



CONDITIONS GÉNÉRALES DE VENTE ET DE SERVICES – SYKIO

Accord de traitement (version en date du 18/11/2025)

1. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Prestataire, en qualité de sous-traitant (le « **sous-traitant** ») s'engage à effectuer pour le compte du Client, en qualité de responsable du traitement (le « **responsable du traitement** ») les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre du Contrat, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, « *le règlement européen sur la protection des données* »).

2. Description du traitement faisant l'objet de la sous-traitance

La description du traitement réalisé par le sous-traitant pour le compte du responsable du traitement figure en [Annexe A](#).

3. Obligations du sous-traitant vis-à-vis du responsable du traitement

Le sous-traitant s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) du Contrat et telles qu'identifiées en Annexe A
- traiter les données conformément aux instructions documentées du responsable du traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable du traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
- 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
- sensibiliser le personnel à la nature particulièrement sensible des données de santé, conformément aux exigences réglementaires en matière de protection des données personnelles
- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut
- ne pas transférer de donnée à caractère personnel vers un pays situé en dehors de l'Union Européenne, ou de l'Espace Economique Européen ou ne bénéficiant pas d'une décision d'adéquation sans avoir mis en place au préalable de mesures techniques, juridiques et organisationnelles permettant de sécuriser les données

4. 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 du 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 du traitement dispose d'un délai maximum de trente (30) jours 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 du traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent accord pour le compte et selon les instructions du responsable du 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 du traitement de l'exécution par l'autre sous-traitant de ses obligations.

Le sous-traitant est autorisé à faire appel aux sous-traitants listés en [Annexe B](#) de la présente Annexe.

Les sous-traitants ultérieurs, hébergeurs de données de santé, sont exclusivement localisés dans l'Espace Economique Européen.

5. Droit d'information des personnes concernées

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

6. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit assister le responsable du traitement à s'acquiescer 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 y compris les directives post-mortem, 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, dès lors que les informations transmises par la personne lui permettent d'identifier le responsable du traitement, doit adresser ces demandes dès réception par courrier électronique au responsable du traitement.

Toute demande d'exercice de droits des personnes peut faire l'objet d'un devis si l'exécution de la demande entraîne des coûts inhabituels pour le sous-traitant.

7. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et par le moyen suivant : rgpd@arche-mc2.fr

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable du traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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 sous-traitant 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.

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

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

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

9. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues dans le plan d'Assurance Sécurité ;
- 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.

10. Sort des données

Au terme de la prestation de services relatifs au contrat et au traitement de ces données, le sous-traitant s'engage à (au choix des parties) détruire toutes les données à caractère personnel dans un délai maximum de 6 mois ou à renvoyer toutes les données à caractère personnel au client (ou au sous-traitant désigné par le client) en cas d'activation de la clause de réversibilité. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant.

Une fois détruites, si le client en fait la demande expresse, le sous-traitant fournira un justificatif de destruction.

11. Délégué à la protection des données

Le sous-traitant a désigné un délégué à la protection des données conformément à l'article 37 du règlement européen sur la protection des données dont les coordonnées figurent ci-dessous.

Délégué à la protection des données : rgpd@arche-mc2.fr

Le responsable de traitement s'engage à fournir au sous-traitant les coordonnées de son Délégué à la protection des données.

12. 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 du traitement comprenant :

- le nom et les coordonnées du responsable du 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 :
 - o des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - o des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais
 - o appropriés en cas d'incident physique ou technique ;
 - o une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

13. Documentation et audit

Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de 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. La réalisation d'audit sera aux seuls frais du responsable du traitement et limitée à un (1) sur la durée initiale du contrat et 1 par période de renouvellement. Un devis sera établi en fonction des éléments demandés lors de l'audit. Le prestataire s'engage à ne pas établir un devis dont le montant serait manifestement disproportionné ou excessif et qui aurait de ce fait un effet dissuasif.

Le responsable du traitement s'engage à notifier avec un préavis minimum de 30 jours ouvrés au sous-traitant tout audit, en lui communiquant notamment l'objet de la mission, la durée envisagée, le nom du ou des auditeur(s), le périmètre d'intervention, les livrables requis ainsi que les personnes habilitées pour cette mission. L'audit sera mené par le responsable du traitement ou un autre auditeur qu'il a mandaté, indépendamment, non concurrent du sous-traitant sur le domaine et soumis à un engagement de confidentialité.

Le sous-traitant pourra opposer un refus d'auditeur notamment pour préserver ses intérêts légitimes. Le sous-traitant fera ses meilleurs efforts pour trouver une solution avec le responsable du traitement et permettre la réalisation d'un audit dans des conditions acceptables.

En cas de refus, le sous-traitant devra notifier le responsable du traitement sous un délai de 30 jours ouvrés suivant la notification faite par le responsable du traitement.

L'audit pourra avoir lieu uniquement sur les contrats de services valides dont dispose le responsable du traitement et ne comporte pas d'accès à tous systèmes, informations, données non liées aux traitements effectués en vertu d'un contrat liant le responsable du traitement et le sous-traitant.

Aucun audit ne pourra être effectué en cas d'impayés ou de litige déclaré.

Le sous-traitant mettra en place les moyens raisonnables pour permettre à l'auditeur de mener à bien son audit. Les opérations d'audit et les demandes d'information devront être effectuées pendant les heures de travail du sous-traitant et ne devront pas perturber le bon fonctionnement des activités de ce dernier. L'auditeur, possédant les qualités professionnelles requises, doit s'engager préalablement par écrit à ne pas mettre en péril l'infrastructure existante.

Les Parties reconnaissent que tous rapports et informations obtenues dans le cadre de cet audit sont des informations confidentielles. Le responsable du traitement se porte garant du respect de la confidentialité par l'auditeur mandaté et s'engage à ne pas divulguer les résultats du rapport à d'autres parties que le sous-traitant et le responsable du traitement.

Un exemplaire du rapport d'audit sera remis gracieusement au sous-traitant. Les Parties examineront de bonne foi le rapport d'audit et identifieront, le cas échéant, les actions qui devront être engagées par l'une ou l'autre des Parties pour mettre en œuvre les décisions. Le sous-traitant ne pourra en aucune façon être tenue pour responsable ni aucune indemnité ne pourra être réclamée en cas de manquements de sa part.

Les actions à mettre en œuvre convenues entre les deux Parties devront être chiffrées et leur coût devra être raisonnable, sans aucune obligation pour le sous-traitant d'en supporter le coût. Le sous-traitant accepte que le contrat soit suspendu, sans indemnité, sans délai ni préavis à l'initiative du responsable du traitement en cas de constatation d'un manquement grave aux dispositions.

14. Obligations du responsable du traitement vis-à-vis du sous-traitant

Le responsable du traitement s'engage à :

- fournir au sous-traitant les données visées au II des présentes clauses lorsque celles-ci sont nécessaires à l'exécution du contrat et de la prestation ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;



- 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 ;

- superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

Annexe A –Description des traitements (à adapter en fonction de l'application et des vendues)

	PRESTATION DE MISE EN ŒUVRE DE LA SOLUTION ou PRESTATION PENDANT LA DUREE DU CONTRAT	MAINTENANCE	HEBERGEMENT
Finalité du traitement	Mise en œuvre de la solution, prestations d'assistance, de formation, réalisées pendant la durée du contrat.	La résolution d'incidents et d'anomalies logicielles ainsi que l'assistance à l'utilisation telles que prévu dans le contrat.	L'hébergement de la solution et des données.
Nature des opérations réalisées sur les données	▪ Reprise de données et test de reprise de données ▪ Paramétrage de la solution et création de requêtes ▪ Création de la base de données et mise en œuvre de sa sauvegarde ▪ Réalisation de la recette, ▪ Formation des utilisateurs ▪ Assistance fonctionnelle et technique	▪ Télémaintenance ▪ Analyse de fichier de logs et de base de données ▪ Installation de correctifs ▪ Recettes ▪ Paramétrage de la solution et création de requêtes ▪ Réalisation de sauvegarde de la base de données ▪ Assistance fonctionnelle et technique	<i>Hébergement Sous-traitant</i> ▪ Stockage ▪ Interfaçage ▪ Mise à disposition des données ▪ Sauvegardes et restaurations de données
Catégories des personnes concernées	Usagers/ bénéficiaires/ tiers présents dans la ou les applications concernées. Clients/prospects présents dans la ou les applications concernées Utilisateurs présents dans la ou les applications concernées et/ou en lien avec les prestations fournies Salariés/Intervenants présents dans la ou les applications concernées et/ou en lien avec les prestations fournies		
Typologie principale des données à caractère personnel traitées	- données d'identification (état civil, identité, images, etc.) - données liées à la vie personnelle (habitudes de vie, situation familiale, etc.) - données liées à vie professionnelle (CV, formation professionnelles, diplômes, etc.) - informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.) - données bancaires (n° compte, RIB, IBAN, n° CB, etc.) - données de connexion (adresse IP, identifiants dans des logs, etc.) - données de localisation (déplacements, données GPS, GSM, etc.) - numéro de sécurité sociale - données concernant la santé		



Annexe B – Sous-traitants ultérieurs

Nom du Sous-traitant ultérieur	Finalité	Localisation géographique du sous-traitant
ITINSELL CLOUD	Hébergement des données	France (La Ciotat) et (Marseille)
SIGMA INFORMATIQUE	Hébergement des données	France (La Chapelle sur Erdre et Carquefou)
ECRITEL	Hébergement des données	France (Clichy)
IMPRESSIONS MODERNES	Hébergement des données	France (Romans-sur-Isère)
SPIE	Hébergement des données	France (Montpellier)
BT BLUE	Hébergement des données	France (Châteaubourg et Nantes)
MICROSFT	Hébergement des données	France (Paris)
FOLIATEAM	Hébergement des données	France (Rennes)
CLOUDADVICE	Hébergement des données	France (Lyon et Limonest)

Fait à _____, le _____

Pour le Client

Pour le Prestataire