Conditions Générales d'Utilisation
et conformité RGPD

Je, soussigné(e) ……

Titulaire de la pharmacie ……

Forme sociale : ……

RCS de la pharmacie : ……
Localisée à l'adresse ……

Ayant le numéro de FINESS ……

Dans la suite du document, dénommé « le Client »

Accepte les conditions générales d'utilisation de la SAS OffiSanté,

Dont le siège social est situé au 83 rue de Rennes, 75 006 PARIS. Immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro B 537 770 273. Représentée par Monsieur Nicolas Buglio, agissant en qualité de président, dûment habilité aux fins des présentes.

Dans la suite du document, dénommée « le Prestataire »

Le Client et le Prestataire, étant individuellement dénommés « Partie » et ensemble « les Parties »,

Il a été préalablement exposé ce qui suit :

Préambule : exposé des motifs

La société OffiSanté offre des services d'analyse de gestion d'officines, par le traitement des données quotidiennes d'exploitation des pharmacies, sous forme de tableaux de bord facilitant la gestion de l'officine via les différentes offres dénommées O2, gratuite ou payantes, accessible en mode SaaS (Software as a Service) via Internet ou mobile.

La société Offisanté offre également le service « Vigirupture » et un observatoire des tensions sur les médicaments, créés à partir des informations sur les stocks disponibles au sein des pharmacies clientes.

La société Offisanté est également co-responsable, d'un entrepôt de données de santé conforme autorisé par la CNIL par décision du 27 Janvier 2023 n°2227515 (ci-après « l'EDS »)

Le Client souhaite utiliser les services d'Offisanté, dans le but de suivre l'activité quotidienne de son officine, d'en optimiser la gestion, et d'évaluer ses performances en termes de contribution à la maîtrise des dépenses de santé.

Le service Vigirupture est inclus dans les offres O2 gratuites ou payantes : il permet, grâce à la mise en commun des seules informations de stock des pharmacies clientes, sans aucune donnée personnelle, d'identifier les pharmacies dans lesquelles les médicaments souhaités sont disponibles. Le Client peut solliciter à tout moment la résiliation du service Vigirupture.

Les fonctionnalités des services O2 nécessitent que le Client autorise OffiSanté, en qualité de sous-traitant, à extraire quotidiennement les données pseudonymisées de santé de l'officine, (i) à les traiter pour élaborer les tableaux de bord de pilotage auxquels il va accéder, (ii) à les agréger pour calculer des échantillons de référence (iii) à extraire les données commerciales de stock aux fins de service Vigirupture.

Le Client reconnaît avoir reçu du Prestataire toutes les informations nécessaires lui permettant d'apprécier l'adéquation du Service à ses besoins et de prendre toutes les précautions utiles pour son utilisation.

Ceci exposé, il a été convenu ce qui suit :

Description du service O2 / O2 Mobile/O2 Premium

L'offre O2/Basic/Mobile/Premium, accessibles sur le Web et via l'Application (ci-après « le Service ») correspond à la production et la mise à disposition du Client de tableaux de bord de pilotage de l'officine, notamment : chiffres d'affaires ventilés par taux de TVA, détail des ventes par taux de TVA et par famille de produits, synthèse des ventes de l'équipe, fiche et analyse mensuelle vendeur, stocks invendus, rendez-vous, analyse de la clientèle, par tranche d'âge et sexe, typologie de prescripteurs les plus fréquent par catégorie de spécialité.

Objet

Au titre du présent contrat, le Prestataire consent au Client, qui accepte, un droit d'accès et d'usage du Service O2 souscrit, soit à titre gratuit pour la formule « OffiSanté Basic », soit à titre payant pour les formules « Offisanté Mobile » ou « Offisanté Premium », chacun de ces Services permettant d'accéder à des tableaux de bord et fonctionnalités respectivement

décrits à l'adresse www.offisanté.fr . Les offres O2 Mobile et Premium sont souscrites au tarif en vigueur mentionné à l'adresse ci-dessus.

Le Client bénéficiera également d'un accès au service Vigirupture disponible à l'adresse www.vigirupture.fr

A cet effet, le Client autorise expressément le Prestataire à :

- Collecter les données ci-après définies, à partir du Logiciel de Gestion de l'Officine (« LGO ») du Client
- Stocker les données de l'officine en vue de leur traitement par le Prestataire, en qualité de sous-traitant, auprès de l'hébergeur de données de santé OVH certifié (« HDS »).
- Traiter lesdites données, notamment aux fins de constituer des échantillons de référence, les tableaux de bord constituant le Service
- Exploiter les seules données commerciales de manière agrégée (i.e. celles objets du présent contrat et celles correspondant à d'autres officines tierces) et anonyme auprès de tout tiers, et notamment dans le cadre du service Vigirupture
- Sauf opposition du Client, transmettre les données pseudonymisées extraites du LGO à l'entrepôt de données de santé, dans les conditions de l'autorisation de la CNIL n°2227515.
- Commercialiser les seules données commerciales agrégées, à l'exclusion de toute donnée directement ou indirectement personnelle, auprès de tiers, notamment auprès des fournisseurs de l'officine.

Utilisation du service

Le Prestataire concède au Client un droit personnel d'accès et d'utilisation du Service et du service Vigirupture, à titre non-exclusif, non-cessible, non transférable pendant toute la durée du contrat.

Le Client s'engage à :

- ne pas reproduire, distribuer, accorder une sous-licence, un accès, louer, prêter ou transférer de quelque manière que ce soit le Service et/ou le service Vigirupture, en tout ou partie;

- à ne pas effectuer d'altération, ajout ou modification du Service et à ne pas décompiler, désassembler ou tenter de toute autre manière que ce soit de dériver le code source du Service ;

- à ne pas modifier, adapter, altérer, traduire ou créer des œuvres dérivées à partir du Service et/ou du service Vigirupture ;

- à ne pas modifier, altérer ou supprimer les mentions de droit d'auteur, les marques ou tout autre droit de propriété intellectuelle ou industrielle apposé dans ou sur le Service et/ou le service Vigirupture ;

- à ne pas introduire de virus, système automatisé quelconque ou tout autre élément de code, susceptible à perturber ou endommager le Service et/ou altérer, endommager ou effacer un contenu quelconque, et/ou récupérer ou enregistrer des informations sur le Service ;

- à ne pas perturber l'intégrité et/ou la performance du Service ou des données qui y sont contenues ;

- à ne pas effectuer d'extraction substantielle de la base de données Vigirupture, au titre de la protection accordée aux bases de données sui-generis.

Le Client s'interdit d'intervenir ou de faire intervenir un tiers sur le Service et/ou le service Vigirupture.

En cas de difficulté technique, un support client Offisanté est disponible dans la rubrique « nous contacter » du site www.offisanté.fr

Propriété intellectuelle

Le Prestataire garantit qu'il dispose de l'ensemble des droits de propriété intellectuelle permettant de fournir le Service.

Le Prestataire garantit le Client contre toute action en contrefaçon qui serait engagée à son encontre de la part d'un tiers revendiquant un droit de propriété intellectuelle portant sur le Service et le service Vigirupture. Dans ce cas, le Client s'engage à apporter toute assistance nécessaire en vue d'assurer la défense des intérêts de Offisanté. La garantie est exclue en cas de modification non autorisée du Service par le Client.

Les présentes Conditions Générales n'entrainent aucune cession de droit de propriété intellectuelle sur les éléments composant le Service et/ou le service Vigirupture.

Durée de la relation contractuelle

Le présent contrat est conclu pour une durée de 1 an, automatiquement reconductible, sauf résiliation par lettre recommandée avec accusé de réception présentée a minima 90 jours avant la date anniversaire.

Résiliation

En cas de manquement par l'une des Parties à ses obligations contractuelles essentielles, le présent contrat pourra être résilié de plein droit par l'autre Partie 15 jours après réception d'une mise en demeure adressée par lettre recommandée avec avis de réception restée sans effet en tout ou partie.

La résiliation anticipée ne libère par le Client de son engagement ferme et définitif de paiement pour la durée prévue contractuellement.

Dans le cadre du Service O2, et *sans préjudice des dispositions du règlement (UE) 2016/679, en cas de manquement du Prestataire*, en qualité de sous-traitant aux obligations qui lui incombent en vertu des clauses contractuelles de sous-traitance, *le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.*

Le Client, en tant que responsable du traitement, est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

1) *le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément* à la disposition ci-dessus, *et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;*
2) *le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679*;
3) *le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679*

Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément aux dispositions ci-dessous*, le responsable du traitement insiste pour que ses instructions soient suivies.*

À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

Pharmacie membre d'un groupement

Si Client est membre d'un groupement de pharmacies, le Client autorise Offisanté à transmettre pour le compte du Client un certain nombre d'informations agrégées au groupement, à l'exclusion de toutes données personnelles et conformément aux accords passés entre Offisanté et le groupement, tous deux agissant en qualité de mandataire du Client.

Dans ce cadre, le Client bénéficiera du service O2 Premium, selon l'accord-cadre conclu entre le Groupement avec Offisanté. Le présent contrat prévaut sur les dispositions de l'accord-

cadre, à l'exception du paiement du service O2 Premium, lequel est exclusivement régi par l'accord entre le Groupement et le Client.

Les données non personnelles transmises au Groupement dont l'officine est membre sont définies telles que suit, sauf opposition du Client :

- des données de ventes de produits agrégées, d'un récapitulatif des chiffres d'affaires des pharmacies du dernier mois clôturé ;
- le chiffre d'affaires cumulé et l'évolution du chiffre d'affaires à date, un récapitulatif des chiffres d'achats des pharmacies en achats cumulés et comparaison avec l'année précédente ;
- des graphiques permettant de positionner chaque officine et analyser le suivi de la politique commerciale du groupement pour optimiser les accords groupements ;
- un récapitulatif des chiffres d'achats des pharmacies ventilées par familles de produits pour assurer le suivi des accords commerciaux.

Autorisation de transmission des données personnelles et de traitements de ces données personnelles

Le Client autorise Offisanté à extraire quotidiennement les données décrites ci-après via un module d'extraction installé dans son logiciel de gestion d'officine, soit directement par l'extracteur d'Offisanté, soit via l'extracteur de l'éditeur du Logiciel de Gestion d'Officine du Client, selon les accords techniques existants entre lesdits éditeurs de LGO et Offisanté à cette fin. Afin de permettre l'établissement des tableaux de bords et les comparatifs souhaités de gestion de l'officine, une reprise d'historique de vingt-quatre (24) mois de données est effectuée, via une connexion sécurisée Internet.

Le Prestataire fournit le Service conformément à la réglementation applicable, notamment le règlement européen sur la protection des données personnelles n° 2016/679 et la loi Informatique et Libertés modifiée, tel que ci-après détaillé selon les traitements effectués.

<u>Qualité de responsable de traitement / de Sous-traitant / de co-traitant de données personnelles</u>

Traitement n°1 - Le Client agit en qualité de responsable de traitement dans le cadre de la fourniture du Service O2. Le Prestataire, agit en qualité de sous-traitant, conformément à l'article 28 du RGPD, aux fins d'exécution de l'offre de Service O2 souscrite par le Client. Dans ce cadre, le Prestataire exécute ses prestations conformément aux clauses type de sous-traitance édictées par la Commission Européenne en date du 21 Juin 2021 *reproduites en Italique* ci-dessous, afin que les parties puissent identifier les obligations en découlant.

Traitement n°2 - Le Prestataire agit en qualité de co-responsable de traitement des données extraites, dans le cadre de l'alimentation de l'entrepôt de données de santé Offisanté/Openhealth, selon autorisation de la CNIL n°2227515, sauf opposition des clients de l'officine au versement de leurs données extraites dans cet EDS. La finalité de ce traitement consiste dans le suivi des pathologies des patients et de l'observance, la création d'outils d'analyse en routine, et/ou de valorisation des prestations rendues par les pharmacies et aide à l'analyse d'information. Ces finalités sont fondées sur la base légale de

l'intérêt public et de l'intérêt légitime des co-responsables Offisanté et Openhealth.. Le Client et ses propres clients peuvent obtenir des précisions sur l'accord de co-traitance de l'EDS sur simple demande adressée à dpo@offisante.fr ou dpo@openhealth.com.

Traitement n°3 - Le Prestataire agit en qualité de responsable de traitement des données liées à l'identité du Client et de ses collaborateurs, dans le cadre de l'information précontractuelle, de la signature et de l'exécution du contrat de Service O2 et Vigirupture, de la facturation, de la gestion des accès, du support client, de la sécurité des Services et l'amélioration des Services, sur le fondement de l'exécution contractuelle et de l'intérêt légitime quant au support client, sécurité, réalisation de statistiques et amélioration des services.

Obligations dans le cadre des traitements de données personnelles

Traitement n°1 relatif au Service O2 : Option 1 des Clauses Contractuelles Type

Les présentes clauses contractuelles types (ci-après les «clauses») ont pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du 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.

Les responsables du traitement et les sous-traitants énumérés en entête du présent contrat ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679.

Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit dans le paragraphe « Données concernées par le Traitement n°1 » ci-dessous.

Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679. Elles ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679.

Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent. Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 figurent dans les clauses, ils s'entendent comme dans le règlement en question.
Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 respectivement. Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

En cas de contradiction entre les présentes clauses en italique et les autres dispositions du présent contrat *ou qui sont conclus ultérieurement, les présentes clauses prévaudront.*

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés ci-dessus dans la définition du Traitement n°1 et ci-après.

Le Prestataire, *sous-traitant, ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées*.

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies dans le présent accord concernant le Service O2, *sauf instruction complémentaire du responsable du traitement.*

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée ci-après.

Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées ci-après *pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.*

Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

Le traitement porte sur des données à caractère personnel concernant la santé d'une personne physique, (« données sensibles »), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires, notamment prévues ci-après.

Les parties doivent pouvoir démontrer la conformité avec les présentes clauses. Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.
Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence

d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable. Ce délai raisonnable est fixé à 15 jours, et notifié par email : dpo@offisanté.fr . Les parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

Le sous-traitant n'est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu'il effectue pour le compte du responsable du traitement en vertu des présentes clauses sans l'autorisation écrite spécifique préalable du responsable du traitement. Le sous-traitant soumet la demande d'autorisation spécifique au moins 15 jours *avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre au responsable du traitement de prendre une décision au sujet de l'autorisation. La liste des sous-traitants ultérieurs autorisés par le responsable du traitement figure* dans la liste des Destinataires ci-après, *que les parties tiennent à jour.*

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679.

À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.

Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel. Le contrat d'hébergement de données de santé OVH souscrit par le sous-traitant stipule que les données seront supprimées en tout état de cause dans ces cas.

Le sous-traitant informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.

Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer

leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations, le sous-traitant se conforme aux instructions du responsable du traitement. Outre cette obligation incombant au sous-traitant d'assister le responsable du traitement, le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

1) *L'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d'impact relative à la protection des données») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;*
2) *L'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;*
3) *L'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;*
4) *Les obligations prévues à l'article 32 du règlement (UE) 2016/679*

Les parties définissent ci-après les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise. Une analyse d'impact a été réalisée sur les traitements requis par les Services O2 et Vigirupture

<u>Violation de données dans le cadre du Service O2 :</u>

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles 34 et 35 du règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

<u>En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement :</u>

a) *Aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);*
b) *Aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins :*
    1) *La nature des 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 ;*
    2) *Les conséquences probables de la violation de données à caractère personnel ;*
    3) *Les mesures prises ou les mesures 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.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;

c) Aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

<u>En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant</u>, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

a) Une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;

b) Les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;

c) Ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679 :

- date de la violation et date de la découverte de la violation
- lieu de la violation et nature accidentelle ou illicite de la violation
- faits et personne morale à l'origine de la violation
- Fichiers, traitements et catégories de données concernées par la violation, notamment si elles concernent des données relevant de l'article 9 ou 10 du RGPD
- La notification projetée aux personnes concernées par la violation
- La justification de l'absence de notification aux personnes concernées

<u>Mesures de sécurité technique et organisationnelle</u>

Traitement n°1 (O2)

Les données personnelles transmises par le Client via son LGO sont pseudonymisées par le LGO, de manière irréversible au moyen d'un algorithme SHA2-256, tant en ce qui concerne les données relatives aux prescripteurs qu'en ce qui concerne le numéro patient. Ce traitement ne comporte pas de traitement du NIR.

Les données sont hébergées sur les serveurs certifiés Hébergement Données de Santé souscrit par le Prestataire. Les données sont cloisonnées pour chaque Client.

L'ensemble des mesures de sécurité techniques et organisationnelles sont documentées et disponibles sur demande du Client.

Traitement n°2 (EDS) :

Les données personnelles versées dans l'EDS font l'objet de mesures de sécurité conformes au référentiel édicté par la CNIL le 17 Novembre 2021, et figurent dans le dossier d'autorisation soumis à la CNIL.

Traitement n°3 (gestion contractuelle) :

Les données relatives aux Clients et leurs collaborateurs sont également stockées sur des serveurs certifiés Hébergement de Données de santé.
L'ensemble des mesures de sécurité techniques et organisationnelles sont documentées et disponibles sur demande du Client.

<u>Données concernées par les traitements :</u>

Traitement n°1 et 2 :

Le Client transmet uniquement à Offisanté les données suivantes, qui comprennent notamment des données de santé pseudonymisées :

- Patient :
    - Numéro aléatoire pseudonymisé
    - Zone Géographique agrégée
    - Sexe
    - Date de naissance (le jour de naissance est supprimé à réception)
    - Rang de naissance
    - Répartition géographique
    - Données d'incidence et de prévalence sur données INSEE
    - Valeur chiffrée du NIR-INS au sein du LGO (aux seules fins de versement dans l'EDS – traitement n°2)
    - Tickets de vente de produits de santé (y compris hors prescription)

- Pharmacie :
    - Nom de la pharmacie
    - Code CIP & FINESS
    - Version du logiciel
    - Opérateur de la vente

- Produits
    - Code EAN 13
    - Taux de TVA
    - Horodatage de la vente

    - Quantité et montant
    - Quantité en stock

- Prescripteur
    - Numéro aléatoire
    - Numéro RPPS et ADELI pseudonymisés par le LGO (uniquement aux fins de versement dans l'EDS – traitement n°2)
    - Zone géographique agrégée
    - Spécialité

Traitement n°3 :

Les données collectées par Offisanté sont : le nom et prénom du pharmacien, son adresse professionnelle, ses informations de contact (téléphone, mail), les logs de connexion à l'interface Offisanté (Internet et/ou mobile) ou Vigirupture

Durée de conservation des données

Traitement n°1 (O2) :
Les données sous-traitées sont conservées pendant 2 années et l'année en cours dans la base analytique.
A expiration de ce délai, les données sont supprimées ou anonymisées.

Traitement n°2 (EDS)

Les données pseudonymes individuelles de l'Observatoire sont conservées pendant 10 ans afin de permettre de réaliser des analyses correspondantes à des périodes représentatives et signifiantes au plan méthodologique.

Les tableaux de bord effectués au sein de l'EDS sont conservés deux ans.

Les analyses effectuées, le cas échéant, dans le cadre d'études, évaluations ou recherches en santé sont conservées pour la durée définie au sein de la formalité effectuée auprès de la CNIL.

Traitement n°3 (gestion commerciale) :
Les données sont conservées pour la durée de la relation contractuelle avec le pharmacien, augmentée de 10 années.

Destinataires des données personnelles

Destinataires internes :
- Collaborateurs du Prestataire, habilités en raison de leurs fonctions, pour le traitement n°1 (O2) et 3 (gestion commerciale)
- Collaborateurs d'Openhealth et Offisanté, co-responsables de traitement, dans les limites de l'autorisation délivrée par la CNIL pour le traitement n°2 (EDS)

Destinataires externes :

- L'hébergeur certifié données de santé OVH (en qualité de sous-traitant, pour les traitements n°1 et 3)
- Le prestataire de maintenance, en qualité de sous-traitant (pour le traitement n° 3)
- Les prestataires de messagerie (pour le traitement n°3)
- L'outil de Customer Relation Management, en qualité de sous-traitant (traitement n°3)
- L'expert-comptable (pour le traitement n°3)
- Les prestataires d'hébergement d'Openhealth, et le cas échéant, le prestataire d'hébergement OVH d'Offisanté pour le traitement n°2 (EDS), en qualité de sous-traitants.

Transfert des données personnelles

Les traitements n°1 et 2 ne comportent aucun transfert de données hors de France.

Traitement de données n°3 (gestion commerciale) :
Offisanté a paramétré la localisation des données en Europe pour les prestataires de messagerie, messagerie instantanée, newsletter et Customer Relation Manager établis hors de l'Union Européenne, auxquels le Prestataire recourt pour gérer la relation commerciale avec ses Clients dans le cadre du traitement n°3. Ces prestataires s'engagent, à titre de mesure de sécurité supplémentaire, à ne permettre l'accès aux données traitées que par des équipes basées au sein de l'Union Européenne. A défaut, Offisanté met en œuvre des moyens de cryptographie des données ainsi sous-traitées dont les clés ne sont pas détenues par le prestataire en question.

Exercice des droits

Traitement n°1 (Service O2) :

Droits du Client :

Sur demande écrite adressée au Prestataire, le Client peut obtenir la communication, la rectification ou la suppression des informations le concernant ou concernant ses collaborateurs, figurant dans les fichiers du Prestataire. Le Client peut également exercer un droit d'opposition pour des motifs légitimes et son droit à la portabilité. Le Client peut également transmettre ses instructions pour la gestion de ses données personnelles en cas de décès. Ces demandes peuvent s'accompagner d'un moyen de vérification de l'identité de la personne concernée lorsque cela est nécessaire.

Droits des clients de l'Officine et des prescripteurs dont les ordonnances ont été délivrées :

Les clients de l'officine et les prescripteurs dont les ordonnances ont été délivrées par l'officine peuvent également exercer leurs droits d'accès, de rectification, d'effacement, d'opposition et de limitation de leurs données ou d'instruction en cas de décès, auprès de l'officine ou du Prestataire à l'adresse suivante : contact@offisante.fr, ou par courrier 83, rue de Rennes, 75006 PARIS.
Le Client garantit Offisanté effectuer vis-à-vis des clients de l'officine l'information requise par l'article 13 du RGPD au titre du traitement de données du service O2 souscrit par le Client.

Pour mettre en œuvre la demande d'opposition et/ou d'effacement de ses clients ou des prescripteurs dont les ordonnances ont été délivrées dans la pharmacie dans le cadre du Service O2, le Client s'engage à ajouter un numéro à la facture du patient, selon une procédure disponible sur le site www.offisante.fr.
L'opposition sera alors prise en compte automatiquement par le Prestataire.

Traitement n°2 (EDS) :

Droits du Client :

Le Client peut obtenir la communication, la rectification ou la suppression (sous réserve de l'exécution du présent contrat) des informations le concernant, figurant dans l'EDS. Le Client peut également exercer un droit d'opposition pour des motifs légitimes, ou solliciter la limitation du traitement. Ces demandes peuvent s'accompagner d'un moyen de vérification de l'identité de la personne concernée lorsque cela est nécessaire.
La demande écrite doit être adressée au Prestataire ou à Openhealth, co-responsable de traitement, par mail adressé à dpo@openhealth.fr ou à l'adresse du siège d'Openhealth : OpenHealth Company, DPO, CP 130, 56038 Vannes Cedex.

Droits des clients de l'Officine et des prescripteurs dont les ordonnances ont été délivrées :

Les clients de l'Officine et les prescripteurs dont les ordonnances ont été délivrées par l'officine peuvent exprimer leur opposition au versement de leurs données pseudonymisées dans l'EDS au moment de la collecte par l'Officine, ou à tout moment ultérieurement. Dans ces cas, le Client doit ajouter le numéro suivant à la facture du patient, selon une procédure disponible sur le site www.offisante.fr.
L'opposition sera alors prise en compte automatiquement par le Prestataire et par Openhealth, co-traitants de l'EDS.

Traitement n°3 (gestion commerciale) :

Droits du Client :

Sur demande écrite adressée au Prestataire, le Client peut obtenir la communication, la rectification ou la suppression des informations le concernant, figurant dans les fichiers du Prestataire. Le Client peut également exercer son droit d'opposition pour des motifs légitimes, de limitation, et son droit à la portabilité. Le Client peut également transmettre ses instructions pour la gestion de ses données personnelles en cas de décès. Ces demandes peuvent s'accompagner d'un moyen de vérification de l'identité de la personne concernée lorsque cela est nécessaire.

En tout état de cause, et quel que soit le traitement concerné, pour toute information ou exercice de droits, le Client peut :

- Contacter Offisanté sur privacy@offisante.fr ou au 83, rue de Rennes – 75006 Paris.

- Contacter le délégué à la protection des données (DPO) d'Offisanté : dpo@offisanté.fr ou à l'adresse DPO Offisanté - 57, Avenue Franklin Delano Roosevelt– 75008 Paris.

- Contacter la CNIL sur https://www.cnil.fr/ ou à l'adresse 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

Violation de Données

En cas de violation de données dans le cadre d'un traitement dont le prestataire est responsable ou co-responsable, le Prestataire, ou Openhealth dans le cadre de l'Entrepôt de Données de Santé s'engage à notifier à la CNIL sans délai et au plus tard soixante-douze (72) heures après la découverte de la violation de données personnelles.

Devoir d'information des patients et des prescripteurs

Le Client devra informer les personnes concernées, ses clients, des traitements effectués (Traitements n°1 et n°2). La personne concernée pourra signifier son opposition aux traitements à tout moment.

Dans le cadre du service O2, le Client, en qualité de responsable de traitement, informe ses clients selon sa politique de confidentialité propre. Le cas échéant, il peut utiliser le module d'information prévu par Offisanté, sous-traitant, afin de faciliter le respect du principe de transparence par les officines. Ce module d'information sur le service O2 est disponible ici : https://o2.offisante.fr/img/logos/Notice%20information%20patient.pdf

Dans le cadre de l'EDS, la mention d'information que le Client s'engage à transmettre et/ou afficher visiblement aux clients de l'officine est disponible à l'adresse suivante : https://o2.offisante.fr/img/logos/Notice_information_patient_EDS.pdf

Dans le cadre de l'EDS, la mention que le client s'engage à transmettre et/ou afficher visiblement aux prescripteurs dont les données sont collectées par l'Officine, est disponible à l'adresse suivante :
https://o2.offisante.fr/img/logos/Notice_information_prescripteurs_EDS.pdf

Maintenance

Le Prestataire se réserve le droit de modifier tout ou partie de l'Application, temporairement ou de manière définitive, sous réserve de ne pas entrainer de régression en termes de performance et de fonctionnalité.

Le Prestataire se réserve le droit d'interrompre exceptionnellement l'accès à l'Application pour des opérations de maintenance, après avoir informé le Client via l'Application et/ou le portail Web, sans indemnité.

Une prestation de support par différents canaux disponibles sur offisante.fr permettant de traiter les anomalies est disponible du lundi au vendredi inclus. Les signalements d'anomalie doivent être confirmés par email au Prestataire sans délai

Le Prestataire n'est pas responsable de la maintenance dans les cas suivants :

- refus ou impossibilité du Client de collaborer avec le Prestataire dans la résolution des anomalies et notamment de répondre aux questions et demandes de renseignement ;

- utilisation des services applicatifs de manière non conforme à leur destination ou à leur documentation ;

- modification non autorisée des solutions par le Client ou par un tiers ;

- manquement du Client à ses obligations au titre du Contrat ;

- implantation de tous progiciels, logiciels ou système d'exploitation non compatibles avec les services applicatifs ;

- utilisation de matériels incompatibles ;

- défaillance des réseaux de communication électronique ;

- acte volontaire de dégradation, malveillance, sabotage ;

-détérioration due à un cas de force majeure ou à une mauvaise utilisation des services applicatifs.

Le Prestataire s'engage à transmettre les documentations mises à jour des nouvelles versions des solutions.

Les corrections et évolutions des services applicatifs sont expressément soumises au présent contrat.

Responsabilité – Force majeure

Le Prestataire est uniquement tenu d'une obligation de moyens dans le cadre de l'accès et l'utilisation du service O2.
Il est notamment expressément entendu que les tableaux de bord mis en place par le Prestataire sont des outils de gestion statistiques, qui ne constituent en aucun cas un conseil
ou une incitation quant aux choix à faire ou décision à prendre pour gérer une officine pharmaceutique. En outre, et en cas de faute prouvée par le Client, le Prestataire ne sera tenu que de la réparation des conséquences pécuniaires des dommages directs et prévisibles du fait de l'utilisation de l'Application. En conséquence, le Prestataire ne pourra en aucune circonstance encourir de responsabilité au titre des pertes ou dommages indirects.

Il est expressément entendu que le Prestataire n'intervient aucunement dans l'une des prestations suivantes, pour lesquelles sa responsabilité ne saurait donc être engagée :

- Fourniture des réseaux de transmission et de services d'accès à internet ;
- Autorisations d'opérer de l'opérateur de télécommunication chez qui les infrastructures de réseau du Prestataire sont hébergées ;
- Gestion des données du Client au sein de son LGO.

Le Client reconnaît qu'il est seul responsable d'effectuer la sauvegarde des données du Client auquel il appartient de prendre toute mesure appropriée, et notamment des sauvegardes régulières, de façon à se prémunir contre toute perte ou détérioration de ses données avant tout opération d'extraction vers le serveur du Prestataire.

Enfin, il est entendu que le Client demeure seul et unique responsable des données extraites de son système. Le Prestataire s'engage à prendre en compte toutes les demandes de correction des données transmises et de mise à jour mais le Prestataire n'est pas en mesure d'en vérifier par lui-même l'absence d'erreur.

Le Prestataire ne pourra en aucun cas être tenu pour responsable de l'usage fait par le Client des informations figurant dans le Service, ou de l'inexactitude des données. L'attention du Client est attirée sur le fait que l'Application a pour finalité l'aide à la gestion, et ne constitue pas une solution comptable. En tout état de cause, la responsabilité du Prestataire ne saurait être mise en cause, pour tout fait générateur donné, plus de dix-huit (18) mois après la survenance dudit fait. Aucune des Parties ne pourra être tenue pour responsable d'un manquement quelconque à ses obligations dans le cadre du Contrat, si un tel manquement résulte d'un événement de force majeure ou de cas fortuit. La responsabilité du Prestataire ne pourra être retenue en cas d'inexécution de ses obligations du fait d'une décision gouvernementale, en ce compris tout retrait ou suspension d'autorisations quelles qu'elles soient, d'une grève totale ou partielle, interne ou externe à l'entreprise, d'un incendie, d'un dégât des eaux, d'une catastrophe naturelle, d'une interruption totale ou partielle ou d'un blocage des réseaux de télécommunications ou électrique, d'une interruption totale ou partielle du service dans le centre de données hébergeant les données.

La Partie constatant l'événement devra sans délai informer l'autre partie de son impossibilité à exécuter sa prestation. La suspension des obligations ou le retard durant la survenance de l'un des événements cités supra ne pourra en aucun cas être une cause de responsabilité pour non-exécution de l'obligation en cause, ni induire le versement de dommages et intérêts ou pénalités de retard.

Garanties

Chaque Partie déclare et garantit être juridique habilitée pour conclure le présent contrat.

Le Prestataire déclare et garantit :

- Qu'il est titulaire de l'ensemble des droits de propriété intellectuelle qui lui permettent de conclure le présent contrat et de permettre au Client d'utiliser le Service et l'Application ;
- Que le Service et l'Application ne contrefait aucun droit de propriété intellectuelle d'un tiers ;

Les seules garanties accordées par le Prestataire sont celles expressément prévues par le présent contrat, à l'exclusion de toute autre garantie.

Le Client garantit que les données qui sont traitées dans le cadre de l'utilisation du Service ont été collectées conformément à la réglementation applicable en matière de données personnelles, et conformément au code de la santé publique.

Non sollicitation de personnel

Chacune des Parties renonce à engager ou à faire travailler, directement ou par personne interposée, tout salarié de l'autre partie, sans accord exprès et préalable de cette dernière. Cette renonciation est valable pendant toute la durée du Contrat et pendant les 12 mois qui suivront sa cessation.

Dans le cas où l'une des Parties ne respecterait pas cette obligation, elle s'engage à dédommager l'autre Partie en lui versant immédiatement et sur simple demande, une somme forfaitaire égale à 24 fois la rémunération brute mensuelle du salarié au moment de son départ.

Confidentialité

Chacune des Parties s'oblige à (i) tenir confidentielles toutes les informations qu'elle recevra de l'autre Partie, et notamment à (ii) ne pas divulguer les informations confidentielles de l'autre Partie à un tiers quelconque, autre que des employés, agents ou d'un groupement dans le cas où le Client fait partie d'un Groupement ayant besoin de les connaître ; et (iii) n'utiliser les informations confidentielles de l'autre Partie qu'à l'effet d'exercer ses droits et de remplir ses obligations aux termes du Contrat.

Sont notamment considérées comme confidentielles, les Données mises à disposition du Client par le Prestataire.

Nonobstant ce qui précède, aucune des Parties n'aura d'obligation quelconque à l'égard d'informations qui (i) seraient tombées ou tomberaient dans le domaine public indépendamment d'une faute par la Partie les recevant, (ii) seraient développées à titre indépendant par la Partie les recevant, (iii) seraient connues de la Partie les recevant avant que l'autre Partie ne les lui divulgue, (iv) seraient légitimement reçues d'un tiers non soumis à une obligation de confidentialité, ou (v) devraient être divulguées en vertu de la loi ou sur ordre d'un tribunal (auquel cas elles ne devront être divulguées que dans la mesure requise et après en avoir prévenu par écrit la Partie les ayant fournies).

Les obligations des Parties à l'égard des informations confidentielles demeureront en vigueur pendant toute la durée du Contrat et aussi longtemps, après son terme, que les informations concernées demeureront confidentielles pour la Partie les divulguant et, en toute hypothèse, pendant une période de deux ans après le terme du Contrat.

Chacune des Parties devra restituer toutes les copies des documents et supports contenant des informations confidentielles de l'autre Partie, dès la fin du Contrat, quelle qu'en soit la cause.

Les Parties s'engagent par ailleurs à faire respecter ces dispositions par leur personnel, et par tout préposé ou tiers qui pourrait intervenir à quelque titre que ce soit dans le cadre du Contrat.

Indépendance juridique réciproque

Les parties déclarent et reconnaissent qu'elles sont et demeureront, pendant toute la durée du présent contrat, des partenaires et professionnels indépendants, assurant chacune en ce

qui la concerne les risques de leur propre activité. Les parties déclarent expressément qu'elles ne sont pas liées entre elles par un lien quelconque de subordination.

Assurances

Le Prestataire déclare être assuré pour sa responsabilité civile professionnelle auprès d'une compagnie notoirement solvable.

Droit applicable et résolution des litiges

Le Contrat est soumis au droit français, à l'exclusion de toute autre législation.

En cas d'apparition d'un litige relatif à l'application du présent accord, les Parties s'engagent à se rapprocher pour régler celui-ci dans les meilleurs délais. Dans l'hypothèse où les Parties ne parviennent pas à trouver une entente dans un délai d'un mois, elles procèdent d'un commun accord, à la désignation d'un médiateur.

A défaut d'accord amiable non susceptible de recours, tout différend sera soumis au tribunal compétent du ressort de la Cour d'Appel de Paris.