Contrat de sous-traitance (article 28 du RGPD)

Conclu en application de l'article 28 du règlement (UE) 2016/679 du 27 avril 2016 (ci-après le « RGPD »)

Version 1.1 (bêta privée) — en vigueur à compter du 5 novembre 2026

Entre les soussignés

Le Praticien, professionnel de santé inscrit au Répertoire partagé des professionnels intervenant dans le système de santé (RPPS), titulaire d'un Compte sur le service TISSIO, agissant en qualité de responsable du traitement (ci-après le « Praticien ») ;

Et la société TISSIO, société par actions simplifiée au capital de 1 000 euros, dont le siège social est situé 8 Traverse Perier, 13008 Marseille, immatriculée au registre du commerce et des sociétés de Marseille sous le numéro 130 079 783, représentée par son Président, agissant en qualité de sous-traitant (ci-après « TISSIO »).

Le Praticien et TISSIO sont ci-après désignés ensemble les « Parties ».

Les termes employés avec une majuscule et non définis au présent contrat ont la signification qui leur est donnée par les conditions générales d'utilisation du Service (ci-après les « CGU »).

Article 1 — Objet et qualité des Parties

1.1. Le présent contrat a pour objet de définir les conditions dans lesquelles TISSIO traite, pour le compte du Praticien, les données à caractère personnel relatives à ses Patients dans le cadre de l'utilisation du Service.

1.2. Le présent contrat s'applique aux Fiches patients, aux Documents transmis et reçus, aux messages et informations qui les accompagnent, ainsi qu'au Journal des accès tant qu'il permet d'identifier un Patient. Pour ces données, le Praticien détermine les finalités et les moyens essentiels du traitement ; TISSIO agit exclusivement pour son compte et sur ses instructions.

1.3. Le présent contrat ne s'applique pas aux données relatives au Praticien lui-même, telles que les données de son Compte, de la vérification de son identité, de ses Clés de l'ordinateur, de son abonnement ou de ses échanges avec l'assistance, pour lesquelles TISSIO a la qualité de responsable du traitement et qui sont régies par la politique de confidentialité.

1.4. La société Clever Cloud, titulaire d'un certificat de conformité pour l'hébergement de données de santé, intervient en qualité de sous-traitant ultérieur, dans les conditions de l'article 8 et de l'Annexe 3.

Article 2 — Conclusion du contrat et documents contractuels

2.1. Le présent contrat est accepté par le Praticien lors de sa première connexion au Service, au moyen d'une case à cocher, après son identification par Pro Santé Connect ou, pour le Compte ouvert dans les conditions de l'article 4.7 des CGU, après sa connexion au moyen du lien de connexion ou de la Clé de l'ordinateur, conjointement avec les CGU. Le Praticien titulaire d'un Compte en attente ne peut accéder à aucune donnée relative aux Patients avant la validation de son identité. TISSIO enregistre la version acceptée, la date et l'heure de l'acceptation ainsi que l'identité du Praticien ; cet enregistrement ne peut être ni modifié ni effacé. Toute nouvelle version du présent contrat doit être acceptée dans les mêmes conditions avant tout nouvel accès aux données, sous réserve de l'accès limité au téléchargement des Documents reçus prévu à l'article 22.1 des CGU, pendant lequel la version précédemment acceptée continue de s'appliquer.

2.2. Le présent contrat s'applique à tout Praticien titulaire d'un Compte, qu'il soit abonné ou non. Le Praticien qui se borne à recevoir des Documents a la qualité de responsable du traitement des données qu'ils contiennent tant qu'ils sont conservés par le Service.

2.3. En cas de contradiction, les documents contractuels prévalent dans l'ordre suivant : les clauses contractuelles types figurant en Annexe 4 ; le présent contrat et ses Annexes 1 à 3 ; les CGU.

Article 3 — Description du traitement

La nature et la finalité du traitement, les catégories de données et de personnes concernées, les durées de conservation et le lieu du traitement sont décrits à l'Annexe 1.

Article 4 — Clauses contractuelles types

4.1. Les Parties adoptent les clauses contractuelles types entre responsables du traitement et sous-traitants figurant à l'annexe de la décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021, dont le texte figure en Annexe 4 et prévaut sur toute stipulation contraire.

4.2. Pour leur application :

- l'annexe I des clauses (liste des parties) correspond à l'en-tête du présent contrat ; l'annexe II (description du traitement) à l'Annexe 1 ; l'annexe III (mesures techniques et organisationnelles) à l'Annexe 2 ; l'annexe IV (liste des sous-traitants ultérieurs) à l'Annexe 3 ;
- en matière de sous-traitance ultérieure (clause 7.7), l'option 2, relative à l'autorisation écrite générale, est retenue, dans les conditions de l'article 8 ;
- les violations de données (clause 9) sont régies par l'article 9 du présent contrat ;
- la clause d'amarrage (clause 5, facultative) n'est pas retenue.

Article 5 — Instructions du Praticien

5.1. Le Praticien donne ses instructions au moyen des fonctionnalités du Service, notamment en créant une Fiche patient, en sélectionnant un Patient, un Destinataire et un Document, en transmettant, consultant, téléchargeant ou retirant un Document, ou en supprimant son Compte. Les CGU et le présent contrat constituent les instructions documentées du Praticien au sens de l'article 28.3, a) du RGPD.

5.2. Toute autre instruction est adressée par écrit à l'adresse contact@tissio.fr. TISSIO informe immédiatement le Praticien si, selon elle, une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union européenne ou du droit français relatives à la protection des données.

5.3. TISSIO ne traite les données que sur instruction documentée du Praticien, sauf si elle y est tenue par le droit de l'Union européenne ou par le droit français ; elle en informe alors le Praticien préalablement au traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

5.4. Le Praticien donne instruction à TISSIO de produire, à partir des seules métadonnées de fonctionnement du Service, des statistiques agrégées et anonymisées, telles que le nombre d'envois, leur volume ou leurs délais d'ouverture, à l'exclusion de toute donnée relative à l'identité d'un Patient et de tout contenu de Document. Ces statistiques ont pour seules finalités le pilotage, la sécurité et l'amélioration du Service, ainsi que, avec l'accord du Praticien, la restitution d'indicateurs d'usage aux structures d'exercice coordonné auxquelles il adhère.

5.5. Le Praticien peut permettre aux personnes placées sous son autorité et tenues au secret professionnel, notamment son secrétariat et ses assistants, d'utiliser le Service pour son compte, dans une session qu'il a lui-même ouverte, dans les conditions de l'article 5.8 des CGU. Ces personnes agissent sur instruction du Praticien, au sens de l'article 29 du RGPD : les opérations qu'elles réalisent au moyen des fonctionnalités du Service constituent des instructions documentées du Praticien au sens de l'article 5.1 et sont inscrites au Journal des accès sous son identité. Il appartient au Praticien, en sa qualité de responsable du traitement, de déterminer les personnes qu'il autorise, de veiller à leur obligation de confidentialité et de les informer des règles d'utilisation du Service. TISSIO n'attribue à ces personnes aucun Compte ni aucun moyen d'identification et ne traite aucune donnée les concernant.

5.6. Les instructions du Praticien s'inscrivent dans l'usage raisonnable défini à l'article 14 bis des CGU. Une limitation temporaire décidée par TISSIO en application de cet article ne constitue pas un refus d'exécuter une instruction au sens de l'article 5.2 ; elle n'affecte ni la sécurité, ni la confidentialité, ni les durées de conservation des données relatives aux Patients, qui demeurent régies par le présent contrat.

Article 6 — Obligations de TISSIO

Sans préjudice des clauses contractuelles types, TISSIO s'engage à :

1. faire héberger les données relatives aux Patients exclusivement par un hébergeur titulaire d'un certificat de conformité pour l'hébergement de données de santé, sur le territoire français, sans aucun transfert en dehors de l'Union européenne ;
2. ne pas accéder au contenu des Documents. Le Service ne met à la disposition du personnel de TISSIO aucun outil permettant de consulter un Document. Un fichier n'est déchiffré par le Service qu'aux fins de sa remise à son Expéditeur ou à son Destinataire, et de la vérification de son intégrité lors de l'établissement d'un Accusé ;
3. réserver l'accès aux environnements de production aux seules personnes habilitées, nominativement désignées par TISSIO, et journaliser ces accès ;
4. soumettre toute personne placée sous son autorité ayant accès aux données à une obligation de confidentialité équivalente au secret professionnel prévu à l'article L. 1110-4 du Code de la santé publique, dont la violation est réprimée par l'article 226-13 du Code pénal ;
5. ne pas traiter les données relatives aux Patients pour ses propres finalités, notamment commerciales ou publicitaires, ni les céder, sous réserve des statistiques anonymisées mentionnées à l'article 5.4 ;
6. ne procéder, par quelque moyen que ce soit, y compris automatisé, à aucune lecture, analyse, synthèse ou classification du contenu des Documents ;
7. ne faire figurer aucune donnée relative à un Patient dans les courriers électroniques adressés par le Service, ni dans les adresses des pages du Service, ni dans ses journaux techniques ;
8. tenir un registre des activités de traitement effectuées pour le compte du Praticien, conformément à l'article 30.2 du RGPD.

Article 7 — Sécurité

TISSIO met en œuvre les mesures techniques et organisationnelles décrites à l'Annexe 2, conformément à l'article 32 du RGPD. Elle peut les faire évoluer, à la condition de ne pas réduire le niveau de sécurité qu'elles garantissent.

Article 8 — Sous-traitants ultérieurs

8.1. Le Praticien autorise de manière générale TISSIO à recourir aux sous-traitants ultérieurs mentionnés à l'Annexe 3.

8.2. TISSIO informe le Praticien par courrier électronique, au moins trente (30) jours à l'avance, de tout projet d'ajout ou de remplacement d'un sous-traitant ultérieur auquel elle recourt directement, y compris pour une fonction déjà mentionnée à l'Annexe 3. Le Praticien peut s'y opposer par écrit pendant ce délai. À défaut d'accord entre les Parties, le Praticien peut résilier le présent contrat et son abonnement sans frais avant l'entrée en vigueur du changement.

8.3. Le délai de trente (30) jours prévu à l'article 8.2 ne s'applique pas aux sous-traitants auxquels la société Clever Cloud recourt elle-même. Pour ceux-ci, TISSIO transmet au Praticien, sans délai dès qu'elle la reçoit de la société Clever Cloud, toute information relative à leur ajout ou à leur remplacement.

8.4. TISSIO impose à chaque sous-traitant ultérieur, par contrat, des obligations de protection des données au moins équivalentes à celles du présent contrat. Elle demeure pleinement responsable envers le Praticien de l'exécution de leurs obligations par ses sous-traitants ultérieurs.

Article 9 — Violations de données

9.1. TISSIO notifie au Praticien toute violation de données à caractère personnel le concernant dans les meilleurs délais, et au plus tard vingt-quatre (24) heures après en avoir pris connaissance.

9.2. La notification comporte, dans la mesure où ils sont disponibles, les éléments mentionnés à l'article 33.3 du RGPD. Les éléments qui ne sont pas disponibles lors de la notification sont communiqués dès qu'ils le deviennent.

9.3. TISSIO assiste le Praticien dans la notification de la violation à la Commission nationale de l'informatique et des libertés (CNIL) et, le cas échéant, dans la communication de la violation aux Patients concernés. Elle lui communique à cette fin la liste de ses Patients concernés, dans la mesure où le Journal des accès permet de les identifier, ainsi qu'un modèle de notification.

9.4. Le Praticien peut, par instruction écrite, donner mandat à TISSIO de notifier en son nom à la CNIL une violation de données le concernant. Le Praticien demeure responsable de cette notification.

Article 10 — Assistance au Praticien

TISSIO assiste le Praticien dans le respect de ses obligations, en tenant compte de la nature du traitement et des informations dont elle dispose :

1. information des Patients : TISSIO met à sa disposition des modèles de textes d'information ;
2. analyse d'impact relative à la protection des données : TISSIO met à sa disposition une analyse d'impact type relative au Service, ainsi que toute information nécessaire à son adaptation ;
3. demandes d'exercice de droits : le Praticien y répond lui-même. Le Service lui permet, tant qu'un Document est conservé, de connaître les personnes qui l'ont transmis, consulté ou téléchargé, ainsi que les dates de ces opérations ; de rectifier ou supprimer une Fiche patient ; et de retirer un Document qu'il a transmis. TISSIO l'assiste pour le surplus ;
4. démonstration de la conformité : TISSIO communique au Praticien, sur demande, toute information nécessaire pour démontrer le respect des obligations prévues au présent contrat.

Article 11 — Audits

11.1. TISSIO met à la disposition du Praticien, sur demande, la documentation relative à la sécurité du Service et les rapports d'audit dont elle dispose.

11.2. Le Praticien peut faire procéder, à ses frais et au plus une fois par année civile sauf en cas de violation de données, à un audit par un auditeur indépendant tenu au secret professionnel, moyennant un préavis de trente (30) jours. L'audit est conduit dans des conditions qui préservent la sécurité du Service et la confidentialité des données des autres Utilisateurs.

11.3. Le Praticien ne dispose d'aucun droit d'audit direct à l'égard de la société Clever Cloud. Un audit portant sur l'hébergement ne peut être conduit que par l'intermédiaire de TISSIO, dans les conditions du contrat d'hébergement de données de santé conclu entre TISSIO et la société Clever Cloud (article 5.4.1) : au plus un audit par période de douze (12) mois ouvert à TISSIO, sauf incident de sécurité affectant les données relatives aux Patients, moyennant un préavis de trente (30) jours et la souscription préalable d'un engagement de confidentialité. Le Praticien peut y être associé en qualité de mandataire de TISSIO, dans les mêmes conditions.

11.4. Pour ce qui concerne l'hébergement, TISSIO communique en outre au Praticien les éléments que la société Clever Cloud met à la disposition de ses clients, notamment son certificat de conformité et la synthèse de ses audits.

Article 12 — Durée et fin du contrat

12.1. Le présent contrat est conclu pour la durée d'existence du Compte du Praticien.

12.2. À la suppression du Compte, dans les conditions de l'article 18 des CGU, les données sont traitées comme suit :

- les Fiches patients qui ne sont rattachées à aucun Document en cours de transmission sont immédiatement effacées ; les autres le sont lors de la purge consécutive à l'expiration du dernier Document qui leur est rattaché ;
- les Documents reçus cessent immédiatement d'être accessibles et sont effacés lors de la purge suivante ;
- les Documents transmis demeurent accessibles à leur Destinataire jusqu'à leur expiration, puis sont effacés ;

- seule subsiste la Trace de transmission, qui ne comporte aucune donnée relative aux Patients, pour la durée prévue à l'article 12.3 des CGU.

12.3. Au choix du Praticien, les données relatives à ses Patients lui sont restituées ou supprimées. La restitution s'opère par le téléchargement, par le Praticien, des Documents encore accessibles avant la suppression de son Compte. À défaut de téléchargement, les données sont supprimées dans les conditions de l'article 12.2. TISSIO ne conserve aucune archive des Documents.

12.4. Les données supprimées peuvent subsister pendant une durée maximale de sept (7) jours dans les sauvegardes de la base de données réalisées par l'hébergeur. Les fichiers des Documents ne font l'objet d'aucune sauvegarde.

12.5. TISSIO confirme par écrit au Praticien, à sa demande, la suppression de ses données.

12.6. En cas de cessation définitive du Service, TISSIO en informe le Praticien au moins quatre-vingt-dix (90) jours à l'avance. Les Documents en cours de transmission demeurent accessibles jusqu'à leur expiration, après quoi l'ensemble des données relatives aux Patients est supprimé.

12.7. En cas de fin du contrat d'hébergement de données de santé conclu entre TISSIO et la société Clever Cloud, notamment en cas de changement d'hébergeur ou de perte par la société Clever Cloud de sa certification, l'hébergeur restitue à TISSIO la totalité des données relatives aux Patients (13° du I de l'article R. 1111-11 du Code de la santé publique) et ne les détruit qu'après l'accord formel du responsable du traitement, sans en garder de copie (14° du même I). TISSIO informe le Praticien sans délai de la fin de ce contrat et lui demande son accord formel avant de transmettre à l'hébergeur toute instruction de destruction. Le Praticien dispose de huit (8) jours ouvrés pour récupérer ses Documents encore accessibles et donner son accord, dans le Service ou par courrier électronique. À défaut de réponse après une relance, son accord est réputé donné, les Documents n'étant conservés que pour la durée de leur transit.

Article 13 — Responsabilité

La responsabilité des Parties est régie par l'article 16 des CGU, sans préjudice des dispositions impératives des articles 82 et 83 du RGPD.

Article 14 — Droit applicable et règlement des différends

Le présent contrat est régi par le droit français. L'article 26 des CGU s'applique aux différends relatifs à sa formation, à son interprétation ou à son exécution.

Annexe 1 — Description du traitement

Responsable du traitement : le Praticien, identifié par son numéro RPPS.

Sous-traitant : TISSIO SAS, 8 Traverse Perier, 13008 Marseille — contact@tissio.fr.

Finalité : permettre au Praticien de transmettre et de recevoir des documents relatifs à ses Patients, échangés avec d'autres professionnels de santé participant à leur prise en charge ; de suivre la réception et l'ouverture de ces documents ; de rattacher chaque document au Patient concerné.

Nature des opérations : collecte, enregistrement, chiffrement, conservation temporaire, transmission, consultation, horodatage, vérification d'intégrité, effacement.

Personnes concernées : les Patients du Praticien ; les professionnels de santé expéditeurs ou destinataires des Documents.

Personnes agissant pour le compte du Praticien : les personnes placées sous son autorité qui utilisent le Service dans une session qu'il a ouverte (article 5.5) ; leurs opérations sont inscrites sous l'identité du Praticien, et aucune donnée les concernant n'est traitée.

Catégories de données :

- identité du Patient : nom, prénom, date de naissance et, à titre facultatif, NIR, chiffré, affiché sous une forme partiellement masquée au seul Praticien qui l'a saisi et jamais communiqué au Destinataire ;
- Documents : fichiers aux formats PDF, JPEG, PNG ou DICOM et, pour les empreintes numériques tridimensionnelles, aux formats STL, PLY, OBJ ou ZIP, dans la limite de huit (8) fichiers et de cinquante (50) mégaoctets (52 428 800 octets) par envoi, y compris pour les empreintes numériques tridimensionnelles, ainsi que le nom d'origine de chaque fichier ;
- informations relatives à l'envoi : Expéditeur, Destinataire, type de Document, dates et heures de l'envoi, de la réception et de l'ouverture, date d'expiration, empreinte numérique du fichier, message et motif, mention de priorité, attestation souscrite et sa version ;
- Journal des accès : pour chaque Document, l'auteur et la date de chaque transmission, consultation, téléchargement, établissement d'Accusé, retrait et tentative d'accès refusée ;
- indicateur de consultation : le fait qu'un Destinataire a sélectionné un Document dans sa liste, visible de lui seul.

Catégories particulières de données : données concernant la santé au sens de l'article 9 du RGPD ; NIR. Les mesures de sécurité applicables sont décrites à l'Annexe 2.

Durées de conservation :

- Documents, messages et informations relatives à l'envoi : quatre-vingt-dix (90) jours au plus à compter de l'envoi ; l'accès est refusé dès l'expiration, et le fichier puis les informations relatives à l'envoi sont effacés lors de la purge de la nuit suivante, sous réserve de la Trace de transmission ;
- Journal des accès : rattaché au Document tant que celui-ci est conservé ; à sa suppression, dissocié de toute donnée relative au Patient, pour ne subsister que sous la forme de la Trace de transmission, conservée cinq (5) ans à compter de l'envoi ;
- Fiches patients : jusqu'à leur suppression par le Praticien, et au plus tard trois (3) ans après le dernier Document qui leur a été rattaché, ou jusqu'à la suppression du Compte ;
- indicateur de consultation : effacé avec le Document ;
- sauvegardes de la base de données : sept (7) jours glissants ;
- fichiers des Documents : aucune sauvegarde ni aucun versionnage.

Lieu du traitement : en France, dans les centres de données utilisés par la société Clever Cloud, dans le périmètre couvert par son certificat de conformité pour l'hébergement de données de santé. Aucun transfert en dehors de l'Union européenne.

Fréquence : continue, pendant toute la durée d'utilisation du Service.

Annexe 2 — Mesures techniques et organisationnelles de sécurité

Identification et contrôle des accès

- identification des Utilisateurs en priorité au moyen de Pro Santé Connect (carte CPS ou application e-CPS), l'identité étant rattachée à l'identifiant délivré par Pro Santé Connect ;
- à défaut de Pro Santé Connect, ouverture du Compte après vérification de l'identité par TISSIO (article 4.7 des CGU) : contrôle immédiat du numéro RPPS, de la profession et du nom dans l'Annuaire Santé, puis comparaison, par un fondateur habilité, de la photographie d'une pièce d'identité avec la fiche de l'Annuaire Santé ; photographie chiffrée, conservée dans un espace de stockage distinct de celui des Documents et effacée dès la décision et au plus tard sept (7) jours après son dépôt ; tant que l'identité n'a pas été validée, aucun accès aux Documents ni aux Fiches patients, ce refus étant appliqué par les règles d'accès de la base de données elle-même ;
- connexion quotidienne possible au moyen de la Clé de l'ordinateur (standards WebAuthn et FIDO2) : vérification de l'utilisateur par l'appareil exigée à chaque utilisation (empreinte, visage ou code), conservation de la seule partie publique de la clé, contrôle à chaque connexion du défi, de l'origine, de la signature et, lorsque l'appareil en tient un, d'un compteur d'utilisations strictement croissant, validité de trois (3) ans au plus,

retrait par l'Utilisateur et révocation par TISSIO, information de l'Utilisateur par courrier électronique à chaque création d'une clé ; aucun mot de passe ;
- vérification de l'inscription au RPPS et de la profession au moyen de l'Annuaire Santé, lors de chaque connexion, quel qu'en soit le moyen, puis quotidiennement ;
- sessions ouvertes au moyen de Pro Santé Connect d'une durée maximale de sept (7) jours, et sessions ouvertes au moyen de la Clé de l'ordinateur ou d'un lien de connexion d'une durée maximale de quatre (4) heures, sans prolongation, toutes verrouillées après une (1) heure sans activité ;
- aucun compte ni aucun moyen d'identification attribué aux personnes placées sous l'autorité du Praticien, qui n'opèrent que dans une session ouverte par celui-ci ;
- cloisonnement des données assuré par la base de données elle-même, au moyen de règles d'accès appliquées à chaque ligne de chaque table : chaque Utilisateur n'accède qu'aux Documents qu'il a transmis ou reçus et à ses propres Fiches patients ; contrôle de ce cloisonnement par des tests automatisés ;
- absence de tout accès direct à la base de données et au service de stockage, qui ne répondent qu'au serveur intermédiaire de TISSIO, protégé par un secret ;
- limitation du nombre de requêtes ;
- inscription au Journal des accès de toute tentative d'accès refusée.

Chiffrement

- chiffrement de l'ensemble des communications au moyen du protocole HTTPS ;
- chiffrement de chaque fichier par l'application, selon l'algorithme AES-256-GCM, avant son dépôt dans le service de stockage, la clé étant conservée hors de la base de données ;
- chiffrement du NIR par l'application, selon le même algorithme ;
- chiffrement au repos des disques de la base de données.

Intégrité et traçabilité

- Journal des accès en ajout seul : la base de données refuse toute modification ou suppression d'une inscription, sous réserve de leur dissociation lors de la purge ;
- empreinte numérique de chaque fichier selon l'algorithme SHA-256, vérifiée lors de chaque ouverture ;
- absence de toute donnée relative à un Patient dans les courriers électroniques et dans les adresses des pages, contrôlée par des tests automatisés ;
- refus, par la base de données, de tout champ non prévu dans la table des Fiches patients.

Conservation et effacement

- purge automatique quotidienne des Documents expirés, le fichier étant effacé avant les informations relatives à l'envoi, avec alerte en cas d'échec ;
- stockage des fichiers sans versionnage ni sauvegarde.

Disponibilité

- hébergement par la société Clever Cloud, titulaire d'un certificat de conformité pour l'hébergement de données de santé (certificat n° FR094504, activités 1 à 6) et titulaire d'une certification ISO/IEC 27001 ;
- sauvegarde quotidienne de la base de données, conservée sept (7) jours dans le périmètre couvert par ce certificat ;
- test de restauration réalisé au moins une fois par trimestre et après chaque évolution importante de la base de données ;
- surveillance permanente de la disponibilité du Service.

Organisation

- absence de toute donnée réelle sur les postes de travail, les développements et les tests étant réalisés sur des données fictives ;

- conservation des secrets de production, notamment les clés de chiffrement, les clés d'accès à la base de données et au service de stockage et les secrets de session, exclusivement dans l'environnement de l'hébergeur ; seuls les secrets qui permettent de déclencher les tâches planifiées (purge, contrôle quotidien de l'inscription au RPPS, rappels) et d'envoyer les alertes par courrier électronique sont en outre conservés, sous forme chiffrée, dans le service d'intégration continue de la société GitHub et dans l'outil de surveillance de TISSIO ; ils ne donnent accès à aucune donnée relative aux Patients ;
- accès aux environnements de production réservé aux seules personnes habilitées et nominativement désignées, avec authentification à deux facteurs sur les comptes d'administration ;
- mise en production subordonnée à l'exécution de tests automatisés complets, avec procédure de retour arrière documentée ;
- versions des composants techniques figées et mises à jour de sécurité régulières ;
- procédure de gestion des violations de données, éprouvée par un exercice annuel ;
- test d'intrusion réalisé par un prestataire indépendant avant l'ouverture du Service, puis renouvelé périodiquement.

Annexe 3 — Sous-traitants ultérieurs

Pour les données relatives aux Patients

Clever Cloud SAS, 4 rue Voltaire, 44000 Nantes, immatriculée au registre du commerce et des sociétés de Nantes sous le numéro 524 172 699. Prestation : hébergement de l'application, de la base de données, du stockage des fichiers chiffrés et des sauvegardes. Lieu : France, dans le périmètre couvert par son certificat de conformité pour l'hébergement de données de santé. Garanties : certificat n° FR094504, délivré par Bureau Veritas, valable jusqu'au 19 décembre 2027, pour les activités 1 à 6 ; certification ISO/IEC 27001 ; contrat d'hébergement de données de santé conclu avec TISSIO ; accord de traitement de données de la société Clever Cloud, mis à la disposition du Praticien à l'adresse https://www.clever.cloud/general-terms-and-conditions-of-use/clever-cloud-data-processing-agreement/ ; aucun transfert en dehors de l'Union européenne.

La société Clever Cloud recourt elle-même, pour la fourniture des sites physiques et du matériel, à des prestataires établis en France et titulaires d'un certificat de conformité pour l'hébergement de données de santé, à savoir Telehouse, Euclyde / nLighten France et OVHcloud, conformément à l'annexe 1 de son contrat d'hébergement.

Intervenants qui ne traitent aucune donnée relative aux Patients

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irlande (service Google Workspace). Prestation : acheminement des notifications, rappels et alertes adressés aux Utilisateurs, qui mentionnent exclusivement le nom et la spécialité du confrère concerné, à l'exclusion de toute donnée relative aux Patients. Lieu : Union européenne ; des transferts vers les États-Unis sont possibles. Garanties : avenant relatif au traitement des données (« Cloud Data Processing Addendum ») accepté le 6 octobre 2026 ; décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 relative au cadre de protection des données UE–États-Unis (le recours en annulation a été rejeté par le Tribunal de l'Union européenne le 3 septembre 2025 ; un pourvoi, affaire C-703/25 P, est pendant devant la Cour de justice) ; à défaut de décision d'adéquation, les clauses contractuelles types intégrées à cet avenant.

La société Stripe traite les données de paiement des Abonnés, dans les conditions de la politique de confidentialité. L'Agence du numérique en santé fournit Pro Santé Connect et l'Annuaire Santé, en qualité de responsable de ses propres traitements. La société GitHub héberge le code source du Service et déclenche les tâches planifiées, sans recevoir aucune donnée réelle. La société Supabase Pte. Ltd héberge la base de données de la démonstration, qui ne contient que des données fictives ; l'application de la démonstration et l'outil de surveillance du Service sont hébergés par la société Clever Cloud, dans la zone de Paris de Clever Cloud, distincte de la zone certifiée pour l'hébergement de données de santé où est hébergé le Service, sans aucune donnée relative aux Patients.

Annexe 4 — Clauses contractuelles types

Texte intégral, reproduit sans modification, de l'annexe de la décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725, dans sa version française publiée au Journal officiel de l'Union européenne L 199 du 7 juin 2021, page 18 (EUR-Lex, CELEX 32021D0915). Les choix opérés pour leur application figurent à l'article 4 du présent contrat ; les annexes I à IV des clauses correspondent aux Annexes 1 à 3 et à l'en-tête du présent contrat.

ANNEXE

Clauses contractuelles types

SECTION I

Clause 1

Objet et champ d'application

a) Les présentes clauses contractuelles types (ci-après les «clauses») ont pour objet de garantir la conformité avec [choisir l'option qui convient: OPTION 1: 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)/[OPTION 2: l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE].

b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.

c) Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II.

d) Les annexes I à IV font partie intégrante des clauses.

e) Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

f) Les clauses 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 et/ou du règlement (UE) 2018/1725.

Clause 2

Invariabilité des clauses

a) 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.

b) 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.

Clause 3

Interprétation

a) Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 ou dans le règlement (UE) 2018/1725 figurent dans les clauses, ils s'entendent comme dans le règlement en question.

b) 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.

c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 / le règlement (UE) 2018/1725 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Clause 4

Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

Clause 5 — Facultative

Clause d'amarrage

a) Toute entité qui n'est pas partie aux présentes clauses peut, avec l'accord de toutes les parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l'annexe I.

b) Une fois que les annexes mentionnées au point a) sont complétées et signées, l'entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d'un responsable du traitement ou d'un sous-traitant, conformément à sa désignation à l'annexe I.

c) Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l'adhésion.

SECTION II

OBLIGATIONS DES PARTIES

Clause 6

Description du ou des traitements

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 à l'annexe II.

Clause 7

Obligations des parties

7.1. Instructions

a) Le 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.

b) 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 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II.

7.4. Sécurité du traitement

a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III 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.

b) 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.

7.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

7.6. Documentation et conformité

a) Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.

c) 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 et/ou du règlement (UE) 2018/1725. 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.

d) 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.

e) 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.

7.7. Recours à des sous-traitants ultérieurs

a) OPTION 1: AUTORISATION SPÉCIFIQUE PRÉALABLE: 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 [PRÉCISER LA DURÉE] 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 à l'annexe IV, que les parties tiennent à jour.

OPTION 2: AUTORISATION ÉCRITE GÉNÉRALE: le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins [PRÉCISER LA DURÉE] à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.

b) 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 et/ou du règlement (UE) 2018/1725.

c) 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.

d) 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.

e) 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.

7.8. Transferts internationaux

a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.

b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

Clause 8

Assistance au responsable du traitement

a) 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.

b) 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 conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.

c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), 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 [OPTION 1] l'article 32 du règlement (UE) 2016/679 / [OPTION 2] aux articles 33, 36 à 38 du règlement (UE) 2018/1725.

d) Les parties définissent à l'annexe III 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.

Clause 9

Notification de violations de données à caractère personnel

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.

9.1. Violation de données en rapport avec des données traitées par le responsable du traitement

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:

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 [OPTION 1] l'article 33, paragraphe 3, du règlement (UE) 2016/679 / [OPTION 2] l'article 34, paragraphe 3, du règlement (UE) 2018/1725, 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 [OPTION 1] l'article 34 du règlement (UE) 2016/679 / [OPTION 2] l'article 35 du règlement (UE) 2018/1725, 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.

9.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, 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 à l'annexe III 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 [OPTION 1] des articles 33 et 34 du règlement (UE) 2016/679/[OPTION 2] des articles 34 et 35 du règlement (UE) 2018/1725.

SECTION III

DISPOSITIONS FINALES

Clause 10

Non-respect des clauses et résiliation

a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, 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.

b) Le 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 au point a) 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 et/ou du règlement (UE) 2018/1725;

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 et/ou du règlement (UE) 2018/1725.

c) 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 à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.

d) 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.

ANNEXE I

Liste des parties

Responsable(s) du traitement: [Identité et coordonnées du ou des responsables du traitement et, le cas échéant, du délégué à la protection des données du responsable du traitement]

1. Nom: …

Adresse: …

Nom, fonction et coordonnées de la personne de contact: …

Signature et date d'adhésion: …

1. …

Sous-traitant(s): [Identité et coordonnées du ou des sous-traitants et, le cas échéant, du délégué à la protection des données du sous-traitant]

1. Nom: …

Adresse: …

Nom, fonction et coordonnées de la personne de contact: …

Signature et date d'adhésion: …

1. …

ANNEXE II

Description du traitement

Catégories de personnes concernées dont les données à caractère personnel sont traitées

…

Catégories de données à caractère personnel traitées

…

Les données sensibles traitées (le cas échéant) et les limitations ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, tels que, par exemple, la limitation stricte de la finalité, les restrictions des accès (y compris l'accès réservé uniquement au personnel ayant suivi une formation spécialisée), la tenue d'un registre de l'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

…

Nature du traitement

…

Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement

…

Durée du traitement

…

…

Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement.

ANNEXE III

Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données

NOTE EXPLICATIVE:
Les mesures techniques et organisationnelles doivent faire l'objet d'une description concrète, et non pas générique.

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants (y compris toute certification pertinente) visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques. Exemples de mesures possibles:

mesures de pseudonymisation et de chiffrement des données à caractère personnel;

mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

mesures assurant de disposer de 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;

procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement;

mesures d'identification et d'autorisation de l'utilisateur;

mesures de protection des données pendant la transmission;

mesures de protection des données pendant le stockage;

mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées;

mesures visant à garantir l'enregistrement des événements;

mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut;

mesures de gouvernance et de gestion de l'informatique interne et de la sécurité informatique;

mesures de certification/assurance des procédés et produits;

mesures visant à garantir la minimisation des données;

mesures visant à garantir la qualité des données;

mesures visant à garantir une conservation limitée des données;

mesures visant à garantir la responsabilité;

mesures permettant la portabilité des données et garantissant l'effacement]

Pour les transferts vers des sous-traitants (ultérieurs), décrire également les mesures techniques et organisationnelles spécifiques que doit prendre le sous-traitant (ultérieur) pour être en mesure de prêter assistance au responsable du traitement.

Description des mesures techniques et organisationnelles spécifiques que le sous-traitant doit prendre pour pouvoir prêter assistance au responsable du traitement.

ANNEXE IV

Liste de sous-traitants ultérieurs

NOTE EXPLICATIVE:
La présente annexe doit être complétée en cas d'autorisation spécifique de sous-traitants ultérieurs [clause 7.7, point a), option 1].

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants:

1. Nom: …

Adresse: …

Nom, fonction et coordonnées de la personne de contact: …

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés): …

1. …