

ANNEXE 1 au CCAP

Dans l'éventualité où le prestataire propose une solution SaaS

La présente annexe a pour objet de compléter le CCAP du marché.

Elle complète les dispositions du CCAP pour encadrer l'éventuelle mise à disposition par le Titulaire d'une Plateforme accessible en mode SaaS (ci-après la **Plateforme**).

Clauses relatives à la mise à disposition d'un service informatique

Dans le cadre de l'exécution du présent marché, le Titulaire met en œuvre une solution technique correspondant à une plateforme de type SaaS (Software As A Service), hébergée par le Titulaire, cette solution est désignée ci-après par le terme de « **Plateforme** ».

Le présent article est applicable à la Plateforme mise en œuvre par le Titulaire pour l'exécution de ses obligations contractuelles.

Définitions

Adaptations : paramétrages réalisés par le Titulaire pour répondre aux besoins de l'Acheteur.

Documentation : désigne l'ensemble des documents afférents à la Solution, décrivant ses caractéristiques en termes de fonctionnalités et de performances ainsi que ses modalités d'utilisation. La Documentation est personnalisée à la Solution fournie à l'Acheteur et intègre le paramétrage réalisé. Au sens du présent Marché, lorsqu'il est fait référence à la Documentation, il s'agit toujours de la dernière version en vigueur de la Documentation, si cette dernière est amenée à évoluer régulièrement.

Donnée : désigne toute information, quel qu'en soit la forme et le fond, contenues et/ou entrées manuellement ou automatiquement, traitées et/ou produites dans le cadre du Marché. Les Données comprennent notamment les informations confidentielles au sens de l'article « Confidentialité » des présentes et les données à caractère personnel telles que définies à l'article 4 du RGPD.

Dysfonctionnement : signifie toute défaillance, faille de sécurité, défaut, erreur, non-conformité, dégradation des performances ou problème d'utilisation de la Solution, de ses mises à jour et/ou nouvelles versions induisant une gêne, une perturbation, ou une impossibilité totale ou partielle de bénéficier d'une ou plusieurs fonctionnalité(s).

Les Dysfonctionnements sont classés en trois catégories, en fonction de leur incidence sur le fonctionnement opérationnel de la Solution :

- **Dysfonctionnement Bloquant** : désigne toute erreur qui, unitairement ou cumulée, a des répercussions sur le fonctionnement de la Solution, empêchant l'utilisation ou l'exploitation normale d'une fonctionnalité ou plusieurs fonctionnalités essentielle(s) de la Solution et notamment se traduisant par l'absence d'exécution d'une fonction ou défaut dans l'exécution d'une fonction ou représentant une gêne importante pour l'Acheteur.
- **Dysfonctionnement Majeur** : désigne toute erreur qui affecte une partie des fonctions de la Solution, celle-ci fonctionnant de manière dégradée, sans bloquer ou risquer de bloquer l'exploitation d'une fonctionnalité essentielle de la Solution.

- **Dysfonctionnement Mineur** : désigne toute autre erreur n'ayant que peu d'impact pour l'Utilisateur.

Heures ouvrées : désigne les heures comprises entre [...] et [...] h.

Incident de Sécurité : désigne tout événement ou une série d'événements imprévus résultant de processus internes inadaptés ou défaillants ou d'événements extérieurs affectant la sécurité ou le fonctionnement des systèmes d'information et de communication (notamment leur disponibilité, leur intégrité, leur confidentialité ou leur continuité) et/ou la sécurité des informations utilisées pour la fourniture de la Solution (notamment sa disponibilité, son intégrité ou sa confidentialité). Ceci inclut les incidents provenant de cyber-attaque ou de la non-pertinence ou de la mise en échec des mesures de sécurité physique.

Programme Malveillant : désigne un code informatique nocif tel que notamment virus, bombes logiques, vers, chevaux de Troie ou tout autre code ou instruction infectant ou affectant tout programme, logiciel, donnée, fichier, base de données, ordinateur ou autre matériel ou élément, endommageant, portant atteinte, compromettant l'intégrité ou la confidentialité, perturbant en tout ou partie le fonctionnement, détournant ou permettant de détourner en tout ou partie un système d'information de l'usage auquel il est destiné.

Solution : désigne l'outil accessible en mode SaaS mis à disposition de la CDC (et la Documentation qui lui est afférente), permettant l'échange des Données, intégrant l'ensemble des fonctionnalités décrites dans le CCTP, paramétrée et personnalisée selon les besoins de l'Acheteur.

SaaS ou « Logiciel en tant que Service » : SaaS est l'acronyme de « *Software as a Service* ». Désigne le mode d'accès distant aux fonctionnalités de la Solution, par le biais d'Internet.

Services : désigne l'ensemble des services liés à l'utilisation de la Solution par l'Acheteur et décrits notamment au présent document et au CCTP.

Utilisateur : désigne toute personne physique autorisée par l'Acheteur à se connecter par accès distant à la Solution pour utiliser ses fonctionnalités.

Fourniture de la Plateforme

a- Hébergement de la Plateforme

Le Titulaire s'engage à héberger les données nécessaires à l'exécution de la Solution, notamment en mettant à disposition une infrastructure d'hébergement correspondant aux exigences de qualité et de sécurité tels que définis dans le présent C.C.A.P et dans le C.C.T.P.

Le Titulaire s'engage à adapter en permanence la capacité de stockage en prenant notamment en compte le volume des Données hébergées, l'évolution prévisible de celles-ci, la périodicité et le volume des Données mises en ligne.

Le centre d'hébergement (les serveurs) du Titulaire doit être localisé dans l'Espace Economique Européen (EEE). Cette exigence de localisation dans l'EEE concerne à la fois le stockage, les sauvegardes et l'archivage des données de l'Acheteur. L'Acheteur doit être informé de tout changement d'hébergeur entraînant un changement de localisation du centre d'hébergement, y compris au sein de l'EEE. Un changement du centre d'hébergement hors de l'EEE doit faire l'objet d'un accord préalable de l'Acheteur.

Le Titulaire s'engage à isoler son activité d'hébergement pour le compte de l'Acheteur, de toutes ses autres activités, au moyen d'un dispositif de séparation logique offrant des garanties de sécurité. Il s'engage à cloisonner les données de l'Acheteur de celles provenant de tiers.

Dans l'hypothèse où le Titulaire déciderait de changer l'un ou l'autre des équipements (serveurs, baies de stockage, disques...) du centre d'hébergement, il ferait son affaire personnelle des coûts éventuels induits, et garantit une continuité de services et de disponibilité des accès aux données.

La gestion des réseaux, les sauvegardes, les Données et la gestion des autorisations d'accès logique et physique notamment devront faire l'objet d'un soin attentif de la part du Titulaire et d'une très forte réactivité de sa part, ainsi que de la mise en œuvre des éléments de traçabilité nécessaires.

b- Conditions de sécurité renforcée et de sauvegarde

Le Titulaire prend toutes les précautions nécessaires pour garantir la protection et l'intégrité des données de l'Acheteur dans le cadre de l'hébergement de ces données. Il prend toutes les mesures pour empêcher l'accès par des tiers aux données qui lui sont confiées pendant l'exécution des présentes.

Le Titulaire est tenu également d'assurer la sécurité physique des Données de l'Acheteur notamment en les conservant dans des endroits sécurisés et en assurant de manière générale leur sécurité en prenant toutes les mesures utiles et nécessaires.

Les moyens informatiques mis en œuvre par le Titulaire pour l'exécution de ses obligations contractuelles, et notamment les postes de travail et outils de sauvegarde, seront conformes aux règles de sécurité définies par l'Acheteur ; sauf procédure exceptionnelle approuvée par l'Acheteur, il ne sera pas utilisé de support de stockage magnétique ou électronique externe (clé USB, disque amovible ou autre). Le Titulaire s'engage à :

- offrir toutes les garanties et notamment mettre en œuvre des solutions techniques et organisationnelles conformes à l'état de l'art assurant la protection des données, notamment au regard des dispositions légales et réglementaires en vigueur, tant sur le plan européen que national, en matière de protection des données à caractère personnel et notamment des exigences posées par le règlement européen n° 2016/679 relatif à la protection des données personnelles (« RGPD ») ;
- Mettre en œuvre toutes les procédures de traitements sécurisés et de prévention afin de garantir le bon fonctionnement de la Plateforme et empêcher toute intrusion non autorisée aux données et garantir leur intégrité ;
- Mettre en œuvre toutes les mesures requises afin de restreindre l'accès au service aux seules personnes autorisées ou habilitées par l'Acheteur ;
- Prendre toutes les mesures permettant, à la suite d'un incident, la restauration dans leur intégrité des données affectées par ledit incident.

Le Titulaire s'engage à communiquer à la demande de l'Acheteur ses plans de stockage et de sauvegarde en vigueur, prévoyant les modalités de stockage et de restauration ainsi que la fréquence des sauvegardes qui seront appliquées aux données de l'Acheteur et de ses utilisateurs. En tout état de cause, le Titulaire s'engage à mettre en œuvre tout moyen permettant d'assurer la sauvegarde des données de l'Acheteur, en particulier à effectuer des copies de sauvegarde ou de secours dans des lieux différents et à procéder à des tests de restauration annuels.

Il est précisé que les sauvegardes effectuées par le Titulaire le seront sans aucun risque, notamment en termes de disponibilité de la Plateforme. Le Titulaire s'engage à prendre toutes les mesures nécessaires pour limiter au maximum les risques de détérioration ou perte de données.

En cas de détérioration ou de perte de données imputables au Titulaire, ce dernier s'engage à procéder immédiatement et à ses frais à la restauration des Données sauvegardées.

c. Paramétrage personnalisé de la Solution

Le Titulaire assurera le paramétrage de la Solution en collaboration avec l'Acheteur pendant la mise en place de la prestation.

d. Accès à la Plateforme

La Plateforme est accessible entre **7h** et **21h** (ci-après les Heures ouvrées), par le biais d'une connexion à distance grâce à une adresse de connexion (URL), un identifiant de connexion (login) et un mot de passe (ci-après Identifiants de connexion).

Les Identifiants de connexion sont strictement personnels et confidentiels. La Plateforme doit permettre une authentification des utilisateurs par la mise en place d'une politique de gestion de mots de passe conforme aux recommandations de la CNIL, cette authentification doit se faire par des comptes nominatifs. Le Titulaire et les Utilisateurs s'engagent à ne pas divulguer à autrui leurs Identifiants de connexion et sont seuls responsables de la préservation de leur confidentialité et, par conséquent, des conséquences d'une divulgation involontaire à quiconque. L'Acheteur est responsable de la gestion des habilitations des Utilisateurs et des moyens informatiques permettant l'accès à la Solution.

A la demande de l'Acheteur, le Titulaire s'engage à mettre en place un système d'authentification forte, ainsi qu'une Plateforme sécurisée de changement de mot de passe en cas de perte de celui-ci par l'Utilisateur, sans surcoût supplémentaire pour l'Acheteur.

Le Titulaire doit assurer qu'il fournit une Plateforme pleinement exploitable avec les navigateurs Internet courants, y compris les montées de version de ces logiciels sur la durée du Marché.

Disponibilité de la Plateforme

La disponibilité s'entend de l'accessibilité complète depuis le réseau de l'Acheteur à la Plateforme (à savoir, à l'interface d'accueil de la Plateforme, à toutes ses fonctionnalités, ainsi qu'aux données qu'elle doit produire et/ou conserver aux termes de l'Marché).

Le Titulaire reconnaît que la disponibilité de la Plateforme est une condition substantielle de la signature de l'Marché par l'Acheteur et s'engage en conséquence à assurer un taux de disponibilité de la Plateforme de **99,9 %** à l'exception des périodes de maintenance prévues et acceptées par l'Acheteur.

A cet effet, le Titulaire s'engage notamment à mettre en œuvre tous les moyens, notamment humains, afin d'assurer une réactivité maximale en cas de problème entraînant ou susceptible d'entraîner un incident en termes de disponibilité de la Plateforme.

A cet effet, le Titulaire s'engage notamment à mettre en œuvre tous les moyens, notamment humains, afin d'assurer une réactivité maximale en cas de problème entraînant ou susceptible d'entraîner un incident en termes de disponibilité de la Plateforme.

Support technique

Le Titulaire met à la disposition de l'Acheteur un service de support technique accessible par téléphone ou par courriel pendant les jours ouvrés. Ce support technique a pour objet de fournir à l'Acheteur une assistance à l'utilisation de la Plateforme.

Respect des niveaux de service

Principes généraux

Dans le cadre de la fourniture d'un service en mode SaaS et afin de maintenir la qualité et la continuité de la Plateforme, le Titulaire s'engage, sur la base d'une obligation de résultat, à respecter les engagements de niveaux de service (qualité et délais) décrits dans les Documents Contractuels dans le cadre de l'hébergement et de l'exploitation de la Plateforme et ceci avec tout le soin et toute la diligence que l'Acheteur est en droit d'attendre d'un professionnel de services accessible par voie électronique.

Le Titulaire s'engage à alerter l'Acheteur sur tout événement, choix ou mesure perturbant la qualité et/ou la continuité du Service. Il s'engage de même à informer l'Acheteur sans délai en cas d'indisponibilité de la Plateforme et à rétablir le service conformément aux engagements de niveaux de service définis aux présentes et des engagements définis dans son offre.

Modalités de prise en compte des Dysfonctionnements

Au sens du présent Marché, « Dysfonctionnement » signifie toute défaillance, défectuosité, erreur, non-conformité, dégradation des performances ou problème d'utilisation de la Plateforme SaaS, de ses mises à jour et/ou nouvelles versions induisant une gêne, une perturbation, ou une impossibilité totale ou partielle de bénéficier d'une ou plusieurs fonctionnalité(s).

En cas de Dysfonctionnement (partiel ou total) de la Plateforme, y compris, en cas d'Indisponibilité et de perte de données/perte d'intégrité de données, les modalités suivantes sont appliquées :

Le Titulaire alerte l'Acheteur du Dysfonctionnement de la Plateforme par tous moyens convenus entre les Parties (immédiatement après sa découverte).

Le cas échéant, l'Acheteur alerte le Titulaire du Dysfonctionnement de la Plateforme par tous moyens convenus entre les Parties.

L'émission de l'information du Dysfonctionnement d'une des Parties à l'autre Partie (ci-après Notification) fait courir les délais de prise en compte du Dysfonctionnement, de fourniture d'une Plateforme de contournement du Dysfonctionnement le cas échéant, et de fourniture d'une correction définitive du Dysfonctionnement, par le Titulaire.

Le délai de prise en compte du Dysfonctionnement par le Titulaire ne devra pas excéder **quatre (4) Heures Ouvrées** à compter de l'émission de la Notification.

- Cette prise en compte prend la forme d'un courriel du Titulaire confirmant la réception de la Notification si l'alerte provient de l'Acheteur, et les motifs estimés du Dysfonctionnement, ainsi que le temps de correction provisoire et/ou définitive estimé.
- Le Titulaire confirme dans sa communication par mail la recherche de solutions.
- Le Titulaire procède au diagnostic de l'incident et met en œuvre sa correction dans le cadre des exigences de service.
- Jusqu'à la mise en place d'une « correction définitive » si elle ne peut être mise en œuvre immédiatement, le Titulaire s'engage à mettre en place, dans les plus brefs délais suivant la Notification une « solution de contournement » permettant la reprise de l'activité de l'Acheteur, même de manière dégradée,
- Le Titulaire s'engage à mettre en place une « correction définitive » dans les meilleurs délais à compter de la Notification.

Les causes précises des dysfonctionnements ainsi que les actions mises en œuvre pour les résoudre devront être communiquées à l'Acheteur dès clôture de l'incident. Seul l'Acheteur est habilité à clôturer un incident suite à la déclaration par le Titulaire de la résolution du problème.

Modalités spécifiques :

Temps de rétablissement du service (GTR)

Le Temps de rétablissement du Service (GTR) est calculé à partir de la Notification du Client jusqu'à la date/heure de mise en place d'une solution de contournement. En cas d'indisponibilité de la Plateforme liée notamment à un Dysfonctionnement, le Temps de rétablissement du Service est de **douze (12) Heures Ouvrées** à compter de la Notification.

Poursuite du Service

Modalités de continuité du Service

Le Titulaire devra assurer la disponibilité du service y compris en cas de « choc extrême » incluant les sinistres « bâtiments » (crue, incendie...) ou les sinistres affectant le personnel et les équipements sur le site en charge de la prestation décrite dans le présent CCTP (pandémie, mouvement social...).

Le Titulaire doit préciser les modalités mises en place pour garantir une continuité d'exploitation ou de services sur son site ou sur un site extérieur.

Le Titulaire doit présenter les garanties minimums qui suivent :

1. Le Titulaire dispose soit d'un Plan de Continuité d'Activité (PCA) soit d'une procédure de gestion de crise (joindre les documents à l'offre).

2. Le Titulaire dispose d'un site de back-up pour assurer la continuité de son activité. Ce back-up peut être organisé par ses propres moyens (par exemple, existence d'un deuxième site à une distance suffisamment éloignée)

3. Le Titulaire dispose d'un Plan de Sauvegarde Informatique (PSI) ou d'un système de sauvegarde informatique permettant que conserver les données à archiver au titre de la prestation. Dans le cas où le Titulaire ne serait pas doté d'un PSI, la procédure de sauvegarde informatique doit préciser :

- a. La fréquence des sauvegardes ;
- b. S'il s'agit de sauvegardes internes ou externes ;
- c. Le lieu de conservation des sauvegardes ;
- d. si le Titulaire dispose d'un contrat de maintenance pour son matériel informatique ;
- e. si le Titulaire dispose d'un contrat de maintenance pour son matériel professionnel ;
- f. si le Titulaire a les moyens d'assurer la continuité de son activité en cas de grève de son personnel, de sinistre affectant ses locaux, de sinistre affectant le matériel d'exploitation.

Par ailleurs, il mettra en œuvre des mécanismes afin d'assurer dans les meilleures conditions la gestion des coupures électriques ou de toute autre anomalie de ce type.

La fin de la durée du PUPA et la reprise de la prestation sur le site du Titulaire seront décidées conjointement entre le Titulaire et l'Acheteur. Les vérifications préalables (techniques, humaines et matérielles) à la reprise des traitements sur le site du Titulaire sont de la responsabilité de ce dernier. Une formalisation de ces vérifications devra être communiquée à l'Acheteur pour une prise de décision et valider le retour à la normale des traitements.

Le Titulaire transmettra à l'Acheteur toute modification de son PCA au cours de la prestation.

Des exercices de déploiement du PCA seront menés avec le Titulaire, au cours de l'exécution de l'Marché, dans des conditions qui seront précisées en accord avec ce dernier.

Modalités de Gestion de crise

Le Titulaire s'engage à communiquer à l'Acheteur les coordonnées d'un contact en sécurité des systèmes d'information et d'un responsable du compte disponible pour répondre en cas de crise, notamment en cas de survenance d'un Dysfonctionnement.

Lorsqu'un dysfonctionnement intervient sur un processus de tout ou partie de la Plateforme, le Titulaire s'engage à :

- apporter sa contribution à la gestion de crise dans le cadre d'une cellule pilotée par l'Acheteur sans délai, même si la Plateforme confiée au Titulaire n'est pas directement concernée par le Dysfonctionnement dès lors qu'il se trouve être en adhérence avec le dysfonctionnement objet de la gestion de crise ;
- impliquer l'Acheteur à la gestion de crise dans le cadre d'une cellule pilotée par le Titulaire en cas de dysfonctionnement impactant directement le Service confié au Titulaire
- appliquer les actions décidées par la cellule de crise pilotée par l'Acheteur dans les délais fixés conjointement.

Restitution et Réversibilité

Les stipulations du présent article complètent l'article 42 du C.C.A.G.-T.I.C.

Au terme de l'exécution du Marché, quelle qu'en soit la cause en ce compris la résiliation du Marché en cours, le Titulaire s'engage à la demande de l'Acheteur à restituer puis à détruire l'ensemble des Données de l'Acheteur en sa possession et/ou ayant fait l'objet d'un stockage par le Titulaire. Cette restitution s'opérera, aux frais du Titulaire dans les conditions et selon le format définis par l'Acheteur au moment de la cessation du marché.

Le Titulaire s'engage à ne conserver aucune Donnée sauf accord préalable de l'Acheteur. La demande de conservation de Données issues du Marché, formulée par le Titulaire à l'Acheteur, devra être justifiée et devra préciser la nature des Données concernées. La destruction des Données sera attestée par la rédaction d'un procès-verbal de destruction. L'Acheteur se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect de ces obligations.

L'Acheteur collaborera activement avec le Titulaire afin de faciliter la récupération des Données et le cas échéant la transmission des Données à un autre prestataire.

Le Titulaire fera en sorte que l'Acheteur puisse poursuivre l'exploitation des Données, sans rupture, directement ou avec l'assistance d'un autre prestataire.

Le Titulaire s'engage à assurer à la demande de l'Acheteur, pouvant être motivée par la fin de l'exécution Marché ou sa résiliation, une prestation de réversibilité afin de permettre à l'Acheteur ou à un prestataire tiers, librement choisi par l'Acheteur, de reprendre les données dans les meilleures conditions, sans rupture de service ou dommage pour l'Acheteur.

Les parties conviennent qu'à l'issue du Marché, et pendant les deux mois qui suivront, le Titulaire s'engage à répondre à toute demande d'assistance de l'Acheteur. Les modalités contractuelles et financières de toute demande d'assistance technique seront fixées par les Parties sur la base de propositions établies par le Titulaire dans les meilleurs délais.

Au titre des prestations de réversibilité, le Titulaire s'engage à :

- a) informer systématiquement l'Acheteur de toute modification pouvant avoir une incidence sur la réversibilité ;
- b) fera figurer dans tous les contrats qu'il serait amené à souscrire ou qui seraient utiles pour l'exploitation et la maintenance, les clauses mettant à la charge de son cocontractant les obligations nécessaires au respect des termes du présent Marché. Si ces clauses ne sont pas acceptées par un fournisseur, le Titulaire s'engage à en informer l'Acheteur et à en discuter avec lui préalablement à toute action, afin de se concerter sur les dispositions à prendre en conséquence ;
- c) fournir à l'Acheteur, au plus tard lors de la restitution des fichiers, données ou informations qui lui appartiennent, toute information, toute recommandation, tout conseil, tout document nécessaire ou utile à l'Acheteur pour la mise en œuvre d'un service de niveau équivalent à celui assuré par le Titulaire dans le cadre du présent Marché ;
- d) veiller à transférer aux équipes de l'Acheteur les compétences lui permettant de faire reprendre par un tiers les données et de permettre la migration vers ce tiers. Le transfert de compétences consiste

d'une manière générale en la communication à l'Acheteur, ou au tiers désigné par l'Acheteur, de toute information de quelque nature que ce soit permettant d'assurer le transfert de ses données vers un autre prestataire ;

e) assurer la continuité de la Solution pendant la phase de réversibilité, dans le respect des niveaux de service prévus au Marché.

L'ensemble de ces prestations est compris dans le prix du marché (cf. Bordereau des prix unitaires – BPU).

Il est entendu que la mise en œuvre de la réversibilité interviendra trois (3) mois avant le terme du Marché et pendant la durée nécessaire à sa mise en œuvre. Dans le cas d'une résiliation, cette phase interviendra dès la notification de la résiliation du Marché par l'Acheteur et pendant la durée nécessaire à la mise en œuvre du plan de réversibilité.

Le Marché sera prorogé, le cas échéant, jusqu'à l'achèvement des prestations de réversibilité qui sera matérialisé par la signature d'un procès-verbal de fin de réversibilité sans réserve par l'Acheteur.

Audit

Les stipulations du présent article complètent l'article 24 du C.C.A.G.-T.I.C.

Outre les audits au titre du Règlement européen sur la protection des données, les Parties conviennent que l'Acheteur, après en avoir avisé le Titulaire par écrit avec un préavis minimum de quinze (15) jours ouvrés (sauf en cas d'intervention urgente faisant suite à un Incident de sécurité), pourra faire procéder, à ses frais, à des audits, notamment de sécurité.

Ces audits pourront être effectués, soit par une structure d'audit interne au Groupe Caisse des Dépôts soumise à l'obligation de confidentialité mentionnée supra, soit par un cabinet extérieur au Groupe Caisse des Dépôts, tenu à une obligation de confidentialité, et qui ne pourra alors être un concurrent direct du Titulaire.

Il est expressément convenu que le Titulaire aura la faculté de refuser de façon motivée un nom de société extérieure proposé par l'Acheteur pour la raison ci-dessus évoquée. Si l'Acheteur estime suffisamment motivé le refus du Titulaire, il lui propose le nom d'une autre société.

Dans le cadre de ces audits, le Titulaire s'engage à coopérer pleinement avec les auditeurs internes de l'Acheteur ou avec la société extérieure qu'il aura mandatée à cet effet et à leur fournir toutes les informations nécessaires.

Au cas où un rapport d'audit ferait apparaître un non-respect des obligations du Titulaire visées au présent Marché, ce dernier s'engage expressément à mettre en œuvre les mesures correctives nécessaires dans un délai de quinze jours (15) ouvrés à compter de la notification du non-respect des obligations par l'Acheteur au Titulaire, aux frais exclusifs de ce dernier.

Il s'engage également à proposer un plan d'action (correction ou solution de contournement) qui résulterait de toute faille de sécurité constatée lors de ces audits ou en toute autre circonstance, mettant en cause la confidentialité ou l'intégrité des Données de l'Acheteur.

Les Parties conviennent, qu'en tout état de cause la procédure d'audit n'exonère pas le Titulaire du respect de ses obligations contractuelles.

L'absence de mesures correctives ou la prise en compte partielle des observations de l'Acheteur entraîne, à la seule discrétion de ce dernier, la résiliation du Marché aux torts exclusifs du Titulaire.

Sécurité informatique

Infection des livrables par un Programme Malveillant

Le Titulaire s'engage à fournir des Livrables exempts de tout dispositif de Programme Malveillant.

Avant toute livraison de supports, le Titulaire s'engage à procéder à une détection de Programme Malveillant au moyen d'outils de détection et d'éradication intégrant des fonctionnalités reconnues sur le marché dans leur dernière version disponible au moment de la livraison.

Si, à l'issue de ce contrôle, il s'avérait que la procédure de détection de Programme Malveillant mise en œuvre par le Titulaire était inopérante, l'Acheteur notifiera par téléphone ou par courrier postal ou électronique au Titulaire qu'un Programme Malveillant a été détecté, et ce dans les plus brefs délais.

En réponse à cette notification, le Titulaire livrera dans les meilleurs délais et à titre gracieux, des supports de remplacement, exempts de Programme Malveillant.

Infection du système d'information par un Programme Malveillant

En cas d'introduction d'un Programme Malveillant dans le système d'information de l'Acheteur, le Titulaire et l'Acheteur conviennent de collaborer afin d'en déterminer l'origine d'un commun accord et d'en éradiquer les conséquences.

S'il s'avérait que l'introduction du Programme Malveillant est imputable au seul Pouvoir Adjudicateur, celui-ci prendra à sa charge les frais de diagnostic et de remise en état.

S'il s'avérait que l'introduction du Programme Malveillant est imputable au Titulaire, celui-ci prendra à sa charge les frais de diagnostic et de remise en état.

Modalités de traitement des Incidents de Sécurité

Le Titulaire s'engage à informer l'Acheteur, dans un délai de 72 heures à compter de sa survenance tout Incident de Sécurité impactant la Plateforme et affectant les systèmes d'information de l'Acheteur comme du Titulaire, mis en œuvre dans le cadre de l'Marché, notamment les cas d'indisponibilité du Service, les infections par des programmes malveillants, l'accès et les modifications non autorisées, l'exploitation avérée ou supposée de vulnérabilités de sécurité.

Le Titulaire documente tout Incident de Sécurité, en indiquant les faits concernant l'Incident de Sécurité, les types de Données concernées, ses effets et les mesures prises pour y remédier.

Le Titulaire s'engage à communiquer les informations dont il dispose dès qu'il a connaissance d'un Incident de Sécurité et les complète au fur et à mesure de son analyse de l'Incident de Sécurité. Le Titulaire répond aux demandes d'informations complémentaires de l'Acheteur concernant l'Incident de Sécurité dans les meilleurs délais.

Les notifications d'Incident de Sécurité par le Titulaire sont à communiquer simultanément :

- aux contacts de l'Acheteur en charge de la relation contractuelle ;
- aux contacts métier/MOA de l'Acheteur avec lequel le Titulaire est en relation dans le cadre du Service ;

- au CERT du Groupe Caisse des Dépôts, l'équipe opérationnelle chargée de gérer les incidents de sécurité informatique pouvant impacter le groupe, via cert@caissedesdepots.fr

Le Titulaire s'engage à mettre en œuvre un processus de traitement des Incidents de Sécurité. Il s'engage à informer l'Acheteur de l'avancement du traitement dans le cadre de comités ad hoc.

Le Titulaire garantit que ses sous-traitants, préposés ou agents n'exploitent aucunement les vulnérabilités de sécurité, sauf autorisation préalable et écrite de l'Acheteur.

Tests d'intrusion et de vulnérabilité

Sans préjudice des tests d'intrusion et de vulnérabilité réalisés par le Titulaire sur ses systèmes d'information, le Titulaire s'engage à réaliser annuellement, des tests d'intrusion et de vulnérabilité sur l'environnement de production aux fins d'évaluer la capacité des systèmes d'information de résister à des attaques de sécurité informatique.

Ces tests pourront, a minima, être conçus pour :

- répondre aux menaces et garder les systèmes d'information protégés en permanence,
- identifier et gérer les vulnérabilités des systèmes d'information,
- réduire les possibilités de pannes des systèmes d'information,
- améliorer le niveau de conformité des systèmes d'information aux standards et normes applicables.

Le Titulaire communiquera à l'Acheteur le rapport des tests d'intrusion et de vulnérabilité réalisés composé du périmètre des tests réalisés ainsi que les principales conclusions de ces tests.

Si le rapport des tests d'intrusion et de vulnérabilité révèle des vulnérabilités, celles-ci seront prises en charges et traitées entre les Parties dans les conditions ci-dessous.

Modalités de corrections des vulnérabilités

Toute vulnérabilité susceptible de compromettre la sécurité de la Plateforme ou des données de l'Acheteur doit être prise en compte dans les meilleurs délais.

Pour toute vulnérabilité impactant la Plateforme, le Titulaire s'engage à :

- proposer un correctif temporaire ou une Plateforme palliative dans les plus brefs délais sur la base d'échanges réguliers avec les responsables sécurité des systèmes d'information de l'Acheteur ;
- mettre en œuvre un correctif définitif dans les meilleurs délais après échanges avec les responsables sécurité des systèmes d'information de l'Acheteur décrits dans le tableau ci-après.

Ces modalités de correction sont calculées sur la base des critères du Common Vulnerability Scoring System (CVSS), système d'évaluation standardisé de la criticité des vulnérabilités.

| CVSS base score v3 | Délai maximal d'application d'un correctif temporaire ou d'une Plateforme palliative | Délai maximal d'application d'un correctif définitif |
|--------------------|--|--|
| 9.0-10.0 | 5 (cinq) jours | 30 (trente) jours |

| | | |
|-------|-------------------|--------------------------------|
| 7-8.9 | 30 (trente) jours | 90 (quatre-vingts dix) jours |
| 4-6.9 | Non applicable | 180 (cent quatre vingts) jours |

Traçabilité

Le Titulaire s'engage à conserver et protéger l'intégrité des journaux d'événements et traces des événements générés par l'utilisation de la Solution par l'Acheteur dans le cadre de l'exécution du présent Marché. Il s'engage à prendre les mesures nécessaires à l'égard de son personnel, de ses sous-traitants et fournisseurs pour assurer, sous sa responsabilité, la conservation des journaux d'événements et traces pour une durée conforme aux textes et recommandations en vigueur.

Le Titulaire mettra à disposition les traces de connexion et journaux d'évènement à la demande de l'Acheteur de manière continue via une API ou un autre mécanisme dédié à même d'être intégré à un système de gestion des logs de l'Acheteur. Le Titulaire s'engage à informer l'Acheteur de toute Dysfonctionnement qu'il détectera dans les traces de connexion.

Protection des données à caractère personnel

Les stipulations de l'article 3 du CCAP sont applicables.

Chacune des parties s'engage à respecter la réglementation en vigueur applicable au traitement des données personnelles, notamment la loi n° 78-17 du 6 janvier 1978 modifiée et mise à jour, et le Règlement Général sur la Protection des Données (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à la libre circulation de ces données et abrogeant la directive 95/46/CE (la « Réglementation Protection des Données Applicable »).

Le Titulaire détermine seul les finalités et moyens des traitements de données effectués dans le cadre de la réalisation des prestations, à ce titre, il agit en tant que Responsable de traitement. Par conséquent, il fera son affaire personnelle du respect de ses obligations dans le cadre de la Réglementation Protection des Données Applicable et en particulier :

- d'information préalable des personnes concernées, du recueil de leur consentement, si nécessaire, de la gestion des droits d'accès, de rectification, d'opposition et de radiation des données personnelles relatives à chaque personne concernée ;
- d'intégrer la protection de la vie privée dans la conception et tout au long de la fourniture des prestations ;
- d'assurer la sécurité des Données notamment en adoptant des mesures techniques et organisationnelles appropriées, précises, détaillées et documentées pour protéger les Données contre tout risque de destruction, perte, altération, divulgation ou accès non autorisé, mais également pour en assurer la disponibilité et l'intégrité selon le règlement n°2016/679.

Droit de propriété intellectuelle applicable à la prestation de service informatique

Licence d'utilisation de la Plateforme

Le Titulaire garantit qu'il dispose ou est investi, de la part des titulaires des droits de propriété intellectuelle, des autorisations nécessaires pour permettre l'utilisation de la Plateforme.

L'Acheteur bénéficie à titre personnel et non exclusif d'un droit d'usage afférent à la Plateforme et à la Documentation associée pour le monde entier et pour la durée de de l'Marché telle que cette durée est définie ci-avant. Ce droit d'usage est compris dans le prix de l'Marché.

Ce droit d'usage permet à l'Acheteur d'utiliser les Services et la Documentation associée pour les besoins de l'Marché.

Ce droit d'usage permet également à l'Acheteur de gérer, utiliser, reproduire et faire tous usages nécessaires de ses contenus dont les Données et les bases de données intégrées ou générées dans la Plateforme ou issues de celle-ci, dans les conditions de l'Marché.

Ce droit d'usage pourra être transféré par l'Acheteur vers l'une de ses filiales après en avoir informé par écrit le Titulaire.

Le Titulaire autorise également expressément l'utilisation de la Plateforme par tout tiers agissant pour le compte de l'Acheteur et sous sa responsabilité, sans coût additionnel et quel que soit le titre auquel ce tiers intervient.

Le prix de la concession décrite dans le présent article est compris dans le prix de l'Marché.