

Annexe 10 – Protection des données à caractère personnel - PN 25-15C ISP

Table des matières

1. Objet	1
2. Rôles et responsabilités des Parties	1
3. Sous-traitance Ulérieure	3
a. Principes généraux	3
b. Prestataire d’hébergement de Données de santé	3
4. Droits des personnes concernées	4
5. Notification des incidents de sécurité et des violations de Données	5
6. Aide du Partenaire dans le cadre du respect par l’AP-HP de ses obligations	5
7. Sort des Données.....	5
8. Audits et contrôles	6
9. Responsabilité	6
10. Sécurité.....	7

1. Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le Titulaire, agissant en tant que sous-traitant (ci-après, le « Partenaire » ou le « Sous-traitant ») au sens du Règlement général sur la protection des Données de l’UE (2016/679) (ci-après, « RGPD »), s’engage à effectuer pour le compte de l’AP-HP (ci-après, le « Responsable de Traitement » ou « l’AP-HP ») les opérations de Traitement de Données personnelles (ci-après, les « Données » ou « Données personnelles ») définies ci-après.

Le Partenaire est informé du caractère sensible des Données traitées, garantit qu’il respecte la réglementation (RGPD et loi IFL notamment) et reconnaît que les garanties de sécurité, de confidentialité et de disponibilité apportées constituent une condition essentielle de l’engagement de l’AP-HP.

Les termes utilisés dans le présent avenant ont le sens qui leur est donné par le RGPD à l’article Définition, notamment : « Responsable de Traitement », « Sous-traitant », « Données personnelles » (ou « Données »), « Violation de Données », « Traitement » et « Personne concernée ».

2. Rôles et responsabilités des Parties

Le Partenaire s'engage à :

- Effectuer pour le compte et sur les instructions de l’AP-HP les opérations de Traitement de Données strictement nécessaires pour fournir ses services prévus au Marché. Le Partenaire garantit qu’il ne traitera pas les Données pour son propre compte ;

- Si le Partenaire considère qu'il n'est pas en mesure de satisfaire à une instruction ou si selon lui, une instruction constitue une violation, il doit en informer l'AP-HP sans délai ;
- Traiter les Données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance et ne pas les traiter à des fins incompatibles avec la finalité du Traitement ;
- Garantir la sécurité, la disponibilité, l'intégrité et la confidentialité des Données traitées et d'empêcher qu'elles ne soient déformées, endommagées, perdues ou communiquées à des tiers non autorisés, par son fait ou celui de ses éventuels Sous-traitants Ultérieurs autorisés ;
- Veiller à ce que les personnes autorisées à traiter les Données personnelles appartenant aux équipes du Partenaire :
 - N'aient accès qu'aux Données dans la mesure strictement nécessaire à l'exécution des services prévus au Marché et
 - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des Données dès la conception (Privacy by design) et de protection des Données par défaut (Privacy by default) ;
- Aider l'AP-HP à garantir le respect de ses obligations, notamment en matière de sécurité, et pour la réalisation d'analyses d'impact et, le cas échéant, pour la réalisation de consultation préalable de la CNIL ou toute autre formalité ou revue de conformité à effectuer ;
- Mettre à la disposition à première demande de l'AP-HP la documentation nécessaire pour démontrer le respect de toutes ses obligations, notamment dans le cadre des audits, y compris des inspections, par l'AP-HP, par un tiers mandaté par l'AP-HP ou par les autorités de contrôle (la CNIL en l'espèce) ;
- Informer l'AP-HP sans délai de toute demande de communication contraignante qui émanerait d'une autorité administrative ou judiciaire et ne communiquer les Données qu'après autorisation écrite de l'AP-HP ;
- Informer immédiatement par écrit l'AP-HP de toute modification le concernant et pouvant avoir un impact sur le Traitement des Données personnelles ;
- Informer sans délai l'AP-HP si les Données reçues sont inexactes ou obsolètes, et coopérer avec l'AP-HP pour les rectifier ou les effacer ;
- Solliciter en temps opportun toutes les informations nécessaires à la bonne réalisation des Services et identifier tout risque sur son périmètre de responsabilité
- Formuler sans délai tous conseils, alertes, mises en garde, préconisations et informations dans le cadre de la réalisation du Marché, notamment en vue d'améliorer la sécurité et la confidentialité des Données ou de manière à permettre à l'AP-HP de prendre les décisions qui lui incombent ;
- Coopérer étroitement avec l'AP-HP et solliciter toute réunion qui se révélerait utile ;

Le Partenaire reconnaît que les Données personnelles de l'AP-HP sont et demeurent la propriété exclusive de cette dernière. Le présent document n'emporte aucune cession, que ce soit à titre onéreux ou gratuit des Données appartenant à l'AP-HP.

3. Sous-traitance Ultérieure

a. Principes généraux

Les sous-traitants du Partenaire sont qualifiés de « Sous-traitants Ultérieurs » au sens de la réglementation. Aucun Sous-traitant Ultérieur n'est autorisé sans l'accord express et préalable de l'AP-HP.

Le Partenaire doit indiquer notamment les activités de Traitement sous-traitées envisagées, l'identité et les coordonnées du Sous-traitant Ultérieur, la localisation des Données et la remise du contrat de sous-traitance ultérieure à première demande. L'AP-HP se réserve le droit de résilier le Marché en cas de désaccord sur ce Sous-traitant Ultérieur.

En tout état de cause tout Sous-traitant Ultérieur est tenu de respecter les mêmes obligations que le Partenaire au titre du présent avenant. Il appartient notamment au Partenaire de contrôler que le Sous-traitant Ultérieur présente en permanence les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles (audits réguliers à faire). Le Partenaire demeure pleinement responsable devant l'AP-HP de l'exécution par le Sous-traitant Ultérieur de ses obligations.

Le Partenaire n'est pas autorisé à transférer les Données personnelles hors de l'UE (lui-même ou via ses Sous-traitants Ultérieurs) sans avoir obtenu l'autorisation préalable de l'AP-HP et sans avoir mis en place les garanties nécessaires prévues par le chapitre 5 du RGPD (ex : clauses contractuelles types dans leur dernière version et mesures supplémentaires, BCR ou décision d'adéquation), étant précisé que tout accès distant aux Données depuis l'extérieur du territoire de l'UE est considéré comme un transfert. Les Sous-traitants Ultérieurs du Partenaire ne sont pas non plus autorisés à transférer à leur tour les Données à des tiers ou à d'autres sous-traitants ultérieurs sans autorisation expresse et préalable de l'AP-HP (interdiction de la sous-traitance en cascade).

Le Partenaire garantit que ni lui ni ses éventuels Sous-traitants Ultérieurs ne sont soumis à des lois et réglementations contraires aux réglementations applicables en UE, et avertira sans délai l'AP-HP en cas d'impossibilité de se conformer au RGPD et la loi IFL en raison de lois étrangères qui lui seraient applicables, à lui ou à ses Sous-traitants Ultérieurs.

b. Prestataire d'hébergement de Données de santé

En cas d'hébergement cloud de données de santé, et sans préjudice des dispositions ci-dessus, le Partenaire garantit expressément que son prestataire d'hébergement (qualifié de Sous-traitant Ultérieur) présente les garanties cumulatives suivantes :

- Serveurs du prestataire localisés en France ou au sein de l'UE
- Prestataire d'hébergement disposant de la certification HDS
- Prestataire d'hébergement conforme au référentiel SecNumCloud publié par l'ANSSI
- Prestataire d'hébergement garantissant sans réserve son immunité contre toute réglementation ou décision extra-européenne sur le transfert des données (garantie écrite, qui pourra être communiquée à l'AP-HP à première demande)

- Prestataire d'hébergement soumis aux lois et réglementations applicables au sein de l'UE en matière de protection des données personnelles et garantissant à tout moment le respect des dispositions du RGPD
- Prestataire d'hébergement fournissant des garanties de réversibilité des services permettant l'AP-HP de récupérer ou faire récupérer l'ensemble des Données sans atteinte à la continuité de son activité
- Conformité des services d'hébergement avec les règles de GAIA-X, notamment en terme d'interopérabilité et de portabilité.

A défaut pour le Partenaire de pouvoir s'engager sur les principes ci-dessus au jour de la signature des présentes, le Partenaire s'engage (à défaut, le marché pourra être résilié sans frais ni indemnité à première demande de l'AP-HP):

- A migrer les services d'hébergement dans un délai de 24 mois maximum vers une offre présentant l'intégralité des garanties exigées ci-dessus;
- A mettre en place sans délai avec son Sous-traitant Ulérieur en charge de l'hébergement cloud des données de santé les garanties appropriées exigées par le chapitre 5 du RGPD (par exemple, intégrer dans son contrat conclu avec son prestataire d'hébergement des clauses contractuelles types publiées par la Commission européenne dûment accompagnée des mesures supplémentaires permettant de garantir un niveau de protection équivalent à celui garanti au sein de l'UE). Le Partenaire garantit à ce titre que la législation du pays tiers à laquelle son Sous-traitant Ulérieur est soumis n'empiètera pas sur ces mesures supplémentaires de manière à les priver d'effectivité, ni ne risque de compromettre le niveau de protection adéquat que les clauses contractuelles types et les mesures supplémentaires sont précisément censées garantir ;
- A avertir sans délai l'AP-HP en cas de demande d'accès ou de risque d'accès par des autorités publiques étrangères aux Données hébergées, prendre toutes les actions légales et recours pour les contester et remettre à l'AP-HP toute documentation en ce sens.

En tout état de cause pour les projets qui le permettent seules des Données pseudonymisées et protégées par un code pourront être transférées, avec conservation de la table de correspondance exclusivement au sein de l'AP-HP, sans aucune possibilité pour le Partenaire ou ses Sous-traitants Ultérieurs d'y avoir accès. Le Partenaire ou ses Sous-traitants Ultérieurs ne sont pas autorisés à procéder à des rapprochements ou croisements avec d'autres bases de données pour tenter de réidentifier tout ou partie des personnes concernées.

4. Droits des personnes concernées

Les Personnes concernées doivent être informées par les opérations de Traitement. Le Partenaire s'engage le cas échéant à transmettre à l'AP-HP préalablement tous les éléments nécessaires à cette information à première demande de l'AP-HP.

Le Partenaire doit aider l'AP-HP à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées et fournir tous les moyens nécessaires à la gestion de ces demandes : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, etc.

Le Partenaire informera l'AP-HP sans délai et au plus tard dans les 24 heures suivant la réception s'il reçoit une demande d'exercice des droits par courrier électronique - protection.donnees.dsi@aphp.fr Le Partenaire ne répondra à aucune demande directement sauf pour confirmer que la demande concerne bien l'AP-HP si tel est bien le cas. Le Partenaire garantit

qu'il aidera l'AP-HP à traiter ces demandes conformément à la réglementation et dans le respect des délais impartis.

En cas de litige avec une Personne concernée ou tout autre tiers, le Partenaire doit coopérer pleinement avec l'AP-HP et assumer ses responsabilités si le litige a pour origine un manquement de sa part.

5. Notification des incidents de sécurité et des violations de Données

Le Partenaire notifie à l'AP-HP toute violation de Données sans délai et au maximum dans les 24 heures après en avoir pris connaissance. Cette notification doit être faite auprès de aphp-signalement-securite@aphp.fr, et être accompagnée de toute documentation utile afin de permettre à l'AP-HP, si nécessaire, de notifier cette violation à la CNIL et/ou aux Personnes concernées.

La procédure de notification d'incident de sécurité doit inclure :

- Une description de la violation de sécurité, la nature et les circonstances de cette violation ;
- Le type de Données ayant fait l'objet de la violation de sécurité et l'identité de chaque personne affectée ou le nombre approximatif de personnes et de Données personnelles concernées ;
- Le nom et les coordonnées du Délégué à la protection des Données du Partenaire et/ou de tout autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Une description des conséquences probables de la violation de sécurité ;
- Une description des mesures pour remédier à la violation de sécurité, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs éventuels ;
- Toute autre information que l'AP-HP peut raisonnablement demander concernant la violation de sécurité.

Le Partenaire enquête immédiatement sur la violation et identifie, prévient et fait ses meilleurs efforts pour atténuer les effets de toute violation de sécurité conformément à ses obligations résultant du présent article et, sous réserve de l'accord ou des instructions préalables de l'AP-HP, effectue toute action propre à remédier à la violation.

Le Partenaire ne publiera aucune communication externe, communiqué de presse ou rapport concernant toute violation de sécurité concernant les Données personnelles de l'AP-HP sans son autorisation écrite préalable. L'AP-HP décidera de notifier seul ou via le Partenaire le cas échéant la violation de sécurité auprès de l'autorité de contrôle concernée et/ou des personnes concernées.

6. Aide du Partenaire dans le cadre du respect par l'AP-HP de ses obligations

Le Partenaire aide l'AP-HP pour la réalisation d'analyses d'impact relative à la protection des données en fournissant tous les éléments relatifs à la sécurité et aux conditions d'utilisation des Données traités pour le compte de l'AP-HP.

Le cas échéant, le Partenaire aide l'AP-HP pour la réalisation de la consultation préalable de l'autorité de contrôle en fournissant à l'AP-HP tous les éléments relatifs à la sécurité et aux conditions d'utilisation des Données traités pour le compte de l'AP-HP.

7. Sort des Données

Au terme du Marché, le Partenaire garantit qu'il renverra toutes les Données à l'AP-HP à première demande dans un format lisible et agréé par cette dernière.

Le renvoi doit s'accompagner de la destruction immédiate de toutes les copies existantes dans les systèmes d'information du Partenaire. Une fois détruites, le Partenaire doit justifier par écrit auprès de l'AP-HP de la destruction. Le Partenaire n'est pas autorisé à anonymiser les Données sans avoir fait valider au préalable sa procédure d'anonymisation par l'AP-HP.

Le Partenaire mettra à la disposition de l'AP-HP à première demande toute la documentation nécessaire pour démontrer le respect de ses obligations.

8. Audits et contrôles

Sous réserve d'un préavis de dix (10) jours ouvrés, l'AP-HP se réserve le droit de procéder ou faire procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Partenaire de ses obligations au titre du Marché, notamment par le biais d'un audit ou d'une inspection de contrôle.

Le Partenaire s'engage à répondre aux demandes d'audit et de contrôle de l'AP-HP et effectuées par l'AP-HP elle-même ou par un tiers de confiance qu'elle aura sélectionné.

Les audits doivent permettre une analyse du respect des dispositions relatives à la protection des Données, notamment : par la vérification de l'ensemble des mesures de sécurité mises en œuvre par le Partenaire, par la vérification des journaux de localisation des Données, de copie et de suppression des Données, par l'analyse des mesures mises en place pour supprimer les Données, pour prévenir toutes transmissions illégales de Données à des juridictions non adéquates ou pour empêcher le transfert de Données vers un pays non autorisé. L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

À ce titre, le Partenaire met à la disposition du Responsable de Traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

Le Partenaire s'engage à collaborer de bonne foi avec tout auditeur ainsi désigné. Il facilitera l'accès des auditeurs à tout document ou information ou autre élément utile au bon déroulement de la mission d'audit et lui facilitera sa mission en particulier en répondant à toute question et en lui accordant l'accès à tous les outils et moyens nécessaires à l'audit. Si les conclusions de l'audit démontrent un manquement du Partenaire à ses obligations contractuelles (i) les mesures correctives seront étudiées en comité de pilotage qui statuera sur la suite qu'il convient d'y donner et des éventuelles mesures correctives à mettre en œuvre, sans surcoût, (ii) les frais d'audit seront mis à la charge du Partenaire.

En cas de contrôle de l'AP-HP par toute autre autorité réglementaire (notamment, CNIL), le Partenaire s'engage à faciliter l'accès aux environnements d'exploitation à ces autorités et à coopérer pleinement avec l'AP-HP. Le Partenaire s'engage à ne communiquer directement aux dites autorités aucune information sans avoir obtenu l'accord préalable et écrit de l'AP-HP, sauf en cas de disposition légale ou réglementaire impérative. Pour les besoins du contrôle, le Partenaire s'engage à communiquer sans délai à l'AP-HP tous les éléments qui lui seront réclamés à cette occasion sur le support requis par lesdites autorités.

9. Responsabilité

La responsabilité du Partenaire sera limitée aux dommages directs résultant d'un manquement de Partenaire ou de ses Sous-traitants Ultérieurs. Ne sauraient être qualifiés de dommages indirects les dommages liés à la sécurité, la confidentialité et à l'intégrité des Données de l'AP-HP.

Aucune limite de responsabilité ne s'appliquera en cas d'atteinte à la confidentialité, à la sécurité et à l'intégrité des Données de l'AP-HP, en cas de dol ou de manquement aux obligations essentielles du Partenaire.

10. Sécurité

Conformément à l'article 32 du RGPD, le Partenaire s'engage à prendre les mesures techniques et organisationnelles optimales afin de garantir un niveau de sécurité adapté au risque et au caractère sensible des Données notamment :

- La pseudonymisation et le chiffrement des Données ;
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité des systèmes et des services de Traitement ;
- Des moyens permettant de rétablir la disponibilité des Données et l'accès à celles-ci dans des délais appropriés en cas d'incident ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement ;
- La sécurité physique et logique (informatique et réseaux de communication) ;
- La mise en place de mesures pour protéger les Données contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé, dont le hacking ou la tentative de hacking des Données ;
- Des mécanismes de restriction et de contrôle d'accès des Données, permettant d'affecter aux individus, les droits d'accès aux Données strictement nécessaires à leur mission
- La conservation d'une documentation appropriée sur les activités de Traitements
- Obtenir les certifications nécessaires (notamment en termes d'hébergement de Données de santé si la réglementation le lui impose)
- Adopter des Clauses d'entreprises contraignantes (BCR) avec ses filiales le cas échéant.