Annexe : Obligations de protection des données à caractère personnel

Préambule

Dans le cadre des relations contractuelles existantes entre Nextpharm et toute personne effectuant un achat auprès des Ets Nextpharm, Am Wëllemt 6, L-9645 Derenbach (ci-après le « **client** »), Nextpharm est amenée à avoir accès et traiter des données pour le compte du client.

Le client et Nextpharm sont ci-après collectivement désignés les « **Parties** » ou individuellement la « **Partie** ».

La présente Annexe règle les relations de sous-traitance en matière de protection des données, telles que prévues notamment par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après « **RGPD** »).

Article 1 – Définitions

Pour les besoins de la présente Annexe, les définitions prévues par l'article 4 du RGPD et des Conditions générales de vente et du contrat de service (ci-après « **Contrat** ») s'appliquent.

Article 2 – Qualité des Parties

Dans le cadre de la mission conclue entre les Parties, le client détermine, en sa qualité de responsable du traitement, les finalités et les moyens du traitement envisagé.

Nextpharm, en sa qualité de sous-traitant, traite les données qui lui sont mises à disposition ou transmises, de quelque manière que ce soit, par le client exclusivement pour le compte du client. Nextpharm ne détermine ni les finalités, ni les moyens du traitement de ces données.

Article 3 – Objet

Afin de garantir une mise en œuvre efficace des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, les Parties s'engagent explicitement à se conformer aux exigences en matière de protection des données, en ce compris, notamment celles prévues par le RGPD.

Nextpharm s'engage en particulier à présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées en matière de protection des données.

Le traitement des données effectué par Nextpharm pour le compte du client a pour objet et finalité la fourniture des services conformément au Contrat, à savoir en particulier :

- la fourniture des programmes, logiciels, formations et de la documentation ;
- l'installation des programmes et logiciels ;
- les prestations de maintenance et d'entretien des équipements ;
- les changements, augmentations, transformations et transferts des installations ;

L'hébergement de données.

Le traitement des données par Nextpharm pour le compte du client est effectué pour la durée du Contrat.

Le traitement des données effectué par Nextpharm pour le compte du client porte notamment sur les catégories de données suivantes :

- données d'identification (p.ex. nom, prénom, âge, sexe) ;
- données concernant la santé ;
- données médicamenteuses ;
- données pathologiques ;
- données à caractère financier et/ou bancaire.

Le traitement des données effectué par Nextpharm pour le compte du client porte notamment sur les catégories de personnes suivantes :

- Patients ;
- Personnes soignées et personnel des maisons de soins (p.ex. CIPA, MRS,) ;
- Praticiens.

Article 4 – Principes applicables à la sous-traitance en matière de protection des données

Nextpharm s'engage à ne traiter les données qui lui ont été mises à disposition ou transmises par le client exclusivement pour le compte du client et dans les limites du Contrat.

Nextpharm s'engage en particulier :

- (i) à transférer les données qui lui ont été mises à disposition ou transmises par le client vers des pays tiers (c'est-à-dire en dehors de l'Espace économique européen) exclusivement pour les besoins d'exécution du Contrat, à moins que Nextpharm ne soit tenu d'y procéder en vertu d'une obligation légale ;
- (ii) à ne pas divulguer ou rendre ces données accessibles à autrui, de quelque manière que ce soit, sauf instruction préalable du client.

Seules les données strictement nécessaires à l'exécution de la mission telle que conclue entre les Parties doivent être traitées par Nextpharm.

Si Nextpharm est tenue de procéder à un traitement des données en vertu d'une obligation légale, Nextpharm informe le client de cette obligation légale préalablement à la mise en œuvre du traitement des données envisagé, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Article 5 – Privacy by design et Privacy by default

Nextpharm s'engage à mettre en œuvre des mesures techniques et organisationnelles appropriées destinées à assurer le respect des principes applicables en matière de protection des données.

Nextpharm s'engage à assurer la mise en place de mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données qui sont nécessaires au regard de chaque finalité spécifique poursuivie par le client sont traitées.

Article 6 – Mesures de sécurité

Nextpharm s'engage à mettre en œuvre – tout en tenant compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes concernées – des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Lors de l'évaluation du niveau de sécurité approprié, Nextpharm doit tenir compte, en particulier, des risques résultant notamment de l'accès non autorisé, de la destruction, de la perte, de l'altération ou de la divulgation non autorisée des données traitées pour le compte du client, que ce soit de manière accidentelle ou illicite.

Nextpharm s'engage à :

- éviter tout accès non autorisé, toute destruction, toute perte, toute altération ou toute divulgation non autorisée des données traitées pour le compte du client, que ce soit de manière accidentelle ou illicite ;
- Garantir que toute personne sous son contrôle (en particulier ses salariés) ou autrement liée à elle qui a accès à des données traitées pour le compte du client ou qui est autorisée à les traiter, les traite exclusivement pour les besoins d'exécution du Contrat et conformément à la législation applicable en respectant la confidentialité.**

Article 7 – Recours par Nextpharm à un autre sous-traitant en matière des traitements de données

Nextpharm peut engager un ou plusieurs sous-traitants pour mener des activités de traitement des données.

Nextpharm s'engage dans ce contexte formellement :

- à faire seulement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences applicables en matière de protection des données et garantisse la protection des droits des personnes concernées ;
- à préalablement imposer les mêmes obligations que celles prévues par la présente Annexe à cet autre sous-traitant ;
- à informer le client de tout changement prévu concernant l'ajout ou le remplacement d'un autre sous-traitant avant que pareille sous-traitance en matière de traitement de données prend effet et avant que les données traitées pour le compte du client sont divulguées au sous-traitant.

Si le client émet des objections à l'encontre d'un sous-traitant en matière de traitement des données, Nextpharm s'abstient d'engager le sous-traitant en question.

Lorsqu'un sous-traitant auquel Nextpharm a recours ne remplit pas ses obligations en matière de protection des données, Nextpharm demeure pleinement et entièrement responsable envers le client et les tiers de l'exécution par ce sous-traitant de ses obligations.

Article 8 – Obligation d'assister le client

Nextpharm s'engage à assister le client dans toute la mesure du possible à s'acquitter de ses obligations en matière de protection des données et en particulier de son obligation de donner suite aux demandes des personnes concernées liées à l'exercice de leurs droits en matière de protection des données, tels que prévus notamment par le Chapitre III du RGPD.

Compte tenu des informations à sa disposition, Nextpharm s'engage à assister le client en vue de garantir le respect des obligations incombant au client en matière de protection des données (en particulier celles prévues aux articles 32 à 36 du RGPD).

Nextpharm s'engage en particulier :

- à assister le client dans la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ;
- à assister le client dans le cadre du respect de l'obligation du client de notifier à l'autorité de contrôle compétente dans les délais impartis une violation de données encourue ;
- à assister le client dans le cadre du respect de l'obligation du client de communiquer toute violation de données directement à la personne concernée ;
- à assister le client dans la réalisation d'une analyse de l'impact des opérations de traitement envisagées sur la protection des données par le client avant la mise en œuvre du traitement envisagé ;
- à assister le client dans l'hypothèse où le client doit consulter l'autorité de contrôle conformément à l'article 36 du RGPD.

Article 9 – Obligation de renvoyer et de supprimer les données

Selon le choix et sur instruction préalable du client, Nextpharm supprime, à tout moment, tout ou partie des données traitées pour le compte du client.

Selon le choix et sur instruction préalable du client, Nextpharm doit, au terme de la mission conclue entre les Parties, (i) soit renvoyer toutes les données traitées pour le compte du client à celui-ci et détruire les copies existantes, (ii) soit supprimer toutes ces données.

L'obligation de suppression ou de destruction ne s'applique pas si une obligation légale à laquelle Nextpharm est soumise exige la conservation des données traitées pour le compte du client.

Article 10 – Obligation de démontrer le respect des obligations

Nextpharm s'engage à mettre à disposition du client toutes les informations nécessaires pour démontrer à tout moment le respect par les Parties des obligations leur incombant en matière de protection des données ou en vertu de la présente Annexe.

Nextpharm informe le client immédiatement si, selon elle, une instruction du client est susceptible de constituer une violation des exigences en matière de protection des données.

Article 11 – Droit d’effectuer des audits

Nextpharm permet au client, ou tout autre auditeur mandaté par le client, de contrôler à tout moment le respect des exigences incombant à Nextpharm en matière de protection des données et aux termes de la présente Annexe par quelque moyen que ce soit, y compris par des audits ou des inspections sur place. Nextpharm s’engage à contribuer par tout moyen à la réalisation de ces contrôles, audits ou inspections.

Lorsque Nextpharm diligente de son propre chef et à ses propres frais un contrôle, un audit ou une inspection interne ou externe, elle fournit au client dans les meilleurs délais toute information ayant un lien, direct ou indirect, avec l’exécution de la présente Annexe.

Article 12 – Durée

La présente Annexe lie les Parties et produit ses effets aussi longtemps que des données qui lui sont mises à disposition ou transmises par le client sont traitées par Nextpharm.

La fin du Contrat est sans incidence sur l’application des dispositions de la présente Annexe à tout fait ou traitement qui s’est produit au cours de la période pendant laquelle Nextpharm a traité des données pour le compte du client.

Pour le client

Pour Nextpharm