Addendum sur la Sécurité des Données de l'Abonné

Les obligations contenues dans le présent Addendum sur la Sécurité des Données de l'Abonné (« **Addendum sur la Sécurité** ») fournissent des détails sur les mesures techniques et organisationnelles prises par iCIMS pour protéger les Données de l'Abonné (y compris les Données à Caractère Personnel de l'Abonné) et les Données à Caractère Personnel traitées pour les Opérations Commerciales d'iCIMS (collectivement les **« Données Protégées »**) qui sont traitées dans le cadre du Contrat d'Abonnement et de l'Addendum sur le Traitement des Données, et pour aider les Membres du Groupe de l'Abonné à remplir leurs obligations de répondre aux demandes des Personnes Concernées pour l'exercice de leurs droits en vertu des Lois sur la Protection des Données et de la Vie Privée. iCIMS maintient un ensemble complet de politiques et de processus liés à la sécurité de l'information et à la protection des données qui sont conformes aux normes ISO 27001, ISO 27701 et SOC2. Ce qui suit identifie les contrôles clés utilisés pour protéger les Données de l'Abonné.

À moins qu'ils ne soient autrement définis ci-dessous, tous les termes en majuscules ont la signification qui leur est donnée dans le Contrat d'Abonnement (« **Contrat d'Abonnement** ») et/ou l'Addendum relatif au Traitement des Données (« **Addendum relatif au Traitement des Données** ») entre iCIMS et l'Abonné. Tous les exemples figurant dans le présent Addendum sur la Sécurité sont donnés à titre d'illustration d'un concept particulier et ne sont pas exhaustifs.

1. Mesures d'anonymisation/pseudonymisation et de cryptage des Données Protégées

Toutes les Données Protégées seront cryptées au repos et en transit par iCIMS ou la plateforme iCIMS sur tout réseau public, en utilisant les mesures standard du secteur.

a. Données Protégées au repos : Utiliser au moins l'AES 256 bits ou supérieur pour le cryptage. Les données au repos incluent les Sauvegardes, telles que définies dans la Politique relative au Support et à la Maintenance d'iCIMS.

b. Données Protégées en transit : Utiliser TLS 1.2 ou supérieur (conformément aux normes du secteur, y compris les algorithmes approuvés par le File Intrusion Prevention Systems (FIPS) et/ou recommandés par le NIST) pour le cryptage.

c. Données hachées : Les données hachées doivent utiliser bcrypt comme algorithme de hachage.

d. Échange de clés et signatures numériques :

i. L'échange de clés doit utiliser les algorithmes cryptographiques RSA, DH ou supérieur avec une longueur minimale de clé de 2048 bits.

ii. Les signatures numériques doivent utiliser les spécifications définies dans le DSS avec une longueur de clé minimale de 2048 bits et une longueur de condensé minimale de 256.

e. Anonymisation et pseudonymisation : iCIMS a une politique interne d'analyse des données qui exige qu'iCIMS utilise certaines ou toutes les mesures de protection et techniques suivantes pour rendre les Données à Caractère Personnel de l'Abonné anonymes, dépersonnalisées et/ou non personnelles, selon le cas :

i. Suppression - supprime les valeurs d'identification d'un enregistrement (ex : suppression du nom et du prénom d'un enregistrement).

ii. Généralisation - remplacement d'un élément de données par un élément plus général (ex : suppression du jour et du mois d'une date de naissance pour ne laisser que l'année).

iii. Ajout de bruit - remplace les valeurs de données réelles par d'autres valeurs sélectionnées dans la même classe de données (par exemple, les données réelles peuvent être rendues aléatoires pour créer une nouvelle valeur, la valeur aléatoire étant considérée comme un ajout de bruit).

iv. Confidentialité différentielle - exige l'utilisation de la méthode d'anonymat « k-anonymity » pour s'assurer que dans un ensemble de données, il y a au moins k individus ou clients qui ont exactement les mêmes valeurs pour les éléments de données qui pourraient devenir identifiants pour chaque individu ou client. La politique d'iCIMS exige une valeur minimale de k=20, ce qui est cohérent avec les pratiques actuelles de diffusion de données publiques d'autres organisations très conservatrices.

v. Suppression des valeurs aberrantes : suppression de toutes les valeurs aberrantes afin de minimiser la mesure dans laquelle ces valeurs permettent de ré-identifier une personne ou un client.

2. Mesures visant à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement

a. Vérification des antécédents : Lorsque la législation applicable l'exige et/ou l'autorise, iCIMS procède à une vérification des antécédents et/ou du casier judiciaire de tous les nouveaux employés avant leur embauche. L'emploi à iCIMS est subordonné à une vérification satisfaisante des antécédents et/ou du casier judiciaire, y compris le cas échéant :

i. Traçage du numéro de sécurité sociale, numéro national d'assurance, numéro de service public personnel ou autre numéro d'identification nationale.

ii. Formation.

iii. Expérience Professionnelle.

iv. Vérification des Antécédents Criminels.

v. Vérification du Crédit, si cela est pertinent pour le poste.

vi. Vérification des Références.

vii. Lorsque la loi applicable l'exige et/ou le permet, iCIMS peut également procéder à des vérifications des antécédents et/ou du casier judiciaire de ses employés tout au long de leur emploi. En général, cela se produit dans des circonstances impliquant une affectation à un poste de sécurité ou de responsabilité de haut niveau.

b. Confidentialité permanente : Obligations de confidentialité telles que précisées dans le Contrat d'Abonnement.

c. Formation sur la sécurité et la protection des données : Lors de l'intégration, puis au moins une fois par année civile, iCIMS exigera que tout le personnel d'iCIMS ayant accès aux Données Protégées suive une formation sur les politiques d'iCIMS en matière de sécurité de l'information et de protection des données.

3. Mesures visant à garantir la capacité de restaurer la disponibilité et l'accès aux Données de l'Abonné en temps utile en cas d'incident matériel ou technique

a. Gestion des incidents : iCIMS a mis en place une politique et un processus de réponse aux incidents à suivre en cas d'incident de sécurité ou de protection des données, y compris en cas de Violation de Données à Caractère Personnel. La politique et le processus de réponse aux incidents d'iCIMS comprennent :

i. Rôles et responsabilités : Les responsabilités et les procédures de gestion sont établies pour garantir une réponse rapide, efficace et ordonnée aux incidents de sécurité ou de protection des données, y compris la formation d'une équipe de réponse aux incidents de sécurité ou de protection des données (SIRT) avec un responsable de réponse aux incidents.

ii. Procédure de Réponse aux Incidents : Basé sur la norme NIST 800-61 Rev.2, elle comprend :

1. Préparation : Établir une capacité de réponse aux incidents visant à prévenir les incidents en assurant des cadres de contrôle et une conformité efficaces.
2. Détection & Analyse : Identifier les événements liés à la sécurité ou à la confidentialité et déterminer leur impact potentiel sur l'iCIMS et les abonnés.

Après avoir consulté la direction d'iCIMS et lorsque cela est justifié ou exigé par une action judiciaire, une loi applicable, une réglementation ou une exigence juridictionnelle similaire, iCIMS déploiera des efforts raisonnables pour informer le personnel d'iCIMS concerné et/ou les abonnés affectés d'un incident de sécurité ou de protection des données. En outre, la notification est requise dans les 24 heures suivant l'identification d'une Violation des Données Personnelles confirmée ou d'Activités Anormales. « Activités Anormales » désigne les attaques infructueuses qui semblent particulièrement importantes d'après la compréhension qu'a iCIMS des risques auxquels elle est confrontée.

3. Confinement, Eradication et Récupération : Atténuer la cause profonde de l'incident de sécurité ou de protection des données afin de prévenir tout autre dommage ou exposition. Éradiquer les vulnérabilités à l'origine de l'incident de sécurité ou de protection des données, et de toute compromission associée, sont supprimées de l'environnement. Rétablir le(s) système(s) affecté(s) après que les problèmes qui ont donné lieu à l'incident de sécurité ou de protection des données, et les conséquences de l'incident de sécurité ou de confidentialité, ont été corrigés.
4. Activités post-incident : Traitement des exigences en matière de notification et de communication, de la coopération avec les parties externes, du partage des informations, du suivi des leçons apprises, de la tenue des dossiers et des améliorations.

b. Reprise après sinistre et continuité des activités : Comme spécifié dans la Politique relative au Support et à la Maintenance d'iCIMS.

4. Processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement

a. Contrôles d'accès :

i. iCIMS doit :

1. Suivre les principes du moindre privilège par le biais d'un modèle de contrôle d'accès basé sur les rôles lorsqu'il s'agit d'accorder au personnel d'iCIMS l'accès aux Données Protégées.
2. Limiter l'accès aux Données Protégées au personnel d'iCIMS ayant un besoin légitime d'accéder aux Données Protégées pour fournir les services conformément au Contrat d'Abonnement.
3. Examiner périodiquement (au moins une fois par trimestre) l'accès du personnel d'iCIMS aux Données Protégées.
4. Mettre rapidement fin à l'accès d'un membre du personnel d'iCIMS aux Données Protégées si l'accès de cette personne n'est plus nécessaire.
5. Examiner et désactiver les comptes d'utilisateurs après 90 jours d'inactivité.

b. Contrôles du réseau : L'accès aux services de réseaux internes et externes qui contiennent les Données Protégées sera contrôlé par une combinaison des types de contrôles suivants :

i. Les listes de contrôle d'accès au réseau (NACL), ou équivalent.
ii. Politiques de pare-feu, ou équivalent.
iii. Groupes de sécurité, ou équivalent.
iv. Listes blanches d'adresses IP, ou équivalent.
v. Une architecture multi-tiers qui empêche l'accès direct aux magasins de données (« data stores ») depuis Internet.
vi. L'utilisation de contrôles d'accès basés sur les rôles (RBAC) doit être mise en œuvre pour garantir un accès approprié aux réseaux.
vii. L'authentification à deux ou plusieurs facteurs (TFA ou MFA) pour l'accès à distance doit être mise en œuvre.

c. Gestion des vulnérabilités et gestion des correctifs : iCIMS doit mettre en œuvre et maintenir un programme de gestion des vulnérabilités conçu pour identifier et corriger les vulnérabilités affectant les réseaux, systèmes

et applications de production qui stockent ou traitent les Données Protégées. Le programme doit comprendre :

i. Des tests de pénétration, effectués par un tiers accrédité choisi par iCIMS, des produits et de l'infrastructure d'iCIMS qui contiennent des Données Protégées sont effectués au moins une fois par année civile. Sur demande raisonnable de l'Abonné par écrit, iCIMS fournira à l'Abonné une attestation exécutive des résultats des tests. L'Abonné doit traiter ces informations comme des informations confidentielles d'iCIMS conformément à l'« Article 7 - Informations Confidentielles » du Contrat d'Abonnement.

ii. Des analyses de vulnérabilité de routine sur tous les produits et l'infrastructure d'iCIMS qui contiennent des Données Protégées ou qui sont utilisés par iCIMS pour accéder aux Données Protégées.

iii. Si des vulnérabilités sont détectées à partir de ces tests et analyses, iCIMS doit y remédier et appliquer les correctifs applicables et nécessaires comme suit :

1. Les systèmes d'exploitation des serveurs doivent être corrigés dans les 30 jours suivant la publication d'un correctif critique et/ou de sécurité.
2. Les postes de travail et les ordinateurs portables doivent être corrigés dans les 30 jours suivant la publication d'un correctif critique et/ou de sécurité.
3. Les dispositifs de réseau doivent être corrigés dans les 30 jours suivant la publication d'un correctif critique ou de sécurité.
4. Les correctifs de type « zero-day » sont appliqués sur tous les systèmes contenant des Données Protégées et sur les systèmes critiques dans un délai de 14 jours, et sur tous les autres systèmes dans un délai de 30 jours.
5. Les correctifs doivent être testés avant d'être déployés dans l'environnement de production. Les systèmes moins critiques doivent être corrigés en premier.
6. Les correctifs d'application doivent être appliqués conformément à la Politique relative au Support et à la Maintenance d'iCIMS.

d. Pratiques de Développement Logiciel d'iCIMS : En ce qui concerne le cycle de vie du développement logiciel, iCIMS maintiendra et suivra un programme écrit de cycle de vie du développement logiciel basé sur les 10 normes principales de l'Open Web Application Security Project (OWASP).

Le personnel d'iCIMS en charge de la conception, du développement, de la configuration, des tests et du déploiement des applications sécurisées reçoit une formation appropriée concernant les pratiques de développement des applications sécurisées d'iCIMS. Les pratiques de développement doivent inclure :

i. Gérer l'ensemble du code par le biais d'un système de contrôle des versions permettant de visualiser l'historique des modifications et le contenu.

ii. Veiller à ce qu'une équipe agile effectue des tests à l'aide d'un cycle de publication d'assurance qualité à phases multiples qui comprend des tests de sécurité.

iii. Apporter des correctifs et des améliorations en matière de sécurité selon un calendrier préétabli, en fonction des niveaux de gravité identifiés.

iv. Effectuer un balayage des vulnérabilités du code source dans le pipeline CI/CD et mener des activités de remédiation appropriées au risque en fonction de l'impact sur l'entreprise et de la hiérarchisation ultérieure des résultats avant la sortie du logiciel, en fonction de la priorité.

v. Veiller à ce que les logiciels ne soient diffusés que par le biais de processus de contrôle des modifications gérés par la production, sans accès ni participation des équipes en charge du développement et des tests

vi. Conduire une formation de sensibilisation au codage sécurisé au moins une fois par année civile.

e. Contrôles des logiciels malveillants : iCIMS installera et maintiendra des contrôles raisonnables et actuels conçus pour protéger les réseaux, systèmes et dispositifs utilisés par iCIMS pour accéder aux Données Protégées contre les logiciels malveillants et les logiciels non autorisés.

f. Évaluations de sécurité et de protection des données : Sur demande écrite de l'Abonné, pas plus d'une fois par période de douze (12) mois, l'Abonné peut réévaluer le programme de sécurité et de protection des données d'iCIMS. iCIMS accepte de fournir une coopération raisonnable à l'égard d'une telle évaluation par la fourniture de documents raisonnables et appropriés ; sous réserve toutefois qu'iCIMS ait un délai de quarante-cinq (45) jours pour répondre à ladite demande d'évaluation. Les évaluations décrites dans la présente Section : (i) ne doivent pas être considérées comme un audit et, à ce titre, iCIMS peut ne pas fournir les renseignements habituellement fournis dans le cadre d'un audit ; et (ii) ne comprennent pas et ne permettent pas à l'Abonné d'effectuer des tests de vulnérabilité/pénétration.

g. Certification et attestation de sécurité : Voir l'Article 12 du présent Addendum sur la Sécurité.

5. Mesures d'identification et d'autorisation des utilisateurs

a. Contrôle d'accès : Le personnel d'iCIMS doit :

i. Établir un processus pour relier tous les accès aux composants du système (en particulier les accès avec des privilèges administratifs tels que « root ») à chaque utilisateur individuel.
ii. Veiller à ce que les administrateurs ne se connectent aux systèmes qu'avec des identifiants qui leur sont attribuables ou suivent des processus qui ne rompent pas l'attribution.
iii. Veiller à ce que l'accès aux bases de données contenant des Données Protégées soit toujours authentifié.
iv. S'assurer que toutes les connexions à l'Abonnement soient sécurisées par une connexion cryptée (par exemple, HTTPS) et authentifiées de manière appropriée.
v. Veiller à ce que le Principe du Moindre Privilège utilisant le contrôle d'accès basé sur les rôles (RBAC) soit respecté pour tous les utilisateurs. Le **« Principe du Moindre Privilège »** consiste à restreindre l'accès aux systèmes et aux données sur la base du rôle ou de la fonction professionnelle, tout en veillant à ce qu'aucun accès supplémentaire non nécessaire ne soit accordé.
vi. Contrôler l'ajout, la suppression et la modification des noms d'utilisateur, des identifiants et d'autres objets d'identification.
vii. S'assurer que les utilisateurs (y compris les intérimaires, les consultants et les contractants) demandent formellement l'accès aux systèmes en ne disposant que des droits nécessaires à l'exercice de leurs fonctions.
viii. Veiller à ce qu'un responsable ou un supérieur et le propriétaire du système approuve formellement les rôles des utilisateurs et les demandes d'accès. Les administrateurs du système agissent en tant que contrôleur final pour garantir que l'accès est accordé en fonction du rôle identifié.
ix. Procéder à un examen périodique de l'accès et des droits d'accès des utilisateurs afin de s'assurer qu'ils sont appropriés au rôle des utilisateurs.
x. Utiliser une authentification à deux facteurs (TFA) ou authentification multifactorielle (MFA) pour tous les services accessibles à distance par le personnel d'iCIMS et/ou les tiers autorisés.

b. Détection des intrusions et assurance de la performance : iCIMS surveille les réseaux, systèmes et applications de production qui stockent ou traitent les Données Protégées pour détecter tout accès non autorisé à l'aide de systèmes de surveillance du trafic et de l'activité.

c. Mots de passe : iCIMS gérera les mots de passe conformément aux normes NIST 800-63b, pour l'identité numérique gérée par iCIMS au sein d'iCIMS.

d. Voir l'Article 9.a.v. du présent Addendum sur la Sécurité pour l'alerte et la surveillance**.**

6. Mesures de protection des Données Protégées pendant la transmission

a. Cryptage : Comme indiqué à l'Article 1 du présent Addendum sur la Sécurité.

7. Mesures de protection des données pendant le stockage

a. Cryptage : Comme indiqué à l'Article 1 du présent Addendum sur la Sécurité.

b. Ségrégation des données : iCIMS conservera les Données de l'Abonné au minimum logiquement séparées des données appartenant aux autres abonnés de iCIMS et mettra en œuvre des mesures et des contrôles conçus pour garantir que les Données de l'Abonné ne sont pas accessibles par les autres Abonnés de iCIMS.

8. Mesures visant à assurer la sécurité physique des lieux où sont traitées les Données Protégées

a. Sécurité des centres de données : iCIMS utilise des centres de données exploités par des tiers, par exemple Amazon Web Services, pour fournir l'Abonnement et exige de ces tiers qu'ils maintiennent des contrôles qui fournissent une assurance raisonnable que l'accès aux serveurs physiques du centre de données est limité aux personnes autorisées et que des contrôles environnementaux sont établis pour détecter, prévenir et contrôler la destruction due à des conditions environnementales extrêmes. Ces contrôles comprennent :

i. La consignation et la surveillance de toutes les tentatives d'accès autorisées et non autorisées au centre de données par le personnel de sécurité du centre de données.
ii. Des systèmes de surveillance par caméra aux points d'entrée internes et externes critiques du centre de données.
iii. Des systèmes qui surveillent et contrôlent la température et l'humidité de l'air à des niveaux appropriés pour l'équipement informatique.
iv. Des Modules d'Alimentation Sans Coupure (UPS) et des générateurs de secours, y compris les services de livraison de carburant qui fournissent une alimentation de secours en cas de panne de courant.
v. La prise en compte des préoccupations environnementales telles que les incendies, les inondations et les catastrophes naturelles.
vi. Tous les visiteurs sur site doivent toujours être accompagnés par le personnel d'iCIMS.
vii. L'obligation pour les centres de données d'effectuer des audits SOC 2 ou équivalents sur une base annuelle tout en remédiant à toute découverte dans un délai raisonnable.

9. Mesures pour assurer l'enregistrement des événements

a. Contrôles d'audit, de journalisation et de surveillance : iCIMS doit mettre en œuvre et maintenir des mesures conçues pour sécuriser, contrôler et surveiller les réseaux, systèmes et applications d'iCIMS qui traitent ou stockent les Données Protégées, y compris :

i. Pare-feu et technologies connexes et contrôles d'authentification.
ii. Systèmes de détection ou de prévention des intrusions pour surveiller les réseaux associés.
iii. Système de journalisation centralisé (y compris la gestion des informations et des événements de sécurité (SIEM)) contrôlé par l'équipe de sécurité de l'information d'iCIMS, avec une conservation des journaux pendant un an.
iv. Pistes d'audit sécurisées et protégées qui ne peuvent être modifiées.
v. Systèmes de surveillance et d'alerte utilisés pour enregistrer les tentatives/échecs de connexion, les connexions réussies et les modifications apportées aux systèmes, avec des alertes associées en place.
vi. Surveillance de toutes les connexions externes d'entrée/sortie.
vii. Protection anti-virus/anti-malware pour les éléments gérés par iCIMS.

10. Mesures pour assurer la configuration du système, y compris la configuration par défaut

a. Gestion des changements et de la configuration : iCIMS maintient des politiques et des procédures pour gérer les changements apportés aux systèmes de production, aux applications et aux bases de données d'iCIMS qui traitent les Données Protégées. Ces politiques et procédures comprennent :

i. Des processus pour documenter, tester et approuver la promotion des changements en production.

ii. Un processus d'application de correctifs de sécurité qui exige l'application de correctifs aux systèmes en temps opportun, sur la base d'une analyse des risques.
iii. Un processus permettant à iCIMS d'effectuer des évaluations de sécurité des changements en production.
iv. Des normes de durcissement basées sur les meilleures pratiques de l'industrie (ex : les normes du Centre pour la Sécurité sur Internet (CIS)).
v. Un programme de gestion des vulnérabilités pour auditer et vérifier la configuration appropriée (voir Article 4.b du présent Addendum).
vi. Les politiques et les processus de gestion des appareils mobiles pour s'assurer que les appareils sont conformes aux politiques internes iCIMS (Politique d'Utilisation Acceptable, politiques de sécurité des informations et « employee handbook » iCIMS) s'ils sont utilisés pour accéder aux Données Protégées.

11. Mesures relatives à la gouvernance et à la gestion de l'informatique interne et de la sécurité informatique

a. Gouvernance : iCIMS doit désigner un ou plusieurs employés pour maintenir le programme de sécurité de l'information d'iCIMS.
i. La direction d'iCIMS doit examiner et approuver toute modification importante du programme de sécurité de l'information.
ii. iCIMS doit revoir le programme de sécurité de l'information au moins une fois par année civile ou lors d'un changement important dans les pratiques commerciales d'iCIMS.
b. Mesures de sécurité de l'information : Comme spécifié dans l'Article « Sécurité des Données » de la Politique relative au Support et à la Maintenance d'iCIMS.
c. Modifications : iCIMS peut modifier ses contrôles et processus de sécurité de temps à autre, à condition que ces modifications :
i. Ne réduisent pas sensiblement le niveau global de protection offert par iCIMS à l'Abonné.
ii. Le cas échéant, sont conformes à la déclaration SOC-2 d'iCIMS alors en vigueur.
iii. Les cas échéant, restent en conformité avec les normes ISO 27001 et ISO 27701.

12. Mesures de certification/assurance des processus et des produits

a. Certifications, audits et attestations de sécurité : le SGIC doit maintenir les certifications, audits et attestations standard du secteur suivants :
i. Certification ISO 27001, ou équivalent, garantissant que le système de gestion de la sécurité de l'information (SGSI) d'iCIMS continue de fonctionner conformément à la norme, pour le traitement des Données de l'Abonné.
ii. Certification ISO 27701, ou équivalent, garantissant que le système de gestion de l'information sur la vie privée (PIMS) d'iCIMS continue de fonctionner conformément à la norme, pour le traitement des Données de l'Abonné.
iii. SOC 2, attestation Type II, garantissant que les contrôles internes fournis par iCIMS sont conformes aux normes de l'American Institute of Certified Public Accountants (AICPA) (c'est-à-dire SSAE-19, TPS-100), pour le traitement des Données de l'Abonné.
iv. Attestations de tests de pénétration concernant les performances, les résultats et les mesures correctives résultant de tests de pénétration internes et externes.

13. Mesures pour assurer la minimisation des données

a. Données de l'Abonné : Les Abonnés contrôlent la nature et la portée des Données de l'Abonné qui sont transférées à iCIMS via l'Abonnement. L'objet, la durée, la nature, la finalité du Traitement des Données à Caractère Personnel de l'Abonné, ainsi que les types de Données à Caractère Personnel de l'Abonné et les

catégories de Personnes Concernées sont définis dans le Contrat d'Abonnement et l'Addendum relatif au Traitement des Données. L'accès par iCIMS aux Données à Caractère Personnel de l'Abonné est strictement limité aux personnes qui ont besoin de connaître/d'accéder aux Données à Caractère Personnel de l'Abonné concernées, comme cela est strictement nécessaire aux fins du Contrat d'Abonnement et pour se conformer aux Lois sur la Protection des Données et de la Vie Privée. Les Données à Caractère Personnel de l'Abonné sont conservées conformément aux éventuelles périodes de conservation configurées par l'Abonné via l'Abonnement, ou si de telles périodes de conservation ne sont pas configurées, conformément au Contrat d'Abonnement. Le cas échéant (comme l'analyse de données), le niveau de détail utilisé pour le Traitement des Données à Caractère Personnel de l'Abonné est limité comme décrit dans l'article 1.e du présent Addendum sur la Sécurité.

b. Données Personnelles Traitées pour les Opérations Commerciales d'iCIMS : Les Données à Caractère Personnel traitées pour les Opérations Commerciales d'iCIMS sont limitées au contexte des données générées pour aider les Opérations Commerciales d'iCIMS liées à l'administration et à la fourniture de l'Abonnement. L'accès d'iCIMS aux Données à Caractère Personnel traitées dans le cadre des Opérations Commerciales d'iCIMS est limité aux personnes et aux équipes qui ont besoin de connaître les données pertinentes ou d'y accéder, dans la mesure où cela est nécessaire pour les Opérations Commerciales légitimes d'iCIMS liées à l'administration et à la livraison de l'Abonnement à l'Abonné, et pour ses autres objectifs légitimes liés aux Opérations Commerciales d'iCIMS. iCIMS ne traitera ces Données à Caractère Personnel qu'aux fins compatibles avec celles contenues dans la définition des Opérations Commerciales d'iCIMS et n'utilisera pas les Données à Caractère Personnel à d'autres fins. Les Données à Caractère Personnel traitées pour les Opérations Commerciales d'iCIMS sont conservées conformément aux politiques et procédures documentées d'iCIMS en matière de stockage et de conservation des données.

14. Mesures visant à garantir la qualité des données

a. Mesures visant à garantir la qualité des données : Les exigences relatives aux conditions, scénarios et responsabilités du Traitement des Données de l'Abonné sont spécifiées dans l'Addendum relatif au Traitement des Données et dans l'Article « Données de l'Abonné » du Contrat d'Abonnement. Le processus d'exercice des droits des personnes concernées est précisé dans l'Addendum relatif au Traitement des Données.

15. Mesures visant à garantir une conservation limitée des données

a. Suppression après la résiliation ou l'expiration de l'Abonnement : Sauf indication contraire dans l'Addendum relatif au Traitement des Données ou le Contrat d'Abonnement, les Données de l'Abonné en possession d'iCIMS ou sous son contrôle seront supprimées dans les trente (30) jours suivant la résiliation ou l'expiration de l'Abonnement et, en ce qui concerne les sauvegardes, au plus tard douze (12) mois après le mois au cours duquel le Contrat d'Abonnement prend fin ou expire.

b. La destruction des données : Les supports contenant des Données à Caractère Personnel de l'Abonné doivent être éliminés de manière à les rendre illisibles ou indéchiffrables, par exemple en les brûlant, en les déchiquetant, en les pulvérisant ou en les écrasant.

i. Les Données à Caractère Personnel de l'Abonné en possession ou sous le contrôle d'iCIMS seront supprimées en utilisant les techniques détaillées dans le document NIST 800-88 (« Guidelines for Media Sanitization »), dans la mesure du possible.

ii. iCIMS certifie la destruction des Données à Caractère Personnel de l'Abonné en délivrant un certificat de destruction, sur demande écrite de l'Abonné.

iii. Les certificats de destruction sont conservés pendant au moins un an.

c. Récupération des Données de l'Abonné : Comme spécifié dans l'Addendum relatif au Traitement des Données et le Contrat d'Abonnement.

16. Mesures visant à garantir la responsabilité

a. Gouvernance : iCIMS doit désigner un ou plusieurs employés pour maintenir le programme de confidentialité d'iCIMS.
   i. la direction d'iCIMS doit examiner et approuver toute modification importante du programme de protection de la vie privée.
   ii. iCIMS révisera le programme de confidentialité au moins une fois par année civile ou lors d'un changement important dans les pratiques commerciales d'iCIMS et/ou dans les Lois sur la Protection des Données et de la Vie Privée.

b. Responsabilité pour les actes, erreurs et omissions des sous-traitants ultérieurs : Comme spécifié dans l'Addendum relatif au Traitement des Données et le Contrat d'Abonnement.

c. Politique disciplinaire : iCIMS maintiendra et appliquera une politique disciplinaire pour les violations des programmes de sécurité de l'information et de confidentialité d'iCIMS par le personnel d'iCIMS.

d. Audit des fournisseurs : iCIMS maintient un processus d'examen pour les fournisseurs qui traitent des Données Protégées.

17. Mesures visant à permettre la portabilité des données et à garantir leur effacement

a. Stockage sur des appareils portables : iCIMS ne doit pas stocker de Données de l'Abonné sur des appareils portables ou des supports amovibles, y compris des ordinateurs portables, des smartphones et des tablettes, sans l'approbation écrite préalable de l'Abonné.

b. Droits d'effacement et de portabilité de la personnes concernée : Le processus d'exercice des droits de la personne concernée est précisé dans l'Addendum relatif au Traitement des Données.

18. Restrictions ou protections appliquées aux données sensibles (le cas échéant)

a. Afin d'assurer la confidentialité des données en cas de perte accidentelle ou malveillante de données, toutes les Données Protégées incluant des données sensibles seront cryptées au repos et en transit (voir Article 1 du présent Addendum sur la Sécurité).