

Convention de sous-traitance
« Responsable de traitements - Sous-traitant »
(Data Processing Agreement)

aux fins de respect du RGPD

l'Agence fédérale des Médicaments et des Produits de santé (AFMPS), situé 5/03 avenue Galilée à 1210 Bruxelles et représenté par Hugues Malonne, administrateur général (ci-après, « **le responsable de traitement** »)

d'une part,

ET

....., situé àet représenté
parà compléter par le fournisseur)

(ci-après, « **le sous-traitant** »)

d'autre part,
(à éventuellement compléter par le fournisseur si un autre sous-traitant intervient)

Les Parties souhaitent, par le biais de la présente convention, satisfaire à leurs obligations aux termes du Règlement général sur la protection des données 2016/679 du 27 avril 2016.

A. Définitions

Des termes comme "traitement", "données à caractère personnel", "intéressé", "responsable du traitement" et "sous-traitant" ont la signification qui leur est donnée dans le Règlement (CE) 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 (Règlement général sur la protection des données : "RGPD").

B. Objet

La présente convention est exclusivement applicable au traitement de données à caractère personnel dans le cadre du marché public 2024-PRAC signé en date du (service contrat) par les parties.

Dans le cadre de l'exécution du contrat susmentionné, le Sous-traitant peut traiter des données à caractère personnel ("Données à caractère personnel") pour le compte et sur instruction du Responsable du traitement.

Un relevé des catégories de Données à caractère personnel, les catégories de personnes concernées, les finalités pour lesquelles elles peuvent être traitées et une description de la ou des

activités de traitement, des mesures de protection et des transferts éventuels de Données à caractère personnel sont énoncés à **L'Annexe 1** à la présente convention.

Le Responsable du traitement est, à l'exclusion de tout autre, seul responsable de la détermination des finalités pour lesquelles des Données à caractère personnel seront (devront être) traitées ainsi que de la manière de procéder.

La propriété des Données à caractère personnel ne sera jamais transférée au Sous-traitant, à moins qu'il s'agisse de ses propres Données à caractère personnel ou de celles de son personnel ou de ses préposés.

C. Exécution de la Convention

1. Exécution du traitement et obligation du sous traitant

1.1 Le Sous-traitant garantit qu'il traitera uniquement les Données à caractère personnel pour le compte du Responsable du traitement de la manière qui est nécessaire pour l'exécution de la Convention. D'autres activités de traitement interviendront uniquement si le Responsable du traitement donne des instructions écrites en ce sens ou s'il existe une obligation légale à cet effet. Le Sous-traitant n'est en aucun cas autorisé à traiter les Données à caractère personnel pour son propre usage ou pour celui de tiers.

1.2. Le Sous-traitant est tenu de suivre toutes les instructions raisonnables du Responsable du traitement concernant le traitement des Données à caractère personnel, conformément au contrat qui les lie et à la présente convention. Si le Sous-traitant est tenu de traiter des Données à caractère personnel à la suite de la législation CE ou de la législation d'un État membre à laquelle est soumis le Sous-traitant, le Sous-traitant informera le Responsable du traitement de l'obligation légale qui lui incombe avant le traitement. Le Sous-traitant informera le Responsable du traitement sur-le-champ s'il estime que certaines instructions vont à l'encontre de la législation applicable en matière de traitement de données à caractère personnel ou de la Convention entre Parties.

Le Sous-traitant informera immédiatement le Responsable du traitement, et ce, par écrit, si des Données à caractère personnel lui sont fournies, transmises, mises à sa disposition ou rendues visible par ou au nom du Responsable du traitement alors que le Sous-traitant n'est raisonnablement pas autorisé à les recevoir dans le cadre du contrat qui les lie ou d'une disposition impérative de la loi, en accordant une attention toute particulière aux données sensibles (Données en matière de : race ou origine ethnique – opinions politiques – conceptions religieuses ou philosophiques – appartenance syndicale – données génétiques – données biométriques – informations en matière de santé d'un individu – comportement sexuel ou orientation sexuelle – informations judiciaires & mesures de sûreté y afférentes).

1.3. Le Sous-traitant traite les Données à caractère personnel correctement et avec soin, et ce, de manière démontrable, et conformément avec ses obligations en tant que sous-traitant en vertu du RGPD. Le Sous-traitant respecte également les prescriptions applicables au traitement en vertu des législations nationales ou locales pertinentes en matière de protection des données

1.4. Le Sous-traitant prendra et maintiendra en place, à ses propres frais, des mesures techniques et organisationnelles adéquates afin de protéger en permanence les Données à caractère personnel contre toute destruction accidentelle ou illicite ou contre toute perte accidentelle,

altération, publication, accès ou traitement non autorisés. Le Sous-traitant peut utiliser tous les instruments qu'il juge utiles pour atteindre ces objectifs.

1.5. Le Sous-traitant conserve et traite les Données à caractère personnel concernant le Responsable du traitement de manière strictement séparée des Données à caractère personnel qu'il traite pour son propre compte ou pour le compte de tiers.

1.6. Le Sous-traitant informera immédiatement le collaborateur du Responsable du traitement tel que nommé à **l'Annexe 2** de tout transfert éventuel (prévu) permanent ou temporaire de Données à caractère personnel. **L'Annexe 1** reprend une liste des transferts pour lesquels le Responsable du traitement accorde son autorisation au moment de la conclusion de la présente convention. Le Responsable du traitement a, à tout moment, le droit d'assortir son autorisation concernant un tel traitement, de conditions supplémentaires

1.7. Le Sous-traitant doit garantir la confidentialité des données à caractère personnel traitées dans le cadre de la présente convention. Il doit veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu de la présente convention :

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel

2. Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

3. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à dpo@fagg-afmps.be .

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

4. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance et par le moyen suivant : mail à dpo@fagg-afmps.be et thierry.roisin@fagg-afmps.be. 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.

Par le terme "violation" on entend dans tous les cas :

(a) une plainte ou une demande (d'informations) émanant d'une personne physique concernant le traitement des Données à caractère personnel par Sous-traitant ;
(b) une enquête ou une saisie portant sur les Données à caractère personnel par des fonctionnaires publics, ou toute élément indiquant l'imminence d'une telle situation ;
(c) tout accès, traitement, échange, perte non autorisé ou accidentel ou toute forme de traitement illégal de Données à caractère personnel ;
(d) tout non-respect de la sécurisation et/ou de la confidentialité tels qu'exposés à l'Article 32 du RGPD, conduisant à la perte ou à toute forme de traitement illégal, en ce compris à une destruction, perte, altération accidentelle ou illicite de Données à caractère personnel ou une publication ou accès non-autorisé à celles-ci, ou encore toute indication laissant penser qu'un tel non-respect s'est déjà produit ou se produira dans un proche avenir.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

5. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

6. Mesures de sécurité

Les obligations générales et spécifiques en matière de sécurité et respect de la confidentialité sont exposées dans l'appel d'offre ou le contrat conclu, objet de la présente fourniture de service.

Sauf indication contraire formulée dans cet appel d'offre ou le contrat conclu, le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- la pseudonymisation ou le chiffrement des données à caractère personnel
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

Le Responsable du traitement a le droit de contrôler et de tester le respect des mesures visées ci-dessus.

Ce contrôle sera effectué par un tiers indépendant. À la demande du Responsable du traitement, le Sous-traitant en donnera dans tous les cas la possibilité, au moins une fois par an, au Responsable du traitement, à un moment déterminé d'un commun accord entre Parties ou, lorsque le Responsable du traitement le juge nécessaire à la suite de (présumés) incidents concernant les données ou le respect de la vie privée. Le Sous-traitant sera tenu de se conformer à toutes les instructions du Responsable du traitement visant la modification de la politique de sécurité à la suite de ce contrôle.

Les Parties reconnaissent que les exigences de sécurisation sont en perpétuelle évolution et qu'une sécurisation effective requiert de fréquentes évaluations et une amélioration régulière de mesures de sûreté dépassées. Le Sous-traitant procédera par conséquent à une évaluation continue des mesures introduites en vertu du présent article 6 et affinera, complètera ou corrigera ces mesures afin de continuer de remplir les obligations qui lui incombent

Le Responsable du traitement a le droit de charger le Sous-traitant de prendre des mesures supplémentaires de sécurisation, aux frais du Sous-traitant. Si une modification du contrat est nécessaire à l'exécution de cette mission, les Parties entameront une négociation de bonne foi.

7. Responsabilité et garantie

Le Sous-traitant garantit le Responsable du traitement et dédommagera le Responsable du traitement en cas de réclamations, actions, demandes de tiers ainsi qu'en cas de pertes, dommages ou frais exposés ou subis par le Responsable du traitement et qui découlent directement ou indirectement ou surviennent à la suite d'un quelconque non-respect par le Sous-traitant ou le sous-sous-traitant des obligations visées dans la présente convention et/ou de toute infraction par le Sous-traitant ou le sous-sous-traitant à la législation applicable en matière de traitement de données à caractère personnel dans le cadre du RGPD.

8. Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minium de 3 mois à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le

sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

9. Sort des données

Le Sous-traitant n'est pas autorisé à conserver les Données à caractère personnel plus longtemps que ce qui est strictement nécessaire et dans tous les cas pas après la fin du contrat ou, si un délai de conservation a été convenu entre les Parties, pas après ce délai.

À l'extinction du contrat, ou s'il y a lieu à l'extinction des délais de conservation convenus, ou à la première demande écrite du Responsable du traitement, le Sous-traitant détruira immédiatement les Données à caractère personnel ou les retournera immédiatement au Responsable du traitement, et ce, au choix du Responsable du traitement. À la demande du Responsable du traitement, le Sous-traitant devra apporter la preuve de la destruction ou de l'élimination des données. En cas d'impossibilité de retour, destruction ou élimination, le Sous-traitant en informera immédiatement le Responsable du traitement. Dans ce cas, le Sous-traitant garantira le respect de la confidentialité des Données à caractère personnel et qu'elles ne seront plus traitées.

À la fin du contrat, le Sous-traitant informera tous les tiers impliqués dans le traitement des Données à caractère personnel, de l'extinction de la Convention et garantira que tous les tiers impliqués détruiront les Données à caractère personnel ou les retourneront au Responsable du traitement, et ce, au choix du Responsable du traitement.

Si, pour des raisons techniques, une destruction ou un effacement intégral des données à caractère personnel n'est pas possible, le Sous-traitant prendra toutes les mesures nécessaires pour

- se rapprocher le plus près possible d'une destruction et/ou d'un effacement complets et permanents et pour
- anonymiser et rendre les données à caractère personnel restantes inutilisables pour tout traitement ultérieur. Le Sous-traitant informera toujours le Responsable du traitement par écrit à ce sujet.

10. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données

11. Registre des catégories d'activités de traitement

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données;
- les catégories de traitements effectués pour le compte du responsable du traitement;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1,

deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - la pseudonymisation et/ou le chiffrement des données à caractère personnel;
 - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
 - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
 - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
 - (autre à définir)

Le sous-traitant communiquera copie de ce registre au responsable du traitement.

12. Documentation

Le sous-traitant met à la disposition du responsable de traitement la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

D. Durée du contrat et extinction

La présente convention entre en vigueur à la date de sa signature et est d'application pour la durée reprise dans l'appel d'offre repris en rubrique.

L'extinction ou l'expiration du présent Addendum ne dispense pas le Sous-traitant de ses obligations qui ont vocation à rester applicables même après l'extinction ou l'expiration de la Convention, en ce compris les obligations découlant des articles 5, 6, 9 et 11 du présent Addendum.

E. Dispositions terminales

Les autres modalités du contrat restent applicables de manière inchangée. Les dispositions de la présente convention prévaudront en cas de contradiction entre la présente convention et le contrat en matière de respect de la vie privée et de protection des données.

La présente convention est régie par le droit belge. Les litiges éventuels découlant ou présentant un lien avec la présente convention relèveront du ressort exclusif des tribunaux compétents de Bruxelles.

L'acceptation du présent document fait office de NDA.

Les preuves du suivi de procédures de sécurités décrites dans les paragraphes précédents seront apportées sur demande du responsable du traitement ou lors d'audits organisés.

F. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. fournir au sous-traitant les données visées à l'annexe 1 des présentes clauses
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant (voir annexe 1)
3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données

Fait en deux exemplaires.

En date du

Représentant de l'AFMPS

Hugues Malonne

Administrateur général

Représentant du sous-traitant

Annexe 1

- 1) Un relevé des catégories de données à caractère personnel à traiter (à compléter par l'adjudicateur, l'adjudicataire peut éventuellement y ajouter des éléments) :

Données personnelles des notificateurs d'effets indésirables et des personnes ayant subi des effets indésirables. Coordonnées administratives + données médicales telles que la taille, le poids, le profil clinique, les allergies, la consommation de médicaments, ...

- 2) Lister les catégories de personnes concernées (à compléter par l'adjudicateur, l'adjudicataire peut éventuellement y ajouter des éléments)

Le notificateur (professionnel de la santé ou patient) de l'effet indésirable et la personne (patient) qui a subi l'effet indésirable.

- 3) Lister les finalités pour lesquelles les données peuvent être traitées (à compléter par l'adjudicateur, l'adjudicataire peut éventuellement y ajouter des éléments)

Le contractant peut, afin d'évaluer correctement le rapport en tant qu'expert, consulter les données personnelles du notificateur et/ou du patient. Il ne traitera pas ces données par la suite.

- 4) Décrire les activités de traitement des données (à compléter par l'adjudicateur, l'adjudicataire peut éventuellement y ajouter des éléments). NB : Une référence à l'offre de l'adjudicataire est admise.

Voir 3/

- 5) Décrire les mesures de protection des données mises en place par l'adjudicataire (à compléter par l'adjudicateur, l'adjudicataire peut éventuellement y ajouter des éléments). NB : Une référence à l'offre de l'adjudicataire est admise.

L'information sera transmise par un canal sécurisé : eudrawemail. Après traitement, le contractant détruira dès que possible et au maximum après 3 mois les données personnelles.

- 6) Des transferts éventuels de données à caractère personnel (à compléter par l'adjudicateur, l'adjudicataire peut éventuellement y ajouter des éléments).

nihil

Annexe 2 : instructions pour le traitement des données

Point(s) de contact du Responsable du traitement (à compléter par l'adjudicateur)

- Pour l'exécution du contrat : thierry.roisin@fagg-afmps.be...
- Pour le DPO : dpo@fagg-afmps.be

Point(s) de contact du sous-traitant (à compléter par l'adjudicataire)

.....

Annexe 3

Politique de Sécurité et de Confidentialité du sous-traitant (à annexer par l'adjudicataire)