Corporation de Gestion de la Voie Maritime du Saint-Laurent
The St. Lawrence Seaway Management Corporation

CONDITIONS DE PROTECTION DES DONNÉES

Dernière mise à jour : Le 26 octobre 2022

Contenu

CONDITIONS DE PROTECTION DES DONNÉES

Les conditions de protection des données suivantes énoncent l'entente mutuelle des parties concernant la confidentialité et la sécurité des Informations de la CGVMSL, l'accès aux systèmes de la CGVMSL et le plan de continuité des activités du Contractant.

1. Définitions

1.1 Aux fins de ce document, les termes ci-dessous ont les significations suivantes lorsqu'ils sont en majuscules et tous les termes qui ne sont pas énumérés ici ont la signification qui leur est attribuée ailleurs dans les Documents contractuels.

« Coûts » désigne les dépenses de toute nature, y compris les frais d'avocat, les frais de contentieux, les frais d'enquête, les frais de notification à toute personne ou organisation en cas d'Incident touchant les données, et les frais de fourniture de services de protection des consommateurs à toute personne en cas d'Incident touchant les données, y compris les services de surveillance du crédit ou de restauration de l'identité.

« CPD » désigne les présentes Conditions de protection des données.

« Examen de la sécurité » désigne l'évaluation par la CGVMSL de l'ensemble ou de certains éléments du Programme de sécurité du Contractant.

« Exigences en matière de confidentialité et de sécurité » signifie dans la mesure où elles s'appliquent à la CGVMSL ou au Contractant :

a) les lois, règles et règlements fédéraux, provinciaux, locaux et internationaux, ainsi que les exigences gouvernementales actuellement en vigueur et à mesure qu'elles entrent en vigueur, concernant de quelque façon que ce soit la vie privée, la confidentialité, l'intégrité, la disponibilité ou la sécurité des Informations de la CGVMSL, y compris, mais sans s'y limiter, la Loi sur la protection des renseignements personnels et les documents électroniques (Canada) et toute loi qui la remplace ;

b) les mesures de protection standard de l'industrie spécifiées dans les Documents contractuels concernant la vie privée, la protection des données, la confidentialité, l'intégrité, la disponibilité ou la sécurité des informations (par exemple, les contrôles de sécurité des informations), y compris, sans s'y limiter, la norme de sécurité des données de l'industrie des cartes de paiement (le cas échéant) et toute autre norme similaire ;

c) toutes les politiques, les déclarations ou les avis fournis par écrit au Contractant par la CGVMSL, conformément aux Documents contractuels ; et

d) tous les contrôles exigés par la CGVMSL, y compris les normes de codage sécuritaires énoncées dans les Documents contractuels.

« Incident touchant les données » signifie tout accès non autorisé raisonnablement soupçonné ou réel à des Informations de la CGVMSL (y compris les dossiers sur papier) ou à leur acquisition, leur divulgation, leur utilisation ou leur perte, ou toute violation ou compromission du Programme de sécurité du Contractant qui présente une menace pour tout renseignement de la CGVMSL ou tout Système de la CGVMSL.

« Informations de la CGVMSL » désigne les éléments suivants, quelle que soit leur forme ou le support sur lequel ils sont conservés, auxquels le Contractant peut avoir accès, qu'il peut utiliser ou qui peuvent lui être divulgués dans le cadre de l'exécution de Services pour la CGVMSL ou en son nom, ou par tout autre moyen :

a) Renseignements personnels : Toute information relative à une personne identifiée ou identifiable, que cette personne soit un client, un employé de la CGVMSL ou ayant un autre statut (y compris, mais sans s'y limiter, le nom, l'adresse postale, l'adresse électronique, le numéro de téléphone, la date de naissance, le numéro d'assurance sociale, le numéro de permis de conduire, autre numéro d'identification émis par le gouvernement, numéro de compte financier, numéro de carte de crédit ou de débit, numéro d'identification ou de compte d'assurance, renseignements médicaux ou sur la santé, rapports sur les consommateurs, vérifications des antécédents, données biométriques, signatures numériques, tout code ou mot de passe qui pourrait être utilisé pour avoir accès à des ressources financières, ou tout autre identificateur unique) ;

b) Informations sensibles : Toute information identifiée comme « Classifiée », « Sensible », « Confidentielle » ou une marque similaire indiquant la nature hautement sensible de l'information et pouvant inclure, sans s'y limiter, (i) des renseignements personnels s'ils sont de nature particulièrement sensible ou (ii) des renseignements du gouvernement fédéral relatifs aux intérêts nationaux du Canada tels que les renseignements R2 ou MARSEC.

c) Informations non publiques : Les informations commerciales confidentielles non publiques et les informations que le Contractant doit raisonnablement croire confidentielles.

« Programme de sécurité » désigne un programme écrit complet de sécurité de l'information décrit ci-dessous à l'Article 5 (Programme de sécurité des données).

« Réclamations » signifie toutes les réclamations, demandes, allégations, assertions, plaintes, pétitions, demandes, procès, actions, procédures, causes d'action et jugements.

« Sous-traitant » signifie tout entrepreneur affilié ou autre agent direct ou indirect agissant au nom du Contractant qui traite les Systèmes de la CGVMSL ou les Informations de la CGVMSL ou y a accès.

« Système de la CGVMSL » désigne tout système de TI/SI/OT appartenant à la CGVMSL ou faisant l'objet d'une licence, tel que, mais sans s'y limiter, les logiciels développés en interne ou acquis, les bases de données, les applications Web, l'infrastructure de serveur sur place ou hébergée, l'infrastructure de réseau, y compris les services loués et en copropriété, les mesures de protection en matière de cybersécurité, les dispositifs de l'utilisateur final, l'équipement de télécommunication et tout autre équipement faisant partie des environnements électroniques de l'entreprise et du contrôle industriel.

2. Reconnaissances

2.1 Le Contractant reconnaît et accepte qu'il est le seul responsable de la protection de la confidentialité, de la sauvegarde et de la sécurité des Informations de la CGVMSL et, le cas échéant, du contrôle de l'accès aux systèmes de la CGVMSL conformément à des normes égales ou supérieures décrites dans le présent CPD, que ces Informations de la CGVMSL soient ou non transférés ou que les systèmes de la CGVMSL soient accessibles à un tiers Sous-traitant, concédant ou fournisseur ou à un autre tiers autorisé par le Contractant .

3. Portée

3.1 Les présentes Conditions de protection des données s'appliquent à toutes les Informations de la CGVMSL et à tout accès aux Systèmes de la CGVMSL dans le cadre du Contrat.

4. Supervision

4.1 Le Contractant doit exercer la supervision nécessaire et appropriée sur son personnel et sur les autres personnes agissant en son nom afin de maintenir la confidentialité, l'intégrité, la disponibilité et la sécurité des Informations de la CGVMSL et, le cas échéant, des systèmes de la CGVMSL.

5. Programme de sécurité des données

5.1 Le Contractant déclare et garantit qu'il a mis en œuvre et qu'il maintiendra un Programme de sécurité qui, au minimum, est conforme aux Exigences en matière de confidentialité et de sécurité. Le Programme de sécurité du Contractant doit comprendre des mesures de protection administratives, techniques et physiques appropriées qui assurent la confidentialité, la disponibilité, l'intégrité et la sécurité des Informations de la CGVMSL et des systèmes de la CGVMSL et comprend les mesures de protection minimales figurant dans la liste ci-dessous dans la mesure requise par les Documents contractuels, sauf si des dérogations sont approuvées par écrit par la CGVMSL :

a) **Les politiques de sécurité de l'information** sont documentées par le Contractant à l'aide d'un cadre de contrôle de la sécurité fondé sur une norme industrielle acceptée pour régir les pratiques de sécurité de l'information (p. ex., NIST, ISO, etc.).

b) **Les contrôles d'authentification des utilisateurs**, y compris les méthodes sécurisées d'attribution, de sélection et d'entreposage des identifiants d'accès, la restriction de l'accès aux utilisateurs actifs et le blocage de l'accès après un nombre raisonnable de tentatives d'authentification infructueuses. L'authentification multifactorielle (AMF) est utilisée pour tout utilisateur accédant aux systèmes du Contractant soutenant les services fournis à la CGVMSL en vertu du présent Contrat.

c) **Des contrôles d'accès sécurisés**, y compris des contrôles qui limitent l'accès aux Informations de la CGVMSL et aux systèmes de la CGVMSL aux personnes qui ont un besoin commercial réel et démontrable de savoir, soutenus par des politiques, des protocoles et des contrôles appropriés pour faciliter l'autorisation, l'établissement, la modification et la cessation de l'accès.

d) **Des ajustements appropriés et opportuns du Programme de sécurité du** Contractant sur la base d'évaluations périodiques des risques, d'évaluations complètes régulières (telles que des évaluations par des tiers comme les audits SSAE SOC 2, type 2) du Programme de sécurité du Contractant, de la surveillance et des tests réguliers de l'efficacité des mesures de protection, et d'un examen des mesures de protection au moins une fois par an ou à chaque fois qu'il y a un changement important dans l'environnement technique ou les pratiques commerciales du Contractant qui peut mettre en cause la confidentialité, la disponibilité, l'intégrité ou la sécurité des systèmes d'information du Contractant.

e) **Des programmes de formation et de sensibilisation** conçus pour s'assurer que le personnel du Contractant et les autres personnes sous contrat avec le Contractant , ou agissant au nom du Contractant, connaissent et respectent les politiques, procédures et protocoles du Programme de sécurité.

f) **Réalisation de tests de sécurité** sur les applications ou le code logiciel développés au nom de la CGVMSL pour s'assurer que le Service est protégé contre les vulnérabilités décrites dans la dernière version de la liste « OWASP Top Dix ».

g) **Surveillance des systèmes** conçus pour assurer l'intégrité des données et prévenir la perte ou l'accès non autorisé aux Informations de la CGVMSL et, le cas échéant, aux systèmes de la CGVMSL, ainsi que l'acquisition, l'utilisation ou la divulgation de ces informations.

h) **Mesures de sécurité techniques**, y compris la protection par pare-feu, IDS/IPS, la protection antivirus, analyses de vulnérabilité, la gestion des correctifs de sécurité, configuration sécurisée du système, l'enregistrement de l'accès aux Informations de la CGVMSL ou de leur utilisation ou divulgation, la détection des intrusions et le chiffrement des données en transit et au repos.

i) **La gestion des vulnérabilités** et l'application de correctifs comprennent un processus permettant de remédier aux vulnérabilités critiques dans les 48 heures, aux vulnérabilités élevées dans les 7 jours et aux vulnérabilités moyennes dans les 30 jours.

j) **Des contrôles de réseau et de communication** doivent être mis en œuvre pour garantir que seuls les dispositifs autorisés bénéficient d'un accès au réseau lorsqu'ils sont physiquement connectés au réseau. Toutes les connexions sans fil contrôlées par le Contractant doivent être sécurisées à l'aide du protocole Wi-Fi Protected Access 2 (« WPA2 ») ou d'un meilleur protocole de sécurité.

k) **Mesures de sécurité des installations physiques**, y compris les contrôles d'accès, conçues pour limiter l'accès aux Informations de la CGVMSL et, le cas échéant, aux systèmes de la CGVMSL aux personnes décrites au point (b) ci-dessus. Les équipements doivent être protégés contre les menaces et les risques environnementaux, ainsi que contre les pannes de courant et autres perturbations causées par des défaillances des services publics de soutien.

l) **Segmentation physique ou logique des Informations de la CGVMSL** par rapport aux données des autres.

m) **Le processus de gestion des risques**, y compris une méthodologie d'évaluation des risques, doit être défini par le Contractant. Le Contractant doit procéder à des évaluations régulières des risques pour s'assurer que les contrôles de sécurité fonctionnent correctement et documenter les résultats et les plans d'action.

n) **Environnements de développement/test/production séparés** : Les environnements de développement, de test et d'exploitation sont séparés afin de réduire les risques d'accès ou de modifications non autorisés de l'environnement d'exploitation.

o) **Vérification des antécédents** du personnel et des autres personnes agissant au nom du Contractant qui auront accès ou dont on peut raisonnablement prévoir qu'ils auront accès aux Informations de la CGVMSL et, le cas échéant, aux systèmes de la CGVMSL, et n'autoriser l'accès qu'au personnel et aux autres personnes dont les antécédents ont été vérifiés au moment de l'embauche. Le Contractant n'autorisera pas sciemment l'accès aux Informations de la CGVMSL ou aux systèmes de la CGVMSL aux membres du personnel ou à d'autres personnes qui ont été condamnés pour vol ou qui ont fait l'objet de condamnations liées à la fraude pour lesquelles un pardon n'a pas été accordé.

6. Transfert des Informations de la CGVMSL

6.1 Informations de la CGVMSL :

a) ne doivent pas être entreposés ou transportés sur un ordinateur portable, tout autre appareil mobile ou tout support d'entreposage amovible, y compris les clés USB, les DVD ou les CD, à moins que ces appareils ou supports ne soient chiffrés au moyen d'une méthode de chiffrement approuvée par écrit par la CGVMSL ;

b) doivent être transférés par le biais d'un FTP sécurisé ou d'un autre protocole ou d'une méthode de cryptage, comme TLS v1.2 ou plus, ou approuvés par écrit par la CGVMSL ; et

c) doivent être physiquement déplacés, enlevés, détruits ou transférés uniquement selon des contrôles élaborés ou approuvés par écrit par la CGVMSL.

7. Entreposage des données

7.1 Le Contractant doit chiffrer toutes les Informations de la CGVMSL, quel que soit leur emplacement, au repos et en transit.

7.2 Le Contractant doit utiliser des clés de chiffrement spécialisées. Toutes les clés de chiffrement utilisées pour protéger les Informations de la CGVMSL doivent être associées de façon unique à la CGVMSL.

7.3 Toutes les clés seront protégées contre toute modification ; les clés secrètes et privées doivent être protégées contre toute divulgation non autorisée.

7.4 Le Contractant doit mettre en œuvre le chiffrement complet du disque sur tout dispositif informatique personnel contrôlé par le Contractant qui peut accéder aux Informations de la CGVMSL, les entreposer, les traiter, les transmettre ou les créer. Ce chiffrement doit au moins satisfaire à la norme de chiffrement avancé avec une clé de chiffrement de 256 bits (" AES-256 "), tel que décrit dans la publication 197 des Federal Information Processing Standards (" FIPS 197 ").

7.5 Si des bandes sont utilisées pour la sauvegarde du système, ces bandes doivent être cryptées, inventoriées et enregistrées de manière appropriée quant à leur emplacement et à leur date de destruction prévue.

8. Résidence de données

8.1 Les Informations de la CGVMSL ne peuvent être transférés, entreposés ou traités à l'extérieur du Canada pour quelque raison que ce soit sans l'approbation écrite préalable de la CGVMSL, y compris les transferts à des Sous-traitants ou à des agents, nonobstant les dispositions de l’Article 10 (Processeurs tiers).

9. Gestion des Incidents touchant les données

9.1 Les Incidents touchant les données doivent être gérés comme suit :

a) Le Contractant doit immédiatement informer le Centre des opérations de la CGVMSL par téléphone au (613) 932-5170, poste 2232 (Québec) ou poste 5370 (Ontario) et le responsable de la cybersécurité de la CGVMSL par courriel à cybersecurite@seaway.ca, de tout Incident touchant les données.

b) Bien que l'avis téléphonique initial puisse être sous forme de résumé, un avis écrit complet doit suivre dans les 48 heures et être adressé au Service de la cybersécurité de la CGVMSL.

c) L'avis doit identifier le point de contact du Contractant pour toutes les questions relatives à l'Incident touchant les données, résumer de façon raisonnablement détaillée la nature et la portée de l'Incident touchant les données (y compris une description des Informations de la CGVMSL touchés) et les mesures correctives déjà prises ou à prendre par le Contractant. L'avis doit, dès que possible, être complété par des détails supplémentaires raisonnablement demandés par la CGVMSL.

d) Le Contractant doit prendre rapidement toutes les mesures correctives nécessaires et coopérer avec la CGVMSL pour enquêter sur l'Incident touchant les données, en atténuer les effets négatifs et empêcher qu'il ne se reproduise. Cette coopération consiste notamment à

répondre en temps opportun aux demandes de la CGVMSL concernant l'Incident touchant les données.

e) Les parties collaboreront pour déterminer s'il est nécessaire ou souhaitable d'aviser de l'Incident touchant les données toute personne, entité gouvernementale, média ou autre partie. Les parties doivent collaborer sur le contenu de l'avis. La CGVMSL prendra la décision finale quant à savoir si un avis sera fourni et à qui, quant au contenu de l'avis et quant à la partie qui sera le signataire de l'avis.

10. Processeurs tiers

10.1 Le Contractant peut transférer, divulguer ou donner accès d'une autre façon aux Informations de la CGVMSL (y compris par l'utilisation de services d'hébergement ou de nuage de tiers) ou aux systèmes de la CGVMSL à un Sous-traitant ou à un agent si la CGVMSL a donné son approbation préalable par écrit à ce transfert, à cette divulgation ou à cet accès au tiers identifié, laquelle approbation sera conditionnelle au respect des éléments suivants :

a) le Sous-traitant ou l'agent, y compris l'accès proposé aux Informations de la CGVMSL ou au système de la CGVMSL par le Sous-traitant ou l'agent, a été évalué d'une manière essentiellement similaire à l'Examen de la sécurité du Contractant par la CGVMSL, à l'entière satisfaction de la CGVMSL ;

b) le Sous-traitant ou l'agent maintient un Programme de sécurité des données substantiellement équivalent au Programme de sécurité exigé du Contractant par le présent CPD, tel que démontré à la CGVMSL et à l'entière satisfaction de cette dernière ;

c) le Contractant a exécuté un accord avec le Sous-traitant ou l'agent qui est substantiellement équivalent à ce CPD, tel que démontré à la CGVMSL à l'entière satisfaction de cette dernière ; et

d) le Sous-traitant ou l'agent a un besoin commercial réel et démontrable de connaître ou d'accéder aux Informations de la CGVMSL ou au système de la CGVMSL auquel il a accès aux fins des Services conformément au Contrat.

11. Avis de procédure

11.1 Si le Contractant reçoit une demande d'un gouvernement ou d'un autre organisme de réglementation, ou encore une procédure ou une demande légale exigeant des Informations de la CGVMSL ou l'accès à un système de la CGVMSL, il doit immédiatement en informer la CGVMSL afin que cette dernière ait la possibilité d'y répondre.

12. Demandes ou plaintes de particuliers

12.1 Le Contractant doit immédiatement aviser la CGVMSL s'il reçoit : (i) des demandes de personnes concernant les Informations de la CGVMSL, y compris des demandes d'accès ou de rectification de renseignements personnels ; ou (ii) des plaintes de toute nature de personnes concernant la vie privée, la confidentialité ou la sécurité des Informations de la CGVMSL. Le Contractant ne doit pas répondre à une telle demande ou plainte sans l'approbation écrite préalable de la CGVMSL.

13. Restrictions d'utilisation

13.1 À moins que la CGVMSL ne donne son approbation écrite préalable, le Contractant ne doit pas utiliser, consulter, divulguer, reconfigurer ou regrouper les Informations de la CGVMSL, que ce soit ou non sous forme anonyme, ni permettre ce qui précède, à d'autres fins que l'exécution des Services prévus dans le Contrat, le respect des obligations de la présente CPD ou ce qui est strictement nécessaire pour se conformer à la loi.

14. Examen de la sécurité de la CGVMSL

14.1 La CGVMSL peut effectuer un Examen de la sécurité complet au plus une fois par année, ou plus fréquemment en cas d'Incident touchant les données et le Contractant doit coopérer pleinement à l'Examen de la sécurité, notamment en mettant à disposition et/ou en fournissant les informations pertinentes requises pour l'Examen de la sécurité. Cet Examen de la sécurité peut être effectué sur place par le personnel de la CGVMSL ou par des évaluateurs tiers sous contrat avec la CGVMSL, ou par le biais d'enquêtes et d'entretiens, au choix de la CGVMSL. Lorsqu'un Examen de la sécurité sur place est prévu, la CGVMSL doit donner au Contractant un préavis raisonnable d'au moins 15 jours ouvrables, sauf en cas d'Incident touchant les données ou si la CGVMSL a de bonnes raisons de croire que le Contractant ne respecte pas le présent CPD, auquel cas le préavis doit être d'au moins 48 heures.

14.2 À la demande de la CGVMSL, le Contractant doit fournir à cette dernière des copies de ses politiques et procédures en matière de confidentialité et de sécurité des données qui s'appliquent aux Informations de la CGVMSL et, le cas échéant, à l'accès aux systèmes de la CGVMSL. Le Contractant peut également être invité, à la demande raisonnable de la CGVMSL, à fournir des réponses écrites à des questions concernant ses pratiques en matière de confidentialité et de sécurité des données qui s'appliquent aux Informations de la CGVMSL et, le cas échéant, à l'accès aux systèmes de la CGVMSL. Le Contractant doit fournir des réponses écrites dans les 10 jours ouvrables suivant la réception de la demande de la CGVMSL.

14.3 Au fur et à mesure qu'elles sont disponibles pendant la durée du présent Contrat, le Contractant doit informer la CGVMSL des constatations susceptibles d'avoir un impact négatif sur les Informations de la CGVMSL ou sur les systèmes de la CGVMSL, constatations qui sont identifiées dans le cadre d'une évaluation ou d'un Examen de la sécurité des systèmes du Contractant ou du Programme de sécurité effectué par le Contractant ou par un tiers, y compris les évaluations de vulnérabilité et de pénétration. L'avis de ces constatations peut être fourni sous la forme d'un résumé écrit. Le Contractant doit tenir la CGVMSL informée des mesures correctives qu'il prend pour remédier à toute constatation négative.

15. Conformité

15.1 Le Contractant doit en tout temps se conformer aux Exigences en matière de confidentialité et de sécurité approuvées par la CGVMSL et précisées dans les Documents contractuels.

16. Certification de sécurité

16.1 Le Contractant doit maintenir un niveau de certification ou d'évaluation de la sécurité conforme aux meilleures pratiques et effectué par un tiers qualifié raisonnablement acceptable pour la CGVMSL. Ces certifications doivent être fournies à la CGVMSL sur demande raisonnable.

17. Indemnisation

17.1 Le Contractant doit indemniser, défendre et dégager la CGVMSL de toute Réclamation et rembourser la CGVMSL de tous les Coûts liés à un Incident touchant les données ou à la non-conformité du Contractant au présent CPD, sauf dans la mesure où les Réclamations et les Coûts sont causés par la négligence de la CGVMSL.

18. Résiliation

18.1 La CGVMSL peut résilier l'entente dans les cas suivants : (i) d'un Incident touchant les données qui, selon la CGVMSL, est susceptible d'avoir un impact négatif important sur les relations de la CGVMSL avec ses clients, ses employés, le gouvernement fédéral ou toute autre partie prenante, ou qui peut autrement nuire de façon importante à sa réputation ; (ii) d'une violation importante du présent CPD par le Contractant, y compris toute violation de l'Article 10 (Processeurs tiers) ; (iii) de toute fausse déclaration importante faite dans le cadre d'un examen, d'une évaluation ou d'un processus de sécurité décrit aux Articles 10 (Processeurs tiers) ou 14 (Examen de la sécurité de la CGVMSL) ; ou (iv) du fait que le Contractant ou un tiers examiné conformément à l'Article 10 (Processeurs tiers) n'a pas remédié en temps opportun ou de manière efficace aux conclusions défavorables importantes d'un examen, d'une évaluation ou d'un autre processus de sécurité décrit aux Articles 10 (Processeurs tiers) ou 14 (Examen de la sécurité de la CGVMSL), selon le cas. Le présent Article ne limite en rien les autres droits de résiliation prévus par le Contrat.

19. Retour ou disposition sécurisés ; résiliation de l'accès

19.1 Le Contractant doit retourner ou, si on le lui demande, éliminer les Informations de la CGVMSL en sa possession, sous sa garde ou sous son contrôle : (i) s'il n'en a plus besoin pour les affaires de la CGVMSL ou à des fins juridiques ou à la résiliation du Contrat dont les présentes CPD font partie, la date la plus éloignée étant retenue ; ou (ii) à la demande de la CGVMSL, laquelle peut être donnée à tout moment.

19.2 Nonobstant ce qui précède, le Contractant sera autorisé à conserver : (i) les Informations de la CGVMSL pendant une période plus longue si cette conservation est strictement nécessaire pour satisfaire aux obligations de conformité juridique du Contractant, si elle est effectuée conformément au programme de gestion des dossiers entièrement mis en œuvre et documenté du Contractant, et si elle est limitée au minimum d'Informations de la CGVMSL et à la période de conservation minimale nécessaires pour satisfaire à ces obligations ; et (ii) les supports de sauvegarde contenant des Informations de la CGVMSL pendant la période autorisée par le programme de gestion des dossiers entièrement mis en œuvre et documenté du Contractant, cette conservation ne devant pas être indéfinie et ne devant pas dépasser les normes de l'industrie.

19.3 Toute élimination des Informations de la CGVMSL doit garantir que les Informations de la CGVMSL sont rendues définitivement illisibles et irrécupérables.

19.4 Dans la mesure où le Contractant accède aux systèmes de la CGVMSL ou a des contacts avec ceux-ci, il doit s'assurer que cet accès est interrompu à la fin du Contrat.

19.5 Sur préavis raisonnable et à la demande de la CGVMSL, le Contractant doit fournir à la CGVMSL un certificat d'un dirigeant attestant que le Contractant respecte le présent Article.

Annexes du CPD

Annexe A – Installations d'hébergement, Sous-traitants et affiliés
Annexe B – Mesures de sécurité techniques et organisationnelles

ANNEXE A

Installations d'hébergement *Où les données sont entreposées*	
Nom et adresse complète de l'organisation	Nature du traitement
	Type d'engagement

Sous-traitants *Liste complète de toutes les entreprises utilisées par le Contractant pour les travaux prévus dans le cadre du présent Contrat, y compris leur emplacement physique.*

Affiliés *Liste complète de toutes les sociétés affiliées utilisées par le Contractant pour les travaux prévus dans le cadre du présent Contrat, y compris leur emplacement physique.*

ANNEXE B

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le Contractant conformément au présent CPD