaines autorités publiques dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

[36] In België wordt een uitsluiting voorzien voor bepaalde overheden in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

et opérationnel du SPF BOSA, du SPF Justice (spécifique IT) ou de la Smals (spécifique IT). Plus d'informations sont disponibles auprès des organisations mentionnées.

De plus, une analyse d'impact de protection des données effectuée avant l'activité de traitement, vous fournira plus d'informations sur les différents risques et leurs mesures de sécurité.

2.5. Origine des produits et des matériaux

Dans un premier temps, il convient d'attirer l'attention sur le fait que les opérateurs économiques des pays tiers qui n'ont pas signé de convention leur ouvrant les marchés publics de l'Union, ou dont les biens, services et travaux ne sont pas visés par une telle convention, n'ont pas un accès garanti aux marchés publics de l'Union et peuvent en être exclus.

Il ne faut toutefois pas déduire de cette affirmation de manière générale qu'il est possible d'exclure les produits ou les matériaux s'ils proviennent d'un tel pays tiers et par conséquent, qu'il est également possible de considérer leur offre comme irrégulière.

En effet, quand un pouvoir adjudicateur reçoit une offre émanant d'un opérateur économique provenant d'un pays tiers, il doit d'abord vérifier si l'offre s'inscrit dans le cadre des conventions internationales signées par l'Union européenne en la matière et si le soumissionnaire a un accès garanti à son marché.

A noter que les traités internationaux peuvent déterminer l'origine de manière différenciée, ce qui complexifie encore la matière.

Citons l'exemple de l'Accord sur les marchés publics. En son article IV, il précise que ce qui compte c'est la seule origine des fournitures, des services et des travaux. Il ne s'agit dès lors pas ici de la nationalité de l'opérateur économique.

D'autres accords internationaux peuvent trouver à s'appliquer. La présente boîte à outils n'a toutefois pas pour vocation de lister de manière exhaustive les différents accords.

Pour déterminer l'origine des produits finis, vous devez vous référer aux règles du code des douanes de l'Union européenne qui stipule qu'elle est déterminée par le pays dans lequel la dernière transformation substantielle a été réalisée. Pour de plus amples informations sur la notion « de dernière transformation substantielle », il est renvoyé audit code des douanes.

via de contracten voor strategische en operationele consultancy van de FOD BOSA, de FOD Justitie (specifiek voor IT) of van Smals (specifiek voor IT). Meer informatie is verkrijgbaar bij de genoemde organisaties.

Een effectbeoordeling inzake gegevensbescherming die voorafgaand aan de verwerkingsactiviteit wordt uitgevoerd, zal u meer informatie verschaffen over de verschillende risico's en de bijbehorende beveiligingsmaatregelen.

2.5 Oorsprong producten en materialen

Ten eerste moet erop worden gewezen dat ondernemers uit derde landen die geen overeenkomst hebben ondertekend waarbij ze toegang krijgen tot overheidsopdrachten van de Unie, of waarvan de goederen, diensten en werken niet onder een dergelijke overeenkomst vallen, niet beschikken over een gegarandeerde toegang tot overheidsopdrachten van de Unie en daarvan kunnen worden uitgesloten.

Hieruit mag echter niet in het algemeen worden afgeleid dat men producten of materialen kan uitsluiten als zij uit een dergelijk derde land afkomstig zijn en men bijgevolg ook de betreffende offerte als onregelmatig kan beschouwen.

Wanneer een aanbestedende overheid een offerte ontvangt van een ondernemer uit een derde land, moet zij immers eerst nagaan of de offerte kadert binnen internationale overeenkomsten die de Europese Unie ter zake heeft ondertekend, en of de inschrijver over een gegarandeerde toegang tot haar opdracht beschikt.

Opgemerkt wordt dat internationale verdragen de oorsprong op verschillende manieren kunnen bepalen, wat de kwestie nog complexer maakt.

Zo bepaalt artikel IV van de Overeenkomst inzake overheidsopdrachten dat alleen de oorsprong van de leveringen, diensten en werken telt. Het gaat hier dus niet om de nationaliteit van de ondernemer.

Andere internationale overeenkomsten kunnen van toepassing zijn. Het is echter niet de bedoeling van deze toolbox om een volledige lijst van de verschillende overeenkomsten te geven.

Om de oorsprong van eindproducten te bepalen, dient u de regels van het douanewetboek van de Europese Unie te raadplegen. Volgens dit wetboek wordt de oorsprong bepaald door het land waar de laatste ingrijpende verwerking heeft plaatsgevonden. Voor meer informatie over het begrip "laatste ingrijpende verwerking" wordt verwezen naar voornoemd douanewetboek.

A noter que la nationalité d'un opérateur économique qui importerait des produits ne détermine pas l'origine de ces produits. Les produits qui seraient par ailleurs importés par une filiale basée sur le territoire de l'Union européenne ne seront pas d'origine européen du fait que la filiale est basée sur le territoire de l'Union.

Opgemerkt wordt dat de nationaliteit van een ondernemer die producten invoert, niet bepalend is voor de oorsprong van deze producten. Producten die worden ingevoerd door een dochteronderneming die op het grondgebied van de Europese Unie gevestigd is, zijn overigens niet van Europese oorsprong door het feit dat de dochteronderneming op het grondgebied van de Europese Unie is gevestigd.

Les règles susmentionnées ne sont pas sans conséquence.

En effet, un opérateur économique issu de l'Union européenne ou de l'Espace économique européen ne pourrait pas être exclu lorsqu'il propose des travaux, des fournitures ou des services originaires d'un pays tiers à l'Union européenne ou à l'Espace économique européen. En d'autres termes, le mécanisme d'exclusion applicable sur la base de l'origine des produits et des matériaux n'est pas applicable aux opérateurs économiques issus de l'Union européenne ou de l'Espace économique européen. Dans un tel cas, un pouvoir adjudicateur pourrait toutefois, à des fins de protection des intérêts essentiels de sécurité, déroger aux règles de passation normalement applicables et invoquer l'article 33 précité, si les conditions d'application sont remplies.

En outre, un opérateur économique non issu de l'Union européenne ou de l'Espace économique européen pourrait très bien remettre une offre régulière lorsqu'il propose des travaux, des fournitures ou des services originaires d'un pays de l'Union européenne ou de l'Espace économique européen si ces travaux, ces fournitures ou ces services sont couverts par un traité international et ce, même si le pays dont provient l'opérateur économique n'a pas signé ledit traité.

Bovenstaande regels zijn niet zonder gevolgen.

Een ondernemer uit de Europese Unie of de Europese Economische Ruimte kan namelijk niet worden uitgesloten wanneer hij werken, leveringen of diensten aanbiedt die afkomstig zijn uit een land buiten de Europese Unie of de Europese Economische Ruimte. Het uitsluitingsmechanisme dat van toepassing is op basis van de oorsprong van producten en materialen is met andere woorden niet van toepassing op ondernemers uit de Europese Unie of de Europese Economische Ruimte. In een dergelijk geval kan een aanbestedende overheid voor de bescherming van essentiële veiligheidsbelangen echter afwijken van de plaatsingsregels die normaal van toepassing zijn, en voornoemd artikel 33 inroepen, als aan de toepassingsvoorwaarden daarvoor voldaan is.

Bovendien is het heel goed mogelijk dat een ondernemer van buiten de Europese Unie of van buiten de Europese Economische Ruimte een regelmatige offerte indient wanneer hij werken, leveringen of diensten aanbiedt die afkomstig zijn uit een land van de Europese Unie of de Europese Economische Ruimte, indien deze werken, leveringen of diensten onder een internationaal verdrag vallen, zelfs als het land waaruit de ondernemer afkomstig is, dit verdrag niet heeft ondertekend.

Notons que les adjudicateurs ne peuvent solliciter des informations sur l'origine des composants des fournitures ou sur l'origine des fournitures intégrées dans le cadre d'un marché de services ou d'un marché de travaux. Seule l'origine globale des travaux, des fournitures ou des services compte.

Er zij op gewezen dat aanbesteders geen informatie mogen vragen over de oorsprong van de componenten van leveringen of over de oorsprong van leveringen die in het kader van een opdracht voor diensten of werken geïntegreerd worden. Alleen de globale oorsprong van de werken, leveringen of diensten telt.

L'origine des produits et des matériaux est reprise à l'article 78, alinéa 1er, 5°, de l'arrêté du 18 avril 2017 relatif à la passation des marchés publics dans les secteurs classiques. Cet article doit dès lors être interprété en fonction de ce qui précède.

De oorsprong van producten en materialen komt aan bod in artikel 78, eerste lid, 5°, van het koninklijk besluit plaatsing overheidsopdrachten in de klassieke sectoren van 18 april 2017. Dit artikel moet dus worden geïnterpreteerd in het licht van wat voorafgaat.

Art 78, alinéa 1er, 5° A.R. relatif à la passation des marchés publics dans les secteurs classiques *[…] L'offre indique, pour autant que les documents du marché aient fixé des exigences à ce propos, l'origine des produits à fournir et des matériaux à utiliser originaires de pays tiers à l'Union européenne, avec indication par pays d'origine de la valeur, droits de douane non compris, pour laquelle ces produits ou matériaux interviennent dans l'offre. Si ces produits ou ces matériaux sont à parachever ou à mettre en œuvre sur le territoire de l'Union européenne, seule la valeur des matières premières est indiquée. […]*

Art 78, eerste lid, 5° KB plaatsing klassieke sectoren *[…] De offerte vermeldt, voor zover de opdrachtdocumenten zulks opleggen, de oorsprong van de te leveren producten en de te verwerken materialen die afkomstig zijn van buiten de Europese Unie, met vermelding per land van oorsprong van de waarde exclusief douanerechten die zij in de offerte vertegenwoordigen. Als de producten of materialen op het grondgebied van de Europese Unie worden afgewerkt of verwerkt, wordt enkel de waarde van deze grondstoffen vermeld. […]*

2.6. Points d'attention lors de l'examen des prix anormaux

Les pouvoirs adjudicateurs sont tenus de vérifier l'absence de prix anormalement bas lors de l'examen des offres. Certains pays subventionnent les entreprises afin que celles-ci puissent intégrer les marchés étrangers. Grâce à ces subventions, ces entreprises sont parfois en mesure de proposer des prix très bas. Un prix anormalement bas peut constituer un motif de rejet d'une offre.

Cependant, il est toujours nécessaire de soumettre cette information au soumissionnaire afin de lui permettre d'y réagir. Si le pouvoir adjudicateur constate qu'une offre paraît anormalement basse du fait de l'obtention d'une aide d'État par le soumissionnaire, il ne peut rejeter cette offre pour ce seul motif que s'il consulte le soumissionnaire et que celui-ci n'est pas en mesure de démontrer, dans un délai suffisant fixé par le pouvoir adjudicateur, que l'aide en question était compatible avec le marché intérieur[37].

Pour plus d'explications concernant l'examen des prix anormaux, veuillez-vous référer au guide « Lutte contre le dumping social dans les marchés publics et les concessions ».

2.6. Aandachtspunten bij het onderzoek naar abnormale prijzen

Aanbestedende overheden moeten in het onderzoek van de offertes een controle doen op abnormaal lage prijzen. Sommige landen subsidiëren bedrijven om op buitenlandse markten actief te worden. Door deze subsidies zijn die bedrijven soms in staat om zeer lage prijzen te bieden. Een abnormaal lage prijs kan een reden zijn om een offerte af te wijzen.

Men moet altijd de inschrijver echter toelaten zijn lage prijs te verklaren. Wanneer een aanbestedende overheid vaststelt dat een offerte abnormaal laag lijkt ten gevolge van door de inschrijver verkregen overheidssteun, kan de offerte alleen op die grond worden afgewezen na overleg met de inschrijver en wanneer deze niet binnen een door de aanbestedende overheid gestelde toereikende termijn kan aantonen dat de betrokken steun verenigbaar is met de interne markt[38].

Voor meer uitleg omtrent het abnormaal prijzenonderzoek wordt verwezen naar de gids "Strijd tegen sociale dumping in het kader van overheidsopdrachten en concessieovereenkomsten".

2.7. Critères d'attribution appropriés - Frais de sécurité en tant que coût

Un pouvoir adjudicateur doit choisir l'offre économiquement la plus avantageuse. L'offre économiquement la plus avantageuse peut être déterminée sur la base du prix, sur la base des coûts, selon une approche fondée sur le rapport coût/efficacité, telle que le coût du cycle de vie, ou en se fondant sur le meilleur rapport qualité/prix évalué sur la base du prix ou du coût ainsi que des critères comprenant des aspects qualitatifs, environnementaux et/ou sociaux[39].

Appliquer des critères d'attribution et/ou fournir des aspects qualitatifs par le biais de critères d'(de sous-)attribution, par exemple en matière de planification, de

2.7 Gepaste gunningscriteria - Beveiligingskosten als kost

Een aanbestedende overheid moet de economisch meest voordelige offerte selecteren. Welke de economisch meest voordelige offerte is kan worden vastgesteld op basis van de prijs, op basis van de kosten, rekening houdend met de kosteneffectiviteit, zoals de levenscycluskosten, of rekening houdend met de beste prijs-kwaliteitsverhouding die bepaald wordt op basis van de prijs of de kosten alsook criteria waaronder kwalitatieve, milieu- en/of sociale aspecten[40].

Het toepassen van gunningscriteria en/of voorzien van kwaliteitsaspecten via (sub)gunningscriteria bv. inzake planning, Plan van Aanpak (PvA), milieukenmerken, hinder,

[37] A.R. Passation art. 36, § 3.
[38] KB Plaatsing art 36, §3.
[39] Loi du 17 juin 2016 relative aux marchés publics, art. 81
[40] Wet van 17 juni 2016 inzake overheidsopdrachten 2016, Art. 81

plan d'approche (PA), de caractéristiques environnementales, de nuisances, de coût du cycle de vie (LCC), de garantie, de rentabilité, de service, de durabilité, de facteurs sociaux, de caractéristiques fonctionnelles, d'accessibilité, de présentation, de caractéristiques esthétiques, de conditions de livraison, etc. pour déterminer l'offre économiquement la plus avantageuse. Un calcul basé sur les coûts permet de prendre en compte les coûts du cycle de vie, tels que les coûts de sécurité. L'utilisation de certains équipements peut entraîner des coûts de sécurité plus élevés, tels que le remplacement des logiciels, la vérification des mises à jour automatiques, etc.

Le recours à une telle mesure permettra certes d'attribuer moins de points en termes de qualité, mais ne pourra toutefois pas exclure complètement la possibilité qu'un opérateur économique présentant certains risques en matière de sécurité puisse tout de même remporter le marché.

2.8. Non Disclosure Agreement (NDA) et autres éléments relatifs à la confidentialité (conditions d'exécution)

Il convient d'abord de distinguer les informations confidentielles au sens de l'article 13, § 3, de la loi relative aux marchés publics du 17 juin 2016 des informations classifiées au sens de l'article 3, 19°, de la loi défense et sécurité du 13 août 2011. Ce dernier concept est beaucoup plus restrictif. Si le marché implique des informations classifiées à des fins de sécurité ou nécessite et/ou contient des informations classifiées, la loi « défense et sécurité » doit être appliquée, comme cela a déjà été indiqué au chapitre 1. Dans ce qui suit, nous supposerons que la condition susmentionnée n'est pas remplie.

Il est possible (et dans certains cas indispensables) de prévoir une **Non Disclosure Agreement** (Déclaration de confidentialité) spécifique au marché. En effet, l'article 13, § 3, de la loi du 17 juin 2016 prévoit que le pouvoir adjudicateur peut imposer à un opérateur économique des exigences visant à protéger la confidentialité des informations qu'il met à disposition. Cela peut être considéré comme une « condition spéciale relative à l'exécution » du marché[41]. Toutefois, l'avis de marché doit déjà préciser les mesures requises pour protéger la confidentialité des informations.

Exemple de clause :

Life Cycle Cost (LCC), garantie, rentabiliteit, service, duurzaamheid, sociale factoren, functionele kenmerken, toegankelijkheid, presentatie, esthetische kenmerken, leveringsvoorwaarden enz. voor het bepalen van de economisch meest voordelige offerte. Een berekening op basis van de kosten laat toe om levencycluskosten, zoals beveiligingskosten, mee in rekening te brengen. Werken met bepaald materiaal kan hogere beveiligingskosten met zich meebrengen, zoals bijvoorbeeld software vervangen, automatische updates controleren etc.

Echter, het gebruik van een dergelijke maatregel zal toelaten op kwalitatief vlak minder punten toe te kennen, maar kan niet geheel uitsluiten dat alsnog een economische operator t.a.v. wie bepaalde veiligheidsrisico's bestaan, finaal de opdracht binnenhaalt.

2.8. Non Disclosure Agreement (NDA) en andere elementen die betrekking hebben op vertrouwelijkheid (uitvoeringsvoorwaarden)

Het onderscheid moet vooreerst gemaakt worden tussen confidentiële informatie in de zin van artikel 13, § 3, van de wet van 17 juni 2016 inzake overheidsopdrachten en geclassificeerde informatie in de zin van artikel 3, 19°, van de wet defensie en veiligheid van 13 augustus 2011. Dit laatste begrip is veel beperkter. Indien de opdracht betrekking heeft op geclassificeerde informatie voor veiligheidsdoeleinden of geclassificeerde informatie noodzakelijk maakt en/of bevat moet, zoals reeds aangegeven in hoofdstuk 1, toepassing gemaakt worden van de wet "defensie en veiligheid". In wat volgt gaan we ervan uit dat niet aan de voormelde voorwaarde voldaan is.

Het is mogelijk (en in sommige gevallen noodzakelijk) om een specifieke **Non Disclosure Agreement** (geheimhoudingsverklaring) te voorzien voor de opdracht. In artikel 13, § 3, van de wet van 17 juni 2016 is immers bepaald dat de aanbesteder aan een ondernemer eisen mag stellen die tot doel hebben de vertrouwelijke aard van de informatie die hij beschikbaar stelt, te beschermen. Dit kan aanzien worden als een 'bijzondere uitvoeringsvoorwaarde' van de opdracht[42]. In de aankondiging van de opdracht moet wel reeds vermeld worden welke maatregelen ter bescherming van het vertrouwelijke karakter van de informatie vereist worden.

Voorbeeldclausule:

[41] voir article 87 de la loi sur les marchés publics du 17 juin 2016

[42] zie artikel 87 van de wet van 17 juni 2016 inzake overheidsopdrachten

« *Le prestataire de services et ses collaborateurs sont liés par un devoir de confidentialité stricte à l'égard des informations dont ils ont connaissance lors de l'exécution du marché. Ces informations ne peuvent en aucun cas être communiquées à des tiers sans l'autorisation écrite du pouvoir adjudicateur. De plus, la relation contractuelle entre le service …[à remplir] et l'adjudicataire du marché ne pourra faire l'objet d'aucune publicité sans que celle-ci ait été préalablement avalisée par le pouvoir adjudicateur.*

Afin de consentir à son devoir de réserve, l'adjudicataire sera tenu d'approuver la déclaration de confidentialité (NDA) présentée en annexe suite à la conclusion du marché.

Le non-respect des engagements présentés dans la déclaration de confidentialité peut entrainer la résiliation unilatérale du marché sans préavis et des poursuites judiciaires conformément au droit belge. »

"*De dienstverlener en zijn medewerkers zijn gehouden tot strikte geheimhouding van de informatie waarvan zij tijdens de uitvoering van de opdracht kennis nemen. Deze informatie mag in geen enkel geval aan derden worden verstrekt zonder de schriftelijke toestemming van de aanbestedende overheid. Voorts mogen de contractuele betrekkingen tussen de dienst ... [vul in] en de opdrachtnemer niet worden bekendgemaakt zonder voorafgaande goedkeuring van de aanbestedende overheid.*

Om te voldoen aan zijn geheimhoudingsplicht zal de opdrachtnemer na de sluiting van de opdracht de bijgevoegde geheimhoudingsverklaring (NDA) moeten goedkeuren.

Niet-naleving van de verbintenissen in de geheimhoudingsverklaring kan leiden tot de eenzijdige beëindiging van de opdracht zonder voorafgaande kennisgeving en tot gerechtelijke stappen overeenkomstig het Belgische recht."

Si, en tant que pouvoir adjudicateur (dans le cadre de l'exécution), vous imposez aux adjudicataires des exigences particulières visant à protéger le caractère confidentiel des informations que vous mettrez à disposition[43], alors, par nature, certaines informations ne peuvent être rendues librement accessibles via la plateforme électronique où les documents du marché sont mis à la disposition de tous. À cet égard, la loi du 17 juin 2016 prévoit une exception à l'accès obligatoire aux documents du marché via un site Internet (voir article 64, § 1er, alinéa 4, de la loi du 17 juin 2016). Cet aspect doit cependant être mentionné dans l'avis de marché. L'avis de marché doit également préciser la manière dont l'accès aux documents concernés peut être obtenu, ainsi que la phase à partir de laquelle cet accès sera possible. Dans des cas très exceptionnels, il ne sera pas possible de ne pas fournir un accès par voie électronique (même par e-mail).

Wanneer u als aanbesteder (in het kader van de uitvoering) bijzondere eisen oplegt aan opdrachtnemers die tot doel hebben de vertrouwelijke aard van de informatie die u zal beschikbaar stellen, te beschermen[44], dan kan sommige informatie uit de aard der zaak niet vrij toegankelijk gemaakt worden via het elektronische platform waar de opdrachtdocumenten voor iedereen worden ter beschikking gesteld. Hieromtrent is in de wet van 17 juni 2016 in een uitzondering voorzien op de verplichte bekendmaking van de opdrachtdocumenten via een website (zie artikel 64, § 1, vierde lid, van de wet van 17 juni 2016). Dit aspect moet wel vermeld worden in de aankondiging van de opdracht. Daarbij moet eveneens worden vermeld hoe (en in welke fase) toegang verkregen kan worden tot de betrokken documenten. In zeer uitzonderlijke gevallen zal het niet mogelijk zijn om niet via elektronische wijze toegang te verstrekken (zelfs niet per e-mail).

En effet, il est rappelé qu'en tant que pouvoir adjudicateur, vous n'êtes pas tenu d'utiliser des moyens de communication électroniques, dans la mesure où l'utilisation de moyens de communication autres que les moyens électroniques (notamment la communication papier) est nécessaire en raison du caractère particulièrement sensible des informations qui exigent un degré de protection extrêmement élevé ne pouvant pas

Als aanbesteder bent u niet verplicht om elektronische communicatiemiddelen aan te wenden, voor zover het gebruik van andere dan elektronische communicatiemiddelen (met name papieren communicatie) nodig is voor de bescherming van de bijzonder gevoelige aard van de informatie waarvoor een dermate hoog beschermingsniveau nodig is dat dit niveau niet afdoende kan worden verzekerd via elektronische middelen.[46]

[43] en application de l'article 13, § 3, précité de la loi du 17 juin 2016

[44] in toepassing van het voormelde artikel 13, § 3, van de wet van 17 juni 2016

[46] zie artikel 14, § 3, van de wet van 17 juni 2016

être assuré convenablement par l'utilisation d'outils et de dispositifs électroniques.[45]

Le gouvernement fédéral a publié un guide en matière de sécurité de l'information des informations non-classifiées. [47]

2.9. Contrôler l'adjudicataire du marché (clauses d'exécution)

Une fois le marché attribué, il est également nécessaire de contrôler l'adjudicataire pour se prémunir des risques. Un pouvoir adjudicateur peut imposer des exigences pour l'exécution du marché. Le pouvoir adjudicateur peut par exemple exiger de l'adjudicataire qu'il autorise certains contrôles sur ses moyens de fonctionnement, qu'il n'utilise pas certains moyens,...

L'imposition d'une habilitation de sécurité au niveau de l'entreprise peut également faire partie des conditions d'exécution. Toutefois, cet aspect devra être justifié et sera abordé plus en détail aux points 3.2 et 3.3.

Les conditions d'exécution sont imposées sans autre précision dans les documents du marché et l'offre qui entre en contradiction avec celles-ci peut être déclarée irrégulière, ou bien l'adjudicataire qui s'en écarte peut se voir sanctionner, éventuellement par la résiliation du marché sans indemnité pour l'adjudicataire, s'il s'agit d'une violation grave.

Les pouvoirs adjudicateurs européens sont en principe soumis au **Règlement Général sur la Protection des Données** (RGPD), si leur marché vise le traitement des données à caractère personnel [49]. Il est toujours nécessaire de préciser l'application du Règlement et de prévoir une résiliation unilatérale du marché en cas de non-respect de ce dernier. Les entreprises étrangères travaillant dans un contexte législatif différent sont souvent légalement obligées de partager leurs données avec les autorités de leur pays d'origine, avec moins de garanties juridiques quant à la protection de la vie privée. Il ressort de la jurisprudence du Conseil d'État qu'un pouvoir adjudicateur ne peut pas déduire que dès qu'il y a un transfert de données à caractère personnel vers une entité située, par exemple, aux États-Unis, elle ne peut pas fournir de garanties pour assurer un niveau de protection des

De federale overheid heeft richtlijnen voor informatiebeveiliging van niet-geclassificeerde informatie. [48]

2.9. De opdrachtnemer controleren (uitvoeringsclausules):

Zodra de opdracht is gegund, is het ook noodzakelijk toezicht te houden op de opdrachtnemer om zich tegen risico's te beschermen. Een aanbestedende overheid kan eisen opleggen voor de uitvoering van de opdracht. Zo kan de aanbestedende overheid bijvoorbeeld eisen dat de opdrachtnemer bepaalde controles van zijn werkmiddelen toelaat, bepaalde middelen niet gebruikt, …

Ook het opleggen van een veiligheidsmachtiging op firmaniveau kan tot de uitvoeringsvoorwaarden behoren. Dit aspect zal echter gemotiveerd moeten worden en wordt verder behandeld onder punt 3.2 en 3.3.

Uitvoeringsvoorwaarden worden zonder meer in de opdrachtdocumenten opgelegd en de offerte die ze tegenspreekt kan onregelmatig verklaard worden of de opdrachtnemer die ervan afwijkt kan bestraft worden, eventueel met verbreking van de opdracht zonder compensatie van de opdrachtnemer, als het een ernstige overtreding betreft.

Europese aanbestedende overheden zijn in beginsel onderworpen aan de **Algemene Verordening Gegevensbescherming (AVG of GDPR)**, indien hun opdracht de verwerking van persoonsgegevens omvat[50]. Het is steeds noodzakelijk om de toepassing van de Verordening te verduidelijken en te voorzien in een eenzijdige beëindiging van de opdracht in geval van de niet-naleving ervan. Buitenlandse bedrijven die in een andere wetgevingscontext opereren, zijn vaak wettelijk verplicht hun gegevens te delen met de autoriteiten in hun land van herkomst, met minder juridische garanties wat betreft de bescherming van de privacy. Uit rechtspraak van de Raad van State blijkt dat een aanbestedende overheid niet kan afleiden dat van zodra er een doorgifte van persoonsgegevens is naar een entiteit in bijvoorbeeld de VS, deze geen waarborgen kan toereiken om een

[45] voir article 14, § 3, de la loi du 17 juin 2016

[47] Vous trouverez plus d'informations sur : https://bosa.belgium.be/fr/themes/administration-numerique/strategie-et-politique-du-numerique/politique-federale-sur-la

[48] U vindt informatie hierover op: https://bosa.belgium.be/nl/themas/digitale-overheid/digitale-strategie-en-beleid/federaal-beleid-voor-informatiebeveiliging

[49] En Belgique, une exclusion est prévue pour certaines autorités publiques dans la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

[50] In België wordt een uitsluiting voorzien voor bepaalde overheden in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

données équivalent à celui existant au sein de l'Union. Cela montre que des mesures sont possibles pour remédier au niveau insuffisant de protection des données, comme le cryptage avec gestion des clés au niveau du pouvoir adjudicateur ou la pseudonymisation (à déterminer bien sûr au cas par cas).

Au-delà du RGPD, il est également possible d'imposer le respect d'une norme internationale de sécurité pour l'exécution du marché telle que la **norme ISO27001** relative au *management de la sécurité de l'information*[51]. Il pourrait être utile de demander aux soumissionnaires disposant d'un certificat ISO27001 une copie de leur "Statement of Applicability (SoA)". Ce document fait partie d'une procédure d'audit ISO et décrit en détail les points sur lesquels le soumissionnaire a été évalué par l'organisation ISO et quels points ont été ignorés.

2.10. RGPD – accord (en matière de traitement)

Le règlement général sur la protection des données (RGPD, règlement 2016/679[53]) impose à tout adjudicateur traitant des données personnelles de prendre les mesures techniques et organisationnelles appropriées afin de sécuriser ces données. Les prestataires de services (et leurs sous-traitants) traitant des données pour le compte de l'adjudicateur doivent également prendre les mesures de sécurité appropriées. Par exemple, les données doivent être protégées contre la perte, la destruction, l'altération ou l'accès et la diffusion non autorisés. Dans ce cas, l'adjudicateur et le prestataire de services concluent un accord (en matière de traitement) qui décrit ces mesures. Les dispositions de l'accord en matière de traitement peuvent être intégrées dans un cahier des charges ou documentées dans un texte séparé.

En particulier, de nombreuses applications « intelligentes » traitent parfois d'importantes quantités de données permettant d'identifier des personnes. Exemples : logiciels permettant de croiser et d'interroger les données des bases de données, caméras avec reconnaissance faciale ou scanners corporels.

Lors de l'achat de logiciels ou appareils de ce type, il est important d'examiner le pays dans lequel le fournisseur ou

gelijkwaardig niveau van gegevensbescherming als binnen de Unie te garanderen. Hieruit blijkt dat er maatregelen mogelijk zijn om het ontoereikende niveau van gegevensbescherming te verhelpen, zoals encryptie met sleutelbeheer bij de aanbestedende overheid of pseudonimisering (dit is uiteraard case-by-case te bepalen).

Naast de GDPR is het ook mogelijk de naleving van een internationale veiligheidsnorm voor de uitvoering van de opdracht op te leggen, zoals de **ISO27001-norm** voor informatiebeveiligingsbeheer[52]. U vraagt aan de inschrijvers met een ISO27001-certificaat best ook een kopie van hun « Statement of Applicability (SoA)» Dit document hoort bij een ISO-auditprocedure en beschrijft in detail op welke punten de inschrijver door de ISO-organisatie werd beoordeeld en welke punten buiten beschouwing bleven.

2.10. GDPR – (verwerkers)overeenkomst

De algemene verordening gegevensbescherming (AVG, verordening 2016/679[54]) verplicht elke aanbesteder die persoonsgegevens verwerkt om passende technische en organisatorische maatregelen te nemen om die gegevens te beveiligen. Ook dienstverleners (en hun onderaannemers) die gegevens verwerken in opdracht van de aanbesteder, moeten passende beveiligingsmaatregelen nemen. De gegevens moeten bijvoorbeeld worden beschermd tegen verlies, vernietiging, wijziging of ongeautoriseerde toegang en verspreiding ervan. In dergelijke dossiers sluiten de aanbesteder en de dienstverlener een (verwerkers)overeenkomst, waarin de maatregelen staan beschreven. De bepalingen van de verwerkersovereenkomst kunnen in het lastenboek worden ingepast of in een aparte tekst worden gedocumenteerd.

Met name veel 'smart'-toepassingen verwerken soms grote hoeveelheden gegevens waarmee mensen kunnen worden geïdentificeerd. Voorbeelden: software om databankgegevens te kruisen en te bevragen, camera's met gezichtsherkenning of personenscanners.

Bij de aanschaf van dergelijke softwaretoepassingen of toestellen is het belangrijk om na te gaan in welk land de

[51] https://www.iso.org/fr/isoiec-27001-information-security.html
[52] https://www.iso.org/isoiec-27001-information-security.html
[53] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE *G*
[54] *VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.*

le fabricant candidat est basé. En effet, les entreprises étrangères (y compris celles qui opèrent dans des États sous régime autoritaire) sont souvent tenues par la loi de rendre leurs données personnelles accessibles à leurs gouvernements d'origine. Les entreprises soumises à un tel régime juridique seront, selon toute vraisemblance, incapables de se conformer aux exigences du RGPD. Ainsi, si un cahier des charges devait imposer aux candidats de se conformer au RGPD, il pourrait être difficile à faire respecter dans la pratique.

Dans quel cas peut-on inclure une spécification technique concernant la protection des données ?Lorsque les données à caractère personnel sont traitées dans le cadre du marché par l'adjudicateur ou en son nom par une autre partie.

Chapitre 3 - Outils pour lesquels une dérogation est invoquée, nécessitant une motivation spéciale en relation avec les intérêts essentiels de sécurité

3.1. Lignes directrices lors de la demande de dérogation concernant les intérêts essentiels de sécurité

L'article 33 de la loi relative aux marchés publics du 17 juin 2016 dispose que cette loi ne s'applique pas, entre autres, aux marchés publics dont l'exécution doit s'accompagner de mesures particulières de sécurité conformément aux dispositions en vigueur dans l'État membre concerné ou dans la mesure où la protection des intérêts essentiels concernés ne peut être garantie par des mesures moins intrusives Les exceptions susmentionnées doivent toutefois être interprétées de manière restrictive. Selon la jurisprudence constante de la Cour de Justice, c'est toujours le cas concernant les exceptions aux libertés fondamentales. [55] Cette exception, ou mieux, cette possibilité de dérogation, peut également être pertinente pour certains marchés dans les secteurs classiques et spéciaux.

Comme l'a rappelé la Cour de justice dans son arrêt C-337/05 du 8 avril 2008 dans une affaire d'attribution directe à une entreprise d'hélicoptères dits « dual-use » destinés à différents services publics, et dans laquelle l'État membre concerné avait invoqué l'application des exceptions précitées, les mesures prises par les États membres dans le cadre de leurs impératifs d'intérêt national ne peuvent être totalement soustraites à l'application du droit communautaire au seul motif qu'elles servent la sécurité publique. Le traité sur le fonctionnement de l'Union européenne prévoit plusieurs dérogations pour les situations dans lesquelles la sécurité

kandidaat-leverancier of -fabrikant gevestigd is. Buitenlandse bedrijven (inclusief zij die werken in staten met een autoritair regime) zijn immers vaak wettelijk verplicht om hun persoonsgegevens toegankelijk te maken voor de overheden van hun thuisland. Bedrijven onder een dergelijk wettelijk regime zullen naar alle waarschijnlijkheid niet kunnen voldoen aan de GDPR-vereisten. Dus als een lastenboek aan kandidaten zou opleggen dat ze aan de GDPR moeten voldoen, is dit wellicht moeilijk af te dwingen in de praktijk.

In welk geval kan een technische specificatie rond gegevensbescherming worden opgenomen? Wanneer er in de opdracht persoonsgegevens worden verwerkt door de aanbesteder of in zijn opdracht door een andere partij.

Hoofdstuk 3 - Tools waarvoor een afwijking wordt ingeroepen, waarbij een bijzondere motivering in verband met essentiële veiligheidsbelangen vereist is

3.1. Krachtlijnen bij het inroepen van een afwijking omtrent essentiële veiligheidsbelangen

In artikel 33 van de wet van 17 juni 2016 inzake overheidsopdrachten is vermeld dat deze wet niet van toepassing is op, onder meer, overheidsopdrachten waarvan de uitvoering overeenkomstig de in de betrokken lidstaat geldende bepalingen met bijzondere veiligheidsmaatregelen gepaard moet gaan of voor zover de bescherming van de essentiële veiligheidsbelangen van een lidstaat niet kan worden gewaarborgd door minder ingrijpende maatregelen. De voormelde uitzonderingen moeten echter restrictief worden uitgelegd. Volgens vaste rechtspraak van het Hof van Justitie is dit altijd zo voor uitzonderingen op de fundamentele vrijheden.[56] Deze uitzondering, of beter, mogelijkheid tot afwijking, kan ook relevant zijn voor bepaalde opdrachten in de klassieke en speciale sectoren.

Het Hof van Justitie heeft er bijvoorbeeld op gewezen in het arrest C-337/05 van 8 april 2008, omtrent een geval waarbij werd overgaan tot rechtstreekse gunning van zogenaamde 'dual-use'-helikopters voor diverse overheidsdiensten aan een onderneming, en waarbij de betreffende lidstaat de toepassing had ingeroepen van de voormelde uitzonderingen, dat de maatregelen die lidstaten treffen in het kader van hun vereisten van nationaal belang, niet volledig aan de toepassing van het gemeenschapsrecht kunnen onttrokken worden om de enkele reden dat zij de openbare veiligheid dienen. In het Verdrag over werking van de Europese Unie zijn diverse afwijkingen voorzien

[55] voir l'arrêt C-187/16, considérant 76 et références

[56] Zie het arrest C-187/16, overweging 76 en verwijzingen aldaar.

publique peut être impactée. Il s'agit toutefois de cas exceptionnels précisément définis, dont il ne faut **pas déduire une réserve générale pour toute mesure prise par un État membre au titre de la sécurité publique.**

Cela ressort également de l'arrêt C-187/16 du 20 mars 2018. Il s'agit d'un cas où un État membre avait procédé à l'attribution directe de certains marchés d'impression sensibles à une ancienne entreprise d'État. Dans cet arrêt, la Cour de Justice a procédé à un contrôle de proportionnalité, indiquant que les États membres souhaitant se prévaloir des exceptions en question doivent **démontrer que la nécessité de protéger les intérêts essentiels de sécurité n'aurait pu être satisfaite dans le cadre d'une procédure concurrentielle**.[57] Enfin, la Cour de Justice a conclu que le marché public en question (en l'espèce un marché d'impression de documents sensibles) a été attribué directement de manière erronée, car l'entreprise a été retenue à tort comme étant la seule entreprise fiable en la matière. Selon la Cour de Justice, aucune indication n'a été donnée quant aux raisons pour lesquelles il aurait été impossible d'attribuer le marché en question à un seul opérateur économique sur une longue période, mais par le biais d'une procédure avec mise en concurrence préalable.

Il faut donc garder à l'esprit que, si l'on demande une dérogation aux règles de passation normalement applicables en vertu de l'article 33 précité, à des fins de protection des intérêts essentiels de sécurité, il faut également être en mesure de présenter la preuve, si nécessaire, que la dérogation en question ne dépasse pas les limites du cas d'espèce. En d'autres termes, le fait de demander l'exception mentionnée à l'article 33 ne constitue pas une autorisation d'ignorer toutes les règles de passation et de procéder à une attribution directe, même si un risque se présente au regard de certains intérêts essentiels de sécurité. En effet, la disposition doit être interprétée de manière restrictive et appliquée de manière proportionnée, de sorte que l'attribution directe ne sera possible que si vous pouvez démontrer que le besoin concret qui se présente de protéger un intérêt essentiel de sécurité n'aurait pas être satisfait par une procédure avec mise en concurrence préalable.

Il ne faut donc pas invoquer avec trop de légèreté la possibilité de dérogation, notamment dans le cadre d'une attribution directe d'un marché. Il existe souvent des mesures alternatives qui constituent également une dérogation aux règles de passation normalement

voor situaties waarin de openbare veiligheid op het spel kan staan. Het betreft echter nauwkeurig omschreven uitzonderingsgevallen, waaruit **geen algemeen voorbehoud voor elke maatregel die een lidstaat neemt uit hoofde van de openbare veiligheid mag worden afgeleid**.

Dit blijkt ook uit het arrest C-187/16 van 20 maart 2018. Het betreft een geval waarbij een lidstaat was overgegaan tot rechtstreekse gunning van bepaalde gevoelige drukopdrachten aan een voormalige staatsonderneming. In dat arrest voerde het Hof van Justitie een proportionaliteitsonderzoek uit en gaf daarbij aan dat lidstaten die zich op de betreffende uitzonderingen willen beroepen, moeten **aantonen dat de behoefte aan de bescherming van de wezenlijke veiligheidsbelangen niet had kunnen worden behartigd bij een procedure met oproep tot mededinging**.[58] Finaal kwam het Hof van Justitie tot het besluit dat de betreffende overheidsopdracht (het betrof een drukopdracht voor gevoelige documenten) ten onrechte rechtstreeks werd gegund, aangezien deze onderneming ten onrechte als enige ter zake betrouwbare onderneming werd weerhouden. Volgens het Hof van Justitie werd niet aangegeven waarom het onmogelijk zou zijn geweest om de betreffende opdracht gedurende lange periode toe te kennen aan één ondernemer maar via een procedure met voorafgaande oproep tot mededinging.

U zal er dus rekening mee moeten houden dat, als u een afwijking inroept op de normaal van toepassing zijnde plaatsingsregels op grond van het voormelde artikel 33, omwille van de bescherming van essentiële veiligheidsbelangen, u ook in staat moet zijn om zo nodig het bewijs aan te brengen dat de betrokken afwijking de grenzen van het betreffende geval niet overschrijdt. Het inroepen van de in artikel 33 vermelde uitzondering vormt met andere woorden geen vrijbrief om alle plaatsingsregels naast zich neer te leggen en over te gaan tot rechtstreekse gunning, zelfs indien zich een risico vormt in het licht van bepaalde essentiële veiligheidsbelangen. De bepaling moet immers restrictief worden uitgelegd en op proportionele wijze worden toegepast, zodat rechtstreekse gunning slechts mogelijk zal zijn indien u kan aantonen dat de concrete noodwendigheid die zich doet voelen om een wezenlijk veiligheidsbelang te beschermen, niet had kunnen worden behartigd via een procedure met voorafgaande oproep tot mededinging.

U mag de afwijkingsmogelijkheid dus niet te lichtzinnig inroepen, met name om zodoende een opdracht rechtstreeks te kunnen toewijzen. Vaak zijn alternatieve maatregelen voorhanden die eveneens een afwijking vormen op de normaal van toepassing zijnde

[57] considérant 79 et suivants

[58] Overweging 79 en verder.

applicables et qui offres également un niveau de protection considéré adéquat par le pouvoir adjudicateur, mais qui ont une portée moindre en termes de restriction de la concurrence. Ces mesures alternatives, qui sont également expliquées dans la présente boîte à outils, doivent également être utilisées de manière proportionnée.

La notion « d'intérêts essentiels de sécurité de l'État » visée à l'article 33, § 2, de la loi du 17 juin 2016 n'est définie ni dans cette loi ni dans la disposition correspondante de la directive. Comme le souligne l'avocat général dans ses conclusions dans l'affaire Commission/Pologne, C-601/21, la notion de « sécurité » peut être considérée comme correspondant aux notions de « sécurité publique » et de « sécurité nationale » figurant dans d'autres dispositions du droit de l'Union (point 48). En ce qui concerne la notion de « sécurité nationale » visée à l'article 4, alinéa 2, du traité sur l'Union européenne (TUE), la Cour de justice a noté que, selon la disposition du traité susmentionnée, la sécurité nationale relève de la responsabilité exclusive de chaque État membre. La Cour a également estimé que cette responsabilité est conforme à la grande importance attachée à la protection des fonctions essentielles de l'État et des intérêts fondamentaux de la société, et que la notion de « sécurité nationale » comprend la prévention et la lutte contre les activités susceptibles de déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays et, en particulier, de constituer une menace directe pour la société, la population ou l'État en tant que tel, telles que les activités terroristes. L'article 33, § 2, fait référence aux intérêts « essentiels » de sécurité. Comme l'a indiqué le Conseil d'État dans l'arrêt n° 256.645 du 31 mai 2023[59], cela semble impliquer que, pour qu'une procédure de passation soit exemptée de l'application des règles relatives aux marchés publics, les intérêts liés à l'essence même de la politique de sécurité - ou aux « composantes essentielles de la politique de sécurité », doivent pouvoir être compromis. Compte tenu de la nature des intérêts en jeu, le pouvoir adjudicateur dispose d'une grande latitude pour évaluer si un marché peut ou non compromettre les intérêts essentiels de sécurité de l'État. Toutefois, ce pouvoir d'appréciation n'est pas illimité. En cas de litige, il incombe au pouvoir adjudicateur de démontrer de manière plausible devant le tribunal, sur la base de données vérifiables, qu'il existe un risque réel que l'application de la législation sur les marchés publics porte atteinte aux intérêts essentiels de sécurité de l'État. Le quick scan vous aidera à identifier les risques en termes d'intérêts essentiels de sécurité.

plaatsingsregels en eveneens eenzelfde niveau van bescherming kunnen waarborgen dat door de aanbestedende overheid passend wordt geacht, maar minder vergaand zijn op het vlak van de beperking van de mededinging. Ook deze alternatieve maatregelen, die eveneens in de onderhavige toolbox worden toegelicht, moeten op proportionele wijze worden ingezet.

Het begrip “essentiële veiligheidsbelangen van het Rijk” waarvan sprake in artikel 33, § 2, van de wet van 17 juni 2016, wordt niet gedefinieerd in deze wet en evenmin in de overeenstemmende richtlijnbepaling. Zoals de advocaat-generaal aangeeft in zijn conclusie in de zaak Commissie t. Polen, C-601/21, kan het begrip “veiligheid” geacht worden overeen te stemmen met de begrippen “openbare veiligheid” en “nationale veiligheid” die in andere bepalingen van het Unierecht voorkomen (punt 48). In verband met het begrip “nationale veiligheid” bedoeld in artikel 4, lid 2, van het Verdrag betreffende de Europese Unie (VEU) heeft het Hof van Justitie opgemerkt dat de nationale veiligheid volgens de voornoemde verdragsbepaling tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Voorts is het Hof van oordeel dat “deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat [het begrip ‘nationale veiligheid’] het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten”. In artikel 33, § 2, gaat het om “essentiële” veiligheidsbelangen. Zoals de Raad van State aangeeft in het arrest nr. 256.645 van 31 mei 2023[60], lijkt met zich te brengen dat, om een plaatsingsprocedure te kunnen onttrekken aan de toepassing van de regelgeving inzake overheidsopdrachten, belangen die te maken hebben met de essentie van het veiligheidsbeleid zelf – of met de “kernonderdelen van het veiligheidsbeleid”, in het gedrang moeten kunnen komen. Gelet op de aard van de in het geding zijnde belangen, beschikt de aanbestedende overheid over een ruime vrijheid bij het beoordelen of een bepaalde opdracht de essentiële veiligheidsbelangen van het Rijk al dan niet in het gedrang kan brengen. Deze beoordelingsruimte is evenwel niet onbeperkt. In geval van betwisting staat het aan de aanbestedende overheid om voor de rechter aannemelijk te maken, op grond van verifieerbare gegevens, dat er een reëel risico bestaat dat de toepassing van de wetgeving inzake overheidsopdrachten afbreuk zou doen aan de essentiële

[59] En renvoyant vers le point 50 des conclusions de l’avocat-général dans l’affaires C-604/21

[60] onder verwijzing naar punt 50 van de conclusies van de advocaat-generaal in de voormelde zaak C-604/21

En outre, il convient de vérifier la proportionnalité de la dérogation invoquée. Pour que la dérogation puisse être valablement invoquée, il faut démontrer, conformément au principe de proportionnalité, que l'exclusion du marché public en question des procédures de passation est une mesure appropriée et nécessaire pour protéger les intérêts essentiels de sécurité du Royaume.

Sur la base de l'examen que vous avez effectué par le biais du quickscan, vous devrez, pour les raisons susmentionnées, examiner très attentivement, au cas par cas, les anomalies qui apparaissent. Sur cette base, une motivation approfondie peut alors être préparée afin d'évaluer si votre approche est proportionnée à la lumière de la jurisprudence de la Cour de Justice. Ce faisant, vous devez toujours vous demander s'il ne suffit pas de prendre des « mesures moins intrusives », sachant que dans de certains cas, compte tenu du risque encouru, une procédure avec mise en concurrence préalable est encore possible.
Cela dépend également de la motivation finale des dérogations invoquées, basée sur des arguments de sécurité détaillés. La question de savoir si une telle justification est jugée suffisante est en définitive une décision qui, du moins en ce qui concerne le gouvernement fédéral, doit être soumise au niveau de la décision politique.

Cette motivation devrait également être disponible avant que le dossier ne soit discuté, le cas échéant, en Conseil des ministres.
Les lignes directrices mentionnées ci-dessus sont importantes pour tous les points présentés dans le chapitre 3. Dans chaque cas, il convient de vérifier si le principe de proportionnalité susmentionné est respecté.

3.2. Habilitation de sécurité, conseils de sécurité ou attestation de sécurité comme exigence lors de la phase de passation

Il sera peut être utile d'ouvrir le marché aux seuls opérateurs économiques disposant d'une habilitation de sécurité (en d'autres mots, comme un critère de sélection de type spécifique).

Exemple de clause :

« *L'adjudicataire doit disposer d'une habilitation de sécurité pour personne morale délivrée par l'Autorité Nationale de Sécurité de niveau SECRET pour le champ d'application national belge ou UE.*

veiligheidsbelangen van het Rijk. De quickscan zal u helpen de risico's op het vlak van de essentiële veiligheidsbelangen in kaart te brengen.

Bovendien moet gewaakt worden over de proportionaliteit van de afwijking. Om rechtsgeldig beroep te kunnen doen op de afwijking, moet men overeenkomstig het evenredigheidsbeginsel kunnen aantonen dat de uitsluiting van de betrokken overheidsopdracht aan de plaatsingsprocedures een maatregel is die passend en noodzakelijk is om de essentiële veiligheidsbelangen van het Rijk te beschermen.

Op basis van de screening die u hebt uitgevoerd door middel van de quickscan, zal u om de voormelde redenen telkens zeer zorgvuldig moeten overwegen welke afwijkingen zich geval per geval opdringen. Op basis daarvan kan dan een zorgvuldige motivering worden klaargemaakt, om na te gaan of uw benadering wel proportioneel is in het licht van de rechtspraak van het Hof van Justitie. Daarbij moet u telkens nagaan of het niet kan volstaan "minder ingrijpende maatregelen" te nemen, wetende dat in een aantal gevallen, in het licht van het risico dat zich stelt, toch een procedure met voorafgaande oproep tot mededinging mogelijk is.
Eén en ander hangt ook af van de finale motivering omtrent de afwijkingen die worden ingeroepen, op basis van gedetailleerde veiligheidsargumenten. Of dergelijke motivering voldoende wordt geacht, is uiteindelijk een beslissing die, althans wat de federale overheid betreft, aan het politieke beslissingsniveau moet worden voorgelegd.

Dergelijke motivering moet eveneens voorhanden zijn alvorens het dossier behandeld wordt, desgevallend, in de ministerraad.
De voormelde krachtlijnen zijn voor alle punten opgenomen in hoofdstuk 3 van belang. Telkens moet nagegaan worden of aan het voormelde proportionaliteitsbeginsel voldaan is.

3.2. Veiligheidsmachtiging, veiligheidsadvies of veiligheidsattest als eis in de fase van de plaatsing

Het kan nuttig zijn de opdracht enkel open te stellen voor ondernemers met een veiligheidsmachtiging (als een bijzonder type selectiecriterium m.a.w.).

Voorbeeldclausule:

"*De opdrachtnemer moet beschikken over een veiligheidsmachtiging voor rechtspersonen, afgeleverd door de Nationale Veiligheidsoverheid*

op het niveau GEHEIM voor het nationale (Belgische) of Europese toepassingsgebied.

Les éventuels sous-traitants de l'adjudicataire doivent disposer de la même habilitation peu importe leur place dans l'échelle de sous-traitance. »

Alle eventuele onderaannemers van de opdrachtnemer moeten over dezelfde machtiging beschikken, ongeacht hun plaats in de onderaannemingsladder."

Normalement, la loi défense et sécurité sera appliquée dans un tel cas.

Normaliter zal in een dergelijk geval echter toepassing worden gemaakt van de wet op defensie- en veiligheidsgebied.

L'habilitation peut également porter sur une personne physique, par exemple les membres de l'équipe de projet qui exécutera le marché.

De machtiging kan ook betrekking hebben op natuurlijke personen, bijvoorbeeld de leden van het projectteam dat de opdracht zal uitvoeren.

Outre l'habilitation, normalement réservée au traitement d'informations classifiées, il est possible de réclamer un **avis ou une attestation de sécurité** comme condition de dépôt des candidatures considérant le caractère sensible du marché. Plus d'informations à ce sujet peuvent être obtenues auprès de l'Autorité Nationale de Sécurité[61].

Naast de machtiging, die normaliter is voorbehouden voor de verwerking van geclassificeerde informatie, is het mogelijk een **veiligheidsadvies of -attest** te eisen als voorwaarde voor het indienen van kandidaturen, rekening houdend met de gevoelige aard van de opdracht. Meer informatie over dit onderwerp kan worden verkregen bij de Nationale Veiligheidsoverheid[62].

3.3. Vérification de la sécurité ou habilitation de sécurité comme condition spéciale d'exécution

Il est nécessaire de bien distinguer la vérification de sécurité, qui débouche sur la délivrance d'une attestation de sécurité (examen superficiel imposé aux personnes qui viennent accomplir à court-terme une tâche non sensible dans un environnement où le risque doit être évité) et l'habilitation de sécurité.

La vérification de sécurité peut être effectuée dans un délai limité et ne ralentira pas beaucoup l'exécution du marché. Cela peut varier lorsque les personnes à vérifier résident à l'étranger.

Vous pouvez dans certains cas exiger une habilitation de sécurité uniquement comme condition d'exécution du marché. Soyez néanmoins conscient que la délivrance d'une habilitation de sécurité nécessite 6 à 12 mois, même plus dans certains cas. Il s'agit donc d'attribuer son marché avec suffisamment d'avance par rapport au début du délai d'exécution. Toutefois, une habilitation de sécurité peut également être imposée comme condition d'exécution, et ce uniquement si le marché est lié à des informations classifiées (même si ce n'est que de manière indirecte, en pénétrant dans des lieux où elles sont stockées).

3.3. Veiligheidsverificatie of veiligheidsmachtiging als bijzondere uitvoeringsvoorwaarde

Men moet een duidelijk onderscheid maken tussen een veiligheidsverificatie, die leidt tot een veiligheidsattest (oppervlakkig onderzoek dat wordt opgelegd aan personen die kortstondig een niet-gevoelige taak komen uitvoeren in een omgeving waar risico dient gemeden te worden) en een veiligheidsmachtiging.

De veiligheidsverificatie kan uitgevoerd worden binnen een beperkt tijdsbestek en zal de uitvoering van de opdracht niet veel vertragen. Dit kan variëren wanneer de te verifiëren personen in het buitenland verblijven.

In sommige gevallen kunt u ervoor kiezen om enkel als voorwaarde voor de uitvoering van de opdracht een veiligheidsmachtiging te eisen. Weet wel dat de aflevering van een veiligheidsmachtiging tussen de 6 en de 12 maanden in beslag neemt, in sommige gevallen zelfs langer. De opdracht moet met andere woorden ruim voor de aanvang van de uitvoeringstermijn gegund worden. Een veiligheidsmachtiging kan echter ook als uitvoeringsvoorwaarde slechts worden opgelegd indien de opdracht verband houdt met geclassificeerde informatie (ook als het slechts zijdelings is, door het betreden van plaatsen waar deze opgeslagen is).

[61] https://www.nvoans.be
[62] https://www.nvoans.be

Exemple de clause :

« *Pour l'exécution du marché, l'adjudicataire doit disposer d'une habilitation de sécurité pour personne morale délivrée par l'Autorité Nationale de Sécurité de niveau SECRET pour les champs d'application national belge ou européen.*

Les éventuels sous-traitants de l'adjudicataire doivent disposer de la même habilitation peu importe leur place dans l'échelle de sous-traitance.

Si l'adjudicataire se voit refuser l'habilitation de sécurité pour le niveau et le champ d'application précité, le marché est rompu de façon unilatérale avec effet immédiat sans que l'opérateur économique ne puisse réclamer de dommages et intérêts du fait de cette décision. Il dispose néanmoins de moyens de recours à l'encontre d'une telle conclusion de l'ANS[63]*.*

Lorsqu'un tel refus concerne l'habilitation d'un sous-traitant, il est remplacé sans délai. À défaut, le pouvoir adjudicateur pourra également imposer la rupture du marché. »

Quand bien même s'il n'est pas question de disposer d'une habilitation de sécurité, vous pouvez également imposer à l'adjudicataire de se soumettre à une **vérification de l'Autorité Nationale de Sécurité** à quelque moment que ce soit durant l'exécution du marché.

Exemple de clause :

« L'adjudicataire (personne morale) et ses collaborateurs (personnes physiques) investis dans l'exécution du marché acceptent de faire l'objet à discrétion d'une vérification de sécurité par l'Autorité Nationale de Sécurité.[65]

Si l'attestation ou l'avis rendu par l'ANS s'avère négatif, le pouvoir adjudicateur exigera sans délai le remplacement du personnel concerné par le refus. Si le refus d'attestation de sécurité ou l'avis négatif concerne l'adjudicataire en tant que tel (personne morale), le marché est rompu de façon unilatérale sans que l'opérateur économique ne puisse réclamer de dommages et intérêts du fait de cette décision. Il dispose néanmoins de moyens de

Voorbeeldclausule:

"Voor de uitvoering van de opdracht moet de opdrachtnemer beschikken over een veiligheidsmachtiging voor rechtspersonen, afgeleverd door de Nationale Veiligheidsoverheid op het niveau GEHEIM voor het nationale (Belgische) of Europese toepassingsgebied.

Alle eventuele onderaannemers van de opdrachtnemer moeten over dezelfde machtiging beschikken, ongeacht hun plaats in de onderaannemingsladder.

Indien de opdrachtnemer een veiligheidsmachtiging voor het bovengenoemde niveau en toepassingsgebied wordt geweigerd, wordt de opdracht eenzijdig en met onmiddellijke ingang beëindigd, zonder dat de ondernemer op grond van dit besluit een schadevergoeding kan eisen. Er staan hem echter rechtsmiddelen ter beschikking om tegen een dergelijke beslissing van de NVO in beroep te gaan[64]*.*

Wanneer een dergelijke weigering betrekking heeft op de machtiging van een onderaannemer, wordt deze onverwijld vervangen. Gebeurt dit niet, dan kan de aanbestedende overheid ook de beëindiging van de opdracht opleggen."

Ook wanneer een veiligheidsmachtiging niet nodig is, kunt u de opdrachtnemer steeds opleggen om zich te onderwerpen aan een **verificatie door de Nationale Veiligheidsoverheid** op gelijk welk moment tijdens de uitvoering van de opdracht.

Voorbeeldclausule :

"De opdrachtnemer (rechtspersoon) en zijn medewerkers (natuurlijke personen) die betrokken zijn bij de uitvoering van de opdracht stemmen ermee in om het voorwerp uit te maken van een verificatie door de Nationale Veiligheidsoverheid[66]*.*

Wanneer het attest of het advies van de NVO negatief blijkt, zal de aanbestedende overheid onverwijld de vervanging eisen van het personeel op wie de weigering betrekking heeft. Wanneer de weigering van een veiligheidsattest of het negatieve advies betrekking heeft op de opdrachtnemer zelf (rechtspersoon), wordt de opdracht eenzijdig beëindigd, zonder dat de ondernemer op grond van dit besluit een

[63] *http://www.beroepsorgaan.be/index.php/fr*
[64] *https://www.beroepsorgaan.be/index.php/nl/*
[65] *https://www.nvoans.be/fr/administrations-publiques/verifications-de-securite*
[66] https://www.nvoans.be/nl/private-ondernemingen/veiligheidsverificaties

recours à l'encontre d'une telle conclusion de l'ANS[67].»

schadevergoeding kan eisen. Er staan hem echter rechtsmiddelen ter beschikking om tegen een dergelijke beslissing van de NVO in beroep te gaan[68]."

3.4. Déclaration relative à l'autonomie

Dans certains cas, il peut être intéressant de demander aux candidats ou soumissionnaires de signer une déclaration dans laquelle ils confirment explicitement que les lois et règlements applicables dans leur pays d'origine offrent des garanties suffisantes quant à l'obligation de confidentialité, vis-à-vis des autorités du pays d'origine.

3.4. Verklaring in verband met autonomie

In sommige gevallen kan het interessant zijn om de kandidaten of inschrijvers te verzoeken een verklaring te willen laten ondertekenen waarbij zij uitdrukkelijk bevestigen dat de wet- en regelgeving die in hun land van herkomst van toepassing is, voldoende waarborgen biedt aangaande de verplichting tot vertrouwelijke behandeling ten opzichte van de overheden in het land van herkomst.

3.5. Exigences spécifiques par rapport à l'origine des produits qui vont au-delà de l'approche normalement applicable

Les moyens normalement mis à disposition du pouvoir adjudicateur et les limites imposées sont décrits au point 2.5 précité. Parfois, ces mesures ne s'avèrent pas suffisantes. Dans certains cas, il semble nécessaire de faire preuve d'une plus grande sévérité, pour autant que cela se justifie eu égard aux intérêts essentiels de sécurité.

Il pourrait par exemple être possible d'exclure des produits ou des matériaux s'ils proviennent de l'extérieur de l'UE (EEE) et d'ainsi considérer une telle offre comme irrégulière.

De ce point de vue, il pourrait également être plus que souhaitable que le pouvoir adjudicateur, en fonction de l'objet du marché et des risques de sécurité associés, ait une idée bien établie, par exemple, de la chaîne d'approvisionnement, de la « Product Breakdown Structure » (PBS) (structure de décomposition du produit) et/ou de la « Work Breakdown Structure (WBS) (Structure de décomposition du travail) associée à ce que l'on souhaite acquérir.

Toutefois, la portée de cette « approche de décomposition » (par ex. à quel niveau de sous-traitance, de composants, etc.) dépend fortement de la complexité du marché et des risques de sécurité identifiés. Par exemple, le boîtier de l'« unité centrale » d'un ordinateur présentera moins de risques que le processeur d'une carte mère.

3.5. Specifieke eisen met betrekking tot de oorsprong van producten die verder gaan dan de benadering die normaal van toepassing is

De middelen waarover de aanbestedende overheid normaal beschikt en de gestelde grenzen staan beschreven in punt 2.5 hierboven. Soms blijken deze maatregelen ontoereikend. In sommige gevallen lijkt het noodzakelijk om strenger te zijn, voor zover dit vanuit essentiële veiligheidsbelangen gerechtvaardigd is.

Een mogelijke maatregel zou er bijvoorbeeld in kunnen bestaan om producten of materialen uit te sluiten indien ze afkomstig zijn van buiten de EU (EER) en een dergelijke offerte aldus als onregelmatig te beschouwen.

Vanuit dit oogpunt kan het ook meer dan wenselijk zijn dat de aanbestedende overheid, in functie van het voorwerp van de opdracht en de daaraan verbonden veiligheidsrisico's, een goed beeld heeft van bijvoorbeeld de toeleveringsketen, de "Product Breakdown Structure (PBS)" en/of de "Work Breakdown Structure (WBS)" verbonden aan hetgeen men wenst te verwerven.

Hoe ver men dient te gaan in deze "Breakdown"-benadering (bijv. tot welk niveau van toelevering, van componenten, enz.) hangt echter sterk af van de complexiteit van de opdracht en van de geïdentificeerde veiligheidsrisico's. Zo zal de behuizing van de "main unit" van een computer minder risico's inhouden dan de processor op een moederbord.

3.6. Application de l'article 346 du TFUE

3.6. Toepassing artikel 346 VEU

[67] http://www.beroepsorgaan.be/index.php/fr
[68] https://www.beroepsorgaan.be/index.php/nl/

Si les conditions d'application sont remplies, il peut être fait appel à l'art. 346, 1, a), du TFUE.

- Les risques en matière de sécurité nationale (IES, intérêts essentiels de sécurité) ne peuvent PAS être garantis par des mesures moins intrusives (proportionnalité) ;
- Les exigences définies se rapportent à l'IES à protéger (en relation avec le marché en question) ;
- Les exigences fixées sont nécessaires et appropriées pour la protection de l'IES ;
- Les exigences énoncées n'entraîneront pas l'altération des conditions de concurrence sur le marché intérieur pour les produits non destinés à des fins spécifiquement militaires.

Il peut en être ainsi pour les marchés et les concours qui comportent des aspects relatifs à la défense ou la sécurité (art. 33 de la loi relative aux marchés publics) et lorsque l'application de la loi relative aux marchés publics exigerait de l'État qu'il mette à disposition des informations dont la divulgation serait considérée par l'État comme contraire à ses intérêts essentiels de sécurité.

Compte tenu de ce qui précède, l'application de l'Art 346 TFUE doit donc être considérée comme l'« ultimum remedium » (dernier recours) auquel le pouvoir adjudicateur peut recourir pour sauvegarder les intérêts (essentiels) de sécurité.

Indien aan de toepassingsvoorwaarden is voldaan, kan Art 346, 1, a) VWEU, ingeroepen worden.

- De risico's inzake nationale veiligheid (EVB) kunnen NIET geborgd worden met minder ingrijpende maatregelen (*proportionaliteit*).
- De gestelde vereisten houden verband met de EVB die beschermd moeten worden (*in relation to the procurement at hand*).
- De gestelde vereisten zijn noodzakelijk en geschikt voor de bescherming van de EVB.
- De gestelde vereisten zullen niet leiden tot de wijziging van de mededingingsverhoudingen op de interne markt voor producten die niet bestemd zijn voor specifiek militaire doeleinden.

Dit kan zo zijn voor opdrachten en prijsvragen waaraan defensie- of veiligheidsaspecten verbonden zijn (Art 33 wet overheidsopdrachten) en waar de toepassing van de wet overheidsopdrachten de staat zou verplichten informatie ter beschikking te stellen waarvan de Staat de openbaarmaking in strijd acht met zijn essentiële veiligheidsbelangen.

Gelet op bovenstaande, dient de toepassing van Art 346 VWEU bijgevolg dan ook te worden beschouwd als het '*ultimum remedium*' (laatste redmiddel) tot hetwelk de aanbestedende overheid zich kan wenden om de (wezenlijke) veiligheidsbelangen te vrijwaren.

Chapitre 4 - Autres initiatives législatives pouvant avoir un impact

Parmi les mesures commerciales autonomes de l'UE applicables aux marchés publics figurent plusieurs instruments. Certains de ces instruments sont déjà opérationnels, tandis que d'autres sont encore en cours de négociation. Le premier est l'instrument relatif aux marchés publics internationaux (IPI, International Procurement Instrument) qui, après des années de négociations, est en vigueur depuis juin 2022. Un deuxième instrument est le règlement relatif aux subventions étrangères (FSR, Foreign Subsidies Regulation) dont les négociations sont terminées depuis juin 2022. Enfin, il y a l'instrument anti-coercition (ACI, Anticoercion Instrument) dont les négociations sont en cours. Chacun de ces instruments donne la possibilité d'intervenir dans les procédures de passation de marchés publics si celles-ci ne respectent pas les règles ou sont influencées de manière déloyale.

Hoofdstuk 4 - Andere wetgevende initiatieven die een impact kunnen hebben

Onder de autonome handelsmaatregelen van de EU die van toepassing zijn op openbare aanbestedingen bevinden zich meerdere instrumenten. Sommige van deze instrumenten zijn reeds operationeel, terwijl anderen nog in onderhandeling zijn. Een eerste is het International Procurement Instrument (IPI) dat na jaren onderhandelen sinds juni 2022 van toepassing is. Een tweede instrument is de Foreign Subsidies Regulation (FSR) waarvan de onderhandelingen sinds juni 2022 zijn afgerond. Tot slot is er het Anticoercion Instrument (ACI) waarvoor de onderhandelingen nog volop lopende zijn. Elk van deze instrumenten geeft mogelijkheid om in te grijpen in openbare aanbestedingsprocedures indien deze niet volgens de regels verlopen of oneerlijk worden beïnvloed.

Un autre accord important applicable aux marchés publics est l'Accord sur les marchés publics (AMP) de l'Organisation mondiale du commerce (OMC). Il s'agit d'un accord plurilatéral au sein de l'OMC, par lequel les États membres concernés ouvrent mutuellement leurs procédures de passation de marchés.

Een ander belangrijk akkoord dat van toepassing is op openbare aanbestedingen, is het Governement Procurement Agreement (GPA) van de Wereldhandelsorganisatie (WTO). Dit is een plurilateraal akkoord binnen de WTO waarbij betrokken lidstaten wederzijds hun aanbestedingsprocedures openstellen voor elkaar.

4.1. Règlement 2022/2560 du Parlement européen et du Conseil du 14 décembre 2022 relatif aux subventions étrangères faussant le marché intérieur - Foreign Subsidies Regulation (FSR)

Le règlement relatif aux subventions étrangères fournit trois outils pour créer des conditions de concurrence équitables en contrôlant l'effet de distorsion des subventions étrangères sur le marché intérieur. Tout d'abord, les entreprises dont le chiffre d'affaires est supérieur à 500 millions d'euros sont soumises à une obligation de notification si elles participent à une acquisition dont l'apport étranger dépasse 50 millions d'euros. Il existe ensuite une obligation de notification pour les marchés publics de plus de 250 millions d'euros lorsqu'un pays tiers a accordé des subventions à hauteur de 4 millions d'euros minimum. Enfin, la Commission dispose également de la possibilité d'ouvrir des enquêtes de sa propre initiative.

Si, sur la base de ces notifications, il est constaté qu'une subvention étrangère reçue (au cours des 3 dernières années) provoque une distorsion du fonctionnement du marché intérieur, la Commission examinera d'abord si ces effets négatifs sont plus importants pour le marché intérieur que les éventuels effets positifs.

En ce qui concerne les marchés publics en particulier, si la Commission constate l'effet de distorsion après enquête et que les effets positifs ne l'emportent pas sur les effets négatifs, elle le communiquera à l'opérateur économique concerné. Si ce dernier prend des mesures pour corriger l'impact négatif, la Commission européenne peut encore l'autoriser à prendre part à la procédure. Si l'opérateur économique n'entreprend rien ou ne prend pas de mesure de manière adéquate, la Commission peut faire le choix de l'exclure.

4.1. Verordening 2022/2560 van het Europees Parlement en de Raad van 14 december 2022 betreffende buitenlandse subsidies die de interne markt verstoren - Foreign Subsidies Regulation (FSR)

De Buitenlandse Subsidies Verordening voorziet drie instrumenten om een gelijk speelveld te creëren door het verstorende effect van buitenlandse (niet-EU) subsidies op de interne markt te monitoren. In de eerste plaats is er een notificatieverplichting voor bedrijven die een omzet hebben van meer dan 500 miljoen EUR indien ze betrokken zijn bij een overname waar de buitenlandse inbreng meer dan 50 miljoen EUR bedraagt. Ten tweede is er notificatieverplichting voor openbare aanbestedingen van meer dan 250 miljoen EUR waarbij een derde land minstens voor 4 miljoen EUR aan subsidies heeft toegekend. Tot slot heeft de Commissie ook de mogelijkheid om op eigen initiatief een onderzoek op te starten.

Indien op basis van deze notificaties wordt vastgesteld dat een ontvangen buitenlandse subsidie (in de laatste 3 jaar) een verstorend effect heeft op de werking van de interne markt zal de Commissie in eerste instantie kijken of deze negatieve effecten voor de interne markt groter zijn dan de mogelijke positieve effecten.

Specifiek voor openbare aanbestedingen geldt dat indien de Commissie na onderzoek het verstorende effect vaststelt en de positieve effecten de negatieve niet overtreffen, de Europese Commissie dit zal meedelen aan de betrokken economische operator. Indien deze maatregelen neemt om het negatieve effect te corrigeren, kan de Europese Commissie alsnog toelaten om deel te nemen aan de procedure. Indien de operator dit niet of onvoldoende doet, kan de Commissie de betrokken operator uitsluiten.

4.2. Instrument relatif aux marchés publics internationaux - International procurement instrument (IPI)

Le règlement (UE) 2022/1031 du 23 juin 2022 concernant l'accès des opérateurs économiques, des biens et des services des pays tiers aux marchés publics et aux concessions de l'Union et établissant des procédures visant à faciliter les négociations relatives à l'accès des opérateurs économiques, des biens et des services originaires de

4.2. Instrument voor internationale overheidsopdrachten - International procurement instrument (IPI)

In de verordening (EU) 2022/1031 van 23 juni 2022 over toegang van ondernemers, goederen en diensten uit derde landen tot de aanbestedings- en concessiemarkten van de Unie en procedures ter ondersteuning van onderhandelingen over toegang van ondernemers, goederen en diensten uit de Unie tot de aanbestedings- en

l'Union aux marchés publics et aux concessions des pays tiers, prévoit que la Commission européenne, de sa propre initiative ou sur la base d'une plainte, peut enquêter sur les pratiques et les mesures adoptées par un pays tiers si elles ont pour effet de rendre les marchés publics dans un pays tiers insuffisamment ouverts à nos opérateurs économiques européens. Ainsi, à l'issue d'une enquête approfondie, des sanctions pourront éventuellement être imposées par la Commission européenne. Ces sanctions visent à restreindre l'accès aux procédures de passation européennes pour les opérateurs, les biens ou les services du pays tiers en question (= « mesure IPI »). La Commission européenne peut demander aux adjudicateurs, selon le cas, d'appliquer un ajustement du score pour les offres soumises par les opérateurs économiques du pays concerné ou d'exclure les offres soumises par les opérateurs économiques du pays tiers concerné. De cette manière, ce règlement peut également avoir un impact indirect sur les questions traitées dans le présent guide.

À l'heure actuelle, aucune enquête n'a été ouverte par la Commission européenne et aucune sanction n'a donc été imposée.

Les sanctions ne peuvent être imposées que pour les marchés publics ou les concessions dont la valeur estimée dépasse un seuil à fixer par la Commission européenne. [69]

La Commission devrait définir clairement le champ d'application de la sanction (secteur/catégorie de biens concernés, adjudicateurs concernés, opérateurs concernés, seuils d'application).

Si une sanction est imposée par la Commission européenne, l'adjudicataire doit également remplir certaines obligations relatives à la chaîne de sous-traitance dans le cadre de la prestation. Par exemple, l'adjudicataire ne peut pas sous-traiter plus de 50 % de la valeur totale du marché à des opérateurs de pays tiers soumis à une mesure IPI.

4.3. Instrument anti-coercition

La Commission européenne a présenté sa proposition d'instrument anti-coercition en décembre 2021. Cet instrument devrait permettre à la Commission européenne de réagir dans le cas où un pays tiers exerce une coercition économique sur un ou plusieurs États membres de l'UE. On entend par « coercition économique » une situation dans laquelle un pays tiers tente de faire pression sur l'Union ou

concessiemarkten van derde landen, is voorzien dat de Europese Commissie, op eigen initiatief of op basis van een klacht, een onderzoek kan instellen naar praktijken en maatregelen van een derde land, indien deze tot gevolg hebben dat de overheidsopdrachten in een derde land onvoldoende open staan voor onze Europese ondernemers. Op die manier kunnen, na afloop van een diepgaand onderzoek, uiteindelijk sancties worden opgelegd door de Europese Commissie. Dergelijke sancties hebben tot doel de toegang tot de Europese plaatsingsprocedures te beperken voor ondernemers, goederen of diensten uit het betreffende derde land (= "IPI-maatregel"). De Europese Commissie kan de aanbesteders naargelang van het geval verplichten een scoreaanpassing toe te passen wat de offertes betreft van ondernemers uit het betrokken land of om offertes van ondernemers uit het betrokken derde land uit te sluiten. Op die manier kan deze regeling zijdelings ook een impact hebben voor de problematiek die geschreven wordt in de onderhavige gids.

Op dit moment werden er nog geen onderzoeken opgestart door de Europese Commissie en werden dus ook nog geen sancties opgelegd.

Sancties kunnen alleen opgelegd worden voor de overheidsopdrachten of concessieovereenkomsten waarvan de geraamde waarde hoger is dan een drempel die door de Europese Commissie zal worden vastgesteld.[70]

De Commissie moet het toepassingsgebied van de sanctie duidelijk omschrijven (betrokken sector/categorie van goederen, betrokken aanbesteders, betrokken ondernemers, toepassingsdrempels).

Indien een sanctie wordt opgelegd door de Europese Commissie, dan moet de opdrachtnemer in het kader van de uitvoering ook bepaalde verplichtingen nakomen met betrekking tot de keten van onderaannemers. Zo mag de opdrachtnemer niet meer dan 50 procent van de totale waarde van de opdracht uitbesteden aan ondernemers uit derde landen waarop een IPI-maatregel van toepassing is.

4.3. Anti-coercion instrument

De Europese Commissie heeft in december 2021 haar voorstel gepresenteerd voor het antidwanginstrument. Dit instrument moet de Europese Commissie toelaten om te kunnen reageren indien een derde land economische dwang uitoefent op één of meerdere EU-lidstaten. Onder "economische dwang" wordt een situatie verstaan waarin een derde land probeert de Unie of een lidstaat onder druk

[69] Dans tous les cas, ce seuil est supérieur ou égal à 15 000 000 euros pour les travaux et concessions et à 5 000 000 euros pour les fournitures et services.

[70] Deze drempel is in alle gevallen hoger dan of gelijk aan 15 000 000 euro voor werken en concessies en 5 000 000 euro voor leveringen en diensten.

un État membre pour qu'elle/il fasse un choix politique particulier en appliquant, ou en menaçant d'appliquer des mesures à son encontre qui affectent le commerce ou les investissements. L'objectif principal de l'instrument est d'avoir un effet dissuasif à l'égard des pays tiers, et ce n'est qu'en dernier recours que la possibilité de contre-mesures est prévue. Des mesures peuvent être prises tant contre les gouvernements que contre les personnes physiques qui peuvent être liées à la coercition économique.

L'une des contre-mesures possibles dans la proposition de la Commission européenne est la suspension des obligations internationales en matière de marchés publics, l'exclusion des biens, services, fournisseurs du pays tiers concerné, ou l'imposition d'une sanction obligatoire de pondération de l'évaluation des prix pour les biens, services ou fournisseurs soumissionnaires.

Les négociations relatives à cet instrument sont actuellement en cours. Le Parlement européen a défini sa position à la mi-octobre 2022, tandis que le Conseil doit encore trouver un accord. Suite à cela auront également lieu des négociations en trilogue.

4.4. Accord sur les marchés publics

Les premières initiatives d'e l'AMP remontent au début des années 1980 dans le cadre du GATT (Accord général sur les tarifs douaniers et le commerce). La dernière grande réforme remonte à 2012 et est en vigueur depuis 2014. Actuellement, cet accord s'applique à 48 membres de l'OMC (dont les 27 États membres de l'UE), et 36 membres y participent en qualité d'observateurs.

Les signataires de cet accord plurilatéral (au sein des structures de l'OMC) s'engagent à ouvrir mutuellement leurs marchés publics. Cet accord est destiné à garantir un traitement ouvert, transparent et équitable des participants d'autres pays pendant les procédures. Toutefois, chaque membre de l'OMC décide des secteurs de marchés publics qu'il est prêt à ouvrir à toutes les autres parties.

L'importance de l'AMP est grande car il va bien au-delà de l'ouverture mutuelle par le biais d'accords commerciaux bilatéraux. Les négociations en vue de l'adhésion du Brésil sont en voie d'achèvement et marqueront une expansion majeure.

4.5. Mesures du Conseil européen

Sur proposition conjointe du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et de la Commission, le Conseil européen, peut, conformément à l'article 215 du traité sur l'Union européenne, prévoir

te zetten om een bepaalde beleidskeuze te maken door tegen de Unie of een lidstaat maatregelen toe te passen die van invloed zijn op de handel of investeringen, of te dreigen dat te doen. Doel van het instrument is vooral om een ontradend effect te hebben naar derde landen toe en enkel in laatste instantie is de mogelijkheid voorzien om tegenmaatregelen te nemen. Maatregelen kunnen zowel genomen worden tegen overheden als natuurlijke personen die gelinkt kunnen worden aan de economische dwang.

Een van de mogelijke tegenmaatregelen in het voorstel van de Europese Commissie is de opschorting van internationale verplichtingen op het vlak van openbare aanbestedingen, de uitsluiting van goederen, diensten, leveranciers uit het betrokken derde land, of het opleggen van een verplichte prijsevaluatiewegingssanctie voor inschrijving van goederen, diensten of leveranciers.

De onderhandelingen voor dit instrument zijn op dit moment nog lopende. Het Europees Parlement heeft midden oktober 2022 haar positie bepaald, terwijl de Raad nog geen akkoord heeft. Nadien volgen ook nog de triloogonderhandelingen.

4.4. Government procurement Agreement

De eerste initiatieven van het GPA dateren reeds van begin jaren '80 onder de GATT. De laatste grote hervorming dateert van 2012 en is sinds 2014 van kracht. Momenteel is dit akkoord van toepassing op 48 WTO-leden (waaronder de 27 EU-lidstaten) en 36 leden nemen deel als observator.

De ondertekenaars van dit plurilateraal akkoord (binnen de WTO-structuren) engageren zich om wederzijds hun marketen voor openbare aanbestedingen open te stellen voor elkaar. Dit moet zorgen voor open, transparante en eerlijke behandelingen van deelnemers uit andere landen tijdens procedures. Elk WTO-lid bepaalt echter zelf welke sectoren van openbare aanbestedingen het bereid is te openen voor alle andere partijen.

Het belang van het GPA is groot omdat dit veel breder gaat dan wederzijdse opening via bilaterale handelsverdragen. Onderhandelingen tot toetreding van Brazilië zijn bijna afgerond en zullen een belangrijke uitbreiding betekenen.

4.5. Maatregelen van de Europese Raad

Op gezamenlijk voorstel van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en de Commissie, kan de Europese Raad, overeenkomstig artikel 215 van het Verdrag betreffende de Europese Unie,

l'interruption ou la réduction, en tout ou en partie, des relations économiques et financières avec un ou plusieurs pays tiers.

Le Conseil peut également adopter des mesures restrictives à l'encontre de personnes physiques ou morales, de groupes ou d'entités non étatiques.

Le Conseil a fait usage de cette faculté pour adopter les sanctions contre la Russie suite à la guerre en Ukraine. Une sanction spécifique sur les marchés publics est prévue dans cet ensemble de sanctions.[71]

Ces sanctions conduisent indirectement à traiter le risque de sécurité du pays subissant la sanction. Toutefois, la sanction pourrait également être levée, ce qui pourrait accroître à nouveau le risque pour la sécurité. Certaines sanctions ne concernent également que les marchés publics qui atteignent le seuil de publication européen.

4.6. Filtrage des investissements étrangers

Les investissements directs étrangers sont très importants pour les économies européenne et belge. Ces dernières années, cependant, des inquiétudes croissantes ont été exprimées quant à la volonté de certains investisseurs étrangers de prendre le contrôle ou l'influence d'entreprises européennes opérant dans des secteurs critiques/stratégiques.

Avec le règlement 2019/452, en vigueur depuis octobre 2020, l'Union européenne a adopté un cadre pour la mise en place et l'utilisation de mécanismes nationaux concernant le filtrage des investissements directs étrangers, sur la base de la sécurité et de l'ordre public. Ce cadre n'oblige pas les pays à mettre en place un mécanisme national, bien que cela soit fortement recommandé, mais fournit des critères ainsi qu'un mécanisme de coopération entre la Commission européenne et les États membres, avec pour principal objectif d'organiser un échange fluide des informations.

Le 1er juin 2022, les différents gouvernements de notre pays ont conclu un accord de coopération visant à développer un mécanisme de filtrage des investissements étrangers dans les secteurs sensibles relevant de l'ordre et de la sécurité publics ou des intérêts stratégiques.

Après avis du Conseil d'État, l'accord de coopération sera débattu par les différents parlements au cours de cette année, pour entrer en vigueur à partir du 1er janvier 2023. Le SPF Économie est le point de contact national pour la

voorzien in de verbreking of de gehele of gedeeltelijke beperking van de economische en financiële betrekkingen met een of meerdere derde landen.

De Raad kan ook beperkende maatregelen treffen tegen natuurlijke of rechtspersonen, groepen of niet-statelijke entiteiten.

De Raad heeft gebruik gemaakt van deze bevoegdheid om sancties op te leggen aan Rusland ten gevolge van de oorlog in Oekraïne. In dit sanctiepakket is een specifieke sanctie voorzien omtrent overheidsopdrachten.[72]

Deze sancties leiden er onrechtstreeks toe dat ook het veiligheidsrisico vanuit het land dat de sanctie ondergaat, wordt aangepakt. De sanctie kan echter ook weer beëindigd worden, waardoor het veiligheidsrisico weer kan toenemen. Sommige sancties hebben ook alleen betrekking op de overheidsopdrachten die de drempel voor de Europese bekendmaking bereiken.

4.6. Screening buitenlandse investeringen

Buitenlandse directe investeringen zijn van groot belang voor de Europese en Belgische economie. De laatste jaren zijn er echter groeiende bezorgdheden over bepaalde niet Europese buitenlandse investeerders die controle of invloed trachten te winnen over Europese bedrijven actief in kritische/ strategische sectoren.

Met Verordening 2019/452, in voege sinds oktober 2020, nam de Europese Unie een kader aan voor het opzetten en aanwenden van nationale mechanismen m.b.t. de screening van directe buitenlandse investeringen op basis van de toetsstenen veiligheid en openbare orde. Dit kader verplicht landen niet om een nationaal mechanisme te installeren, al wordt dit sterk aanbevolen, maar voorziet in criteria én in een samenwerkingsmechanisme tussen de Europese Commissie en lidstaten met als hoofddoel een vlotte informatie-uitwisseling te organiseren.

De verschillende regeringen van ons land hebben op 1 juni 2022 een samenwerkingsakkoord bereikt voor de ontwikkeling van een screeningsmechanisme voor buitenlandse investeringen in gevoelige sectoren die van belang zijn voor de openbare orde en veiligheid of strategische belangen.

Na advies van de Raad van State, zal het samenwerkingsakkoord in de loop van dit jaar door de verschillende parlementen worden behandeld, om vanaf 1 januari 2023 in werking te kunnen treden. De FOD

[71] https://bosa.belgium.be/fr/news/sanctions-europeennes-envers-la-russie-en-matiere-de-marches-publics
[72] https://bosa.belgium.be/nl/news/europese-sancties-tegen-rusland-inzake-overheidsopdrachten

Belgique dans le cadre du règlement et dirige également la poursuite du déploiement opérationnel du mécanisme de filtrage belge. Ce mécanisme de filtrage n'affectera normalement pas les marchés publics puisqu'il concerne les investissements étrangers.

Economie is het nationaal contactpunt voor België onder de Verordening en leidt ook de verdere operationele uitrol van het Belgisch screeningsmechanisme. We verwachten niet dat dit screeningsmechanisme invloed zal hebben op overheidsopdrachten, aangezien het gaat om inkomende investeringen.

4.7. Cyber Resilience Act

De manière générale, ce « Cyber Resilience Act » (ci-après CRA)prévoit des exigences obligatoires en matière de cybersécurité pour les produits matériels et logiciels, l'évaluation de la conformité et la surveillance du marché. Ces exigences essentielles de cybersécurité couvrent l'ensemble du cycle de vie ou une période de 5 ans, et doivent être mises en œuvre par les fabricants, distributeurs ou importateurs. Les exigences essentielles en matière de cybersécurité concernent la conception, le développement et la production de produits comportant des éléments numériques. Cette proposition comprend également des exigences essentielles pour le traitement des vulnérabilités. Plusieurs produits comportant des éléments numériques sont en dehors du champ d'application. La loi sur la cyberrésilience ne couvre par exemple pas les produits comportant des éléments numériques développés exclusivement à des fins nationales ou militaires, ni les produits spécifiquement conçus pour traiter des informations classifiées.

4.7. Cyber Resilience Act

In het algemeen voorziet de Cyber Resilience Act (hierna CRA) verplichte cyberveiligheidseisen voor hardware- en softwareproducten, conformiteitsbeoordeling en markttoezicht. Deze essentiële eisen inzake cyberveiligheid hebben betrekking op de gehele levenscyclus of 5 jaar en moeten door de fabrikanten, distributeurs of importeurs geïmplementeerd worden. De essentiële cyberveiligheidseisen hebben betrekking op het ontwerp, de ontwikkeling en de productie van producten met digitale elementen. Ze omvatten eveneens essentiële eisen voor de behandeling van kwetsbaarheden. Verschillende producten met digitale elementen vallen buiten de scope. De CRA heeft bijvoorbeeld geen betrekking op producten met digitale elementen die uitsluitend ontwikkeld zijn voor nationale of militaire doeleinden of op producten die specifiek ontworpen zijn om geclassificeerde informatie te verwerken.

Douze exigences différentes en matière de cybersécurité sont décrites, qui doivent être mises en œuvre par le fabricant, le distributeur ou l'importateur. Par exemple, tous les produits comportant des éléments numériques doivent être livrés sans vulnérabilité exploitable connue. Les 11 autres obligations sont fondées sur une analyse des risques du produit lui-même. Par exemple : une configuration par défaut sécurisée, y compris la possibilité de remettre le produit dans son état d'origine ; la protection contre les accès non autorisés grâce à des mécanismes de contrôle appropriés, y compris, mais sans s'y limiter, l'authentification, l'identité ou le système de gestion des accès. La protection de la confidentialité des données stockées, transmises ou traitées d'une autre manière en cryptant les données pertinentes au repos ou en transit au moyen de mécanismes avancés est également décrite[73].

Er worden 12 verschillende cyberveiligheidseisen omschreven, die geïmplementeerd moeten worden door de fabrikant, distributeur of importeur. Zo moeten alle producten met digitale elementen geleverd worden zonder bekende exploiteerbare kwetsbaarheden. De andere 11 verplichtingen zijn gebaseerd op een risicoanalyse van het product zelf. Voorbeelden hiervan zijn: veilige standaardconfiguratie, inclusief de mogelijkheid om het product in zijn oorspronkelijke staat terug te brengen; bescherming tegen ongeoorloofde toegang door middel van passende controle mechanismen, met inbegrip van maar niet beperkt tot authenticatie, identiteits- of access management systeem. Ook de bescherming van de vertrouwelijkheid van opgeslagen, verzonden of anderszins verwerkte gegevens door het versleutelen van relevante gegevens in rust of in transit door middel van geavanceerde mechanismen, wordt beschreven[74].

Lors de la mise sur le marché d'un produit comportant des éléments numériques et pendant la durée de vie prévue du produit ou pendant une période de cinq ans à compter de

Bij het in de handel brengen van een product met digitale elementen en voor de verwachte levensduur van het product of voor een periode van vijf jaar vanaf het in de

[73] Annexe I, point 1

[74] Bijlage 1, punt 1

la mise sur le marché du produit, la période la plus courte étant retenue, les fabricants veillent à ce que les vulnérabilités de ce produit soient traitées efficacement et conformément aux exigences essentielles de l'annexe I, section 2. La section 2 de l'annexe I décrit les exigences du processus de traitement des vulnérabilités. Par exemple, les produits doivent traiter et corriger les vulnérabilités sans délai, notamment en fournissant des mises à jour. Le fabricant, le distributeur ou l'importateur doit également effectuer des tests et des évaluations efficaces et réguliers de la cybersécurité du produit comportant des éléments numériques et, dès qu'une mise à jour de sécurité est disponible, divulguer des informations sur les vulnérabilités corrigées, y compris une description de celles-ci.

handel brengen van het product, afhankelijk van welke periode korter is, zorgen fabrikanten ervoor dat kwetsbaarheden van dat product doeltreffend en in overeenstemming met de essentiële eisen in punt 2 van Annex I worden aangepakt. Punt 2 van Annex I beschrijft de vereisten van het vulnerability handling proces. Zo moeten producten bijvoorbeeld kwetsbaarheden onverwijld aanpakken en verhelpen, onder meer door updates te verstrekken. De fabrikant, distributeur of importeur moet ook doeltreffende en regelmatige tests en evaluaties van de cyberveiligheid van het product met digitale elementen uitvoeren en zodra een beveiligingsupdate beschikbaar is gesteld, informatie openbaar maken over verholpen kwetsbaarheden, met inbegrip van een beschrijving van de kwetsbaarheden.

Différents types d'évaluation de la conformité sont décrits dans la loi sur la cyberrésilience, les produits comportant des éléments numériques étant classés en « catégorie par défaut », « classe 1 » et « classe 2 ». Dans la catégorie par défaut, qui représentera environ 90 % des produits selon la Commission européenne, le fabricant, le distributeur ou l'importateur doit procéder à une auto-évaluation. Les classes 1 et 2 requièrent soit un certificat de cybersécurité assorti d'une auto-évaluation, soit une évaluation de la conformité par un organisme d'évaluation de la conformité (évaluation par une tierce partie). L'annexe III énumère les produits qui appartiennent à la classe 1 ou 2. En voici quelques exemples : Navigateurs autonomes et intégrés ; Gestionnaires de mots de passe ; Dispositifs de l'Internet industriel des objets qui peuvent être utilisés par un fournisseur de services essentiels ; Routeurs, modems destinés à la connexion Internet, et commutateurs, destinés à un usage industriel.

Er zijn verschillende soorten conformiteitsbeoordelingen beschreven in de CRA, waarbij producten met digitale elementen ingedeeld worden in 'default category', 'Class 1' en 'Class 2'. Bij de default categorie, wat ongeveer volgens de Europese Commissie 90% van de producten zullen zijn, moet de fabrikant, distributeur of importeur een zelfbeoordeling doen. Bij klasse 1 en 2 moet ofwel een cyberveiligheidscertificaat bestaan plus een zelfbeoordeling of een conformiteitsbeoordeling door een conformiteitsbeoordelingsinstantie (third-party assessment). Annex III geeft een lijst van producten die ofwel klasse 1 of 2 zijn. Enkele voorbeelden zijn: Standalone and embedded browsers; Password managers; Industrial Internet of Things devices die gebruikt zullen worden door een essentiële dienstverlener; Routers, modems intended for the connection to the internet, and switches, intended for industrial use.

En résumé, le CRA appelle à renforcer la cybersécurité essentielle des produits comportant des éléments numériques, et ce tout au long de leur cycle de vie.

Samenvattend verzoekt de CRA de essentiële cyberveiligheid van producten met digitale elementen te verhogen, en dit voor hun gehele levenscyclus.

4.8. Autonomie stratégique

Dans le cadre de la Space Regulation, du programme pour une Europe numérique (DIGITAL) et du mécanisme pour l'interconnexion en Europe (MIE) s'appuient davantage sur l'autonomie stratégique et imposent plusieurs conditions d'éligibilité et de participation dans le cadre de certains marchés, subventions ou attributions en vue de préserver la sécurité, l'intégrité et la résilience des systèmes opérationnels de l'UE. En particulier, plusieurs articles des règlements exigent que l'entité juridique éligible ne soit pas soumise au contrôle d'un pays tiers ou d'une entité de ce pays tiers. Il s'agit de la capacité directe ou indirecte d'exercer un pouvoir décisif sur l'entité. Toutefois, ce sont

4.8. Strategische autonomie

In het kader van de Space Regulation, het Digital Europe Programme (DEP) en de Connecting Europe Facility (CEF) wordt meer ingezet op strategische autonomie en worden er verscheidene toelatings- en deelnemingsvoorwaarden voorgeschreven in het kader van bepaalde aanbestedingen, subsidies of prijzen met het oog op de vrijwaring van de veiligheid, integriteit en veerkracht van operationele systemen van de EU. Verschillende artikels in de desgevallende verordeningen vragen in het bijzonder dat de in aanmerking komende juridische entiteit niet onderworpen is aan controle uit een derde land of door een entiteit uit dat derde land. Het gaat dan om de directe of indirecte mogelijkheid om beslissende macht uit te oefenen over de entiteit. Het zijn evenwel de lidstaten

les États membres qui doivent vérifier et transmettre ces informations aux institutions de l'UE.

die dergelijke informatie moeten nagaan en overmaken aan de EU-instellingen.

Annexe II – Quickscan

1. Introduction

Le Quickscan consiste en un nombre limité de questions permettant de déterminer rapidement si un marché public présente un risque pour la sécurité nationale ou si une enquête plus approfondie est nécessaire pour le déterminer. Le Quickscan doit être effectué avant le lancement de la procédure de passation de marché, notamment avant la publication de l'avis de marché, ou, si la procédure négociée sans publication préalable est utilisée, avant la soumission d'une demande de participation ou d'une offre. De cette manière, les mesures nécessaires peuvent être prises si le Quickscan montre qu'il existe des risques pour la sécurité nationale. C'est au pouvoir adjudicateur qu'il revient de remplir le Quickscan. Dans des cas où plusieurs services publics sont impliqués dans un achat, ils sont tous tenus de contribuer au Quickscan.

Le présent document fait partie d'un ensemble de lignes directrices dans ce domaine et complète les directives et/ou procédures visant à déterminer et contrôler les risques susceptibles d'affecter la sécurité nationale au cours du processus de passation des marchés. La Toolbox sécurité nationale et marchés publics fait partie de cet ensemble d'instruments.

Sécurité nationale

La sécurité nationale englobe la sécurité de notre État, de sa population et la pérennité de notre société en assurant une protection contre les menaces tant externes qu'internes. Une stratégie de sécurité nationale (SSN)[1] fournit le cadre du déploiement coordonné de tous les instruments de pouvoir nationaux pour protéger les intérêts vitaux du pays contre ces menaces dans la poursuite d'objectifs de politique nationale, qu'ils soient de nature économique, politique ou sociale ou même strictement de sécurité. Le gouvernement fédéral est responsable de la SSN belge.

La SSN, récemment développée à partir d'un effort coordonné de tous les acteurs de la sécurité nationale, identifie ainsi les intérêts vitaux du pays suivants:

(1) L'État de droit, la démocratie, la résilience et les valeurs nationales ;
(2) La sécurité physique, l'intégrité territoriale ;
(3) L'Environnement
(4) La prospérité économique ;
(5) L'ordre international ;
(6) Le fonctionnement de l'UE.

Par une approche intégrée, il est donc nécessaire que des mesures soient prises pour renforcer notre résilience nationale (sensu lato)[2] au profit de la sécurité économique et d'une autonomie stratégique belge renforcée. Cela comprend des mesures telles que :

(1) Protéger les opérateurs économiques (européens) ;
(2) Renforcer l'autonomie stratégique en diversifiant les chaînes de production et d'approvisionnement, en constituant des stocks stratégiques, en favorisant la production et/ou l'investissement au sein de l'Europe, etc.
(3) Protéger la propriété intellectuelle et le potentiel scientifique et économique ;
(4) Sensibiliser aux évolutions technologiques et aux menaces d'espionnage (économique), d'ingérence et/ou de sabotage qui y sont associées.

Compte tenu de ces intérêts vitaux, certaines des acquisitions peuvent donc englober une dimension de sécurité nationale. La question de savoir si un marché présente un risque pour la sécurité nationale dépend fortement du secteur et du type de produit ou de service fourni, du pouvoir adjudicateur et de l'adjudicataire. Dans certains cas, il est donc important de faire une bonne analyse des risques. Les risques pour la sécurité

[1] Voir également la stratégie de sécurité nationale du 1er décembre 2021.
[2] Résilience des services vitaux, changement climatique, santé publique, cybersécurité, ...

nationale, par exemple, sont plus susceptibles de survenir dans les secteurs critiques[3] et les infrastructures critiques[5], ainsi que chez les opérateurs de services essentiels (OSE)[4].

a. Exemples de risques pour la sécurité nationale

(1) Perturbation des infrastructures critiques

Une commande peut compromettre la continuité de l'approvisionnement, du service ou de la production d'un des secteurs vitaux, par exemple les télécommunications ou l'approvisionnement énergétique. Une panne ou une perturbation peut entraîner de graves perturbations sociales et constitue donc une menace pour la sécurité nationale.

(2) Une dépendance stratégique (vulnérable) vis-à-vis d'acteurs économiques et/ou de pays avec lesquels la Belgique ne partage pas les mêmes intérêts géopolitiques.

Un marché public peut mener à une dépendance stratégique (vulnérable) vis-à-vis d'un acteur économique - contrôlé ou non par un gouvernement étranger - ou de ses sous-traitants. Une telle dépendance peut alors être exploitée, par exemple, pour exercer une pression politique sur la Belgique.

(3) La perte de connaissances de haut niveau et d'informations sensibles

Il est possible que dans le cadre de l'exécution d'un marché, un adjudicataire ou son sous-traitant ait accès à des connaissances de haut niveau et/ou à des informations sensibles. L'accès au connaissances concernant des développements technologiques est aussi une possibilité. Il existe alors un risque que ces connaissances de haut niveau et/ou ces informations sensibles soient perdues. De telles données peuvent ainsi, par exemple, se retrouver dans des pays dont les lois permettent aux services de renseignement de ces pays de demander et/ou de consulter les données.

b. Quand est-il important d'effectuer un Quickscan ?

S'il existe des soupçons ou des doutes sur les risques pour la sécurité nationale lors du démarrage d'une procédure d'achat, le QuickScan doit être appliqué. Le pouvoir adjudicateur est le principal responsable de l'évaluation du risque qu'un marché peut comporter pour la sécurité nationale. Le pouvoir adjudicateur est responsable de l'atténuation ultérieure des risques potentiels. Les autres parties concernées (par exemple des services qui utiliseront le produit) sont tenues de contribuer à l'analyse de risques.

c. Que se passe-t-il après le Quickscan ?

Si le Quickscan montre qu'il peut y avoir un risque pour la sécurité nationale associé au marché, une analyse de risque supplémentaire est nécessaire pour déterminer quelles mesures devraient idéalement être mises en œuvre afin d'atténuer autant que possible les risques identifiés (par exemple, les exigences concernant les droits d'accès/ motifs d'exclusion, critères de sélection qualitatifs, conditions spécifiques relatives à l'exécution du marché, etc.).

---

[3] Infrastructure critique = installation, système ou partie de celui-ci, d'importance fédérale, qui est essentiel au maintien des fonctions sociétales vitales, de la santé, de la sécurité, de la prospérité économique ou du bien-être social, et dont l'interruption du fonctionnement ou la destruction aurait un impact significatif en perturbant ces fonctions (Art 3, 4° Loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques).

[4] Opérateurs de services essentiels = une entité publique ou privée opérant en Belgique dans un des secteurs énumérés à l'annexe I de la loi du 7 avril 2019 instaurant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, qui répond aux critères visés à l'article 12, § 1er, et qui a été désignée comme telle par le gouvernement sectoriel (Art 6, 11°, de la loi du 7 avril 2019 instaurant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique). Il s'agit d'entités qui fournissent des services essentiels à notre société ou à notre économie et qui dépendent des systèmes de réseaux et d'information. Il est important que ces réseaux et systèmes d'information soient sécurisés.

Méthologie pour le Quickscan

Ce formulaire est destiné à évaluer, avant de lancer la procédure de passation de marché, s'il existe des risques pour la sécurité nationale. Le QuickScan doit être effectué le plus tôt possible, afin que les mesures nécessaires puissent être prises si ce QuickScan montre qu'il existe effectivement des risques pour la sécurité nationale. Le pouvoir adjudicateur est chargé de remplir le QuickScan.

QUICKSCAN		
		Explication
1. Intérêts, processus et secteurs vitaux Le marché touche-t-il à un secteur, un intérêt ou un processus vital ? *Voir le paragraphe 1.1 pour un aperçu des intérêts et secteurs vitaux.*	☐ Oui/Possible ☐ Non	
2. Dépendance stratégique L'acquisition crée-t-elle une forte dépendance vis-à-vis d'un acteur économique ou de ses sous-traitants, contrôlés ou non par un gouvernement étranger, de sorte qu'en cas de conflit, il est possible que l'adjudicateur soit mis sous pression par l'*adjudicataire* (qu'il s'agisse ou non pour le compte d'un acteur gouvernemental étranger) ? *Une dépendance stratégique peut survenir, par exemple, lorsque le marché concerne un produit ou un service pour lequel il existe peu d'adjudicataires disponibles sur le marché, ou lorsqu'une interruption soudaine d'une livraison, par exemple en raison d'un conflit (d'État), entraîne une perturbation des processus primaires d'une organisation.*	☐ Oui/Possible ☐ Non	
3. Accès aux informations classifiées L'adjudicataire (ou ses sous-traitants) a-t-il besoin d'accéder à des informations classifiées pour exécuter le marché ? *Voir le paragraphe 1.2 pour plus de précisions sur les informations classifiées.*	☐ Oui/Possible ☐ Non	
4. Accès aux informations sensibles L'adjudicataire (ou ses sous-traitants) a-t-il besoin d'accéder à des informations sensibles pour exécuter le marché ? *Voir le paragraphe 1.3 pour plus de précisions sur les informations sensibles.*	☐ Oui/Possible ☐ Non	
5. Accès à un lieu sensible Le personnel de l'adjudicataire (ou de ses sous-	☐ Oui/Possible	

traitants) a-t-il accès aux lieux sensibles du pouvoir adjudicateur ? *Voir le paragraphe 1.4 pour plus de précisions sur les lieux sensibles.*	☐ Non	
6. Espionnage et/ou sabotage L'acquisition crée-t-elle un risque de surveillance technique, d'écoute, d'espionnage et/ou de sabotage ? *Voir le paragraphe 1.5 pour plus de précisions sur l'espionnage.*	☐ Oui/Possible ☐ Non	
Si la réponse est "oui/possible" à l'une des questions précédentes:		
7. Recours à des sous-traitants Est-ce que, pendant l'exécution du marché, une situation dans laquelle l'adjudicataire a le droit de déployer de nouveaux/d'autres sous-traitants pour l'exécution du marché pourrait se présenter?	☐ Oui/Possible ☐ Non	

CONCLUSION	
Oui/Possible	**Non**
Si la réponse à l'une des questions ci-dessus est « oui/possible », cela signifie qu'il existe des risques possibles pour la sécurité nationale. Une analyse approfondie des risques s'impose. Une analyse des risques examine plus en détail la détection des risques pour la sécurité nationale et vérifie si et comment les risques peuvent être atténués → prévoir des mesures dans la phase de sélection (motifs d'exclusion/droit d'accès, critères de sélection qualitative, choisir la bonne procédure de passation/les critères d'attribution ou formuler des conditions particulières concernant l'exécution. *Voir point 1.6 dans le tableau ci-dessous pour plus d'informations sur l'analyse des risques.*	Si les réponses sont tous négatives, la procédure peut se poursuivre sans mesures supplémentaires dans le cadre de la sécurité nationale.

1. Apercu des intérêts, processus et secteurs vitaux

Les intérêts vitaux à considérer sont les suivants :
- L'État de droit, la démocratie, la résilience et les valeurs nationales ;
- La sécurité physique, l'intégrité territoriale ;
- L'environnement
- La prospérité économique ;
- L'ordre international ;
- Le fonctionnement de l'UE.

- L’énergie
- Le transports
- Les finances
- L’eau potable
- La santé
- Les infrastructures numériques
- Les communications électroniques
- Le domaine spatial

Les processus vitaux nécessaires à la sauvegarde de ces intérêts vitaux doivent être examinés. Toutes les activités gouvernementales dans les services dont le domaine d'activités touche à des intérêts vitaux, ne sont pas vitales. Par exemple, l'achat d'un logiciel de gestion des bases de données policières est un processus vital, mais la fête pour la retraite des policiers ne l'est pas.

L'évaluation des processus vitaux au sein d’un service public incombe au service public lui-même. Les service publics peuvent utiliser des plans de de poursuite des activités déjà existants au sein de ce service pour guider cette évaluation.

2. Informations classifiées

Informations classifiées : « toute information ou tout matériel, quel qu'en soit la forme, la nature ou le mode de transmission, auquel un certain niveau de classification ou un niveau de protection a été attribué et qui, dans l'intérêt de la sécurité nationale et conformément aux dispositions législatives, réglementaires ou administratives en vigueur dans un Etat membre, requiert une protection contre tout détournement, toute destruction, suppression, divulgation, perte ou tout accès par des personnes non autorisées, ou tout autre type de compromission »[5].

Actuellement en Belgique, il existe trois (3) niveaux de classification[6] :

CONFIDENTIEL
SECRET
TRES SECRET
Le niveau de classification est déterminé en fonction du contenu. D'autres pays ou organisations internationales ont souvent un quatrième niveau de classification inférieur (par exemple EU/NATO RESTRICTED).

3. Informations sensibles

Il s'agit d'informations non classifiées au sens de la loi du 11 décembre 1998, mais sensibles.

Les informations non classifiées peuvent également revêtir une importance stratégique si elles tombent entre de mauvaises mains et/ou peuvent permettre l’ingérence de tiers dans des processus décisionnels. Pensez à l'état de préparation de l'armée grâce à des informations sur différents lieux ou une meilleure compréhension du fonctionnement des organisations qui fournissent des services vitaux.

Considérons également, par exemple, les informations dont l'accès par des personnes non autorisées peut avoir des conséquences néfastes pour les intérêts de l'État et de ses alliés ou d'un ou de plusieurs services publics fédéraux.

---

[5] Article 3, 19° Loi Défense et Sécurité 2011

[6] Art. 4 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité

4. Lieux sensibles

Considérons:

- Lieux où des informations classifiées ou sensibles sont traitées.
- Bâtiments des services de renseignement et de sécurité
- Postes de travail des représentants politiques
- Postes de travail des autorités judiciaires
- Postes de travail des personnes occupant des postes clés

5. Espionnage ou sabotage

Certains marchés peuvent impliquer un risque accru d'espionnage ou de sabotage. Par exemple, pensez à :

- la fourniture d'infrastructure informatique au cabinet d'un ministre
- L'installation d'imprimantes chez un Secrétaire d'État
- La nomination du personnel de sécurité

6. Analyse de risques

Si le Quickscan montre que des risques pour la sécurité nationale existent, ou que des recherches supplémentaires sont nécessaires, il est recommandé de procéder à une analyse des risques. Une analyse des risques détermine exactement quels risques existent et comment agir pour atténuer ces risques. Ce qui suit est destiné à aider le responsable chargé de l'évaluation.

L'analyse des risques tient compte des intérêts de sécurité nationale suivants :

- Continuité des infrastructures vitales ;
- Indépendance stratégique vis-à-vis des parties et des pays avec lesquels notre pays ne partage pas les mêmes intérêts géopolitiques ;
- Intégrité et exclusivité des connaissances de haut niveau et des informations confidentielles (secrets d'État, données personnelles BE, connaissances technologiques sensibles).

a. Quels risques réels pour la sécurité nationale peuvent découler du marché ?

- Perturbation de la continuité des infrastructures vitales :
  Le marché risque-t-il de mettre en péril la continuité d'approvisionnement, de service ou de production de processus vitaux ?

- Une dépendance stratégique vis-à-vis de parties et de pays avec lesquels notre pays ne partage pas les mêmes intérêts géopolitiques :
  Le marché crée-t-il une forte dépendance stratégique à l'égard d'un acteur du marché - contrôlé ou non par un gouvernement étranger - ou de ses sous-traitants, de sorte qu'en cas de conflit, il est possible que le pouvoir adjudicateur soit mis sous pression par l'adjudicataire (que ce soit ou non pour le compte d'un acteur gouvernemental étranger) ?

  Cela est particulièrement pertinent lorsqu'un produit ou un service est lié à la sécurité nationale. Par exemple, le marché concerne-t-il un produit ou un service pour lequel seuls quelques entrepreneurs sont disponibles sur le marché, ou l'arrêt brutal de la livraison, par exemple en raison d'un conflit (d'État), entraîne-t-il une perturbation des processus primaires de l'organisation ?

- La fuite de connaissances de haut niveau et d'informations confidentielles :

  Le marché pourrait-il conduire à ce que des connaissances et des informations stratégiques ou sensibles tombent entre des mains étrangères ?
  Par exemple, l'adjudicataire (ou tout sous-traitant) a-t-il besoin d'accéder à des informations sensibles pour effectuer le marché ? Cela inclut : les secrets d'État, les données personnelles et les informations sur l'infrastructure commerciale ou l'infrastructure TIC.
  Le personnel de l'adjudicataire (et/ou ses sous-traitants) aura-t-il accès aux lieux physiquement sensibles du pouvoir adjudicateur ? Pensez aux endroits où des secrets d'État sont utilisés, aux bâtiments des services de renseignement et de sécurité et aux lieux de travail des ministres.
  Le marché crée-t-il la possibilité d'espionnage ? Pensez à l'embauche de personnel des services de renseignement et de sécurité, l'embauche de personnel de sécurité ou la livraison/installation d'imprimantes à un ministre ou secrétaire d'État.

b. Quels sont les instruments disponibles pour couvrir ces risques ?

Divers instruments sont disponibles pour sauvegarder les intérêts de la sécurité nationale dans l'attribution et l'exécution des marchés. Par exemple, des procédures de passation spécifiques, des motifs d'exclusion et la définition d'exigences d'aptitude et de conditions spéciales relatives à l'exécution du marché.

c. Ces instruments sont-ils adéquats par rapport aux risques identifiés ?

Le risque est-il couvert dans la situation actuelle ou y a-t-il une lacune dans les instruments ? S'il existe un risque résiduel, il faut déterminer si ce risque résiduel est acceptable. Cela dépend du marché et du jugement de valeur du risque (résiduel) (probabilité x impact). Par exemple, un marché implique-t-il le remplacement partiel d'un réseau, ce qui signifie que les risques ont un impact moindre, ou le marché implique-t-il un réseau entièrement nouveau, ce qui signifie que l'impact peut être élevé ? C'est un examen qui doit être fait pour chaque marché.

d. Dans quels domaines les risques peuvent-ils survenir ?

(1) La gestion et l'organisation de l'adjudicataire à engager

Les caractéristiques de l'adjudicataire, les changements dans l'actionnariat, la propriété ou le contrôle de son entité juridique, ou la composition de la chaîne d'approvisionnement logistique peuvent affecter les informations sensibles contenues dans le marché. Si les risques existants dans ce domaine ne sont pas suffisamment couverts, une dépendance stratégique vis-à-vis d'un adjudicataire peut survenir.

⇨ L'adjudicataire est-il bien équipé pour les informations avec lesquelles il doit travailler ? Savent-ils quoi faire si des incidents de sécurité se produisent et les sous-traitants répondent-ils également aux exigences de sécurité du marché ? Si ce n'est pas le cas, des informations sensibles peuvent fuir pendant l'exécution du marché.

⇨ En termes de gestion et d'organisation de l'adjudicataire, des risques peuvent-ils survenir si l'entreprise est ouvertement, ou secrètement, dirigée par un État qui pourrait ainsi, via l'entreprise, accroître son emprise géopolitique stratégique et économique ? Dans certains pays, il est inscrit dans la loi que les informations doivent être partagées avec les services de renseignement et de sécurité. En concluant un partenariat avec une telle entreprise, une dépendance stratégique peut survenir,

des informations peuvent fuir ou la continuité de l'approvisionnement/du service peut être mise en danger.

Si ce qui précède ne s'applique pas au futur adjudicataire, cela ne signifie pas qu'aucun risque ne peut survenir. Par exemple, ce dernier peut être repris pendant l'exécution du marché ou les administrateurs peuvent changer. Pensez aussi à une fermeture d'entreprise, un changement de sous-traitants ou une faillite.

(2) L'affectation du personnel

Si le personnel entre en contact avec des informations sensibles, il est nécessaire que des exigences de fiabilité soient définies (par exemple, une habilitation de sécurité). Le cas échéant, cela s'applique à la fois à l'adjudicataire lui-même en tant qu'entité juridique et au personnel de l'adjudicataire (et à sa chaîne d'approvisionnement logistique).

(3) Sécurité physique

Si l'emplacement de l'adjudicataire implique le stockage, le traitement ou le transport d'informations sensibles relatives au marché, que ce soit ou non dans un compartiment désigné à cet emplacement (par exemple, un espace physique dans un bâtiment), cet emplacement ou le compartiment doit également être physiquement sécurisé. Les mesures concernant l'accès physique doivent rendre impossible l'accès non autorisé et, dans tous les cas, signaler les tentatives de le faire en temps opportun (enregistrement, contrôle des laissez-passer, etc.).

(4) Résilience numérique

Outre la sécurité physique, la résilience numérique est également importante et les informations peuvent se retrouver entre de mauvaises mains s'il n'y a pas de politique de « cybersécurité » ou de supervision d'une conception sécurisée de l'infrastructure numérique. Si cela n'est pas contrôlé régulièrement (ex. par un audit), on peut également se demander si une attention suffisante y est accordée pendant la durée du marché. Il est également conseillé de fixer des exigences et de prendre les dispositions nécessaires dans ce domaine.

e. Conclusion

Les conclusions suivantes peuvent être tirées de l'analyse des risques :

- Les risques peuvent être maîtrisés de manière adéquate (par exemple en rédigeant des motifs d'exclusion, des conditions contractuelles ou en déclarant un marché secret).
- Des recherches supplémentaires sont nécessaires pour tirer une conclusion correcte, grâce par exemple à des informations provenant de sources non publiques.

Bijlage II – Quickscan

1. Leeswijzer

De Quickscan bestaat uit een beperkt aantal vragen om snel te kunnen bepalen of een overheidsopdracht een risico vormt voor de nationale veiligheid, of om vast te stellen of er eventueel nader onderzoek nodig is om dit te bepalen. De Quickscan moet worden uitgevoerd voorafgaand aan de lancering van de plaatsingsprocedure, meer bepaald vóór de aankondiging van de opdracht, of vooraleer wordt uitgenodigd tot het indienen van een aanvraag tot deelneming of offerte, in de gevallen waarbij gebruikt wordt gemaakt van de onderhandelingsprocedure zonder voorafgaande bekendmaking. Zodoende kunnen de nodige maatregelen genomen worden als uit de Quickscan naar voren komt dat er risico's zijn voor de nationale veiligheid. De aanbestedende overheid is verantwoordelijk voor het invullen van de Quickscan. In gevallen waarin meerdere overheidsdiensten betrokken zijn bij een aankoop dienen zij allen bij te dragen tot de Quickcan.

Dit document maakt deel uit van een breder instrumentarium aan richtlijnen in dit domein en betreft in se een aanvulling op de richtlijnen en/of procedures die gericht zijn op het identificeren en beheersen van risico's die raken aan de nationale veiligheid en die zich kunnen voordoen tijdens het verwervingsproces. De Toolbox Nationale Veiligheid bij Overheidsopdrachten maakt eveneens deel uit van dit instrumentarium.

Nationale veiligheid

Nationale veiligheid omvat de veiligheid van onze Staat, zijn bevolking en het voortbestaan van onze samenleving, door bescherming te bieden tegen zowel externe als interne dreigingen. Een Nationale Veiligheidsstrategie (NVS)[1] biedt in deze het kader voor de gecoördineerde inzet van alle nationale machtsinstrumenten, om de vitale belangen van het land te beschermen tegen deze dreigingen bij het nastreven van de nationale beleidsdoelstellingen, ongeacht of deze van economische, politieke of sociale aard zijn, of zelfs strikt veiligheid gerelateerd zijn. Het is de federale regering die verantwoordelijk is voor de Belgische NVS.

De NVS, die onlangs is ontwikkeld vanuit een gecoördineerde inspanning vanwege alle nationale veiligheidsactoren, identificeert aldus de volgende vitale belangen van het land:

(1) de rechtsstaat, democratie, weerbaarheid en nationale waarden
(2) de fysieke veiligheid, territoriale integriteit
(3) de leefomgeving
(4) de economische welvaart
(5) de internationale orde
(6) de functionering van de EU

Via een geïntegreerde aanpak is het bijgevolg noodzakelijk dat, ten behoeve van de economische veiligheid en een versterkte Belgische strategische autonomie, maatregelen worden getroffen die onze nationale weerbaarheid (sensu lato)[2] versterken. Men beoogt hierbij onder andere maatregelen:

(1) ter bescherming van de (Europese) economische operatoren;
(2) ter versterking van de strategische autonomie door het diversifiëren van de productie- en aanvoerketens, het aanleggen van strategische voorraden, het bevorderen van productie en/of investeringen binnen Europa enz.;
(3) ter bescherming van intellectuele eigendom en het wetenschappelijke en economisch potentieel;
(4) ter bewustwording van de technologische ontwikkelingen en de dreigingen inzake (economische) spionage, inmenging en/of sabotage die hiermee gepaard gaan.

Rekening houdende met deze vitale belangen zal er dus bij een gedeelte van de verwervingen mogelijks sprake zijn van een nationale veiligheidsdimensie. Of een opdracht een risico vormt voor de nationale veiligheid hangt sterk af van de sector en het type product of dienst dat geleverd wordt, de aanbestedende overheid en de opdrachtnemer. In sommige gevallen is het daarom van belang een goede risicoanalyse te maken. Bij kritieke

[1] Zie hiervoor ook de Nationale Veiligheidsstrategie (NVS) van België van 1 december 2021.
[2] Weerbaarheid van de vitale dienstverlening, klimaatverandering, volksgezondheid, cybersecurity, …

sectoren en kritieke infrastructuur[3] en bij Aanbieders van Essentiële Diensten (AED)[4] treden bijvoorbeeld sneller risico's voor de nationale veiligheid op.

a. Voorbeelden van nationale veiligheidsrisico's

(1) Verstoring van de kritieke infrastructuur

Een verwerving kan ertoe leiden dat de continuïteit van levering, dienstverlening of productie van één van de vitale sectoren in gevaar komt, bv. telecommunicatie of energievoorziening. Uitval of verstoring kan leiden tot ernstige maatschappelijke ontwrichting en vormt bijgevolg een bedreiging voor de nationale veiligheid.

(2) Een strategische (kwetsbare) afhankelijkheid van economische actoren en/of landen met wie België niet dezelfde geopolitieke belangen deelt

Een opdracht kan leiden tot een strategische (kwetsbare) afhankelijkheid van een - al dan niet door een buitenlandse overheid aangestuurde - economische actor of diens onderaannemers. Een dergelijke afhankelijkheid kan vervolgens dan misbruikt worden om bijvoorbeeld politieke druk uit te oefenen op België.

(3) Het verlies van hoogwaardige kennis en gevoelige informatie

Het is mogelijk dat in het kader van de uitvoering van een opdracht een opdrachtnemer of diens onderaannemer toegang verkrijgt tot hoogwaardige kennis en/of gevoelige informatie. Ook de toegang tot hoogwaardige kennis inzake technologische ontwikkelingen is een mogelijkheid. Het risico bestaat er dan in dat deze hoogwaardige kennis en/of gevoelige informatie verloren gaat. Dergelijke gegevens kunnen aldus bijvoorbeeld in landen terechtkomen met wetten die het mogelijk maken dat de inlichtingendiensten van deze landen de gegevens kunnen opvragen en/of inzien.

b. Wanneer is het van belang om een QuickScan uit te voeren?

Indien er bij het opstarten van een verwerving vermoedens van of twijfels over risico's voor de nationale veiligheid bestaan, dient de QuickScan te worden toegepast. De aanbestedende overheid is primair verantwoordelijk voor het beoordelen of er bij een verwerving mogelijk sprake is van een risico voor de nationale veiligheid. De aanbestedende overheid is verantwoordelijk voor het vervolgens beperken van de mogelijke risico's. Hierbij dienen andere betrokken partijen (vb overheidsdiensten die eindgebruiker zijn) uiteraard actief bij te dragen.

c. Wat na de Quickscan?

Indien uit de Quickscan blijkt dat er mogelijk een risico voor de nationale veiligheid verbonden is aan de opdracht, dringt een verdere risicoanalyse zich op om na te gaan welke maatregelen idealiter geïmplementeerd dienen te worden teneinde de geïdentificeerde risico's maximaal te verkleinen (bv. eisen inzake toegangsrecht/uitsluitingsgronden, kwalitatieve selectiecriteria, bijzondere uitvoeringsvoorwaarden enz.).

---

[3] Kritieke infrastructuur = installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken (Art 3, 4° Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren).

[4] Aanbieder van essentiële diensten (AED) = een publieke of private entiteit die actief is in België in een van de sectoren opgenomen in bijlage I aan de Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en die aan de criteria bedoeld in artikel 12, §1, voldoet en die als dusdanig is aangewezen door de sectorale overheid (Art 6, 11° Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid). Het zijn entiteiten die essentiële diensten verlenen aan onze maatschappij of economie en die afhankelijk zijn van netwerk- en informatiesystemen. Het is belangrijk dat deze netwerk- en informatiesystemen (NIS) beveiligd zijn.

.

Eigenlijke Quickscan

Dit formulier is bedoeld om voor de lancering van de plaatsingsprocedure te beoordelen of er zich risico's voor de nationale veiligheid voordoen. De QuickScan dient in een zo vroeg mogelijk stadium te worden uitgevoerd, zodat de nodige maatregelen genomen kunnen worden als uit deze QuickScan zou blijken dat er wel degelijk risico's bestaan voor de nationale veiligheid. De aanbestedende overheid is verantwoordelijk voor het invullen van de QuickScan.

QUICKSCAN		
		Toelichting
1. Vitale belangen, processen en sectoren Raakt de verwerving aan een vitale sector, belang of proces? *Zie Par 1.1 voor het overzicht van de vitale belangen en sectoren.*	☐ Ja/Mogelijk ☐ Neen	
2. Strategische afhankelijkheid Ontstaat er door de verwerving een sterke afhankelijkheid van een – al dan niet door een buitenlandse overheid aangestuurde – economische actor of diens onderaannemers, waardoor bij een conflict de mogelijkheid bestaat dat de opdrachtgever door de opdrachtnemer onder druk kan worden gezet (al dan niet in opdracht van een buitenlandse overheidsactor)? *Een strategische afhankelijkheid kan bijvoorbeeld ontstaan wanneer de opdracht een product of dienst betreft waarvoor maar weinig opdrachtnemers op de markt beschikbaar zijn, of wanneer plotselinge beëindiging van een levering, bijvoorbeeld door een (statelijk) conflict, tot verstoring leidt in de primaire processen van een organisatie.*	☐ Ja/Mogelijk ☐ Neen	
3. Toegang tot geclassificeerde informatie Heeft de opdrachtnemer (of diens onderaannemers) toegang nodig tot geclassificeerde informatie voor het uitvoeren van een opdracht? *Zie Par 1.2 voor verdere toelichting over geclassificeerde informatie.*	☐ Ja/Mogelijk ☐ Neen	
4. Toegang tot gevoelige informatie Heeft de opdrachtnemer (of diens onderaannemers) toegang nodig tot gevoelige informatie voor het uitvoeren van een opdracht?	☐ Ja/Mogelijk ☐ Neen	

Zie Par 1.3 voor verdere toelichting over gevoelige informatie.		
5. Toegang tot een gevoelige locatie Krijgt het personeel van de opdrachtnemer (of diens onderaannemers) toegang tot fysieke gevoelige locaties van de opdrachtgever? *Zie Par 1.4 voor verdere toelichting over gevoelige locaties*	☐ Ja/Mogelijk ☐ Neen	
6. Spionage en/of sabotage Ontstaat door de verwerving een risico op technische surveillance, afluisteren, spionage en/of sabotage? *Zie Par 1.5 voor verdere toelichting over spionage*	☐ Ja/Mogelijk ☐ Neen	
Indien 'ja/mogelijk' is geantwoord bij één van de voorgaande vragen:		
7. Inzet van onderaannemers Ontstaat er bij de uitvoering van de opdracht een situatie, waarin de opdrachtnemer de bevoegdheid heeft nieuwe/andere onderaannemers voor de uitvoering van de opdracht in te zetten?	☐ Ja/Mogelijk ☐ Neen	

CONCLUSIE	
Ja/Mogelijk	**Neen**
Indien op één van de bovenstaande vragen 'ja/mogelijk' is geantwoord, zijn er mogelijke risico's voor de nationale veiligheid en is een grondige Risicoanalyse de volgende stap. In een Risicoanalyse wordt uitgebreider stilgestaan bij het identificeren van de risico's voor de nationale veiligheid en wordt gekeken of en hoe risico's kunnen worden gemitigeerd ⇨ het voorzien van maatregelen in de selectiefase (uitsluitingsgronden/toegangsrecht, kwalitatieve selectiecriteria, het kiezen van de juiste plaatsingsprocedure/gunningswijze of het formuleren van bijzondere uitvoeringsvoorwaarden). *Zie in onderstaande tabel, punt 1.6 voor een meer informatie over de risicoanalyse.*	Indien er alleen 'neen' geantwoord is, kan de verwerving worden voortgezet zonder extra maatregelen in het kader van de nationale veiligheid.

1. Overzicht van vitale belangen, processen en sectoren

De vitale belangen en sectoren die in aanmerking moeten worden genomen zijn de volgende:

- de rechtsstaat, democratie, weerbaarheid en nationale waarden
- de fysieke veiligheid, territoriale integriteit
- de leefomgeving
- de economische welvaart
- de internationale orde
- de functionering van de EU
- energie
- vervoer
- financiën
- drinkwater
- gezondheid
- digitale infrastructuur
- elektronische communicatie
- ruimtevaart

Binnen deze vitale belangen moet gekeken worden naar de vitale processen die nodig zijn voor het vrijwaren van deze belangen. Niet elke overheidsactiviteit in diensten wiens actiedomein raakt aan vitale belangen is vitaal. Zo is bijvoorbeeld de aankoop van software voor het beheer van politiedatabanken wel een vitaal proces, maar het pensioenfeest van de politie niet.

De inschatting van wat vitale processen zijn binnen de overheidsdienst, ligt bij de overheidsdienst zelf. Overheidsdiensten kunnen eventueel de business continuity plannen die reeds bestaan binnen de overheidsdienst gebruiken voor deze evaluatie.

2. Geclassificeerde informatie

Geclassificeerde informatie: “Gegevens of materiaal, ongeacht de vorm, aard of transmissiemethode ervan, waaraan een bepaald niveau van veiligheidsclassificatie of een beveiligingsniveau is toegekend en die in het belang van de nationale veiligheid en overeenkomstig de wettelijke en bestuursrechtelijke bepalingen die in een lidstaat gelden, bescherming vereisen tegen ontvreemding, vernietiging, verwijdering, onthulling, verlies of toegang ertoe door een onbevoegd persoon, of tegen enige andere vorm van compromittering.” [5]

In België zijn er actueel drie (3) beveiligingsniveaus of niveaus van veiligheidsclassificatie[6] :

VERTROUWELIJK
GEHEIM
ZEER GEHEIM
Het classificatieniveau wordt bepaald op basis van de inhoud. Andere landen of internationale organisaties hebben vaak ook nog een lager, vierde classificatieniveau (bv. EU/NAVO RESTRICTED).

3. Gevoelige informatie

Hiermee wordt informatie bedoeld die niet geclassificeerd is in de zin van de wet van 11 december 1998, maar die wel gevoelig is.

Ook informatie die niet geclassificeerd is kan van strategisch belang zijn als deze informatie ongewenst in verkeerde handen valt en/of ertoe kan leiden dat derden zich kunnen mengen in de besluitvorming.

[5] Artikel 3, 19° Wet Defensie en Veiligheid 2011
[6] Art 4 van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

Denk aan de paraatheid van het leger door informatie over verschillende locaties of meer inzicht in de werking van organisaties die vitale diensten leveren.

Denk bijvoorbeeld ook aan informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer federale overheidsdiensten.

4. Gevoelige locaties

Denk hierbij aan:

- locaties waar gewerkt wordt met geclassificeerde of gevoelige informatie;
- gebouwen van de inlichtingen- en veiligheidsdiensten;
- werkplekken van politieke mandatarissen;
- werkplekken van rechtsprekende instanties;
- werkplekken van personen in sleutelfuncties.

5. Spionage of sabotage

Bepaalde opdrachten kunnen een verhoogd risico op spionage of sabotage inhouden. Denk bijvoorbeeld aan:

- het leveren van IT-infrastructuur op een kabinet van een minister;
- de installatie van printers bij een staatssecretaris;
- het aanstellen van beveiligingspersoneel.

6. Risicoanalyse

Wanneer uit de Quickscan blijkt dat deze risico's er zijn, of dat er aanvullend onderzoek nodig is, wordt geadviseerd om een risicoanalyse uit te voeren. In een risicoanalyse wordt precies vastgesteld welke risico's er zijn en hoe kan worden gehandeld om deze risico's te mitigeren. Onderstaande is bedoeld als hulpmiddel voor de behoeftestellende partij.

Bij de risicoanalyse wordt stilgestaan bij de volgende nationale veiligheidsbelangen:

- continuïteit van de vitale infrastructuur;
- strategische onafhankelijkheid van partijen en landen met wie ons land niet dezelfde geopolitieke belangen deelt;
- integriteit en exclusiviteit van hoogwaardige kennis en vertrouwelijke informatie (staatsgeheimen, BE-persoonsgegevens, gevoelige technologische kennis).

a. Welke reële risico's voor de nationale veiligheid kunnen ontstaan door de opdracht ?

- Verstoring van de continuïteit van de vitale infrastructuur:
  Is er een risico dat de opdracht ertoe leidt dat de continuïteit van levering, dienstverlening of productie van vitale processen in gevaar komt?

- Een strategische afhankelijkheid van partijen en landen met wie ons land niet dezelfde geopolitieke belangen deelt:
  Ontstaat er door de opdracht een sterke strategische afhankelijkheid van een – al dan niet door een buitenlandse overheid aangestuurde – marktpartij of diens onderaannemers, waardoor bij een conflict de mogelijkheid bestaat dat de

opdrachtgever door de opdrachtnemer onder druk kan worden gezet (al dan niet in opdracht van een buitenlandse overheidsactor)?

Dit is met name relevant wanneer een product of dienst, betrekking heeft op de nationale veiligheid. Betreft de opdracht bijvoorbeeld een product of dienst waarvoor maar weinig ondernemers op de markt beschikbaar zijn of leidt plotselinge beëindiging van levering, bijvoorbeeld door een (statelijk) conflict, tot verstoring in primaire processen van de organisatie?

- Het weglekken van hoogwaardige kennis en vertrouwelijke informatie:
  Kan de opdracht ertoe leiden dat strategische of gevoelige kennis en informatie ongewenst in buitenlandse handen valt?
  Heeft de ondernemer (of een eventuele onderaannemer) bijvoorbeeld toegang nodig tot gevoelige informatie voor het uitvoeren van de opdracht? Denk hierbij aan: staatsgeheime informatie, persoonsgegevens en informatie over bedrijfsinfrastructuur of ICT-infrastructuur.
  Krijgt het personeel van de opdrachtnemer (en/of diens onderaannemers) toegang tot fysieke gevoelige locaties van de opdrachtgever? Denk aan locaties waar gewerkt wordt met staatsgeheime informatie, gebouwen van de inlichtingen- en veiligheidsdiensten en werkplekken van bewindspersonen.
  Ontstaat er door de opdracht de mogelijkheid op spionage? Denk aan inhuur van personeel bij de inlichtingen- en veiligheidsdiensten, inhuur van beveiligingspersoneel of de levering/installatie van printers aan een minister of staatssecretaris.

b. Welke instrumenten zijn beschikbaar om deze risico's af te dekken?

Om nationale veiligheidsbelangen bij het gunnen van opdrachten en de uitvoering ervan te kunnen waarborgen, zijn verschillende instrumenten beschikbaar. Bijvoorbeeld specifieke plaatsingsprocedures, uitsluitingsgronden en het stellen van geschiktheidseisen en bijzondere voorwaarden voor de uitvoering van de opdracht.

c. Zijn deze instrumenten afdoende in verhouding tot de onderkende risico's?

Is het risico in de huidige situatie afgedekt of is er sprake van een lacune in het instrumentarium? Als er een restrisico is, moet worden bepaald of dit restrisico acceptabel is. Dit hangt af van de opdracht en het waardeoordeel van het (rest)risico (waarschijnlijkheid x impact). Betreft een opdracht bijvoorbeeld de gedeeltelijke vervanging van een netwerk waardoor risico's minder impact hebben, of betreft de opdracht een volledig nieuw netwerk waardoor de impact groot kan zijn? Dit is een afweging die per opdracht moet worden gemaakt.

d. In welke domeinen kunnen zich risico's voordoen?

(1) Het bestuur en de organisatie van de te contracteren opdrachtnemer

Kenmerken van de opdrachtnemer, wijzigingen in aandeelhouderschap, eigendom of zeggenschap in diens rechtspersoon, of de samenstelling van de logistieke toeleveringsketen, kunnen van invloed zijn op de in de opdracht aanwezige gevoelige informatie. Indien aanwezige risico's op dit gebied niet voldoende zijn afgedekt, kan er een strategische afhankelijkheid van een opdrachtnemer ontstaan.

⇨ Is de opdrachtnemer goed ingericht voor de informatie waar ze mee moet werken? Weten ze wat ze moeten doen als beveiligingsincidenten zich voordoen en voldoen ook de onderaannemers aan de beveiligingseisen van de opdracht? Indien dit niet het geval is, kan er tijdens de uitvoering van de opdracht gevoelige informatie weglekken.

⇨ Kunnen er op het gebied van het bestuur en de organisatie van de opdrachtnemer risico's ontstaan wanneer het bedrijf openlijk of verborgen wordt gestuurd door een staat, waardoor via het bedrijf de geopolitieke strategische en economische macht vergroot kan worden? In sommigen landen is het in de wet verankerd dat er informatie gedeeld moet worden met inlichtingen- en veiligheidsdiensten. Door de samenwerking met een dergelijk bedrijf aan te gaan, kan een strategische afhankelijkheid ontstaan, kan informatie weglekken, of kan de continuïteit van de levering/dienstverlening in gevaar komen.

Indien bovenstaande niet van toepassing is op de toekomstige opdrachtnemer, betekent het niet dat er geen risico meer kan ontstaan. Deze kan bijvoorbeeld tijdens de uitvoering van de opdracht worden overgenomen, of de bestuurders kunnen wisselen. Denk ook aan een bedrijfsbeëindiging, wisseling in onderaannemers of een faillissement.

(2) De inzet van personeel

Als het personeel in aanraking komt met gevoelige informatie is het noodzakelijk dat betrouwbaarheidseisen worden gesteld (bv. veiligheidsmachtiging). Dit geldt desgevallend zowel voor de opdrachtnemer zelf als rechtspersoon, als voor het personeel van de opdrachtnemer (en diens logistieke toeleveringsketen).

(3) Fysieke beveiliging

Als op de locatie van de opdrachtnemer sprake is van de opslag, de verwerking of het transport van gevoelige informatie met betrekking tot de opdracht, al dan niet in een daartoe aangewezen compartiment op die locatie (bijvoorbeeld een fysieke ruimte in een gebouw), zal die locatie of het compartiment ook fysiek beveiligd moeten worden. Maatregelen in verband met fysieke toegang moeten onrechtmatige toegang onmogelijk maken en pogingen daartoe in elk geval tijdig aan het licht brengen (registratie, pascontrole …).

(4) Digitale weerbaarheid

Naast fysieke beveiliging is ook digitale weerbaarheid van belang en kan informatie in verkeerde handen komen als er geen beleid is in verband met 'cybersecurity' of als er geen toezicht wordt gehouden op een veilige inrichting van de digitale infrastructuur. Als dit niet regelmatig gecontroleerd wordt (bv. audit), rijst bovendien de vraag of hier gedurende de looptijd van de opdracht voldoende aandacht aan wordt besteed. Ook op dit gebied is het aan te raden om eisen te stellen en afspraken te maken.

e. Conclusie

De volgende conclusies kunnen uit de risicoanalyse komen:

- De risico's kunnen voldoende worden beheerst (bijvoorbeeld door het opstellen van uitsluitingsgronden, contractvoorwaarden of door een opdracht geheim te verklaren).
- Er is aanvullend onderzoek nodig om een juiste conclusie te kunnen trekken, zoals bijvoorbeeld onderzoek op basis van informatie uit niet-openbare bronnen.