
ANNEXE I : PROTECTION DES INFORMATIONS – CONFIDENTIALITE – MESURES DE SECURITE

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 type de marché contractualisé.

Le titulaire est tenu d'aviser tout sous-traitant intervenant au titre du marché, que les obligations du titulaire sont intégralement applicables audit sous-traitant. 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. Mesures de sécurité

2.1 Mesures de sécurité applicables à l'accès aux locaux

Tout agent du titulaire, que celui-ci soit l'un de ses salariés ou salarié d'un des sous-traitants du titulaire, 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 MI 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 trente (30) 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 :
 - carte nationale d'identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires (les ressortissants portugais et roumains doivent fournir en sus une copie de l'extrait de naissance) ;
 - titre de séjour en cours de validité avec une autorisation de travail valable ou carte de résident pour les étrangers extracommunautaires et un justificatif de domicile (pour les personnes hébergées : justificatif de domicile ou attestation d'accueil et une copie recto-verso lisible de la pièce d'identité/passeport en cours de validité de l'hébergeur) ;
- adresse actuelle de l'agent si celle-ci diffère de celle portée sur le titre d'identité fourni.

2.2 Mesures 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 communiquer à l'Administration la liste de ses agents, que ceux-ci soient salariés du titulaire ou salariés d'un de ses sous-traitants, susceptibles d'intervenir dans l'exécution du marché (ci-après désignée par la « Liste »). Tout changement dans la composition de cette Liste doit être porté à la connaissance de l'Administration sans délai. A défaut, un état de lieux

annuel de cette Liste sera adressé à l'administration à la date anniversaire de la notification du marché.

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 est tenu à l'obligation de faire signer par tous ses agents identifiés dans la « Liste », appelés sous sa responsabilité à un titre quelconque à intervenir pour le compte du titulaire dans le cadre de l'exécution du marché, un engagement de reconnaissance de responsabilité (ERR - joint en annexe II au présent CCAP). Le volet 1 de l'ERR (« *Entrée* ») est signé avant tout commencement d'exécution des prestations ; le volet 2 (« *Sortie* ») à la fin d'exécution des mêmes prestations.

MODALITES DE TRANSMISSION DE LA « LISTE » ET DE L'ERR

La « Liste », ainsi que l'engagement de reconnaissance de responsabilité (« *Entrée* » et « *Sortie* »), doivent être simultanément transmis au responsable du projet de l'administration, ainsi qu'à l'officier de sécurité de la mission Politique SSI, à l'adresse suivante : dtnum-mpssi@interieur.gouv.fr

Le titulaire s'engage à ce que seules les personnes ayant préalablement souscrit l'engagement de reconnaissance de responsabilité précité interviennent de quelque manière que ce soit dans l'exécution du marché.

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

Par défaut, toutes les informations du MI doivent être considérées comme « sensibles » et à ce titre bénéficient des obligations de confidentialité prévues à l'article 5 du CCAG applicable au type de marché contractualisé.

Des informations sensibles peuvent se voir attribuer une protection par le marquage *Diffusion Restreinte* selon les règles de l'annexe 1 à l'IGI 1300 approuvée par l'arrêté du 9 août 2021. 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 MI, que ces systèmes soient en mode projet ou en mode opérationnel ;
- les dossiers d'architecture et d'installation ;

- les données de production.

Les documents *Diffusion Restreinte* sont identifiés sur la première page avec les références de l'autorité émettrice ou de l'organisme auteur, la date d'émission et le numéro d'enregistrement. Ils portent le marquage suivant :

DIFFUSION RESTREINTE

sur chaque page, le timbre *Diffusion Restreinte* est apposé au milieu du haut de la page ; - pour les messages et autres documents électroniques, la mention *Diffusion Restreinte* est rappelée en début de chaque page ;

- pour les documents reliés, le timbre *Diffusion Restreinte* est apposé au milieu de la page de garde et de la couverture ;
- sur un support non papier, la mention *Diffusion Restreinte* est adaptée au type de support, définitive et toujours visible.

Les documents *Diffusion Restreinte* sont enregistrés au départ et à l'arrivée

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'événements, 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.

Toute information sensible dont le titulaire a connaissance à l'occasion de l'exécution du marché ne peut en aucun cas être communiquée à un tiers (autre que les agents du titulaire préalablement déclarés et autorisés par l'Administration dans la Liste) sans accord préalable exprès et écrit de l'Administration.

La réalisation d'une copie sans autorisation préalable est considérée par l'Administration comme une violation des dispositions relatives au respect du secret dans l'exécution du marché.

La politique générale de sécurité numérique du MI (PGSN-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 préalablement à tout commencement d'exécution du marché. Le titulaire s'engage à respecter, et faire respecter par ses agents, l'ensemble des obligations de ces PSSI/PGSN.

Dans les locaux du prestataire, les informations sensibles font l'objet d'une gestion spécifique. 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.

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 des documents, celle-ci doit être réalisée par broyage ou incinération. 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 MI. 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).

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 « qualifié » 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 de la Liste.

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 à l'Administration sans délai et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles.

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 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 de la liste pour un strict respect des obligations du titulaire en matière de SSI et d'en présenter un bilan de fréquence au moins semestrielle à l'occasion d'un des comités 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 MI.

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. Acronymes

ANSSI	Agence nationale de la sécurité des systèmes d'information
CCAG	Cahier des clauses administratives générales
CCAP	Cahier des clauses administratives particulières
CCATP	Cahier des clauses administratives et techniques particulières
CCTP	Cahier des clauses techniques particulières
CNI	Carte nationale d'identité
CSN	Conseillé de la Sécurité Numérique
DCE	Dossier de consultation des entreprises
DES	Dossier des exigences de sécurité
DTNUM	Direction de la transformation numérique du MI
DR	Diffusion restreinte
ERR	Engagement de reconnaissance de responsabilité
FEROS	Fiche d'expression rationnelle des objectifs de sécurité
IGI	Instruction générale interministérielle
IP	Internet Protocol
MAQE	Mission audit, qualité et évaluation (DTNUM)
MI	Ministère de l'intérieur et des outre-mer

MPSSI	Mission politique de sécurité des systèmes d'information
OS	Officier de sécurité
PES	Procédure d'exploitation de la sécurité des systèmes d'information
PGSN MI	Politique générale de sécurité numérique du MI
PSSI	Politique de sécurité des systèmes d'information
RC	Règlement de consultation
RCSSI	Responsable central de la sécurité des systèmes d'information
RSSI	Responsable de la sécurité des systèmes d'information
RSSI-B	Responsable de la sécurité des systèmes d'information « Bureautique »
RSSI-E	Responsable de la sécurité des systèmes d'information « Expertise »
RSSI-H	Responsable de la sécurité des systèmes d'information « Homologation »
SGNM	Service de la gouvernance numérique ministérielle (DTNUM)
SDGGP	Sous-direction de la gouvernance et des grands projets (DTNUM)
SDRAC	Sous-direction des ressources et de l'accompagnement au changement (DTNUM)
SDID	Sous-direction de l'innovation et de la donnée (DTNUM)
SDENTAT	Sous-direction de l'environnement numérique de travail et de l'animation territoriale (DTNUM)
SDAS	Sous-direction des architectures sécurisées (DTNUM)
SDAN	Sous-direction des applications numériques (DTNUM)
SDLP	Service de la protection
SI	Système d'information
SSI	Sécurité des systèmes d'information
VA	Vérification d'aptitude
VABF	Vérification d'aptitude et de bon fonctionnement
VSR	Vérification de service régulier