



MINISTÈRE DE L'INTÉRIEUR

**ATTESTATION
DE
RECONNAISSANCE DE RESPONSABILITE**

Relative 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

L'accès aux installations et l'utilisation des ressources informatiques du ministère doit se faire dans le strict respect de la législation et, en particulier, celle applicable au respect des personnes et de la propriété intellectuelle ainsi qu'aux actes de fraude, de détournement et de malveillance informatique.

Société _____ :

Nom _____ :

Prénom _____ :

Qualité _____ :

Réf du Marché _____ :

Je soussigné(e) reconnais avoir été sensibilisé par le titulaire responsable de l'exécution du marché 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 mon activité s'exerce en zone protégée telle que définie à l'article 73 de l'Instruction Générale Interministérielle n°1300 ;
- que toute éventuelle action contraire aux règles édictées doit être immédiatement signalée à la DSIC 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 321-3 du code pénal, et des dispositions concernant la propriété intellectuelle et notamment ses articles L.111-1, L.112-1 et L.112-2 (des extraits de ces textes sont fournis en annexe de ce document) ;
- 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 ;

Je m'engage par ailleurs à :

- respecter l'obligation de discrétion professionnelle pour tous les faits, informations ou documents dont j'aurais connaissance dans l'exercice ou à l'occasion de l'exercice de mes activités ;
- prendre connaissance, suivre et respecter les dispositions décrites en annexe I du CCAP relative à la protection des informations, à la confidentialité et aux mesures de sécurité ;
- ne divulguer, ou ne communiquer à un tiers, en aucun cas des informations ou données tant personnelles que professionnelles que je pourrais être amené(e) à apprendre dans l'exercice de ma mission ;
- ne pas reproduire, stocker, copier, diffuser, modifier, altérer ou détruire toute information ou donnée dont je pourrais avoir connaissance à d'autres fins que celles de l'exercice de ma mission ;
- respecter le principe fondamental du « besoin d'en connaître » et ainsi de ne pas tenter d'accéder, de reproduire, de stocker, de copier, de diffuser, de modifier, d'altérer ou de détruire toute information dont je ne suis pas supposé avoir connaissance dans l'exercice de ma mission.

Si, à l'occasion de l'exécution du marché, je dispose d'un accès à un système d'information de l'administration et, par conséquent, d'un compte nominatif, je m'engage également à :

- ne pas tenter d'introduire et 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 pas modifier sans autorisation la configuration des moyens mis à ma disposition et notamment de ne pas raccorder 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 pas me livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des services, applications et moyens auxquels j'ai accès ;
- ne pas mettre à la disposition d'utilisateurs non autorisés un accès privilégié aux ressources informatiques, données ou services ;
- ne pas perturber ou interrompre le fonctionnement normal du système d'information ou de l'un de ses composants ;
- ne pas installer, 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 ma disposition ;
- ne pas introduire, tester ou utiliser des supports informatique ou médias dont l'origine m'est inconnue, douteuse ou incertaine ;
- ne pas générer 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 terme de failles de sécurité ou de pollution virale ;

Je déclare être pleinement conscient(e) de mes responsabilités et reconnais être informé(e) des conséquences pénales, et contractuelles qui pourraient résulter de la non application des procédures et dispositions édictées ci-dessus.

Date :

Signature de l'intéressé(e)

Date :

Signature d'une personne physique ayant qualité pour engager la personne morale du titulaire du marché de prestation et cachet de la société.

EXTRAITS DES ARTICLES RELATIFS AUX DISPOSITIONS GÉNÉRALES RELATIVES À LA FRAUDE INFORMATIQUE

Art. 323-1 du nouveau code pénal : l'accès frauduleux à un système de traitement automatisé de données est sanctionné.

Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende.

Art. 323-2 : l'atteinte en disponibilité d'un système de traitement automatisé de données est sanctionnée.

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Art. 323-3 : l'atteinte en intégrité d'un système de traitement automatisé de données est sanctionnée.

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, ou de supprimer ou de modifier frauduleusement des données qu'il contient, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Art. 323-3-1 : l'utilisation, sans motif légitime, d'outils permettant de porter atteinte à un système de traitement automatisé de données est sanctionnée.

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

DISPOSITIONS CONCERNANT LA PROPRIÉTÉ INTELLECTUELLE

Art. L.111-1 du code de la propriété intellectuelle : l'auteur est titulaire des droits sur les logiciels qu'il crée.

L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Toute utilisation faite sans son consentement est considérée comme illicite et sanctionnée pénalement. La seule exception : le droit de courte citation qui permet de reproduire partiellement l'œuvre à condition d'en indiquer clairement l'auteur et la source.

Art. L.112-1&2 du code de la propriété intellectuelle : les logiciels sont protégés par les droits d'auteur.

Sont protégées toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, et notamment les logiciels. La mise sur le réseau informatique d'un document doit donc être conditionnée au fait d'être titulaire des droits sur ce document, ou pour le moins d'être autorisé à le reproduire sur le réseau.

nota : la licence d'un logiciel définit les droits accordés pour son utilisation. En règle générale, une copie de sauvegarde est autorisée.

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

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.

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.

Si un sous-traitant est susceptible d'intervenir pour le compte du titulaire durant l'exécution du marché, 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. 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 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 :
 - carte nationale d'identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires ;
 - titre de séjour en cours de validité avec une autorisation de travail valable ou carte de résident pour les étrangers extracommunautaires ;
- 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 signature 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 reconnaît avoir fait 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, une attestation de reconnaissance de responsabilité (ARR - jointe en annexe II au présent CCAP) par laquelle lesdits agents attestent d'une part, avoir pris connaissance des articles 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 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 sensibles du Ministère de l'Intérieur ou des informations couvertes par le secret de la défense nationale.

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

L'attestation de reconnaissance de responsabilité doit être obligatoirement signée, après la notification du marché et avant tout commencement d'exécution, par les agents susceptibles d'intervenir dans le marché, identifiés dans la « Liste ».

La « Liste », ainsi que l'attestation de reconnaissance de responsabilité, doivent être simultanément transmises au responsable du projet de l'administration, ainsi qu'à l'officier de sécurité du pôle SSI, à l'adresse suivante : dsic-poleSSI@interieur.gouv.fr

Le titulaire s'engage à ce que seules les personnes ayant préalablement souscrit l'attestation de reconnaissance de responsabilité précitée 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 Ministère de l'Intérieur 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 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 classifiées « 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'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 de Sécurité des Systèmes d'Information 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 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.

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 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 connaître¹ : 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.

¹ 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.

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 à l'occasion de la réunion de chaque comité de suivi du marché (COSUI).

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
CNI	Carte Nationale d'Identité
COSUI	Comité de suivi de marché
DR	Diffusion Restreinte
DSIC	Direction des Systèmes d'Information et de Communication du MI
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
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
Pôle SSI	Pôle Sécurité des Systèmes d'Information
ARR	Attestation de Reconnaissance de Responsabilité

Article à insérer à la suite de l'article IV du CCAP relatif aux « Engagements et responsabilités des parties »

IV.4 Sanction pécuniaire pour non-respect de la politique de sécurité des systèmes d'information

En cas de violation des mesures de sécurité et de protection des informations sensibles, ainsi que des obligations de confidentialité exposées en annexe n° 1 au présent C.C.A.P, le titulaire s'expose à l'application d'une sanction pécuniaire.

Cette sanction pécuniaire est calculée de la façon suivante :

- En cas de non-respect des règles de sécurité et de protection des informations sensibles n'impliquant pas des données à caractère personnel
Pour chacun des faits constatés, application d'une sanction égale à 0,5% du montant exécuté HT du marché à la date de constatation du fait générateur
- En cas de non-respect des règles de sécurité et de protection des informations sensibles impliquant des données à caractère personnel :
Pour chacun des faits constatés, application d'une sanction égale à 2% du montant exécuté HT du marché à la date de constatation du fait générateur

La clause doit toujours intégrer les deux niveaux de sensibilité des informations, quel que soit l'objet du marché.
Dans le cas des informations nominatives sensibles, sur recommandation spécifique du BACGOM, le taux peut être modifié en fonction du montant du marché.

En cas de constatation de plusieurs faits générateurs, indifféremment du niveau de sensibilité des informations concernées, les sanctions pécuniaires ainsi établies sont appliquées de façon cumulative.

Les sanctions pécuniaires sont appliquées après mise en demeure du titulaire de se conformer aux mesures de sécurité et de protection des informations sensibles exposées en annexe n° 1 du présent C.C.A.P, adressée par tout moyen vérifiable de correspondance.

L'application par le titulaire des mesures correctives visées dans sa mise en demeure ne sauraient l'exonérer du paiement des sanctions pécuniaires.

Le montant des sanctions pécuniaires ainsi établies vient en déduction des paiements à effectuer au titre de toute facture afférente aux prestations exécutées à la date de survenance du fait générateur.

Les sanctions pécuniaires sont appliquées sans préjudice des sanctions pénales encourues par le titulaire.