MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ANNEXE I – PROTECTION DES INFORMATIONS – CONFIDENTIALITE – MESURE DE SECURITE

Référence : Arrêté du 15 mars 2021 portant approbation de l'instruction ministérielle n°900 sur la protection du secret et des informations diffusion restreinte et sensibles NOR : ARMM2108698A

Dans la présente annexe, les dispositions relatives aux sous-traitants ne valent que dans les cas où la sous-traitance est autorisée par le marché. De la même façon, les dispositions relatives au support ou à la maintenance ne valent que si ces prestations sont prévues au marché.

1. Référence au CCAG

Le titulaire est tenu de respecter les obligations de confidentialité, de protection des données à caractère personnel et les mesures de sécurité prévues à l'article 5 du CCAG applicable au marché contractualisé.

Si un sous-traitant est susceptible d'intervenir pour le compte du titulaire durant l'exécution de l'accord-cadre, le titulaire est tenu de l'aviser de ce que ces obligations lui sont applicables. Quel que puisse être le statut de ce sous-traitant vis-à-vis du titulaire, ce dernier reste responsable du respect de ces obligations.

2. Mesure de sécurité

2.1 Mesure de sécurité applicables à l'accès des locaux

Tout agent du titulaire, que celui-ci soit l'un de ses salariés ou salarié d'un de ses sous-traitants, devant avoir accès aux locaux de l'administration doit être préalablement nommément agréé selon la procédure en vigueur au ministère de l'intérieur (MI). Cet agent du titulaire demeure soumis pendant son séjour aux mêmes règles intérieures que les agents de l'administration, notamment les politiques et procédures de sécurité des systèmes d'information, ainsi que les chartes administrateurs et utilisateurs. Le ministère de l'intérieur peut retirer son agrément à tout moment sans avoir à énoncer ses motifs, le titulaire doit alors proposer immédiatement un remplaçant de niveau équivalent.

L'intervention dans les locaux de l'administration est conditionnée à l'obtention d'une autorisation d'accès délivrée à l'agent du titulaire après enquête diligentée par le service de sécurité compétent pour l'autorité contractante au profit de laquelle le marché est exécuté.

Le délai d'enquête est en moyenne de quinze (15) jours ouvrés et il est fait obligation au titulaire de fournir à l'administration :

- le patronyme et les prénoms de son agent ;
- une photocopie lisible et recto-verso d'un titre d'identité dont la nature varie selon la situation individuelle de l'agent visé :

o carte nationale d'identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires ;
o titre de séjour en cours de validité avec une autorisation de travail valable ou carte de résident pour les étrangers extracommunautaires ;

- l'adresse actuelle de l'agent si celle-ci diffère de celle portée sur le titre d'identité fourni.

2.2 Mesure de sécurité applicables à l'accès aux ressources de l'administration

Dès notification du marché et avant tout commencement d'exécution de celui-ci, le titulaire a obligation de remettre à l'administration l'engagement de reconnaissance de responsabilité signé (joint en annexe II au CCAP) en sa qualité de titulaire. En cas de sous-traitance, acceptée préalablement par l'administration, le titulaire du marché s'engage à remettre un engagement de reconnaissance de responsabilité signé par le sous-traitant.

En cours d'exécution du marché, le titulaire a obligation de communiquer à l'administration la liste actualisée de ses agents, que ceux-ci soient salariés du titulaire ou salariés d'un de ses sous-traitants, susceptibles d'intervenir dans son exécution (ci-après désignée par la A Liste B). L'actualisation de la Liste a lieu au minimum une fois par an, à la date anniversaire de la signature du marché.

Un original de l'engagement de reconnaissance de responsabilité est remis au responsable du projet de l'administration, ainsi qu'à l'officier de sécurité (OS) du pôle SSI, à l'adresse suivante :

Officier de sécurité DEPAFI
Immeuble Lumière
40, Avenue des Terroirs de France
75 012 PARIS

La Liste doit être transmise au responsable du projet de l'administration, ainsi qu'à l'officier de sécurité du pôle SSI à l'adresse suivante :

os-securite@interieur.gouv.fr

Le titulaire s'engage à prendre toutes les mesures nécessaires et conformes à l'état de l'art en matière de sécurité des systèmes d'information pour assurer, lors de l'exécution du marché, la protection effective et efficace des informations ou supports qui peuvent être détenus dans le service, au profit duquel le marché est exécuté, ou dans tout lieu où ce marché est exécuté. Le titulaire veille à sensibiliser ses personnels sur la nature et la sensibilité des informations et données communiquées par les agents du ministère de l'intérieur aux services supports. Il s'agit de s'assurer que dans le cadre de la résolution d'un incident ne sont communiquées ni données métiers ni données techniques (adresses IP, configuration d'équipement de sécurité [règles et exceptions]). S'il venait à être indispensable de détenir de telles informations, la communication entre les deux parties devra être effectuée au moyen d'un outil de chiffrement homologué par l'ANSSI et validé par l'administration. Le cas échéant, cet outil de chiffrement peut être fourni par l'administration.

Le titulaire reconnaît avoir pris connaissance, pour tous les agents appelés sous sa responsabilité à intervenir à un titre quelconque dans le cadre de l'exécution du marché, des articles 323-1 à 323-3-1 et 413-9 à 413-12 du code pénal et des dispositions de l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle (IGI) n°1300 sur la protection du secret de la défense nationale, et d'autre part, qu'ils n'ont pas, sous peine de

poursuite pénale, à connaître ou détenir des informations couvertes par le secret de la défense nationale.

Aucune dérogation aux présentes mesures de sécurité ne pourra être acceptée de l'autorité contractante ou exigée d'elle, y compris en vue de pourvoir au remplacement inopiné, fortuit ou même urgent d'un agent du titulaire.

Le non-respect ou l'inobservation par le titulaire de ces mesures de sécurité, même dans les cas où ils résultent d'une imprudence ou d'une négligence, peuvent entraîner le prononcé d'une sanction contractuelle, sans préjudice des sanctions pénales.

3. Protection des informations sensibles

3.1 Principes

Toute information sensible du ministère de l'intérieur doit être considérée comme un bien à protéger et ce tout au long de son cycle de vie.

Les niveaux de sensibilité des informations sont définis dans le tableau ci-après :

Niveau de sensibilité	Niveau de sensibilité Définition
Non sensible	**Données ou informations pouvant être diffusées volontairement ou dont la diffusion involontaire à l'extérieur du ministère ne porte pas de préjudice pour lui, ses partenaires du service public ou privés.**
Sensible	**Données ou informations ne devant pas être rendues publiques et/ou restreintes à la diffusion d'un domaine spécifique.**
Sensible « Diffusion Restreinte »	**Données ou informations soumises à une restriction de diffusion particulière. La « Diffusion Restreinte » relève de la nécessité d'éviter la divulgation, dans le domaine public, d'informations dont le regroupement ou l'exploitation pourraient :** **- conduire à la découverte d'une information classifiée ;** **- porter atteinte à la sécurité ou à l'ordre public, au renom des institutions, à la vie privée de leurs membres ;** **- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics.**

Le titulaire s'engage à ce que les informations sensibles, pendant tout leur cycle de vie, ne puissent être portées, même fortuitement, à la connaissance de personnes n'ayant pas le besoin d'en connaître sauf accord préalable exprès et écrit de l'administration.

La politique de sécurité des systèmes d'information (PSSI) du ministère de l'intérieur (PSSI-MI), comme la PSSI pertinente pour le service au profit duquel le marché est exécuté, sont réputées connues du titulaire comme de ses agents de la Liste qu'il aura déclarée à l'administration. Le

titulaire s'engage à respecter, et faire respecter par ses agents, l'ensemble des obligations de ces PSSI. Dans les locaux du prestataire, les informations sensibles font l'objet d'une gestion spécifique.

Des informations sensibles peuvent se voir attribuer une protection par un marquage « Diffusion Restreinte » selon les règles posées par l'annexe 3 de l'IGI 1300. Les informations « Diffusion Restreinte » sont déterminées en fonction de la nature de la prestation et du type de données à protéger dans le marché. Sont notamment systématiquement considérés comme « Diffusion Restreinte » :

- les plans d'adressage IP du ministère (ou une partie de ces plages si cela permet de cartographier un sous-ensemble du système d'information) ;
- les mots de passe ;
- les fichiers de configuration ;
- les codes sources des applications (ou un extrait de ces codes sources) ;
- les fiches d'expression rationnelle des objectifs de sécurité (FEROS) et dossiers d'analyse de risques ;
- les dossiers de sécurité des systèmes d'information du ministère de l'intérieur, que ces systèmes soient en mode projet ou en mode opérationnel ;
- les dossiers d'architecture et d'installation ;
- les données de production.

Les informations sensibles considérées « Diffusion Restreinte » sont marquées avec la mention « Diffusion Restreinte » conformément au modèle ci-dessous :

DIFFUSION RESTREINTE

Pour les documents papier, cette mention « Diffusion Restreinte » est portée en haut de toutes les pages du document.

Les informations techniques au format électronique, ne pouvant donc faire l'objet d'un marquage réglementaire comme indiqué ci-dessus (comme par exemple les journaux d'évènements, les fichiers de configuration, les codes sources), sont de facto considérées comme « Diffusion Restreinte » et le titulaire a l'obligation d'appliquer les dispositions réglementaires qui s'imposent pour la gestion de ces données.

La réalisation d'une copie d'une information considérée « Diffusion Restreinte » sans autorisation préalable est considérée par l'administration comme une violation des dispositions relatives au respect du secret dans l'exécution du marché.

3.2 Protection des informations sensibles sur support papier

Le titulaire a l'obligation de mettre en place un système de gestion permettant d'identifier tous les documents comportant des informations sensibles, quel que soit leur marquage, et pour chacun de ces documents ainsi identifié :

- de connaître la liste des personnes physiques comme morales en ayant eu connaissance ou communication ;
- d'en connaître soit la date de restitution à l'administration soit la date de destruction, ainsi que le nom et la qualité de la personne ayant réalisé l'opération.

En cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie le ou les documents détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les agents du titulaire ayant assisté à la destruction en qualité de témoin(s), et le moyen de

destruction utilisé (broyage ou incinération). Ce bordereau est transmis, sans délai, à l'officier de sécurité du OS Securité, à l'adresse suivante :

os-securite@interieur.gouv.fr

Le bordereau de destruction stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles.

En cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui est remis le document. Au surplus, le bordereau doit stipuler que le titulaire certifie n'avoir ni établi ni conservé de copie du document.

La diffusion des documents papier se fait sous double enveloppe. L'enveloppe extérieure ne porte aucune mention particulière hormis le nom et l'adresse du destinataire.

L'enveloppe interne porte le nom du destinataire et la mention pertinente, à savoir « Sensible » ou « Diffusion Restreinte ». Les agents du titulaire qui gèrent les arrivées courrier doivent être sensibilisés à l'usage de ces mentions, ne pas ouvrir l'enveloppe et la distribuer au destinataire.

3.3 Protection des informations sensibles sur support électronique

Il est fait obligation au titulaire que le traitement des informations sensibles sur support électronique ne soit pas réalisé sur des moyens informatiques connectés à un réseau non maîtrisé. L'administration considère qu'un réseau d'entreprise connecté à Internet ne permet pas de garantir ce niveau adéquat de protection des informations sensibles.

Le cas échéant, le titulaire peut s'efforcer de démontrer à l'administration son aptitude à protéger les informations sensibles qu'il serait amené à traiter en dehors des systèmes d'information du ministère de l'intérieur. Pour ce faire :

- soit l'isolation des moyens de traitement des informations s'effectue de manière physique ;
- soit cette isolation s'effectue par une interface logique de sécurité présentant des garanties suffisantes afin d'empêcher l'accès aux moyens de traitement des informations sensibles par des tiers.

Le titulaire doit alors soumettre à l'administration une documentation relative aux règles de gestion et aux règles techniques de sécurité de ces moyens de traitement des informations sensibles. Ces règles de gestion et règles techniques de fonctionnement concourant à la sécurité des informations sensibles doivent faire l'objet d'une validation formelle par l'administration. Cette dernière se réserve le droit de procéder à leur contrôle préalablement à toute validation comme après validation pendant l'exécution du marché.

Il est fait obligation au titulaire de respecter le besoin d'en connaître seuls ses agents de la Liste ont accès aux informations nécessaires pour l'exécution du marché. Le respect de cette obligation par le titulaire doit être garanti par la mise en place et l'utilisation de mécanismes de sécurité (authentification individuelle, gestion des droits et traçabilité des accès).

Le besoin d'en connaître désigne la nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise.

La confidentialité des informations sensibles, quel que soit leur marquage, sur support électronique est réalisée au moyen d'un mécanisme de chiffrement reposant sur un logiciel A qualifié B par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Ces logiciels sont fournis par l'administration dès notification du marché. Un document relatif à l'utilisation de ces logiciels est remis au titulaire dès notification du marché, il doit faire l'objet d'une diffusion auprès de ses agents intervenant dans le cadre des prestations prévues.

A l'issue du marché, le titulaire procède soit à la restitution, soit à la destruction de l'ensemble des informations sensibles sur support électronique et des documents associés incluant les courriels :

- en cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui sont remis les informations sensibles sur support électronique, en déclare la liste et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles ;
- en cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie les supports électroniques détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les agents du titulaire ayant assisté à la destruction en qualité de témoin(s), le ou les moyens de destruction utilisés. Ce bordereau est transmis, sans délai, à l'officier de sécurité DEPAFI, à l'adresse suivante : os-securite@interieur.gouv.fr

Le bordereau de destruction stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles. Le mécanisme de destruction utilisé doit reposer sur un outil A qualifié B par l'ANSSI. Le cas échéant, cet outil est fourni par l'administration.

3.4 Sécurisation des locaux du titulaire

Dans le cas où des informations sensibles, quel que soit leur marquage et quelle que soit la forme de leur support, sont appelées à être conservées dans les locaux du titulaire, leur support papier ou électronique doivent être disposés en dehors de leur utilisation dans des armoires fermant à clé et dont la clé est conservée par la seule personne responsable de leur utilisation.

Préalablement à toute exécution du marché, le titulaire doit désigner un responsable sécurité qui devient l'interlocuteur privilégié de l'administration pour tous les sujets de sécurité pendant l'exécution du marché. L'administration se réserve le droit de vérifier le niveau de compétences en sécurité des systèmes d'information (SSI) de ce responsable et de le récuser si elle juge ce niveau insuffisant, le titulaire ayant alors l'obligation de proposer sans délai à l'administration un nouveau responsable sécurité.

Il appartient à ce responsable sécurité de sensibiliser les agents du titulaire susceptibles d'intervenir dans l'exécution du marché au strict respect des obligations du titulaire en matière de SSI et d'en présenter un bilan à l'occasion de la réunion du comité de suivi ou de toute instance équivalente prévus dans les documents du marché.

3.5 Modalités d'exécution

A tout moment pendant l'exécution du marché, l'administration se réserve le droit de réaliser tout contrôle, après un préavis de vingt-quatre (24) heures, dans les locaux du titulaire pour vérifier que sont effectivement respectées les préconisations validées par l'administration s'agissant des règles de gestion et des mesures techniques de sécurisation des moyens de traitement des informations sensibles du ministère de l'intérieur.

En cas de défaillance constatée dans la mise en œuvre de mesures de sécurité en adéquation avec le niveau de sensibilité des données traitées, il pourra être fait obligation au titulaire de réaliser à ses frais tous travaux de mise en conformité de ses locaux.

Le titulaire a le devoir d'informer sans délai l'administration de toute difficulté dans l'application de ces mesures, de fuite ou de suspicion de fuite d'informations sensibles qu'il rencontre ou constate.

4. Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information

DSIC	Direction des Systèmes d'Information et de Communication du ministère de l'intérieur
FEROS	Fiche d'Expression rationnelle des Objectifs de Sécurité
IGI	Instruction Générale Interministérielle
IP	Internet Protocol
MI	Ministère de l'Intérieur
PSSI	Politique de Sécurité des Systèmes d'Information
PSSI-MI	Politique de Sécurité des Systèmes d'Information du Ministère de l'Intérieur
PES	Procédure d'Exploitation de la Sécurité des Systèmes d'Information
RCSSI	Responsable Central de la Sécurité des Systèmes d'Information
RGSSI	Responsable Général de la Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
RSSI-E	Responsable de la Sécurité des Systèmes d'Information – « Expertise »
RSSI-H	Responsable de la Sécurité des Systèmes d'Information – « Homologation »
RSSI-TU	Responsable de la Sécurité des Systèmes d'Information – « Terminal utilisateurs »
OS	Officier Sécurité
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
SSMI	Service de Sécurité du Ministère de l'Intérieur

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ANNEXE II – ENGAGEMENT DE RECONNAISSANCE DE RESPONSABILITE

ENGAGEMENT DE RECONNAISSANCE DE RESPONSABILITE

Relatif au bon respect des obligations de confidentialité, de protection des données à caractère personnel ou sensibles et des mesures de sécurité en vigueur au Ministère de l'Intérieur.

LA PERSONNE DESIGNEE CI-APRES :

NOM – PRENOM :			
Né€ le :		**A :**	
Déclarant avoir toute autorité pour agir en tant que (fonctions dans l'entreprise) :			
Au nom de la société désignée ci-contre (raison sociale et adresse du siège social) :			

dans le cadre de l'exécution du marché relatif à l'acquisition d'un logiciel de captation et d'analyse de données en source ouverte (ROSO) et prestations associées,

Reconnaît avoir été sensibilisée et de ce fait avoir pleinement connaissance :

- que l'autorisation d'accès aux locaux de l'administration est conditionnée à l'obtention d'une autorisation d'accès délivrée après enquête diligentée par le

service de sécurité compétent, ce droit d'accès est strictement personnel, incessible et limité dans le temps ;
- que toute éventuelle action contraire aux règles édictées doit être immédiatement signalée à la DNUM et à sa voie fonctionnelle SSI ;
- que l'administration peut, à tout instant, demander à en contrôler sans restriction l'utilisation qui en est faite ;
- des dispositions générales relatives à la réglementation et à la législation française en vigueur dans le domaine de la sécurité des systèmes d'information et plus particulièrement à la fraude informatique, notamment les articles 323-1 à 323-3-1 du code pénal ;
- des dispositions des articles 413-9 à 413-12 du code pénal relatifs aux atteintes au secret de la défense nationale ;
- des dispositions de l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale ;
- qu'un dispositif (journalisation des notifications techniques et de sécurité) permet d'assurer la traçabilité de l'ensemble des actions menées sur le système d'information, pour raisons de sécurité.

S'engage à ce que tous les agents appelés, sous sa responsabilité, à intervenir à un titre quelconque dans le cadre de l'exécution du marché :
- respectent l'obligation de discrétion professionnelle pour tous les faits, informations ou documents dont ils auraient connaissance dans l'exercice ou à l'occasion de l'exercice de leurs activités ;
- prennent connaissance et respectent les dispositions décrites en annexe I du CCAP relative à la protection des informations, à la confidentialité et aux mesures de sécurité ;
- ne divulguent en aucun cas à un tiers des informations ou données tant personnelles que professionnelles qu'ils pourraient être amenés à apprendre dans l'exercice de leur mission ;
- ne reproduisent, ni ne stockent, ni ne copient, ni ne diffusent, ni ne modifient, ni n'altèrent, ni ne détruisent toute information ou donnée dont ils pourraient avoir connaissance à d'autres fins que celles de l'exercice de leur mission ;
- respectent le principe fondamental du A besoin d'en connaître B et ainsi ne tentent pas d'accéder, ni de reproduire, ni de stocker, ni de copier, ni de diffuser, ni de modifier, ni d'altérer, ni de détruire toute information dont ils ne sont pas supposés avoir connaissance dans l'exercice de leur mission.

S'engage à ce que tous les agents disposant d'un accès à un système d'information de l'administration et, par conséquent, d'un compte nominatif :
- ne tentent pas de connecter tout appareil électronique communicant ou non, personnel ou de la société, au système d'information sans avoir reçu préalablement l'autorisation formelle de la voie fonctionnelle SSI ;
- ne modifient pas sans autorisation la configuration des moyens mis à leur disposition et notamment ne raccordent pas de moyens informatiques qui n'auront pas été convenus au préalable avec le ministère de l'Intérieur dans le cadre de la définition de l'architecture ;
- ne se livrent pas à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des services, applications et moyens auxquels ils ont accès ;
- ne mettent pas à la disposition d'utilisateurs non autorisés un accès privilégié aux ressources informatiques, données ou services ;

- ne perturbent ni n'interrompent le fonctionnement normal du système d'information ou de l'un de ses composants ;
- n'installent pas, sans autorisation préalable et formelle de la voie fonctionnelle SSI (ou de son représentant) de logiciels sur le système d'information ou sur les équipements mis à leur disposition ;
- n'introduisent, ni ne testent, ni n'utilisent des supports informatiques ou médias dont l'origine leur est inconnue, douteuse ou incertaine ;
- ne génèrent pas volontairement ou involontairement des perturbations sur les ressources du SI que ce soit par des manipulations anormales ou par l'introduction illicite de logiciels contrefaits ou piratés potentiellement nuisibles en termes de failles de sécurité ou de pollution virale.

Déclare être pleinement consciente de ses responsabilités et reconnait être informée des conséquences pénales et contractuelles qui pourraient résulter de la non application des procédures et dispositions édictées ci-dessus.

A :		**LE :**	
Recopier ci-dessous la formule manuscrite suivante : « *je m'engage* »			
CACHET DE L'ENTREPRISE		**SIGNATURE**	

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ANNEXE III – PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 dite directive « police-justice ».

Dans le cas où le titulaire a accès à des données à caractère personnel lors de la réalisation des prestations, il agit en qualité de sous-traitant au sens de l'article 4 du RGPD et de l'article 22 de la directive « police-justice », et ce pour le compte de l'administration qui demeure le responsable de traitement.

La présente annexe a pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour l'exécution du présent accord-cadre.

La nature des opérations réalisées sur les données correspond à l'identification des utilisateurs et de leurs matériels.

La finalité du traitement est la mise en place d'une connexion sécurisée à la plateforme.

Les données à caractère personnel traitées sont les identifiants correspondants à chaque utilisateur et au matériel et l'ensemble des données attachées à la sécurité de ces connexions.

Les catégories de personnes concernées sont les utilisateurs de la plateforme, agents du ministère de l'intérieur.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes : toutes données en rapport avec les connexions des utilisateurs (date de connexion, durée, fréquence, lieu de connexion).

SECURITE

Le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

Le sous-traitant s'engage à :

1.traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance.

2.traiter les données **conformément aux instructions documentées** du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des états membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3.garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent accord-cadre.

4.veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent accord-cadre :

- s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité ;
- reçoivent la **formation** nécessaire en matière de protection des données à caractère personnel.

5.prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut.**

6.l**a sous-traitance**
Le sous-traitant, titulaire de l'accord-cadre, peut faire appel à un autre sous-traitant (ci-après, A ***le sous-traitant ultérieur*** B) pour mener des activités de traitement spécifiques. Dans ce cas, il s'engage notamment à présenter à l'administration, les entreprises auxquelles il envisage de confier la réalisation d'activités de traitement spécifiques. Pour ce faire, il remplit une déclaration relative à la présentation d'un sous-traitant ultérieur, en vertu de l'article L. 2193-5 du code de la commande publique (DC4). En cas d'accord, l'administration accepte le sous-traitant proposé et agréer ses conditions de paiement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent accord-cadre pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et/ou de la directive A police-justice B. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7.le droit d'information des personnes concernées
Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données en fonction de la catégorie de traitement. L'information fait l'objet d'une diffusion lors de la connexion des utilisateurs par l'intermédiaire d'une fenêtre A pop-up B rappelant la collecte des données lors de la première connexion de la journée au service.

8.l'exercice des droits des personnes
Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage) dans le cadre du RGPD.

Lorsque le traitement relève de la directive « police-justice », l'exercice des droits des personnes fait l'objet de mesures spécifiques compte tenu de la finalité du traitement.

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au représentant du responsable de traitement.

9.notification des violations de données à caractère personnel
Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et par

tout moyen. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

10.aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11.le sort des données

Dans un délai d'un (1) mois calendaire avant la date de fin de l'accord-cadre, le titulaire interroge le responsable de traitement sur le sort des données traitées. Au choix du responsable de traitement, le sous-traitant s'engage à :

- détruire toutes les données à caractère personnel ;
- à renvoyer toutes les données à caractère personnel au responsable de traitement ;
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

12.le délégué à la protection des données

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

13.registre des catégories d'activités de traitement

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
  • la pseudonymisation et le chiffrement des données à caractère personnel ;

•des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
•des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
• une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

14.documentation
Le sous-traitant met à la disposition du responsable de traitement, dans le délai fixé par la demande, la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données à caractère personnel nécessaires pour l'exécution du présent accord-cadre ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement de la part du sous-traitant ;
- superviser le traitement, y compris réaliser, le cas échéant des audits et des inspections auprès du sous-traitant.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ANNEXE IV – CYBERSECURITE

Arrêté d 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité

NOR : ECOP1825228A
ELI : https://www.legifrance.gouv.fr/eli/arrete/2018/9/18/ECOP1825228A/jo/texte
JORF n°0223 du 27 septembre 2018

Texte n° 32

Le ministre de l'économie et des finances et le ministre de l'action et des comptes publics, Vu le code de la défense, notamment ses articles L. 1141-1, R. 1143-1 (3°) et R. 1143-5 (8°) ;
Vu l'arrêté du 1er août 2016 portant approbation de la politique générale de sécurité des systèmes d'information pour les ministères économiques et financiers ;
Vu la circulaire n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information de l'Etat,
Arrêtent :

Article 1
Est approuvé le cahier des clauses simplifiées de cybersécurité annexé au présent arrêté. Ce cahier des clauses n'est applicable qu'aux marchés qui s'y réfèrent.

Article 2
Le présent arrêté sera publié au Journal officiel de la République française.

Article ANNEXE

CAHIER DES CLAUSES SIMPLIFIÉES DE CYBERSÉCURITÉ

Article 1er Champ d'application

1.1.Ce cahier de clauses simplifiées de cybersécurité (CCSC) n'est applicable qu'aux marchés qui s'y réfèrent.

1.2.Les clauses ont pour vocation d'assurer un premier cadre de sécurisation des systèmes d'information et des données associées via tout type de marché, aussi bien un marché à objet principal directement associé aux technologies de l'information et de la communication (ordinateurs, logiciels, développements ou hébergement d'application via le web) que des fournitures et services annexes (extranet de

commande et service clients), ou même les simples échanges d'information par messageries électroniques.

1.3.Pour les marchés ayant un objet principal numérique comme l'externalisation d'une brique de système d'information, les présentes clauses simplifiées peuvent être complétées dans le cahier de clauses particulières du marché auquel fait écho la production par les candidats puis la contractualisation avec le titulaire d'un plan d'assurance sécurité (PAS).

Article 2 Politiques de sécurité

2.1. Les candidats et titulaires sont tenus de respecter les prescriptions des politiques de sécurité des systèmes d'information (PSSI) des bénéficiaires des marchés, dès lors que ces politiques ont été publiées avant la contractualisation des marchés, a fortiori si elles sont fournies au cours de l'appel d'offres.

2.2. Il en est de même pour les annexes techniques des PSSI dès lors qu'elles sont disponibles à première demande motivée.

2.3. Le référentiel général de sécurité (RGS) et la PSSI Etat s'appliquent aux marchés des entités couvertes par ces textes, sans qu'il soit besoin que le cahier des charges en fasse mention explicitement.

Article 3 Contrôles et audits

3.1. Durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants.

3.2. Dans tous les cas, des audits légitimés par la sélection ou le suivi de titulaires de marchés peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier (par exemple, User-Agent référençant une URL d'explication, reverse-DNS permettant de donner une origine claire à une adresse IP, etc).

Article 4 Documentations

4.1. Les politiques de sécurité prévoient généralement une revue formelle de sécurité appelée homologation, auquel les titulaires doivent apporter leur concours en matière de documentations et de réponses aux questions, permettant d'analyser les risques résiduels en matière de confidentialité, authentification, traçabilité, intégrité, disponibilité et résilience.

4.2. Par ailleurs, les règlementations applicables par exemple à la protection des données à caractère personnel (RGPD) ou aux données de santé prévoient la tenue de registres des traitements et la documentation des mesures de protection. Le candidat ou titulaire et leurs sous-traitants identifient proactivement les traitements de données personnelles ou sensibles et aident à la réalisation d'analyses d'impact relative à la protection des données et à la consultation préalable des autorités de contrôle.

4.3. Dans tous les cas, un titulaire de marché est tenu de fournir à première demande la documentation nécessaire à la sécurisation de leurs fournitures dans les systèmes d'information, la protection des données des bénéficiaires et aux démonstrations du respect de leurs obligations par les bénéficiaires du marché.

4.4. En particulier, la documentation explicite tous les flux échangés (entrants et sortants, applicatif mais aussi de maintenance, de statistiques, de mise à jour, d'administration distante, etc), et les dispositifs de contrôle d'accès et de maintien en condition de sécurité.

4.5. Si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part des bénéficiaires du marché, elles doivent être clairement identifiées dans un chapitre Sécurité du mode d'emploi (par exemple, la procédure de changement des mots de passe par défaut ou des interfaces exposées, de mise à jour de composants logiciels…).

Article 5 Maintien en condition de sécurité

5.1. Les politiques de sécurité convergent pour exiger les mises à jour des composants logiciels vers des versions supportées par l'éditeur ou la communauté Open Source qui les produisent. Dans ces conditions, une vérification d'aptitude au bon fonctionnement ou au service régulier (VABF et VSR) est refusée si des composants ne sont pas à jours des correctifs de failles de sécurité.

5.2. La responsabilité du maintien en condition de sécurité d'un titulaire comprend les composants et services développés en propre mais aussi ses composants et dépendances amont (librairies, cadriciels, environnement d'exploitation, API tierces) ou sous-traités.

5.3. Un candidat ou titulaire ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations qu'il fournit à l'emploi de composants dans une version non supportée, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi.

5.4. Dans tous les cas, les unités d'œuvre portant le maintien en condition opérationnelle (labellisée MCO mais aussi tierce maintenance applicative (TMA) ou simplement hébergement) incluent le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité.

Article 6 Signalements de sécurité

6.1. Pour les prestations, produits et services qu'ils fournissent dans le cadre du marché, les titulaires mettent à disposition des fils publics par abonnement (flux RSS, liste de diffusion par courriel) ou autre dispositif d'information dédié à la sécurité informatique. Ces fils, identifiés dans le chapitre Sécurité des modes d'emploi, permettent aux bénéficiaires d'être tenu informés en continu des événements et changements impactant la sécurité, par exemple annonce de correctif, attaque en cours, nouvelle configuration à appliquer, violation de données à caractère personnel…

6.2. Afin de garder leur pouvoir d'alerte, ces canaux de diffusion ne sont pas mélangés avec des flux commerciaux et marketing. Les fils peuvent être multiples dans le cas de fournitures en plusieurs composants mais sans laisser de vide d'information.

6.3. Réciproquement, les outils numériques mis à disposition permettent aux bénéficiaires et leurs experts en cybersécurité de signaler directement aux équipes appropriées du titulaire de possibles failles ou détournements de dispositifs de sécurité.

6.4. Afin que ces signalements soient effectifs et efficaces, les conventions d'usage en cybersécurité sont respectées (security.txt, abuse@). Dans tous les cas, il faut moins d'une minute pour trouver le point d'entrée approprié du signalement.

6.5. Après analyse partagée et vérification, le titulaire a obligation d'enregistrer les failles auprès des autorités compétentes (CERT nationaux pour les éditeurs, registres RGPD et CNIL ou équivalent pour la divulgation de données personnelles, ANSSI pour les opérateurs d'importance vitale ou de services essentiels, etc.) en suivant les réglementations établies. L'emploi d'un système de cotation connu (par exemple CVSS) permet de hiérarchiser l'urgence pour tous les acteurs en aval. A défaut d'action sous 3 mois, l'acheteur a la possibilité de se substituer aux titulaires dans les actions précédentes ou de pratiquer une divulgation responsable (annonce de la faille avec embargo pendant au moins 90 jours sur les détails techniques).

Article 7 Hébergement de données

7.1. A première demande, le candidat ou titulaire identifie tous les prestataires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

Peuvent être exclus de cette déclaration les prestataires qui seraient dépositaires de copies chiffrées à condition que l'algorithme soit sans faille connue et que les prestataires ne soient pas en possession des clés cryptographiques.

Article 8 Sous-traitances

8.1. Les clauses de ce cahier s'appliquent aux marchés publics en incluant tous les soustraitants. Comme les titulaires sont responsables de leurs sous-traitants, les contrôles et les éventuelles actions de remédiation en cas de défaut, y compris jusqu'au remplacement, sont donc à la charge des titulaires.

Article 9 Labels et certificats

9.1. Afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché, candidats et titulaires sont invités à présenter des labels et certificats qui permettent à l'acheteur d'avoir un premier niveau d'assurance au cours de l'évaluation d'offres.

9.2. Ces qualifications peuvent parfois être globales (ISO27000), partielles (référentiel en Tier 1 à 4 pour l'hébergement), ou très ponctuelles (rapports de test de l'état de l'art sur des interfaces spécifiques, cf. clause ci-dessous).

Article 10 Défauts et règlement des différends

10.1. Tout au long des processus d'attribution et d'exécution d'un marché, l'acheteur et les bénéficiaires peuvent constater ou découvrir des non-conformités à la politique de sécurité de l'entité et des défauts de sécurisation.

10.2. L'entité apprécie l'enjeu du défaut eu égard à la sensibilité des données manipulées, de leurs volumes, et des conséquences prévisibles si le défaut persiste.

10.3. En fonction de cette analyse, ces défauts peuvent avoir comme conséquence le rejet d'une candidature, d'une offre, la non-validation d'aptitude au service régulier, pénalités de retard, l'ajournement, la suspension ou la résiliation des bons de commandes ou du marché.

10.4. Comme les différends peuvent être techniques et nécessiter un traitement confidentiel, le règlement des éventuelles contestations sur les décisions précitées passera systématiquement par un comité consultatif de règlement amiable.

10.5. Un comité consultatif est composé de membres qualifiés et habilités pour cette fonction, désignés au préalable ou choisis conjointement.

Article 11 Etats de l'art

11.1. La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient à chaque titulaire de marché de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition. Pour les interfaces web, les services de courriels, les appareils connectés, les sauvegardes de données et l'administration de systèmes d'information, les référentiels à retenir sont résumés ci-après et détaillés dans les textes techniques publiés sur www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi. Les respects de référentiels sont aussi vérifiés par les agences de notation en cybersécurité.

11.2. A première demande, le candidat ou titulaire fournit la conformité à ces référentiels pour les services et objets numériques qu'il inclut dans son offre de fournitures. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration).

11.3. Interfaces web
- Interfaces utilisables par des navigateurs à l'état de l'art (part de marché cumulée supérieure à 50%), sans générer d'alerte de sécurité.
- sans module d'extension.
- dans leur mode Grand public le plus protecteur (souvent appelé navigation Incognito).
- et en exploitant les techniques de protections associées.
- connexion TLS (https) pour authentifier la source et chiffrer les communications.
- marquage approprié des cookies ou jetons de session pour se protéger des vols ou exploitation de sessions déjà ouvertes.
- politique de sécurité des contenus pour se protéger contre les injections de contenus actifs malicieux.
- activation des protections des navigateurs par l'emploi d'entêtes de sécurité.
- Publication d'un point de contact via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des bonnes équipes techniques.

11.4. Services de courriels
- Authenticité des émetteurs garantie par l'émission de messages depuis des serveurs associés publiquement aux domaines, signature numérique par domaine et une politique publique liant le tout.
- Identification claire du statut des comptes émetteurs de courriels, par exemple en ajoutant un suffixe à ceux fournis aux personnels qui ne sont pas agents ou salariés directs.
- Intégrité des messages par leur signature numérique.
- Confidentialité des échanges de machines en machines, confidentialité compatible avec les obligations d'interceptions légales.
- Analyse des rapports d'anomalies via DMARC ou abuse@.

11.5. Appareils connectés
- Dispositif de lutte contre les logiciels malveillants (anti-virus, ou système de vérification et détection à base de signatures ou condensats des logiciels autorisés).
- Dispositif de mise à jour sécurisé.
- Limitation de l'exposition via les réseaux en réduisant les ports acceptant des connexions entrantes et en authentifiant les accès distants, sans faille connue (ceci exclut les connections non chiffrés TELNET, HTTP/SMTP sans TLS, et l'emploi de mots de passe génériques ou faciles à découvrir, par exemple du fait d'un hachage insuffisant).

11.6. Sauvegardes des données stockées
- Sauvegardes 3-2-1 (3 copies, 2 technologies, 1 exemplaire hors site principal, donc avec chiffrement) pour se protéger des rançongiciels, des erreurs de manipulations ou des défaillances de matériels.

11.7. Administration des systèmes d'information
- Consoles dédiées à l'exploitation et l'administration, et au minimum isolées des réseaux bureautiques et d'Internet, web et courriel notamment.
- Connexions aux machines administrées par des protocoles chiffrés, authentifiants et sans faille connue et bien configurés (VPN IPsec, TLS, ssh, RDP avec NLA).

Fait le 18 septembre 2018.

Le ministre de l'économie et des finances,

Pour le ministre et par délégation :

Le fonctionnaire de la sécurité des systèmes d'information,
J.-P. Papillon

Le ministre de l'action et des comptes publics,

Pour le ministre et par délégation :

Le fonctionnaire de la sécurité des systèmes d'information,
J.-P. Papillon