AVENANT SUR LA PROTECTION DES DONNÉES

Le présent Avenant sur la Protection des Données (« APD ») complète le Contrat conclu entre vous (« Fournisseur ») et Iron Mountain France (« Client ») pour la Fourniture de Biens et/ou de Services (« Contrat ») entre le Client et le Fournisseur.
Si les conditions contenues dans la présente sont en conflit avec celles énoncées dans le Contrat, les conditions stipulées dans le présent Avenant sont considérées comme ayant préséance dans le cadre strict dudit conflit. Sauf indication contraire aux présentes, tous les termes en lettres capitales revêtent le même sens que celui qui leur est attribué dans le Contrat. Sous réserve des modifications indiquées ci-après, les termes du Contrat conservent la même force et les mêmes effets.
Les parties conviennent par la présente que les conditions précisées ci-dessous seront ajoutées au Contrat sous forme d'Avenant.

1. Définitions

1.1 Dans le présent Avenant, les termes suivants ont la signification qui leur est donnée ci-dessous et les termes apparentés sont interprétés en conséquence :
1.1.1 « Sous-traitants n-1 agréés » signifie tout Sous-traitant ayant reçu le consentement écrit du Client conformément à la section 6.1 ;
1.1.2 « Société affiliée du Client » désigne une entité qui détient ou contrôle, qui est détenue ou contrôlée par ou qui est sous le contrôle ou la détention commun(e) avec le Client, où « contrôle » s'entend comme la possession, directe ou indirecte, du pouvoir d'orienter ou de faire orienter la gestion et les politiques d'une entité, que ce soit par la détention de titres conférant le droit de vote, par contrat ou autrement ;
1.1.3 « Données à caractère personnel du Client » désigne les données décrites en Annexe 1 et toutes autres Données à caractère personnel traitées par le Fournisseur ou un Sous-traitant pour le compte du Client, ou de l'une de ses Sociétés affiliées, du fait du Contrat ou relativement à celui-ci ;
1.1.4 « Lois sur la protection des données » désigne, en lien avec les Données à caractère personnel qui sont traitées dans le cadre de l'exécution du Contrat, le Règlement général sur la protection des données (UE) 2016/679 (« RGPD »), selon le cas comprenant toutes les lois appliquant ou complétant les mêmes ou d'autres lois en vigueur relativement à la protection des données ou de la vie privée ;
1.1.5 « EEE » désigne l'Espace économique européen ;
1.1.6 « Traiter/Traitement », « Responsable de traitement », « Sous-Traitant», « Personne concernée », « Violation de données à caractère personnel » et « Catégories spéciales de données à caractère personnel » revêtent le même sens que celui qui leur est attribué dans les Lois sur la protection des données ;
1.1.7 « Pays soumis à restrictions » désigne un pays qui (i) n'est pas un État membre de l'Union européenne ; et (ii) n'a pas été approuvé par la Commission européenne comme étant en mesure d'assurer un niveau de protection adéquat conformément aux Lois sur la protection des données ;
1.1.8 « Services » désigne tous biens et/ou services fournis au Client en vertu du Contrat ;
1.1.9 « Clauses contractuelles types » désigne les dispositions contractuelles types pour le transfert de données à caractère personnel aux Responsables de leur traitement établis dans des pays tiers, approuvées par la Commission européenne par décision 2010/87/UE, ou un ensemble de clauses approuvées par la Commission européenne qui modifie, remplace ou annule celles-ci ;
1.1.10 « Sous-traitant n-1 » désigne toute entité (y compris toute tierce partie et Société affiliée du Fournisseur) chargée par le Fournisseur de traiter les Données à caractère personnel pour le compte du Client ou de l'une de ses Sociétés affiliées ;
1.1.11 « Autorité de surveillance » désigne (a) une autorité publique indépendante instituée par un État membre conformément à l'article 51 RGPD ; et (b) toute autorité réglementaire similaire responsable de l'application des Lois sur la protection des données ;
1.1.12 « Société affiliée du Fournisseur » désigne une entité qui détient ou contrôle, qui est détenue ou contrôlée par ou qui est sous le contrôle ou la détention commun(e) avec le Fournisseur, où « contrôle » s'entend comme la possession, directe ou indirecte, du pouvoir d'orienter ou de faire orienter la gestion et les politiques d'une entité, que ce soit par la détention de titres conférant le droit de vote, par contrat ou autrement.

2. Conditions de traitement des données

2.1 Dans l'exercice de l'octroi de services au Client en vertu du Contrat, le Fournisseur peut Traiter les Données à caractère personnel du Client pour le compte de ce dernier ou de l'une de ses Sociétés affiliées conformément aux conditions du présent Avenant ; Le Fournisseur s'engage à se conformer aux dispositions suivantes concernant toutes Données à caractère personnel soumises par ou pour le Client ou l'une de ses Sociétés affiliées dans le cadre de la prestation de Services ou encore collectées et Traitées par ou pour le Client ou l'une de ses Sociétés affiliées ou par le Fournisseur ou l'une de ses Sociétés affiliées.

3. Traitement des Données à caractère personnel du Client

3.1 Le Fournisseur ne peut Traiter les types de Données à caractère personnel ayant trait aux catégories de Personnes concernées qu'aux fins du Contrat (et qu'à ces fins spécifiques) dans chaque cas visé en Annexe 1 du présent Avenant et n'est pas autorisé à Traiter, transférer, modifier, amender ou remanier les Données à caractère personnel du Client ni à les divulguer, ou à en autoriser la divulgation, à une tierce partie autrement que dans le cadre du consentement écrit préalable du Client (prévu au Contrat ou dans un autre document) à moins que ce Traitement ne soit exigé par la législation de l'UE ou d'un État membre à laquelle le Fournisseur est soumis. Dans ce cas, et dans la mesure permise par cette législation, le Fournisseur informe par écrit le Client de cette exigence légale avant de procéder au Traitement de ces Données à caractère personnel.

4. Personnel du Fournisseur

4.1 Le Fournisseur doit prendre les mesures appropriées pour s'assurer de la fiabilité de tout salarié, mandataire ou prestataire susceptible d'avoir accès aux Données à caractère personnel du Client. Le Fournisseur veille à ce que cet accès soit, à chaque fois, strictement réservé aux personnes qui ont besoin d'accéder aux Données à caractère personnel pertinentes du Client, dans la mesure strictement nécessaire aux fins prévues par la section 3.1 qui précède et dans le cadre des obligations que ces personnes doivent assumer à l'égard du Fournisseur, en s'assurant que toutes ces personnes :
4.1.1 sont informées de la nature confidentielle des Données à caractère personnel du Client et connaissent les obligations du Fournisseur en vertu du présent Avenant et du Contrat relatif aux données à caractère personnel du Client ;
4.1.2 ont entrepris des activités de formation adéquates par rapport aux Lois sur la protection des données ;
4.1.3 obéissent à des engagements, ou à des obligations professionnelles ou réglementaires, en matière de confidentialité ;
4.1.4 sont soumises à des procédures d'authentification et de connexion lorsqu'elles accèdent aux Données à caractère personnel du Client.

5. Sécurité

5.1 Compte tenu de l'état de l'art, des coûts de mise en œuvre, et de la nature, de la portée, du contexte et des finalités du Traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le Responsable de Traitement met en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque. Le cas échéant, il peut notamment s'agir des mesures suivantes :
5.1.1 la pseudonymisation et le chiffrement des Données à caractère personnel du Client ;
5.1.2 la capacité de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ;
5.1.3 la capacité de restaurer la disponibilité et l'accès aux Données à caractère personnel du Client sans délai indu en cas d'incident physique ou technique ;

5.1.4 un processus servant à régulièrement tester, mesurer et évaluer l'efficacité des mesures techniques et organisationnelles pour garantir la sécurité du Traitement.

5.2 Conformément aux dispositions de la section 5.1, mais sans s'y limiter, le Fournisseur met en œuvre et tient à jour chacune des mesures techniques et organisationnelles figurant en Annexe 2 (Mesures techniques et organisationnelles).

5.3 Dans le cadre de l'évaluation du niveau de sécurité approprié, le Fournisseur prend notamment en compte les risques que présente le Traitement des données, en particulier ceux liés à la destruction, la perte ou l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

5.4 Le Client peut demander, par écrit, au Fournisseur une modification des mesures techniques et organisationnelles stipulées en Annexe 2, afin de tenir compte de tous changements à la Loi sur la protection des données. A réception, le Fournisseur s'engage à appliquer ces changements sans délai indu et sans frais additionnels pour le Client. Cet avis écrit comprendra une description du changement de loi et les détails des modifications à apporter à l'Annexe 2.

5.5 Le Fournisseur est tenu de prendre à sa charge les modifications à apporter aux mesures techniques et organisationnelles stipulées en Annexe 2, pour s'assurer le cas échéant du respect continu de la clause 5.1.

6. Sous-traitance n-1

6.1 Le Fournisseur n'est pas autorisé à recruter des Sous-traitants n-1 pour traiter les Données à caractère personnel du Client, sans le consentement écrit préalable du Client.

6.2 En ce qui concerne chaque Sous-traitant n-1 agréé, le Fournisseur est tenu :

6.2.1 de fournir au Client toutes les informations relatives au Traitement que chaque Sous-traitant n-1 doit entreprendre ;

6.2.2 de faire preuve de la diligence requise à l'égard de chacun des Sous-traitants n-1 pour vérifier qu'ils sont en mesure de fournir un niveau de protection adéquat des Données à caractère personnel du Client, comme l'exige le présent Avenant. Ceci comprend, mais sans s'y limiter, les garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées, de manière à ce que le Traitement réponde aux exigences du RGPD et du présent Avenant ;

6.2.3 d'assortir des conditions au contrat conclu entre le Fournisseur et le Sous-traitant n-1 équivalentes à celles stipulées dans le présent Avenant. Sur demande, le Fournisseur fournit au Client, aux fins d'examen, une copie du contrat de sous-traitance ;

6.2.4 dans la mesure où ce contrat implique le transfert hors de l'EEE des Données à caractère personnel du Client (après accord spécifique du Client), d'insérer les Clauses contractuelles types ou tout autre mécanisme, conformément aux instructions du Client, dans le contrat conclu entre le Fournisseur et chaque Sous-traitant n-1, pour garantir le degré de protection adéquat des Données à caractère personnel du Client transférées. À la demande du Client, le Fournisseur fait également en sorte que chaque Sous-traitant n-1 s'engage à respecter les clauses contractuelles types ou tout autre mécanisme similaire dans un contrat direct avec le Client ;

6.2.5 de rester pleinement responsable vis-à-vis du Client de tout manquement d'un Sous-traitant n-1 aux obligations que lui impose le Traitement des Données à caractère personnel du Client.

7. Droits des Personnes concernées

7.1 Le Fournisseur est tenu d'avertir rapidement (dans les 72h) le Client s'il reçoit une demande d'une Personne concernée, au titre des Lois sur la protection des données, concernant les Données à caractère personnel du Client.

7.2 Le Fournisseur se doit de coopérer avec le Client, à la demande de ce dernier, pour permettre au Client de s'acquitter de l'obligation de respecter les droits exercés par une Personne concernée en vertu des Lois sur la protection des données relatives aux Données à caractère personnel du Client. Le Fournisseur se doit de se conformer à toute évaluation, enquête, notification ou instruction au titre des Lois sur la protection des données portant sur les Données à caractère personnel du Client, ou en vertu du présent Avenant, et notamment :

7.2.1 fournir toutes les données sollicitées par le Client, dans un délai raisonnable spécifié par ce dernier, y compris l'ensemble des détails et des copies de toute plainte, la communication ou la demande et toutes les Données à caractère personnel du Client qu'il détient en lien avec une Personne concernée ;

7.2.2 le cas échéant, dispenser l'aide que pourrait raisonnablement demander le Client pour lui permettre de répondre à une requête pertinente, dans les délais prescrits par les Lois sur la protection des données ;

7.2.3 mettre en œuvre toutes les mesures techniques et organisationnelles que le Client peut raisonnablement demander, pour lui permettre de répondre efficacement aux plaintes, communications ou à toute demande pertinente.

8. Violation de données à caractère personnel

8.1 Le Fournisseur notifie le Client immédiatement et en tout état de cause dans les vingt-quatre (24) heures après avoir pris connaissance d'une Violation de données à caractère personnel ou l'avoir raisonnablement suspectée, en fournissant au Client les informations dont il a besoin afin de respecter toute obligation en vertu de la Loi sur la protection des données. Cette notification doit, a minima :

8.1.1 décrire la nature de la Violation des données à caractère personnel, les catégories et le nombre de Personnes concernées, ainsi que les catégories et le nombre de données concernées ;

8.1.2 communiquer le nom et les coordonnées du délégué à la protection des données du Fournisseur ou de tout autre contact pertinent susceptible de fournir des informations supplémentaires ;

8.1.3 décrire les conséquences probables de la Violation des données à caractère personnel ;

8.1.4 décrire les mesures prises ou proposées pour remédier à la Violation des données à caractère personnel, ainsi que toute mesure à mettre en œuvre pour réduire le risque qu'une Violation du même type se reproduise à l'avenir.

8.2 Le Fournisseur coopère avec le Client et prend toute mesure raisonnable que celui-ci lui préconise pour appuyer le travail d'enquête, d'atténuation et de correction de chaque Violation des données à caractère personnel.

8.3 En cas de Violation des données à caractère personnel, le Fournisseur n'informe aucune tierce partie sans en avoir obtenu au préalable le consentement écrit du Client, à moins qu'il n'en soit tenu par le droit de l'UE ou d'un État membre auquel il est soumis. Dans cette dernière hypothèse, le Fournisseur est tenu, dans toute la mesure permise par la loi, d'informer le Client de cette obligation, de lui fournir une copie de la notification proposée et de tenir compte des commentaires laissés par le Client avant tout signalement de la Violation des données à caractère personnel.

9. Analyse d'impact relative à la protection des données et consultation préalable

9.1 Le Fournisseur procure une assistance raisonnable au Client pour toute analyse d'impact relative à la protection des données, qui serait requise au titre de l'Article 35 du RGPD et pour toute consultation préalable d'une autorité de contrôle du Client ou de l'une de ses Sociétés affiliées qui serait requise au titre de l'Article 36 du RGPD. Dans chaque cas, l'assistance requise concerne uniquement le Traitement des Données à caractère personnel du Client réalisé par le Fournisseur pour le compte du Client et tient compte de la nature du Traitement et des informations disponibles pour le Fournisseur.

10. Restitution ou suppression des Données à caractère personnel du Client

10.1 Sous réserve de la section 10.2, le Fournisseur est tenu dans les plus brefs délais, et en tout état de cause dans les 90 (quatre-vingt-dix) jours suivant la première des dates ci-après : (i) arrêt du Traitement des Données à caractère personnel du Client par le Fournisseur ; ou (ii) résiliation du Contrat ; selon le choix du Client (choix devant être notifié par écrit au Fournisseur), de procéder de l'une des manières suivantes :

10.1.1 restituer au Client une copie intégrale de toutes les Données à caractère personnel le concernant, au moyen d'un mode de transfert de fichiers sécurisé et dans le format indiqué au Fournisseur par le Client et effacer de façon définitive et sécurisée toutes les autres copies des Données à caractère personnel du Client dont le Traitement a été effectué par le Fournisseur ou un Sous-traitant n-1 agréé ;

10.1.2 effacer de façon définitive et sécurisée toutes les copies des Données à caractère personnel du Client dont le Traitement a été effectué par le Fournisseur ou un Sous-traitant n-1 agréé, et dans tous les cas, fournir au Client une attestation écrite certifiant que toutes les dispositions de la section 10.1 ont été respectées.

10.2 Nonobstant les dispositions de la section 10.1, le Fournisseur peut conserver les Données à caractère personnel du Client afin de se conformer à toute législation de l'Union ou d'un État membre, pour les finalités, dans les limites et pour les périodes décrites par lesdites législations.

11. Droits d'audit

11.1 Le Fournisseur met à la disposition du Client, sur demande, toutes les informations nécessaires pour démontrer le respect du présent Avenant.

Le Fournisseur autorise et contribue à tout audit en lien avec le Traitement des Données à caractère personnel du Client, y compris toute inspection des installations de traitement des données par le Client ou tout auditeur tiers mandaté par ce dernier.

A ce titre le Fournisseur autorise le Client ou tout auditeur tiers mandaté par le Client à inspecter, vérifier et copier tous documents, processus et systèmes pertinents afin que le Client puisse s'assurer du respect des dispositions du présent Avenant. Il appartient au Fournisseur de collaborer sans réserve avec le Client en mettant à sa disposition tout élément de preuve lui permettant de démontrer le respect de ses obligations en vertu du présent Avenant.

Le Fournisseur informe le Client sans délai indu si, selon lui, une instruction en vertu du présent article enfreint le RGPD ou toute autre disposition de l'UE ou d'un État membre en matière de protection des données.

12. Transferts internationaux de Données à caractère personnel du Client

12.1 Le Fournisseur n'est pas autorisé à Traiter les Données à caractère personnel du Client ou à autoriser un Sous-traitant n-1 agréé à le faire dans un Pays soumis à restrictions, sans l'autorisation écrite préalable du Client.

12.2 À la demande du Client, le Fournisseur conclut sans délai indu (ou fait en sorte qu'un Sous-traitant n-1 pertinent conclu) un accord avec le Client ou l'une de ses Sociétés affiliées, incluant les clauses contractuelles types et/ou les variations que les Lois sur la protection des données peuvent exiger, concernant le Traitement des Données à caractère personnel du Client dans un Pays soumis à restrictions. Ces conditions spécifiques prévaudront sur celles figurant dans le présent Avenant.

13. Codes de conduite et certification

13.1 À la demande du Client, le Fournisseur est tenu de se conformer à un Code de conduite approuvé au titre de l'Article 40 du RGPD et d'obtenir toute certification approuvée au titre de l'Article 42 du RGPD, dans la mesure où ils sont liés au Traitement des Données à caractère personnel du Client.

14. Responsabilité

14.1 Nonobstant toute limite ou exclusion de responsabilité prévue au Contrat, le Fournisseur s'engage à dégager le Client de toute responsabilité et à l'indemniser de tous coûts, dommages, pertes, amendes et sanctions découlant d'une réclamation par un tiers ou une autorité de surveillance relevant d'une violation du présent Avenant.

15. Dispositions générales

15.1 Sous réserve de la section 15.2, les Parties conviennent que le présent Avenant et les clauses contractuelles types prennent automatiquement fin à la résiliation du Contrat (ou à l'expiration ou la résiliation de tous les accords que le Fournisseur a conclus avec le Client en vertu du Contrat, à compter de la date la plus tardive).

15.2 Toutes les obligations imposées au Fournisseur au titre du présent Avenant relatives au Traitement des Données à caractère personnel perdurent à la cessation ou l'expiration du présent Avenant.

15.3 Le Fournisseur déclare connaître les Lois sur la protection des données applicables et s'acquitter de l'ensemble de ses obligations en tant que Responsable de traitement.

15.4 Tout manquement au présent Avenant constitue une violation essentielle du Contrat.

15.5 La conformité du Fournisseur via-à-vis des dispositions du présent Avenant n'entraîne pas de frais supplémentaires pour le Client.

15.6 Une Société affiliée du Client peut faire valoir toute disposition du présent Avenant qui lui bénéficie expressément ou implicitement.

15.7 Le droit des Parties d'annuler ou de modifier le présent Avenant n'est soumis à aucun consentement tiers.

15.8 Si une disposition quelconque du présent Avenant est tenue pour nulle ou non applicable, l'ensemble des autres dispositions de cet Avenant restent en vigueur et demeurent applicables. La disposition nulle ou inapplicable est (i) modifiée si nécessaire pour en garantir la validité et la force exécutoire, tout en préservant au mieux les intentions des Parties ou, en cas d'impossibilité, (ii) réputée non écrite.

ANNEXE 1 : INFORMATIONS SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU CLIENT

Cette Annexe 1 contient les renseignements relatifs au Traitement des Données à caractère personnel du Client, conformément aux dispositions de l'article 28(3) du RGPD.

L'objet et la durée du Traitement des Données à caractère personnel du Client sont stipulés dans le Contrat qui décrit la fourniture de biens et/ou services au Client.

Les Données à caractère personnel traitées en vertu du présent Avenant peuvent comporter les catégories suivantes :

i. Données personnelles de base (nom, adresse, titre, grade ou diplôme, date de naissance) ;
ii. Coordonnées (numéro de téléphone, numéro de téléphone portable, courriel, numéro de télécopieur, adresse) ;
iii. Données contractuelles de base ;
iv. Historique clients ;
v. Accès au système / utilisation / données d'autorisation ;
vi. Données à caractère personnel relatives aux informations financières et/ou relations professionnelles ;
vii. Données à caractère personnel révélant l'origine raciale ou ethnique ;
viii. Données à caractère personnel révélant les opinions politiques ;
ix. Données à caractère personnel révélant des convictions religieuses ou philosophiques ;
x. Données à caractère personnel révélant l'appartenance syndicale ;
xi. Données génétiques ou biométriques ;
xii. Données concernant la santé ;
xiii. Données concernant la vie ou l'orientation sexuelle d'une personne physique ;
xiv. Données à caractère personnel relatives aux infractions et condamnations pénales.

Les groupes de Personnes concernées dont les Données à caractère personnel sont traitées en vertu du présent Avenant peuvent comporter les catégories suivantes :

Anciens et nouveaux clients ; anciens et nouveaux salariés ; anciens et nouveaux contractuels ou consultants ; contractuels ou consultants missionnés par une agence et employés détachés externes ; demandeurs d'emploi et candidats ; étudiants et bénévoles ; personnes identifiées comme salariées ou retraitées (notamment ayants droit, conjoint(e), partenaire civil, concubin, personnes à charge, personnes à joindre en cas d'urgence) ; retraités ; anciens et nouveaux administrateurs et dirigeants ; actionnaires ; obligataires ; titulaires de comptes ; utilisateurs / consommateurs finaux (adultes, enfants) ; patients (adultes, enfants) ; passants (caméras de vidéosurveillance) ; utilisateurs de site Web.

ANNEXE 2 : MESURES TECHNIQUES ET ORGANISATIONNELLES

Commentaire général :
Iron Mountain conçoit que certaines de ces mesures ne s'appliquent pas dès lors que le Fournisseur ne Traite pas les Données à caractère personnel de manière électronique sur ses systèmes (ou ceux de ses Sous-traitants n-1) ou qu'il dispose de l'accès aux systèmes d'Iron Mountain traitant les Données à caractère personnel.

1.1 Contrôle des accès physiques.
Les personnes non autorisées ne peuvent pas accéder physiquement aux locaux, bâtiments ou salles dans lesquels se trouvent les systèmes de Traitement des données qui gèrent et/ou utilisent les Données à caractère personnel.
Mesures :
• Le Fournisseur protège ses actifs et ses installations à l'aide des moyens appropriés en fonction d'une classification de sécurité réalisée par un service de sécurité interne.
• En général, les bâtiments sont sécurisés par le biais de systèmes de contrôle d'accès (par exemple, par badge).
• A minima, les points d'entrée les plus à l'extérieur du bâtiment doivent être dotés d'un système de clé certifié comportant un dispositif ultra-moderne de gestion active des clés.
• En fonction de la classification de sécurité, les bâtiments, les secteurs individuels et les locaux environnants peuvent être protégés par des mesures supplémentaires, notamment : des profils d'accès spécifiques, de la vidéo-surveillance, des systèmes d'alarme contre l'intrusion et des systèmes de contrôle d'accès biométriques.
• Ces droits d'accès sont attribués aux personnes autorisées à titre personnel conformément aux mesures en place de contrôle d'accès au système et aux données (voir les articles 1.2 et 1.3 ci-après). Ces exigences s'appliquent également à l'accès des visiteurs. Les invités et les visiteurs qui accèdent aux bâtiments du Fournisseur doivent inscrire leur nom à la réception. Par ailleurs, ils doivent être accompagnés de membres du personnel autorisés du Fournisseur.
• Les employés et le personnel externe doivent porter leur badge d'identification sur tous les sites du Fournisseur.

1.2 Contrôle de l'accès au système.
Il convient d'empêcher l'utilisation non autorisée des systèmes de Traitement des données permettant de fournir les services du Fournisseur.
Mesures :
• Plusieurs niveaux d'autorisation sont utilisés pour l'octroi de l'accès à des systèmes sensibles, notamment ceux qui permettent le stockage et le traitement des Données à caractère personnel. Des processus sont en place pour garantir que les personnes autorisées disposent des droits appropriés pour ajouter, supprimer ou modifier des utilisateurs.
• Tous les utilisateurs accèdent aux systèmes du Fournisseur à l'aide d'un identifiant unique (ID utilisateur).
• Le Fournisseur a mis en place des procédures pour veiller à ce que les changements d'autorisation demandés soient uniquement appliqués conformément aux directives (par exemple, aucun droit n'est accordé sans autorisation). Si un utilisateur quitte la société, ses droits d'accès sont révoqués sans délai.
• Le Fournisseur a instauré une stratégie de gestion des mots de passe qui interdit leur partage, régit les réponses à apporter à leur divulgation et exige de changer régulièrement de mot de passe et de modifier les mots de passe par défaut. Les ID utilisateurs personnalisés sont attribués aux fins d'authentification. Tous les mots de passe doivent remplir des exigences minimales définies et sont encryptés. En ce qui concerne les mots de passe de domaine, le système impose qu'ils soient changés tous les six mois conformément aux exigences associées aux mots de passe complexes. Chaque ordinateur est doté d'un écran de veille protégé par mot de passe.
• Le réseau de l'entreprise du Fournisseur est protégé du réseau public via un pare-feu.
• Le Fournisseur utilise un logiciel antivirus à jour aux points d'accès au réseau de l'entreprise (pour les comptes de messagerie), ainsi que sur tous les serveurs de fichiers et tous les postes de travail.
• La gestion des correctifs de sécurité est mise en œuvre pour garantir le déploiement régulier et périodique des mises à jour de sécurité pertinentes.
• L'accès distant complet au réseau d'entreprise du Fournisseur et à son infrastructure critique est protégé par une authentification forte.

1.3 Contrôle de l'accès aux données.
Les personnes habilitées à utiliser les systèmes de Traitement des données accèdent uniquement aux Données à caractère personnel pour lesquelles elles disposent d'un droit. Les Données à caractère personnel ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation lors de leur traitement, utilisation et stockage.
Mesures :
• Dans le cadre de la stratégie de sécurité du Fournisseur, les Données à caractère personnel requièrent au moins le même niveau de protection que les informations « confidentielles », selon le standard de classification des informations du Fournisseur.
• L'accès aux informations à caractère personnel, confidentiel ou sensible est accordé aux seules personnes qui en ont besoin. Autrement dit, les salariés ou les tierces parties extérieures accèdent aux informations dont ils ont besoin pour accomplir leur tâche. Le Fournisseur utilise des procédures d'autorisation qui décrivent comment les autorisations sont octroyées et qui déterminent quelle autorisation est accordée et qui en bénéficie. Toutes les données à caractère personnel, confidentiel ou sensible sont protégées conformément aux stratégies et standards de sécurité du Fournisseur. Les informations confidentielles doivent être traitées en toute discrétion.
• Tous les serveurs de production sont gérés dans des centres de données ou des salles de serveurs sécurisées. Les mesures de sécurité qui protègent les applications traitant les informations à caractère personnel, confidentiel ou sensible sont vérifiées régulièrement. Dans cette optique, le Fournisseur procède à des contrôles de sécurité internes et externes ainsi qu'à des tests de pénétration sur ses systèmes informatiques.
• Le Fournisseur interdit l'installation des logiciels personnels ou ceux qui n'ont pas reçu son approbation.
• Les standards de sécurité du Fournisseur régissent la façon dont les données et leur support sont supprimés ou détruits lorsqu'ils ont perdu leur utilité.

1.4 Contrôle de la transmission des données.
Il est interdit de lire, copier, modifier ou supprimer les Données à caractère personnel sauf si cela est nécessaire à la prestation de services conformément au Contrat. Lorsque des supports de données sont transportés physiquement, il convient de prendre les mesures adéquates chez le Fournisseur pour veiller au respect des niveaux de service convenus (par exemple, par le recours au chiffrement ou à des conteneurs scellés).
• Le transfert de Données à caractère personnel sur les réseaux internes du Fournisseur est protégé de la même manière que pour toutes autres données confidentielles, conformément à la stratégie de sécurité du Fournisseur.
• Lorsque des données sont transférées entre le Fournisseur et ses clients, les mesures de sécurité appliquées dans un tel cas sont convenues d'un commun accord et intégrées au Contrat. Cette disposition s'applique au transfert de données physique ou électronique. En tout état de cause, le Client assume la responsabilité de tout transfert de données intervenant à l'extérieur des systèmes contrôlés par le Fournisseur (c.-à-d., les données transmises à l'extérieur du pare-feu du centre de données du Fournisseur).

1.5 Contrôle de la saisie des données.

Il est possible d'examiner et de déterminer rétroactivement si les Données à caractère personnel ont été saisies, modifiées ou supprimées des systèmes de traitement des données du Fournisseur et par qui elles l'ont été.

Mesures :

• Le Fournisseur autorise uniquement les personnes habilitées à accéder aux Données à caractère personnel, si elles en ont besoin dans le cadre de leur travail.

• Le Fournisseur a mis en œuvre un système de journalisation pour consigner, autant que possible, la saisie, la modification, la suppression et le blocage des Données à caractère personnel par lui-même ou par l'un de ses Sous-traitants n-1, dans le cadre de la délivrance de ses services et produits.

1.6 Contrôle de la disponibilité.

Les Données à caractère personnel sont protégées de la destruction ou de la perte accidentelle ou non autorisée.

Mesures :

• Le Fournisseur emploie des processus et toute autre mesure pour garantir la restauration rapide de ses systèmes métiers critiques lorsque cela est nécessaire.

• Le Fournisseur utilise des sources d'alimentation ininterrompue (par exemple : onduleurs, batteries, groupes électrogènes, etc.) pour assurer l'alimentation en courant.

• Le Fournisseur a défini des plans d'urgence ainsi que des stratégies métier et des stratégies de reprise après sinistre pour les services fournis.

• Les processus et les systèmes d'urgence sont testés de manière régulière.

1.7 Contrôle de la séparation des données.

Les données à caractère personnel qui ont été collectées à des fins différentes doivent être traitées séparément.

Mesures :

• Le Fournisseur utilise les capacités techniques du logiciel déployé (par exemple : des environnements système multi-location ou distincts) pour réaliser la séparation des données parmi des Données à caractère personnel provenant de plusieurs clients.

• Les Clients (y compris leurs Sociétés affiliées) ont uniquement accès à leurs propres données.

• S'il est nécessaire de disposer de Données à caractère personnel pour gérer un incident lié à un client particulier, les données sont assignées à ce message et ne sont utilisées qu'aux fins du traitement dudit message. Elles ne sont pas accessibles pour gérer les autres messages. Ces données sont stockées dans des systèmes de support dédiés.

1.8 Contrôle de l'intégrité des données.

Les Données à caractère personnel demeurent intactes, complètes et à jour au cours des activités de traitement.

Mesures :

Le Fournisseur a implémenté une stratégie de défense à niveaux multiples pour lutter contre les modifications non autorisées.

En effet, le Fournisseur se sert des méthodes suivantes pour mettre en œuvre les procédures décrites dans les sections ci-dessus portant sur le contrôle et les mesures.

• Pare-feux ;

• Centre de surveillance de la sécurité ;

• Logiciel antivirus ;

• Sauvegarde et récupération ;

• Test de pénétration interne et externe ;

• Vérifications externes régulières pour éprouver les mesures de sécurité.