ACCORD DE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Préambule

Le Prestataire étant amené à traiter des Données à caractère personnel dans le cadre de sa relation contractuelle avec le client, les Parties souhaitent préciser leurs droits et obligations. Dans le cadre du présent accord, le Prestataire sera ci-après désigné comme le « Sous-Traitant ».

1. Définitions

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

- « Accord » désigne le présent accord de traitement de données à caractère personnel qui vient préciser les droits et obligations des Parties concernant le traitement des données à caractère personnel.
- « Contrat » désigne le Contrat cadre et les Contrats d'application conclus avec le Prestataire dans le cadre duquel s'inscrit le présent Accord.
- « Données à caractère personnel 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 ;
- « Personne Concernée » désigne la personne physique dont les DCP font l'objet d'un Traitement ;

- « 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 du Contrat et du présent Accord, 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 et du présent Contrat, le sous-traitant est le Prestataire.
- « 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 (ci-après le « RGPD »).
- « Traitement » : désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des Données à caractère personnel 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 », « État 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 du Client

Le Client s'engage à respecter les obligations lui incombant en qualité de Responsable de Traitement issues de la Réglementation.

Le Client reconnait que le Sous-Traitant se limite à suivre les instructions du Client, sous réserve d'informer le Client en cas d'instructions données non conformes à la Réglementation.

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.

3. Obligations du Sous-Traitant

3.1 Obligations générales

Le Sous-Traitant s'engage à respecter la Réglementation dans le cadre du Contrat. Il s'engage notamment, sans que cette liste ne soit limitative, à :

- Ne traiter les DCP du Client que sur instructions du Client afin de fournir les services et de remplir ses obligations au titre du Contrat.
  Il est ici précisé que la description du traitement de DCP confié au Sous-Traitant figure dans chaque Contrat d'application selon le modèle figurant en Appendice A du présent Accord L'Appendice pourra faire l'objet de modifications par le Client. Toute modification de l'Appendice A sera communiquée par écrit au Sous-Traitant.
  Dans l'hypothèse où le Sous-Traitant serait tenu de procéder à un traitement de Données à caractère personnel en vertu d'une disposition impérative résultant du droit communautaire ou du droit de l'État membre auquel il est soumis, le Sous-Traitant informera le Client de cette obligation juridique avant le traitement des Données, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

- S'abstenir d'agir d'une manière qui constituerait ou entrainerait une violation de la Réglementation par le Client et alerter le Client sans délai en cas de détection par le Sous-Traitant d'une conformité ou d'un risque de non-conformité ;

- Garantir et indemniser le Client en cas d'action, réclamation, demande de toute tierce partie résultant de son manquement ou de sa défaillance à l'égard de la Réglementation dans le cadre du présent Contrat ;

- Tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client. Ce registre contient au moins les informations obligatoires requises par la Réglementation, notamment :

(i) le nom et les coordonnées du Responsable de traitement pour le compte duquel il agit, des éventuels Sous-Traitants Ultérieurs et, le cas échéant, du délégué à la protection des Données ;
(ii) les catégories de traitements effectués pour le compte du Responsable de traitement ;
(iii) 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, les documents attestant de l'existence de garanties appropriées ;
(iv) 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 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.

Le Sous-Traitant met ce registre à la disposition de toute autorité de contrôle qui en fait la demande et du Client à première demande.
Le Sous-Traitant garantit également :

- mettre en œuvre les ressources humaines, techniques et organisationnelles suffisantes pour opérer les traitements en conformité avec la Réglementation, telles que, et sans que cette liste ne soit limitative : former son personnel, nommer un DPO, le cas échéant, appliquer les principes de privacy by design et by default, etc.
- Garantir la confidentialité des Données à caractère personnel traitées dans le cadre du Contrat.
- Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu du Contrat :
  - 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.

3.2 Obligations de coopération et d'assistance

Le Sous-Traitant assiste le Client et coopère activement avec le Client pour lui permettre d'assurer la conformité du Traitement à la Réglementation, en particulier pour ce qui est des demandes d'exercice des droits des personnes concernées. Le Sous-Traitant s'engage notamment au respect des dispositions suivantes.

✔ **Droit d'information des personnes concernées**

Il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des DCP ou, au choix du Client, de demander au Sous-Traitant, au moment de la collecte des DCP, de fournir, aux personnes concernées par les opérations de traitement, l'information relative aux traitements de DCP qu'il réalise. Dans cette dernière hypothèse, la formulation et le format de l'information seront convenus par le Client avant toute collecte de DCP.

✔ **Exercice des droits des personnes**

Dans la mesure du possible, le Sous-Traitant doit aider 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 sur la protection des DCP, à savoir principalement : 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).

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 la personne désignée par le Client, en *Appendice A* ou communiqué par tout

autre moyen au choix du Client. Le Sous-Traitant ne pourra répondre directement à la demande d'une personne concernée que sur instruction du Client.

- ✔ **Notification des violations de Données à caractère personnel**

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.

Lors d'une violation de Données à caractère personnel, le Sous-Traitant s'engage à procéder à toutes investigations utiles sur les manquements aux règles de protection afin d'y remédier dès que possible et de diminuer l'impact de tels manquements sur les personnes concernées.

Le Sous-Traitant notifie au Client toute violation de Données à caractère personnel dans les 24 heures après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.
Sur ce point, le Sous-Traitant est informé qu'en cas de notification d'une violation de Données à caractère personnel par le Client à l'autorité de contrôle compétente, la notification doit contenir au moins :

(i) 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 ;
(ii) la description des conséquences probables de la violation de Données à caractère personnel ;
(iii) la description des mesures prises ou que le Responsable de 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 est impossible de fournir toutes ces informations simultanément, les informations peuvent être communiquées de manière échelonnée sans retard indu. En tout état de cause, le Sous-Traitant s'engage à informer le Client de ses investigations sur les manquements aux règles de protection ayant entraîné la violation de Données à caractère personnel, de l'évolution de la nature et des conséquences de la violation, ainsi que des mesures prises ou envisagées pour diminuer l'impact des manquements identifiés, et ce de manière régulière.

Le Sous-Traitant s'engage à collaborer activement avec le Client pour qu'ils soient en mesure de répondre à leurs obligations réglementaires et contractuelles. Seul le Client peut notifier la violation des Données à caractère personnel à l'autorité de contrôle compétente et

communiquer des informations sur cette violation aux personnes concernées ; le Sous-Traitant s'interdit en conséquence de procéder à une telle notification et à une telle communication.

- ✔ **Aide du Sous-Traitant dans le cadre de l'analyse d'impact**

Le Sous-Traitant aide le Client pour la réalisation d'analyses d'impact relatives à la protection des Données que le Client déciderait d'effectuer.

Le Sous-Traitant aide le Client dans le cadre de la consultation préalable de l'autorité de contrôle, suite à la réalisation des analyses d'impact.

- ✔ **Aide du Sous-Traitant dans le cadre du respect par le Client de son obligation d'accountabilty**

Le Sous-Traitant fournit au Client, à la première demande, les documents et informations nécessaires pour démontrer le respect de toutes ses obligations au titre du présent Accord.
En cas de contrôle d'une autorité compétente, les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le Sous-Traitant en tant que responsable de traitement, le Sous-Traitant fera son affaire du contrôle et s'interdira de communiquer ou de faire état des Données à caractère personnel du Client.

Dans le cas où le contrôle mené chez le Sous-Traitant concernerait les traitements mis en œuvre au nom et pour le compte du Client, le Sous-Traitant s'engage à en informer immédiatement le Client et à ne prendre aucun engagement pour elle.

En cas de contrôle d'une autorité compétente chez le Client portant notamment sur les prestations délivrées par le Sous-Traitant, ce dernier s'engage à coopérer avec le Client et à lui fournir toute information dont il pourrait avoir besoin ou qui s'avèrerait nécessaire.

4. <u>Obligation en matière de sécurité et de confidentialité</u>

Le Sous-Traitant met en œuvre les mesures de sécurité et de confidentialité nécessaires à la conformité du Traitement à la Réglementation.

Sans préjudice des dispositions du corps du Contrat, le Sous-Traitant met en œuvre toutes mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel, en considérant l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du Traitement ainsi que les risques, dont le degré de probabilité

et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

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

En particulier, le Sous-Traitant s'engage à assurer une étanchéité totale entre les Données du Responsable de traitement et les données des autres clients du Sous-Traitant, par une séparation physique et logique.

Les moyens mis en œuvre par le Sous-Traitant destinés à assurer la sécurité et la confidentialité des Données incluent notamment les mesures suivantes :

- pseudonymisation et le chiffrement des DCP,
- 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 l'accès et la disponibilité des DCP dans les 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 Sous-Traitant s'engage à maintenir ces moyens tout au long de l'exécution du Contrat et, à défaut, à en informer immédiatement le Client.

En tout état de cause, le Sous-Traitant s'engage en cas de changement des moyens visant à assurer la sécurité et la confidentialité des DCP et des fichiers, à les remplacer par des moyens d'une performance supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

5. 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 Client de tout changement envisagé concernant l'ajout ou le remplacement d'autres Sous-Traitants Ultérieurs. Cette information doit explicitement indiquer les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-Traitant Ultérieur, les dates du contrat de sous-traitance et l'existence éventuelle de flux de DCP en dehors de l'Union européenne ou vers une organisation internationale. Le Client dispose d'un délai maximum de deux mois calendaires à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Client n'a pas émis d'objection pendant ce délai.

Le Sous-Traitant Ultérieur est tenu de respecter les obligations du Contrat, et de ne traiter des Données à caractère personnel que pour le compte et selon les instructions du Client. En conséquence, le Sous-Traitant initial s'engage à signer avec son Sous-Traitant ultérieur un contrat écrit faisant référence au Contrat, et imposant au Sous-Traitant ultérieur les mêmes obligations en matière de protection des DCP que celles fixées dans le Contrat.

Il appartient au Sous-Traitant initial de s'assurer, notamment à travers ce contrat écrit, 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.

Si le Sous-Traitant Ultérieur ne remplit pas ses obligations en matière de protection des DCP, le Sous-Traitant initial demeure pleinement responsable à l'égard du Responsable de traitement de l'exécution par le Sous-Traitant Ultérieur de ses obligations, notamment en ce qui concerne la notification des violations de Données à caractère personnel.

6. Retour ou suppression des Données Personnelles

Au terme du Contrat, le Sous-Traitant 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 Sous-Traitant.

Au terme de la prestation de services relatifs au traitement des Données, le Sous-Traitant s'engage à :

- restituer toutes les Données à caractère personnel et les fichiers au Client dans un format exploitable et dans les conditions spécifiées par le Client ou
- adresser les Données à caractère personnel au sous-traitant désigné par le Client, et ensuite.
- détruire toutes les DCP et les fichiers manuels ou informatisés comportant les informations collectées dans un délai de deux (2) mois après la restitution, afin de permettre au Client de disposer du temps nécessaire pour vérifier que les Données restituées sont exploitables et lisibles, sauf disposition impérative contraire résultant du droit communautaire ou du droit d'un État membre de l'Union européenne applicable aux traitements objets des présentes.

Le Client pourra demander à ce que ce délai de deux (2) mois soit prolongé pour une nouvelle durée maximale de deux (2) mois, sous réserve de respecter un délai de prévenance de quinze (15) jours calendaires avant l'expiration du premier délai de deux (2) mois.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Sous-Traitant. Une fois détruites, le Sous-Traitant doit justifier par écrit de leur destruction au plus tard dans le délai d'un mois.

7. Audit

Le Sous-Traitant s'engage à se conformer sans délai aux demandes du Client ou des auditeurs qu'il aurait mandatés :

- D'accéder à ou d'inspecter (i) les locaux, (ii) les systèmes d'information, (iii) les registres ainsi que (iv) tous documents et informations, et
- D'interroger le personnel du Sous-Traitant, et ce afin de permettre au Client d'auditer et de vérifier que le Sous-Traitant et ses Sous-Traitants Ultérieurs respectent pleinement les dispositions des présentes.

Les frais de l'audit sont à la charge du Client. Par exception à ce qui précède, si l'audit révèle des manquements du Sous-Traitant ou de ses Sous-Traitants Ultérieurs, le Sous-Traitant rembourse au Client les frais de l'audit, sans préjudice de toute indemnisation qui pourrait être réclamée par le Client. Le Sous-Traitant s'assure que le contrat conclu avec tout Sous-Traitant Ultérieur permet au Client de procéder ou de faire procéder aux audits prévus au présent article, chez ce Sous-Traitant Ultérieur et ses propres sous-traitants.

8. Localisation et transferts des données

En cas de transfert de Données à caractère personnel vers un pays tiers, n'appartenant pas à l'Union européenne, ou vers une organisation internationale, le Sous-Traitant devra obtenir l'accord préalable écrit du Client. Si cet accord est donné, le Sous-Traitant s'engage à coopérer avec le Client afin d'assurer :

- le respect des procédures permettant de se conformer à la réglementation DCP, par exemple dans le cas où une autorisation de la part de l'autorité de contrôle compétente apparaîtrait nécessaire ;
- si besoin, la conclusion d'un ou plusieurs contrats permettant d'encadrer les flux transfrontières de DCP. Le Sous-Traitant s'engage en particulier, si nécessaire, à signer de tels contrats avec le Client et/ou à obtenir la conclusion de tels contrats par ses Sous-Traitants Ultérieurs. Pour ce faire, il est convenu entre les Parties que les clauses contractuelles types publiées par la Commission européenne seront utilisées pour encadrer les flux transfrontières de Données.

9. Responsabilité

Le Sous-Traitant indemnise pleinement le Client en cas de condamnation du Client résultant du non-respect par le Sous-Traitant de ses obligations au titre du présent Accord.

Appendice A :

DESCRIPTION DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Cet Appendice contient certaines informations relatives au Traitement des DCP, conformément à l'article 28.3 du RGPD.

Date de début des Traitements des DCP *La date de début des Traitements est la date du début d'exécution des prestations objet du contrat par le Client*	Cliquez ou appuyez ici pour entrer une date.
Finalité du Traitement *La finalité est le but à atteindre recherché par le client et justifiantleu choix de solution opéré par le client*	

Nature de traitement
(article 4 du RGPD)

Opérations de traitement (article 4 RGPD)	
La collecte	
L'enregistrement	
L'organisation	
La structuration	
La conservation/stockage	
L'adaptation/la modification	
L'extraction	
L'accès/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/la destruction	
Autres (à compléter) :	

Sous-Traitants

Autres : à compléter selon la nature du projet

Cliquez ou appuyez ici pour entrer du texte.

Catégorie de Destinataires des Données Personnelles (qui manipule, qui copie, qui visualise, qui réutilise les données)

Ex : personnes en charge de l'exécution de la prestation/personnes en charge du contrat/personnes gérant la facturation etc…

Cliquez ou appuyez ici pour entrer du texte.

Catégorie de Personnes Concernées

(Préciser et compléter au besoin les catégories de personnes concernées dont les données sont traitées.
Ex : clients et prospects, salariés, utilisateurs, etc…)

Catégories de personnes concernées	OUI/NON
Utilisateurs de la solution chez le client	
Utilisateurs de la solution chez le client du client ou son partenaire	
Salariés du client	
Autres (à compléter)	

Catégorie de données personnelles traitées *(Préciser et compléter au besoin les catégories de données personnelles traitées. Par exemple, données économiques et financières, caractéristiques personnelles, données culturelles, photos, etc.…)*	

Catégories de DCP traitées	OUI/NON
Données d'identification (civilité, nom, prénom, identifiant, matricule)	
Données de contact professionnel ou personnel (téléphone, adresse email)	
Données de localisation (adresse postale, position géographique)	
Données de connexion (identifiants, adresses IP, URL)	
Données de contenu (copies d'écran, commentaires)	
Autres (à compléter)	

Conservation des données (date de début et durée en mois)	Cliquez ou appuyez ici pour entrer du texte.
Coordonnées de l'interlocuteur du Fournisseur, et le cas échéant de son Délégué à la protection des données	Nom : Prénom : Fonction : Adresse mail : Téléphone :
Coordonnées du Délégué à la protection des données du Client	Fonction : DPO Adresse mail : dpo.healthcare@orisha.com