**Accord sur la protection des données**

***Préambule***

Le Fournisseur est amené à traiter des Données à caractère personnel dans le cadre de ses relations commerciales avec ses clients (ci-après le « Client »). La présente Charte a pour objet de préciser les droits et obligations des Parties.

## *1. Définitions*

Dans la présente Charte, les mots ou expressions commençant avec une majuscule auront la signification suivante :

- « **Charte** » désigne le présent document ;
- « **Données à caractère personnelles ou DCP** » désigne toute information relative à une personne physique identifiée ou qui peut être identifiée (ci-après « Personne Concernée »), directement ou indirectement, notamment par référence à un numéro d'identification, une donnée de localisation, des identifiants en ligne (par exemple, pseudo et mot de passe) ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;
- **« Règlementation »** : désigne l'ensemble des lois et règlements applicables dans l'Union Européenne en matière de DCP, y compris la loi dite « Informatique et Libertés » n°78-17 du 6 janvier 1978 modifiée, et le Règlement Général sur la Protection des Données Personnelles 2016/679 en date du 27 avril 2016 dès son entrée en application.
- « **Prestations** » signifie l'ensemble des prestations réalisées par le Fournisseur pour ses Clients ;
- « **Responsable de Traitement** » désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Dans le cadre des Prestations réalisées par le Fournisseur, le Responsable de Traitement est le Client.
- « **Sous-traitant** » désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des DCP pour le compte du Responsable de Traitement, et conformément à ses instructions. Dans le cadre des Prestations réalisées par le Fournisseur, le Sous-traitant est le Fournisseur.
- **« Traitement »** : désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des Données ou des ensembles de Données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
- Les termes et expressions **« Violation de DCP », « Traiter », « Personne concernée », « Etat membre », « Autorité de contrôle », « Clauses types »,** ont le même sens que celui qui leur est donné dans la Réglementation, et les expressions voisines doivent être interprétées de la même manière.

## 2. Obligations générales du Client

Le Client s'engage à respecter la Réglementation.

Le Fournisseur, en sa qualité de Sous-Traitant, ne traitera des Données à caractère personnel que sur instructions documentées du Client et exclusivement pour accomplir les Prestations qui lui sont confiées.

Si le Client utilise les Prestations pour traiter d'autres données ou catégories de Données à caractère personnel ou pour d'autres Traitements, le Client le fait à ses risques et périls et le Fournisseur ne peut être tenu pour responsable en cas de manquement à la Réglementation.

Le Client, en sa qualité de Responsable de Traitement s'engage à alerter sans délai le Fournisseur en cas d'évolution des Prestations, entraînant ou risquant d'entraîner un changement potentiel du statut Sous-traitant du Fournisseur au regard de la Réglementation.

Le Client reconnait que les engagements du Fournisseur dans le cadre de la présente Charte constituent des garanties suffisantes de la conformité du Fournisseur à la Réglementation.

Le Client reconnait que le Fournisseur se limite à suivre les instructions documentées du Client, sous réserve d'informer le Client en cas d'instructions données non conformes à la Réglementation. Toute instruction non documentée par écrit ou non conforme à la Réglementation n'est pas prise en compte.

Le Client tient un registre de toutes les opérations de traitement qu'il effectue en qualité de Responsable de Traitement. Ce registre contient au moins les informations obligatoires requises par la Réglementation.

Il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des DCP. Au choix du Responsable de traitement, le Fournisseur assistera le Client dans la mise en œuvre de cette obligation d'information. Dans cette dernière hypothèse, les modalités d'assistance demandée par le Client seront convenues d'un commun accord entre le Client et le Fournisseur.

## 3. Obligations du Fournisseur vis-à-vis du Client

✓ <u>Agir sur instructions documentées du Responsable de Traitement</u>

Le Fournisseur s'engage à traiter les Données à caractère personnel conformément à la présente Charte et aux instructions du Client, à moins que le Fournisseur ne soit tenu de traiter les DCP en vertu d'une disposition impérative résultant du droit

communautaire ou du droit de l'Etat Membre auquel il est soumis. Dans ce cas, le Fournisseur en informera le Client dans les meilleurs délais, et si possible avant le Traitement.

Si le Fournisseur considère qu'une instruction constitue une violation de la Réglementation, le Fournisseur s'engage à en informer le Client.

- ✓ Garantir la confidentialité des DCP

Le Fournisseur s'engage à garantir la confidentialité des Données à caractère personnel traitées.

Le Fournisseur s'engage à veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu des présentes :

- S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- Reçoivent la sensibilisation nécessaire en matière de protection des Données à caractère personnel.

- ✓ Sous-Traitance

Le Fournisseur peut faire appel à un autre sous-traitant (« Sous-Traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il en informe par écrit le Client. Le Client dispose d'un délai de cinq (5) jours ouvrés pour faire valoir ses potentielles réserves.

Il appartient au Fournisseur de s'assurer que le Sous-Traitant ultérieur présente les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences de la Règlementation.

- ✓ Droits des personnes

Dans la mesure du possible, le Fournisseur aidera le Client à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées au titre de la Règlementation à savoir : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des DCP, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage au sens de la Réglementation).

Lorsque les personnes concernées exercent auprès du Fournisseur des demandes d'exercice de leurs droits, le Fournisseur adressera ces demandes par courrier électronique à la personne désignée par le Responsable de traitement ou communiqué par tout autre moyen. Le Fournisseur ne pourra répondre directement à la demande d'une personne concernée que sur instruction documentée du Responsable de traitement.

Le Client reconnait que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Fournisseur à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation. En cas de nécessité de mettre en œuvre des diligences additionnelles, les Parties conviennent de se réunir et discuter de bonne foi des conditions de ces diligences additionnelles.

- ✓ Notification des violations de Données à caractère personnel

Une violation de Données à caractère personnel s'entend de toute violation de la sécurité entraînante, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de DCP transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles DCP.

Le Fournisseur notifie au Client toute violation de Données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et conformément à la procédure définie par le Responsable de Traitement, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Le Client reconnait que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Fournisseur à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation. En cas de nécessité de mettre en œuvre des diligences additionnelles, les Parties conviennent de se réunir et discuter de bonne foi des conditions de ces diligences additionnelles.

- ✓ Analyses d'impact

Le Fournisseur aide le Responsable de Traitement pour la réalisation d'analyses d'impact relatives à la protection des Données que le Responsable de Traitement déciderait d'effectuer.

Le Client reconnait que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Fournisseur à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation. En cas de nécessité de mettre en œuvre des diligences additionnelles, les Parties conviennent de se réunir et discuter de bonne foi des conditions de ces diligences additionnelles.

### 4. Obligation en matière de sécurité et de confidentialité

Le Fournisseur s'engage à mettre en œuvre l'ensemble des mesures d'ordre technique et organisationnel appropriées et à prendre toutes précautions utiles pour garantir un niveau de sécurité adapté au risque existant.

Le Fournisseur s'engage à prendre toutes précautions utiles au regard de la nature des Données et des risques par le Traitement, pour préserver la sécurité des Données et empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation, et/ou tout accès par des tiers non autorisés préalablement.

Les mesures prises par le Fournisseur doivent tenir compte des possibilités techniques les plus récentes et du coût de leur mise en œuvre, des caractéristiques du traitement (nature, portée, finalité etc.) ainsi que des risques présentés pour les droits des Personnes Concernées. Il peut notamment s'agir :

- ✓ de mesures de chiffrement des données ;
- ✓ de mesures permettant de s'assurer, pendant la mise en œuvre du traitement, de la confidentialité, de l'intégrité, de la disponibilité et de la résistance des systèmes et services traitant les données ;
- ✓ de mesures permettant de restaurer l'accès et la disponibilité des données dans les plus brefs délais en cas d'incident matériel ou technique ;
- ✓ de procédures destinées à évaluer et tester l'effectivité des mesures techniques et organisationnelles.

Le Client reconnait que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Fournisseur à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation. En cas de nécessité de mettre en œuvre des diligences additionnelles, les Parties conviennent de se réunir et discuter de bonne foi des conditions de ces diligences additionnelles.

## 5. Retour ou suppression des Données Personnelles

Au terme du Contrat, le Fournisseur doit, au choix du Client, soit retourner l'ensemble des Données Personnelles traitées, soit les supprimer et certifier au Client par écrit que la suppression a bien été réalisée sous réserve et dans la limite des obligations légales et réglementaires de conservation s'imposant au Fournisseur.

## 6. Audit

Le Client pourra, s'il le souhaite, dans la limite d'une (1) fois par an, réaliser, à ses frais, un audit au sein des locaux du Fournisseur, directement ou par l'intermédiaire de tout tiers indépendant, non concurrent du Fournisseur, afin de s'assurer du respect des mesures de protection des DCP, traitées dans le cadre des Prestations.

Dans l'hypothèse où le Client souhaiterait faire appel à un tiers pour la réalisation de l'audit, ce dernier s'engage expressément à faire signer audit tiers un accord de confidentialité et à se porter fort du respect de ses termes.

Le Client communiquera au Fournisseur avec un préavis d'au moins quarante (45) jours calendaires, toute demande d'opération d'audit, la date de l'audit ainsi que le nom de l'éventuel tiers en charge de l'audit. Le Fournisseur pourra refuser le cabinet d'audit et les personnes désignées pour réaliser l'audit, si la proposition du Client fait apparaitre un conflit d'intérêt et/ou si le cabinet d'audit est un concurrent du Fournisseur. En cas de refus, le Fournisseur devra le notifier sous un délai de huit (8) jours calendaires suivant la notification de l'audit faite par le Client ou par un cabinet d'audit en charge de le réaliser (l'Auditeur) dans les conditions définies par la présente Charte.

Les modalités de réalisation de l'audit feront l'objet d'un accord préalable signé par les Parties, dans lequel figureront notamment les conditions suivantes :

- Planning d'audit, étant ici précisé que l'audit ne pourra se tenir que les jours et heures ouvrés ;
- Les intervenants concernés ;
- Les qualités du cabinet d'audit et de l'auditeur, étant ici précisé que le cabinet d'audit et l'auditeur devront être certifiés ISO 27 001 et/ou GDPR compliant ;
- Les modalités de communication du rapport d'audit au Fournisseur ;
- Les modalités de mise en place d'un plan d'actions correctives issues du rapport d'audit précité.

Le Fournisseur collaborera de bonne foi avec l'Auditeur et lui communiquera toutes informations ou documents ou explications nécessaires à la réalisation de l'audit. Les procédures d'accès seront communiquées par le Fournisseur au Client qui devra les respecter. Les connexions logiques pour accéder aux données Client seront réalisées par le Fournisseur à la demande de l'Auditeur et, lorsque cela est nécessaire, en présence de l'Auditeur.

Le Fournisseur prendra à sa charge le temps passé par son personnel pour les besoins de l'audit dans la limite d'un (1) jour par an. Le rapport d'audit sera adressé gratuitement au Fournisseur par les auditeurs ou par le Client, dans un délai défini dans l'accord d'audit, de telle sorte que celui-ci puisse formuler, dans un délai de vingt (20) jours ouvrés suivant la date de sa communication, toutes observations ou objections par lettre recommandée avec accusé de réception adressée à l'auditeur et au Client.

Ce rapport d'audit est confidentiel.

Au cas où le rapport d'audit ferait apparaître un manquement à une obligation essentielle en matière de DCP, directement et exclusivement imputable au Fournisseur, ce dernier s'engage expressément à mettre en œuvre à ses frais toutes les mesures correctives nécessaires.