

## PROTECTION DES DONNEES PERSONNELLES

### DEFINITIONS

Dans le présent contrat, les mots ou expressions commençant avec une majuscule auront la signification suivante :

« **Contrat** » désigne le contrat conclu avec le Prestataire dans le cadre duquel s'inscrit la présente annexe.

« **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 le Règlement Général sur la Protection des Données Personnelles 2016/679 en date du 27 avril 2016 (« RGPD ») ;

« **Prestations** » : désigne l'ensemble des prestations réalisées par le Prestataire pour le Client et telles que visées dans le Contrat ;

« **Responsable de Traitement** » : désigne le Client 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 du Contrat pour l'exécution des Prestations et de la présente annexe, 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 du Contrat pour l'exécution des Prestations et de la présente annexe, le Sous-traitant est le Prestataire, soit GENERIX ;

« **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.

### ARTICLE 1 : OBLIGATIONS GENERALES DU CLIENT

- 1.1 Le Client s'engage à respecter la Réglementation dans le cadre du Contrat.
- 1.2 Le Prestataire, en sa qualité de Sous-Traitant, ne traitera des Données à caractère personnel que sur instructions documentées du Client, telles que figurant dans l'annexe « Fiche d'instructions de traitement » dans le Contrat de souscription concerné, et exclusivement pour accomplir les prestations confiées au titre du Contrat. Les instructions du Client portant sur les Traitements sont décrites dans l'annexe « Fiche d'instructions de traitement » dans le Contrat de souscription concerné. Le Client s'engage à renseigner cette Fiche d'instructions de traitement à la signature du Contrat de souscription et au plus tard dans les quatre semaines suivant la signature du Contrat de souscription. Si le Client utilise les Services objet du Contrat pour traiter d'autres données ou catégories de Données à caractère personnel ou pour d'autres Traitements que ceux décrits dans la Fiche d'instructions de traitement, le Client le fait à ses risques et périls et le Prestataire ne peut être tenue pour responsable en cas de manquement à la Réglementation.
- 1.3 Le Client reconnaît que le Prestataire 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 demande du Client modifiant le Service et qui engendrerait un changement au niveau des instructions de traitement figurant dans la Fiche d'instructions de traitement fera faire l'objet d'un devis séparé. Toute instruction non documentée par écrit ou non conforme à la Réglementation n'est pas prise en compte.

- 1.4 En outre, tout paramétrage et/ou développement spécifique à la demande du Client pour l'utilisation des Services et accepté par le Prestataire entraînant une évolution des instructions entraîne automatiquement une Mise à Jour de l'Appendice « Fiche d'instructions de traitement ». Toute utilisation ultérieure des Données par le Client est réalisée aux risques et périls de ce dernier, le Prestataire ne pourra être tenue pour responsable en cas de manquement à la Réglementation.
- 1.5 En cas d'évolution des Services demandés, entraînant ou risquant d'entraîner un changement potentiel du statut du Prestataire au regard de la Réglementation, les Parties s'engagent à se rapprocher afin d'encadrer la relation et de définir leurs obligations et responsabilités respectives.
- 1.6 Le Client reconnaît que les engagements du Prestataire dans le cadre de la présente annexe constituent des garanties suffisantes de la conformité du le Prestataire à la Réglementation.
- 1.7 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.
- 1.8 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 Prestataire 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 Prestataire.

## **ARTICLE 2 : OBLIGATIONS DU PRESTATAIRE VIS-A-VIS DU CLIENT**

### **2.1 Agir sur instructions documentées du Responsable de Traitement**

1. Le Prestataire s'engage à traiter les Données à caractère personnel, objet de la présente Annexe, conformément aux instructions listées dans la Fiche d'instructions de traitement du Contrat de souscription concerné dans tout devis complémentaire ou par tout moyen écrit émanant du Client à moins que le Prestataire 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 Prestataire en informera le Client dans les meilleurs délais, et si possible avant le Traitement.
2. Si le Prestataire considère qu'une instruction constitue une violation de la Réglementation, le Prestataire s'engage à en informer le Client.

### **2.2 Garantir la confidentialité des DCP**

1. Le Prestataire s'engage à garantir la confidentialité des Données à caractère personnel traitées dans le cadre de la présente Annexe.
2. le Prestataire s'engage à veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu des présentes :
  - 2.1. S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
  - 2.2. Reçoivent la sensibilisation nécessaire en matière de protection des Données à caractère personnel.

### **2.3 Sous-Traitance**

Le Prestataire 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. Il appartient au Prestataire 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 Réglementation.

### **2.4 Droits des personnes**

1. Dans la mesure du possible et de manière raisonnable, le Prestataire 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 Réglementation 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).
2. Lorsque les personnes concernées exercent auprès du le Prestataire des demandes d'exercice de leurs droits, le Prestataire adressera ces demandes par courrier électronique à la personne désignée par le Responsable de traitement dans la Fiche d'instructions de traitement du Contrat de souscription ou

communiqué par tout autre moyen. Le Prestataire ne pourra répondre directement à la demande d'une personne concernée que sur instruction documentée du Responsable de traitement.

3. Le Client reconnaît que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Prestataire à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation concernant les droits des personnes. 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, qui feront l'objet d'un avenant aux présentes.

## **2.5 Notification des violations de Données à caractère personnel**

1. Une violation de Données à caractère personnel s'entend de toute violation de la sécurité entraînant, 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.
2. Le Prestataire notifie au Client toute violation de Données à caractère personnel dans les meilleurs délais après en avoir pris connaissance par courrier électronique à la personne désignée par le Responsable de traitement dans la Fiche d'instructions de traitement du Contrat de souscription ou communiqué par tout autre moyen, 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. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.
3. Le Client reconnaît que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Prestataire à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation en matière de notification des violations de DCP. 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, qui feront l'objet d'un avenant aux présentes.

## **2.6 Analyses d'impact**

1. Le Prestataire 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 de manière raisonnable.
2. Le Client reconnaît que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Prestataire à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation concernant l'analyse d'impact. 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, qui feront l'objet d'un avenant aux présentes.

## **ARTICLE 3 : SECURITE ET CONFIDENTIALITE**

- 3.1 Le Prestataire 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.
- 3.2 Le Prestataire 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.
- 3.3 Les mesures prises par le Prestataire 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 :
  1. De mesures de chiffrement des données ;
  2. 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 ;
  3. De mesures permettant de restaurer l'accès et la disponibilité des données dans les plus brefs délais en cas d'incident matériel ou technique ;

4. De procédures destinées à évaluer et tester l'effectivité des mesures techniques et organisationnelles.
- 3.4 Le Client reconnaît que les diligences précitées satisfont à l'obligation de coopération et d'assistance du Prestataire à l'égard du Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation concernant la sécurité et la confidentialité. 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, qui feront l'objet d'un avenant aux présentes.

#### **ARTICLE 4 : RETOUR OU SUPPRESSION DES DONNEES PERSONNELLES**

Au terme du Contrat, le Prestataire 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 Prestataire.

#### **ARTICLE 5 : AUDIT**

- 5.1 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 Prestataire, directement ou par l'intermédiaire de tout tiers indépendant, non concurrent du Prestataire, afin de s'assurer du respect des mesures de protection des DCP, traitées dans le cadre du Contrat.
- 5.2 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 et à communiquer cet accord sur demande expresse du Prestataire.
- 5.3 Le Client communiquera au Prestataire avec un préavis d'au moins quarante-cinq (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 par écrit. Le Prestataire pourra refuser le cabinet d'audit et les personnes désignées pour réaliser l'audit, si la proposition du Client fait apparaître un conflit d'intérêt et/ou si le cabinet d'audit est un concurrent du Prestataire. En cas de refus, le Prestataire 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 le présent Contrat.
- 5.4 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 ;
  - Les modalités de communication du rapport d'audit au Prestataire.
- 5.5 Le Prestataire 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 Prestataire au Client qui devra les respecter. Les connexions logiques pour accéder aux données Client seront réalisées par le Prestataire à la demande de l'Auditeur et, lorsque cela est nécessaire, en présence de l'Auditeur.
- 5.6 Le Prestataire 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. Au-delà, l'audit sera facturé 3 000 (trois mille) euros hors taxe par jour ouvré d'audit.
- 5.7 Le rapport d'audit sera adressé gratuitement au Prestataire 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 selon les conditions de l'Article « Confidentialité » du Contrat.
- 5.8 Au cas où le rapport d'audit ferait apparaître un manquement grave à une obligation essentielle en matière de DCP, directement et exclusivement imputable au Prestataire, ce dernier s'engage expressément à mettre en œuvre, à ses frais, toutes les mesures correctives nécessaires afin d'être conforme au Contrat.