



## **Annexe de Sécurité (SAL)**

### **Annexe I.L du Cahier des charges et Annexe IX du Contrat-cadre GSA/OP/05/17**

Participants:



## Sommaire

<b>1. Introduction</b>	<b>3</b>
<b>2. Classification du Contrat</b>	<b>4</b>
<b>3. Instructions de Sécurité concernant l'Information Classifiée</b>	<b>4</b>
<b>4. Accès aux locaux de la GSA et des autres parties au contrat</b>	<b>13</b>
<b>5. Document applicables et références</b>	<b>16</b>



## 1. Introduction

Ce document constitue l'Annexe de Sécurité (en anglais « Security Aspects Letter » ou SAL) applicable au Contrat GSA-OP-05-17. Elle définit les conditions de sécurité requises par la GSA dans le cadre de ce Contrat. Ces conditions font partie intégrante du Contrat, en vertu duquel des informations classifiées sont susceptibles d'être transmises ou produites.

Ce document identifie les éléments du Contrat qui comportent des informations classifiées, soumises à protection particulière, et identifie les exigences essentielles de sécurité. Conformément au Règlement précisant les règles de sécurité applicables au Pouvoir adjudicateur (AD1), ce dernier a l'obligation de protéger cette information classifiée en accord avec les termes de la Décision de la Commission européenne (EU, Euratom) 2015/444 (AD4). Cette obligation de protection est assurée par le biais de l'application de cette SAL au présent contrat. Cette SAL s'applique à toute entité juridique engagée dans une activité contractuelle ou précontractuelle au travers du présent Contrat.

L'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») est l'Autorité de Sécurité chargée d'assurer le respect de la Décision de la Commission européenne (EU, Euratom) 2015/444 (AD4). Les modes de communication entre le Contractant et l'AAI doivent être communiqués au Contractant par le Pouvoir adjudicateur.

Ce document inclut en annexe un Guide de la Classification de Sécurité (« *Security Classification Guide* »— SCG), décrivant les éléments classifiés du Contrat Cadre et de ses Contrats Spécifiques et précise les niveaux de sécurité ainsi que les marquages applicables par le Contractant (ainsi que tous les membres du consortium le cas échéant) et ses sous-traitants éventuels, lors de la production de délivrables issus de la mise en œuvre de ces contrats. Le contenu du SCG étant basé sur le « *GNSS Programme Security Classification Guide* » (RD 2), document régulièrement mis à jour afin de prendre en compte les évolutions du Programme GNSS en matière de sécurité, la version communiquée en annexe de la présente est susceptible d'être mise à jour durant toute la durée du Contrat, impliquant des exigences de reclassification ou déclassification.

Ce document est destiné à fournir un aperçu des exigences essentielles de sécurité que le Contractant (ainsi que tous les membres du consortium le cas échéant) et ses sous-traitants éventuels doivent mettre en œuvre. Ces dispositions de sécurité, fondées sur l'instruction de sécurité relative au Programme du GNSS européen (« *European GNSS Programme Security Instruction* » ou « *European GNSS PSI* ») (AD2) précisent les exigences de sécurité applicables à un contrat spécifique. L'instruction de sécurité « *European GNSS PSI<sup>1</sup>* » (AD2) doit être considérée comme un document applicable au Contrat Cadre et à ses Contrats Spécifiques, fournissant les directives du Programme du GNSS européen quant à l'interprétation et l'application des mesures de sécurité figurant dans la Décision de la Commission 2015/444 et plus particulièrement dans son Chapitre 6, relatif à la sécurité industrielle.

Dans les cas où les dispositions législatives et réglementaires nationales diffèrent des dispositions de la présente

<sup>1</sup> Voir paragraphe 6 "Documents applicables".



SAL, les dispositions législatives et réglementaires nationales peuvent être appliquées à condition de ne pas être moins strictes que les dispositions énoncées dans la SAL. Dans une telle hypothèse, le Contractant (ainsi que tous les membres du consortium le cas échéant) doit porter à la connaissance de l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») les procédures de sécurité modifiées.

Le GSA est responsable de l'approbation de cette SAL et de ses éventuelles modifications. De telles modifications, opérées par la GSA en conformité avec de nouvelles exigences et en particulier celles émanant de la législation applicable, de l'instruction de sécurité relative au Programme du GNSS européen (« *European GNSS Programme Security Instruction* » ou « *European GNSS PSI* ») (AD2) ou du Guide de la Classification de Sécurité (« *Security Classification Guide* » – SCG), deviennent parties intégrantes du Contrat et applicables au Contractant dès leur communication par la GSA.

Ce document ne s'applique qu'aux activités, requises en application du Contrat Cadre et au travers des Contrats Spécifiques, dont la réalisation nécessite :

- la consultation ou la production d'Informations Classifiées.
- l'accès à des zones sécurisées dans lesquelles des Informations Classifiées sont immédiatement accessibles, jusqu'au niveau SECRET UE.

## 2. Classification du Contrat

En référence à la Décision (UE, Euratom) 2015/444, le niveau général de classification de sécurité du Contrat s'élève au niveau SECRET UE/EU SECRET, compte tenu du fait que le personnel du Contractant est en mesure d'accéder à des zones de sécurité accréditées au niveau SECRET UE/EU SECRET, d'escorter, d'avoir accès ou de fournir des informations ou matériels classifiés jusqu'au niveau SECRET UE/EU SECRET.

## 3. Instructions de Sécurité concernant l'Information Classifiée

### 3.1 Applicabilité

- [REQ A.1] Le Contractant (ainsi que tous les membres du consortium le cas échéant) doit, sous peine de résiliation du contrat, se conformer aux exigences de sécurité prescrites par le Pouvoir adjudicateur telles que détaillées dans la présente SAL.
- [REQ A.2] L'instruction de sécurité « European GNSS PSI » (AD2) doit être considérée comme un document applicable au présent Contrat Cadre et tout Contrat Spécifique qui en résulte. Ce document fournit aux programmes européens de GNSS des instructions sur l'interprétation et l'application des règles de sécurité établies dans la Décision de la Commission 2015/444 et plus particulièrement dans son Chapitre 6 relatif à la sécurité industrielle.



- [REQ A.3] Les documents cités à l'article 6 (Documents Applicables – AD 1, AD 3, AD 4 et AD 5), considérés dans leur dernière version, sont applicables au Contractant (ainsi qu'à tous les membres du consortium le cas échéant) et aux sous-traitants, en vertu de leur applicabilité à leur Autorité Nationale de Sécurité (ANS) par le biais de l'appartenance de l'Etat-membre de cette ANS au Conseil européen ou dans le cadre d'un accord international avec l'Union européenne. Les principes de sécurité qu'ils contiennent régissent l'exécution du contrat.

### 3.2 Contrats et sous-traitance

- [REQ B.1] La responsabilité ultime de la protection des informations classifiées au sein des entités, industrielles ou autres, incombe à la Direction de ces entités.
- [REQ B.2] l'Autorité Nationale de Sécurité (ANS) ou l'Autorité de Sécurité Désignée (ASD) du Contractant (ainsi que tous les membres du consortium le cas échéant) sera informée par le Contractant et par la GSA, de manière séparée, de la date d'attribution du Contrat classifié dans un délai d'un mois à compter de cette attribution.
- [REQ B.3] A l'expiration du Contrat classifié, le Contractant (ainsi que tous les membres du consortium le cas échéant) et la GSA communiquent séparément cette expiration dans un délai d'un mois à l'ANS/ASD compétente.
- [REQ B.4] Il peut être nécessaire pour le Contractant (ainsi que tous les membres du consortium le cas échéant) de négocier des contrats de sous-traitance classifiés à différents niveaux. Le Contractant (ainsi que tous les membres du consortium le cas échéant) est responsable de s'assurer que toute sous-traitance et toute activité des sous-traitants sont menées en conformité avec les normes minimales communes figurant dans la présente SAL. Les procédures visant la sous-traitance contenue dans le document « European GNSS PSI » (AD2) sont appliquées par le Contractant (ainsi que tous les membres du consortium le cas échéant) à tous les contrats de sous-traitance potentiels.
- [REQ B.5] Lorsque le Contractant (ainsi que tous les membres du consortium le cas échéant) attribue un contrat de sous-traitance classifié dans le cadre du présent Contrat, le Contractant (ainsi que tous les membres du consortium le cas échéant) doit informer son Autorité Nationale de Sécurité (ANS/ASD) compétente et la GSA de cette attribution dans un délai d'un mois à compter de cette attribution.
- [REQ B.6] A l'expiration du Contrat de sous-traitance classifié, le Contractant (ainsi que tous les membres du consortium le cas échéant) doit informer son Autorité Nationale de Sécurité (ANS/ASD) compétente et la GSA de cette expiration dans un délai d'un mois.
- [REQ B.7] Une Annexe de sécurité (SAL) et un guide de classification de sécurité (SCG) doivent faire partie de tout contrat de sous-traitance classifiée. La SAL doit décrire les éléments classifiés et spécifier les niveaux de classification de sécurité applicables. Les dispositions de la SAL et du SCG appliquées à ces sous-traitants ne doivent pas être moins strictes que celles applicables au Contractant (ainsi que tous les membres du consortium le cas échéant) dans le cadre du Contrat.



### 3.3 Certification de sécurité, accréditation, habilitations et gestion des incidents de sécurité

- [REQ C.1] Toute entité participant à des activités en vertu de, ou en relation avec le Contrat classifié, qui impliquent l'accès à des informations de classification CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieure, doit détenir une Habilitation de Sécurité d'Etablissement (HSE) de niveau correspondant. Cette habilitation est délivrée par l'ANS/ASD de l'État membre dans lequel il se trouve, confirmant que ses installations peuvent assurer et garantir la protection adéquate de la sécurité des informations classifiées jusqu'au niveau de classification approprié. Les questions concernant les HSE doivent être adressées à l'ASN/ASD de l'Etat concerné, dont les détails peuvent être trouvés dans le document « European GNSS PSI » (AD2).
- [REQ C.2] Toute entité participant à des activités en vertu de, ou en relation avec le Contrat classifié, qui impliquent l'accès à des Informations Classifiées, ne doit en donner accès à son personnel que dans les conditions visées à l'Article 17(c) et 17(d) de AD 6. Lorsque l'Article 17(d) de AD 6 est invoqué, l'Autorité de sécurité (ASN/ASD) de l'entité doit confirmer cette situation et l'entité concernée doit la notifier à la GSA préalablement à l'accès aux Informations Classifiées. Dans de telles circonstances, la GSA, en consultation avec la Commission européenne<sup>2</sup>, se réserve le droit, sur la base de motifs justifiables, de demander à l'entité de refuser l'accès au personnel concerné.
- [REQ C.3] Tout personnel qui a accès en vertu du présent Contrat à des Informations Classifiées de l'Union européenne jusqu'au niveau SECRET UE / EU SECRET, doit être titulaire d'une Habilitation de Sécurité du Personnel (HSP) de niveau SECRET UE / EU SECRET délivrée par un participant du Programme de GNSS européen<sup>3</sup> (les Etats membres de l'UE et, lorsqu'ils sont éligibles pour l'accès aux contrats GNSS, les citoyens de Norvège et de Suisse) permettant cet accès pour la durée de mise en œuvre du Contrat.
- [REQ C.4] Le Contractant (ainsi que tous les membres du consortium le cas échéant) et les sous-traitants ne doivent donner accès aux Informations Classifiées PRS qu'aux personnes physiques effectuant des tâches pour le Contractant (ainsi que tous les membres du consortium le cas échéant) et les sous-traitants dument autorisés à accéder à l'Information Classifiée conformément à la législation applicable, aux règlements listés en Section 6.1 (et en particulier dans AD 5) et seulement lorsque cet accès est justifié nécessaire à l'accomplissement des tâches du Contrat.
- [REQ C.4.1] Le Contractant (ainsi que tous les membres du consortium le cas échéant) et les sous-traitants donnant accès à une Information Classifiée PRS peuvent être amenés (sur demande) à rendre compte à leur Autorité PRS compétente des motifs ayant justifié un tel accès. Ils doivent, à cette fin, conserver des enregistrements internes appropriés.

<sup>2</sup> Au titre d'Autorité de Sécurité des Programmes GNSS (AD 6 Article 13.1)

<sup>3</sup> A noter que l'Agence spatiale européenne est un participant du Programme de GNSS européen, mais ne délivre pas d'habilitations de sécurité



[REQ C.5] Le Contractant (ainsi que tous les membres du consortium le cas échéant) est responsable de la bonne compréhension des certifications de sécurité et/ou d'accréditation de l'ensemble des membres du consortium, le cas échéant, et des sous-traitants impliqués dans l'exécution du Contrat. Toute modification doit être notifiée à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI »). Lorsqu'une certification de sécurité et/ou d'accréditation requise pour la mise en œuvre du Contrat est perdue, La GSA peut résilier le Contrat avec effet immédiat, conformément aux dispositions du Contrat) et sans préjudice d'éventuelles procédures pénales et civiles contre le Contractant (ainsi que tous les membres du consortium le cas échéant) et ses sous-traitants. Néanmoins, si il est possible pour le Contractant (ainsi que tous les membres du consortium le cas échéant) de remédier à une telle situation, les options envisagées devront être présentées à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») et agréées avec la GSA afin d'éviter la résiliation du Contrat. En particulier :

[REQ C.5.1] Si l'Habilitation de Sécurité d'Etablissement (HSE) du Contractant (ainsi que tous les membres du consortium le cas échéant) ou d'un sous-traitant est retirée par l'Autorité de sécurité (ASN/ASD), l'Autorité PRS ou par le *GNSS Security Accreditation Board*, le Contractant, membre du consortium ou sous-traitant doit immédiatement en référer à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») par l'intermédiaire du Responsable local de la Sécurité de la GSA.

[REQ C.5.2] Si l'autorisation d'accès au PRS du Contractant (ainsi que tous les membres du consortium le cas échéant) ou d'un sous-traitant, requise pour l'exécution du Contrat, est retirée par l'Autorité de sécurité (ASN/ASD), l'Autorité compétente PRS ou par le *GNSS Security Accreditation Board*, le Contractant, membre du consortium ou sous-traitant, doit immédiatement en référer à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») par l'intermédiaire du Responsable local de la Sécurité de la GSA.

[REQ C.5.3] Lorsqu'un membre du consortium ou un sous-traitant perd une certification de sécurité ou accréditation requises pour l'exécution du Contrat, la GSA est fondée à réclamer respectivement au Contractant (ainsi qu'à tous les membres du consortium le cas échéant) la révision de la composition du consortium ou la résiliation du contrat de sous-traitance avec effet immédiat et sans préjudice du droit de la GSA à résilier le Contrat avec effet immédiat.

[REQ C.6] Tout au long de la durée du contrat classifié, la conformité à toutes les dispositions de sécurité doit être contrôlée par l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI »). Tout incident de sécurité affectant cette conformité doit être signalé par le Contractant (ou par tout membre du consortium le cas échéant) à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») . Cet incident sera analysé puis communiqué conformément aux dispositions prévues par le document « European GNSS PSI » (AD2).



- [REQ C.6.1] Lorsque le Contractant (ou le membre du consortium le cas échéant) met en place des contrats de sous-traitance dans le cadre de la mise en œuvre du Contrat, le Contractant (ou le membre du consortium le cas échéant) doit établir un processus clair et efficient de gestion des incidents de sécurité en mesure de traiter l'identification, le confinement, l'investigation et le compte rendu des incidents de sécurité résultant des activités sous-traitées du Contrat et affectant la conformité avec la présente SAL.
- [REQ C.6.2] Les incidents de sécurité doivent être gérés par le Contractant (ou le membre du consortium le cas échéant) conformément aux dispositions prévues par le document « European GNSS PSI » (AD2).
- [REQ C.6.3] Tout incident de sécurité affectant la conformité avec la présente SAL doit être signalé sans délais et sous 72 heures maximum par le Contractant (ou le membre du consortium le cas échéant) à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») par l'intermédiaire du Responsable local de la Sécurité de la GSA .
- [REQ C.6.4] Le Contractant (ainsi que tous les membres du consortium le cas échéant) et tout sous-traitant doit classifier les rapports d'incident de sécurité au niveau approprié et les communiquer en conséquent. En cas de classification du rapport supérieure à RESTREINT UE/EU RESTRICTED, un rapport expurgé autorisant une classification de niveau RESTREINT UE/EU RESTRICTED ou au-dessous devra être généré par l'entité émettrice afin de permettre la transmission rapide par les moyens et outils de communication adaptés de l'existence de l'incident à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») .
- [REQ C.6.4.1] En outre, l'entité émettrice devra observer les procédures nationales en vigueur relatives aux incidents de sécurité, lorsque requises par l'Autorité de sécurité (ASN/ASD). Dans ce cas, l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») doit être informé de la mise en œuvre de ces procédures nationales et une référence appropriée lui sera communiquée en vue d'échanger avec l'Autorité de sécurité (ASN/ASD) si besoin.

### 3.4 Manipulation de l'Information Classifiée

- [REQ D.1] Les Informations Classifiées communiquées au Contractant (ainsi que tous les membres du consortium le cas échéant) et ses sous-traitants, ou générées par toute activité prévue ou liée au Contrat, ne doivent pas être utilisées à des fins autres que celles définies par le Contrat classifié correspondant et ne peuvent être communiquées à des tiers sans l'accord préalable écrit de l'émetteur et de la GSA.



[REQ D.2] L'information générée par le Contractant (ainsi que part tout membre du consortium le cas échéant) et par chaque sous-traitant et qui nécessite d'être classifiée doit être identifiée à l'aide des marquages de classification de sécurité listés dans le document « European GNSS PSI » (AD2), avec une préférence pour l'utilisation du marquage de classification de sécurité de l'UE lorsque cette Information Classifiée est susceptible d'être communiquée à la GSA. Lorsque requis, un marquage CRYPTO ou CCI doit être ajouté en conformité avec l'Instruction de sécurité COMSEC Galileo (AD 3).

[REQ D.2.1] L'Information Classifiée PRS générée par le Contractant (ainsi que part tout membre du consortium le cas échéant) et par un sous-traitant doit être clairement identifiée comme telle par l'apposition de la phrase : « **Ce document contient de l'Information Classifiée PRS** » sur la page de couverture. Lorsque seule une partie du document contient de l'Information Classifiée PRS, les sections, paragraphes, images ou clauses concernées doivent être marquées en conséquent avec la marque « [PRS] » précédent le début de l'information concernée<sup>4</sup>.

[REQ D.3] Le marquage de toute information classifiée devant être générée par le Contractant (ainsi que tous les membres du consortium le cas échéant) et ses sous-traitants devra (chaque fois qu'il sera possible et réalisable de faire ainsi) être envisagé et attribué avant de produire cette information sous une forme enregistrée. Le SCG fourni avec cette SAL devra être utilisé comme une aide par le Contractant (ainsi que tous les membres du consortium le cas échéant) et chacun de ses sous-traitants pour décider du marquage de chaque information qu'ils génèrent.

[REQ D.3.1] Dans le cas où un marquage attribué par le Contractant (ainsi que part tout membre du consortium) et chacun de ses sous-traitants, diffère du marquage spécifié ou sous-entendu par le SCG (et quand aucune autorisation préalable de la GSA d'utiliser un autre marquage n'existe), le Contractant (ainsi que tous les membres du consortium le cas échéant) et chacun de ses sous-traitants devront fournir une justification écrite du marquage envisagé pour examen et approbation par la GSA<sup>5</sup>.

[REQ D.3.1.1] En attendant la réponse de la GSA, l'information devra, soit ne pas être produite sous forme enregistrée, soit être classifiée tel que spécifié dans la SCG et chaque partie devra la traiter en conséquence jusqu'à ce que la GSA décide du niveau de classification final à attribuer et communique celui-ci par écrit au Contractant (ainsi que tous les membres du consortium le cas échéant).

[REQ D.4] le Contractant (ainsi que tous les membres du consortium le cas échéant) et chacun de ses sous-traitants devra traiter et protéger l'information classifiée et les moyen qui leurs sont fournis ou générés par eux, dans le but de remplir ce contrat en accord avec le marquage attribué à ces moyens comme décrit dans l'instruction de sécurité « European GNSS PSI » (AD2) ou, à la condition qu'elle

<sup>4</sup> Par exemple en début de paragraphe, dans une diapositive/graphique/tableau/diagramme/schéma titre... etc. Quand la totalité du document est lié à des informations PRS, aucune mention n'est nécessaire car cela sera présumé du fait du marquage sur le titre/page de couverture du document.

<sup>5</sup> GSA ne doit communiquer sur les demandes de marquage avec les sous-traitants que si il existe une justification claire que le Contractant principal ou certain membre particuliers du consortium) n'ont pas le besoin d'en connaître.



ne soient pas moins strictes, selon les règles nationales applicables au Contractant (ainsi qu'à tout membre du consortium) ou ses sous-traitants.

[REQ D.4.1] Dans le cas où, un marquage diffère du marquage du programme défini dans la L'instruction de sécurité « European GNSS PSI » (AD2) et dans les instructions « European COMSEC GNSS » (A3), alors l'information et le matériel devront être traités tel que prévu dans la L'instruction de sécurité « European GNSS PSI » (AD2) et dans les instructions « European COMSEC GNSS » (A3) et chaque fois que cela sera possible d'un point de vue pratique, le marquage devra être révisé en conséquence.<sup>6</sup>

[REQ D.5] Le Contractant, (ainsi que tous les membres du consortium et les sous-traitants le cas échéant) ne devront pas transférer (c'est-à-dire transporter ou transmettre) une quelconque information classifiée à un sous-traitant ou une entité extérieure aux participants du Contrat sans l'accord préalable écrit de l'autorité d'origine et de l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI »). De façon à éviter toute perturbation dans l'exécution des activités contractuelles résultant de la mise en œuvre de ces exigences sur la base du cas par cas, il est attendu du Contractant (ainsi que tous les membres du consortium le cas échéant), d'identifier et de requérir ce consentement pour un panel d'activité, par avance, auprès de l'AAI.

[REQ D.6] Les instructions pour la transmission des informations classifiées décrites dans L'instruction de sécurité « European GNSS PSI » (AD2), doivent s'appliquer à toutes les transmissions d'information classifiées résultant des activités contractuelles en vertu du présent Contrat.

[REQ D.7] Quand les activités contractuelles exigent la gestion de ou l'accès à des moyens COMSEC, les Contractants (ainsi que tous les membres du consortium le cas échéant) et chaque sous-traitant devront mettre en œuvre les instructions prévues en AD 3, instructions « European COMSEC GNSS » (A3).

[REQ D.8] En complément des instructions du L'instruction de sécurité « European GNSS PSI » (AD2) le Contractant (ainsi que tous les membres du consortium le cas échéant) et chaque sous-traitant devront chiffrer les informations classifiées chaque fois qu'elles seront stockées sur un support numérique dans le but d'être transmises ou transportées.

[REQ D.8.1] Les informations classifiées devront être chiffrées uniquement au moyen de produits cryptographiques agréés par l'autorité CRYPTO du GNSS de la Commission Européenne. L'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») peut fournir une liste une liste de ce type de produit sur demande.

<sup>6</sup> Ces circonstances peuvent survenir en cas de révision de AD2, AD3 et RD2 aboutissant ce que des marquages existants dénués de fondement attribués à des informations et à des actifs déjà existants, ou lorsque l'ancien marquage des informations ou des matériel atouts doit être révisé / mis à jour. Dans tous les cas où une ambiguïté persiste, le service de sécurité de GSA doit être consulté pour obtenir clarifier la situation.



[REQ D.8.2] Sauf accord écrit contraire, l'outil 'Chiasmus for Windows' développé par la NSA allemande (BSI) devra être utilisé par le Contractant (ainsi que tous les membres du consortium le cas échéant) et chaque sous-traitant pour le chiffrement des informations de niveau RESTREINT UE/EU RESTRICTED<sup>7</sup> et la transmission ultérieure via un réseau public.

[REQ D.8.2.1] Le Contrat et les futurs appels d'offre de sous-traitance le cas échéant peuvent nécessiter le transfert d'informations classifiées jusqu'au niveau RESTREINT UE/EU RESTRICTED aux soumissionnaires, et comme il est envisagé un besoin de transférer de l'information classifiée jusqu'au niveau RESTREINT UE/EU RESTRICTED de la GSA au Contractant (ainsi que tous les membres du consortium le cas échéant) ou de la GSA ou du Contractant (ainsi que tous les membres du consortium le cas échéant) à un sous-traitant, peu de temps après l'attribution du contrat/sous-contrat, la mise en conformité avec le REQ D.8.2 devrait être réalisée à la signature du contrat/sous-contrat. Si un soumissionnaire n'était pas en conformité au moment de la signature, le plan visant à se mettre en conformité devra être indiqué.

[REQ D.8.3] Tous les produits de chiffrement utilisés par le Contractant (ainsi que tous les membres du consortium le cas échéant) et chaque sous-traitant, pour le chiffrement de l'information au niveau CONFIDENTIEL UE/EU CONFIDENTIAL devront être, préalablement à leur utilisation, acceptés par l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI »).

[REQ D.8.4] Le Contractant (ainsi que tous les membres du consortium le cas échéant) et chaque sous-traitant, devront s'assurer qu'ils possèdent les licences d'exploitation requises et toute autre certificats de propriété et/ou d'utilisation pour chaque produit cryptographique utilisé pour la mise en œuvre de ce Contrat.

[REQ D.9] Toute personne impliquée dans ces activités contractuelles, qui doit accéder aux moyens de sécurité (équipement, dispositifs, outils, applications, y compris le matériel/consommables de support associés à ces moyens, et les produits créés ou modifiés par ces moyens) qu'ils soient fournis ou non par la GSA, devra le faire en conformité avec les Procédures opérationnelles de Sécurité (en anglais Security Operating Procedures (SecOPs)) applicables à ces moyens de sécurité et approuvées par l'autorité de sécurité accréditant ces moyens de sécurité.

### 3.5 Gestion des exigences de sécurité

[INFO E] En vertu de l'article 21 de l'AD 6, la GSA peut à tout moment décider du besoin de réviser ou d'ajouter des exigences de sécurité pour protéger l'information classifiée relative au programme

<sup>7</sup> Ou en dessous, ainsi les informations non classifiées peuvent également être protégées par un cryptage lorsque ces informations sont jugées sensibles par la GSA et / ou le Contractant (membres du consortium inclus) et les sous-traitants



GNSS. Ceci devra être réalisé par la GSA sur la base d'une procédure d'analyse de sécurité constante alimentée par les développements de sécurité du programme GNSS. Quand ces révisions ou ajouts aux exigences de sécurité sont justifiés, les exigences suivantes s'appliquent :

- [REQ E.1] Si un changement des exigences de sécurité contenues dans cette SAL ou des exigences de sécurité de niveau « contrat spécifique » apparaissaient durant l'exécution de ce contrat (incluant les contrats de sous-traitance s'y rapportant) et si de tels changement s'écartaient significativement des dispositions initiales, le contrat initial et/ou spécifiques devront être amendés ou résiliés, selon ce qu'il convient et comme convenu entre la GSA et les parties au contrat.
- [REQ E.2] Si un changement des exigences de sécurité donne lieu à des mesures de sécurité ou des investissements, supplémentaires, devant être réalisés par le Contractant (ainsi que tous les membres du consortium le cas échéant), un amendement au contrat devra être négocié et accepté par la GSA de façon juste et raisonnable.
- [REQ E.3] Dans le cas où, le Contractant (ainsi que tous les membres du consortium le cas échéant) ne peut pas se conformer au renforcement des exigences de sécurité, le contrat ou les contrats spécifiques respectifs, devront être résiliés conformément aux dispositions du contrat cadre. Cependant, toute résiliation du contrat résultant d'un changement des exigences de sécurité ne devra pas être par défaut la responsabilité du Contractant (ainsi que tous les membres du consortium le cas échéant) ; et le Contractant (ainsi que tous les membres du consortium le cas échéant) peut prétendre à une indemnisation par la GSA conformément aux dispositions du contrat cadre.

### 3.6 Organisation de la sécurité

- [REQ F.1] Le Contractant ((ainsi que tous les membres du consortium le cas échéant) devra établir et maintenir une organisation de sécurité responsable du suivi et de la mise en œuvre du contenu de cette SAL.
- [REQ F.1.1] La GSA et le Contractant (ainsi que tous les membres du consortium le cas échéant).devront déclarer l'interface avec leurs organisation de sécurité respectives en désignant des points de contact, dans chaque cas il sera spécifié : le nom, la fonction, l'adresse, le numéro de téléphone et l'adresse e-mail du point de contact.
- [REQ F.1.2] Le point de contact pour toutes les affaires de sécurité devra être à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») par l'intermédiaire du Responsable local de la Sécurité (LSO) de la GSA. Ses coordonnées devront être fournies comme celle du point de contact. Le Contractant (ainsi que tous les membres du consortium le cas échéant) devra s'assurer qu'au moins un des points de contact soit le LSO en charge pour le Contractant (ainsi que tous les membres du consortium le cas



échéant) du département/ zone / équipe/ projet<sup>8</sup>, mettant en œuvre les activités classifiées du contrat et capable d'établir la liaison et de coopérer avec le LSO de la GSA concernant les affaires de sécurité (dont les incidents de sécurité) afférentes au contrat.

- [REQ F.2] Le Contractant (ainsi que tous les membres du consortium le cas échéant) devra s'assurer que tous les sous-traitants impliqués dans des contrats de sous-traitance classifiés établissent et maintiennent une organisation de sécurité responsable du suivi et de la mise en œuvre du contenu de cette SAL (ou de toute SAL issue de cette SAL).
- [REQ F.2.1] Quand cela est nécessaire, afin que le sous-traitant mette en œuvre ses obligations (sous) contractuelles, le Contractant (ainsi que tous les membres du consortium le cas échéant) devra informer le sous-traitant de tous les points de contacts désigné pour les affaires de sécurité, de la GSA, du Contractant (ainsi que tous les membres du consortium le cas échéant) et des (autres) sous-traitants.
- [REQ F.2.2] Pour chaque sous-traitant, le Contractant (ainsi que tous les membres du consortium le cas échéant) devra déclarer au LSO de la GSA au moins un point de contact désigné par le sous-traitant pour les affaires de sécurité.
- [REQ F.3] Toutes les communications entre les parties au contrat (ainsi que tous les membres du consortium et sous-traitant le cas échéant) concernant la conformité à cette SAL devront émaner des points de contact désignés pour les affaires de sécurité.
- [INFO F.] Les coordonnées du gestionnaire du contrat et du LSO du Contractant (ainsi que de tous les membres du consortium le cas échéant) responsables de la mise en œuvre de cette SAL, seront publiés dans la liste des Contractant de l'instruction de sécurité « European GNSS PSI » (AD2) pour la durée du contrat.
- [REQ F.4] En cas de changement quel qu'il soit dans l'organisation de sécurité établie par le Contractant (ainsi que tous les membres du consortium et sous-traitants le cas échéant<sup>9</sup>) ceci pour toute la durée de réalisation du contrat, le Contractant (ainsi que tous les membres du consortium le cas échéant) et chaque sous-traitants doivent immédiatement mettre à jour toutes les informations pertinentes ayant trait au changement et en rendre compte à l'Autorité chargée de l'assurance de l'information GNSS de l'UE (« AAI ») par l'intermédiaire du Responsable local de la Sécurité de la GSA par écrit dans les 30 (trente) jours suivant le changement.

#### 4. Accès aux locaux de la GSA et des autres parties au contrat

<sup>8</sup> La portée et la désignation de l'agent de sécurité local sont laissées la discrétion du Contractant.

<sup>9</sup> Quand précédemment communiqué à la GSA



- [REQ G.1] Quand l'accès aux locaux de la GSA ou des autres parties au contrat est nécessaire pour réaliser une activité contractuelle, Le Contractant (ainsi que tous les membres du consortium le cas échéant), les sous-traitants et leur personnel doivent respecter les règles et règlements internes de la GSA ou selon le cas des autres parties au contrat et doivent suivre les instructions données par la GSA, ou le cas échéant, et sans préjudice de toutes autre instruction d'une autre partie au contrat, le LSO de cette partie au contrat. Pour accéder aux emprises de la GSA, ils seront informés en conséquence par le LSO de la GSA, les briefings portant sur l'emprise d'une autre partie au contrat ressortent de sa responsabilité et de son autorité. Ils devront fournir leur pleine coopération pour éviter et rendre compte de tout incident (de sécurité) qu'ils détecteraient.
- [INFO G] Tout manquement aux consignes de sécurité de la GSA peut entraîner l'interdiction d'accès ou l'expulsion du personnel des locaux de la GSA. Les conséquences du non-respect des consignes de sécurité d'une autre partie au contrat demeurent sous sa responsabilité et son autorité.
- [REQ G.2] Le Contractant (ainsi que tous les membres du consortium le cas échéant), les sous-traitants et leur personnel réalisant un travail dans les locaux de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou au-dessus, de la GSA ou d'une autre partie au contrat, doivent posséder une habilitation de sécurité nationale (et toute autorisation complémentaire<sup>10</sup> requise par les règles de sécurité applicables à ce personnel).du niveau de classification et des marquages le plus élevé requis pour le travail en cours de réalisation et délivré par l'Autorité de Sécurité d'un des participant<sup>11</sup> au programme européen du GNSS. (C'est-à-dire les membres de l'Union Européenne, et, dans les cas où ils sont admis à participer à des contrats du GNSS, les citoyens de la Norvège et de la Suisse).
- [REQ G.2.1] La GSA peut autoriser, de façon temporaire et au cas par cas le personnel du Contractant (ainsi que celui de tout membre du consortium le cas échéant) ou des sous-traitants pour lequel un contrôle de sécurité initial, réalisé par l'autorité de sécurité d'un participant<sup>12</sup> au programme européen GNSS (C'est-à-dire les membres de l'Union Européenne, et, dans les cas où ils sont admis à participer à des contrats du GNSS, les citoyens de la Norvège et de la Suisse) n'a révélé aucun renseignement défavorable ou dont la procédure d'habilitation a été engagée ou est toujours en cours, à réaliser une tâche dans ses locaux.
- [REQ G.3] Toute Information Classifiée ou matériel fourni au personnel du Contractant (ainsi que tous les membres du consortium le cas échéant) ou sous-traitants pour un usage temporaire ou un transfert devra être traité par ceux-ci comme si il était fourni officiellement par la GSA. Les exigences concernant l'Information Classifiées ou le matériel fourni par le personnel du Contractant (ainsi que tous les membres du consortium le cas échéant) ou du sous-traitant, pour un usage temporaire ou

<sup>10</sup> Par exemple, les autorisations requises pour accéder aux moyens CRYPTO quand imposés par l'Autorité de sécurité ou l'organisation pour la personne en question.

<sup>11</sup> A noter que l'Agence spatiale européenne est un des participants au programme GNSS de l'UE, mais ne délivre pas d'autorisations de sécurité.

<sup>12</sup> A noter que l'Agence spatiale européenne est un des participants au programme GNSS de l'UE, mais ne délivre pas d'autorisations de sécurité.



un transfert, par les autres parties au contrat, devront rester entièrement sous leur responsabilité et autorité respectives et devront en conséquence être obligatoire.

- [REQ G.3.1] Quand le Contractant (ainsi que tous les membres du consortium le cas échéant) ou les sous-traitants ont l'intention d'envoyer par coursier du matériel classifié de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou au-dessus, de ou vers la GSA, ou, sans préjudice des exigences propres des autres parties au contrat, vers les locaux des autres parties au contrat, alors le personnel devra détenir la preuve de son habilitation de sécurité personnelle, l'autorisation de leur LSO de transporter ce matériel et les coordonnées et informations de manière que le bordereau de réception, pour la livraison ou le transfert de cette information depuis ou vers leur LSO puisse être rempli précisément par la GSA ou une des parties au contrat, comme ils en ont respectivement l'obligation.
- [REQ G.4] La procédure visant à simplifier les visites classifiées<sup>13</sup>, contenue dans la L'instruction de sécurité « European GNSS PSI » (AD2) devra être utilisée quand le Contractant (ainsi que tous les membres du consortium le cas échéant) ou chaque sous-traitant aura à visiter les emprises de la GSA, pour effectuer une tâche (y compris participer à une réunion) de niveau RESTREINT UE/EU RESTRICTED ou au-dessus. S'il y a un choix de la procédure à suivre, alors la GSA devra sélectionner le processus ou la procédure particulière à utiliser.
- [REQ G.5] La GSA est en droit de refuser l'accès à ses emprises à tout personnel du Contractant (ainsi que tous les membres du consortium le cas échéant) ou du sous-traitant sans justification, quand cela est jugé nécessaire pour des raisons de sécurité.

---

<sup>13</sup> Y compris, le cas échéant, la procédure de demande de visite.



## 5. Document applicables et références

### 5.1 Documents applicables

- AD 1 Règlement (UE) No 912/2010 du Parlement européen et du Conseil du 22 septembre 2010 établissant l'Agence du GNSS européen, amendé par le Règlement (UE) No 512/2014;
- AD 2 « European GNSS Programme Security Instruction » ou « European GNSS PSI », dernière version;
- AD 3 Instructions COMSEC du Programme de GNSS de l'UE, dernière version;
- AD 4 Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne ;
- AD 5 Décision No 1104/2011/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo
- AD 6 Règlement (UE) No 1285/2013 du Parlement européen et du Conseil du 11 décembre 2013 relatif à la mise en place et à l'exploitation des systèmes européens de radionavigation par satellite et abrogeant le règlement (CE) no 876/2002 du Conseil et le règlement (CE) no 683/2008 du Parlement européen et du Conseil

### 5.2 Documents de référence

- RD 1 Guide de classification de sécurité Galileo, dernière version (RESTREINT UE/EU RESTRICTED)
- RD 2 Guide de classification de sécurité du Programme GNSS de l'UE, dernière version (RESTREINT UE/EU RESTRICTED)

Signature par le représentant légal du Contractant	
Contractant	
Nom du représentant légal	
Signature	
Fonction	
Date	