Conditions de traitement des données
pour les Services
En date du : 30 avril 2025, version 1.0

SECTION I

Clause 1
Objet et champ d'application

a) Les présentes Conditions de traitement des données (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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

b) Olympus France, dont le siège social est sis 19 rue d'Arcueil, CS700014 - 94150 RUNGIS, société par actions simplifiée (S.A.S.) immatriculée au registre du commerce et des sociétés (RCS) de Créteil sous le n° 582 026 324 (sous-traitant) et le responsable du traitement 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 I.

d) Les annexes I à III 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
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.

SECTION II – OBLIGATIONS DES PARTIES

Clause 3
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 I.

Clause 4
Obligations des parties

4.1. 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.

4.2. 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 I, sauf instruction complémentaire du responsable du traitement.

4.3. 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 I.

4.4. Sécurité du traitement

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

4.5. 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.

4.6 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.

4.7. Recours à des sous-traitants ultérieurs

a) 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 en annexe III. Le sous-traitant informe spécifiquement le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins quatre (4) semaines 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.

4.8. 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 4.7 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 5
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 5, 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 II 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 6
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.

6.1 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 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.

6.2 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 II 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.

SECTION III – DISPOSITIONS FINALES

Clause 7
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

DESCRIPTION DU TRAITEMENT

Activité de traitement : Service, Assistance, Conseil, Administration, Maintenance à distance

− Le début du traitement des données est : le début du contrat de service

− La durée prévue du traitement des données est : à la résiliation du contrat de service

Le contexte du traitement des données et les obligations des parties concernant la relation contractuelle commerciale sont précisés dans le contrat de service conclu entre le responsable du traitement et le sous-traitant.

Les catégories de personnes concernées, la nature/finalité du traitement, les catégories de données et les catégories particulières de données à caractère personnel dépendent du type de service fourni, des services auxquels les services se rapportent et des données à caractère personnel stockées par le client auxquelles Olympus a accès dans le cadre de la fourniture du service.

Catégories de personnes concernées	**Opérations de traitement**	**Catégories de données**	**Catégories particulières de données à caractère personnel – le cas échéant**
☒ Patients ☒ Personnes de contact ☒ Employés ☒ Anciens employés ☒ Fournisseurs et leurs employés	☒ Exploitation et maintenance des systèmes et infrastructures informatiques, par exemple les systèmes d'analyse ☒ Conseil sur l'utilisation des produits ☒ Assistance informatique ☒ Assistance technique ☒ Administration ☒ Réparation, test ou maintenance sur site ou dans un centre de réparation Olympus ☒ Diagnostic à distance du matériel informatique ☒ Test/maintenance à distance des produits logiciels	☒ Informations de compte ☒ Entreprise ☒ Date de naissance ☒ Consentement et autorisations liés à l'appareil ☒ Identifiant de l'appareil, nom de l'appareil ☒ Données de connexion de l'appareil ☒ Adresse e-mail ☒ Sexe ☒ Identifiants (analyse, contrat, appareil) ☒ Langue ☒ Localisation ☒ Journaux (logs) ☒ Nom ☒ Nom d'utilisateur	☒ Données relatives à la santé (par exemple, nom du patient, informations médicales)

	☒ Mise à disposition d'appareils de prêt	☒ Données principales/de base de l'utilisateur ☒ Données d'utilisation (adresse IP, journalisation, enregistrement téléphonique) ☒ Données d'utilisation des appareils et systèmes ☒ Données d'image et de vidéo	

Le travail sur l'appareil peut nécessiter la copie et l'analyse du fichier journal de l'appareil. Ce fichier peut contenir des noms de patients. L'assistance/support de premier et de deuxième niveau est assuré au sein de l'Union européenne. L'assistance/support de troisième niveau est fourni par une entité Olympus basée aux États-Unis (« Olympus Surgical Technologies America »). Par conséquent, si une assistance/support de troisième niveau est nécessaire pour le dépannage, un transfert de données vers les États-Unis peut s'avérer nécessaire. Afin de garantir un niveau de protection adéquat, Olympus a conclu des accords internes de traitement des données (DPA) appropriés avec ses entités affiliées aux États-Unis.

ANNEXE II

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES GARANTISSANT LA SÉCURITÉ DES DONNÉES

Compte tenu de l'état de l'art, des coûts de mise en œuvre, ainsi que de la nature, de la portée, du contexte et des finalités du traitement, de même que des risques – dont la probabilité et la gravité varient – pour les droits et libertés des personnes physiques, le sous-traitant mettra en œuvre les mesures techniques et organisationnelles suivantes :

MESURE	DESCRIPTION
1. CONFIDENTIALITÉ	
a) Contrôle de l'accès – sites d'Olympus	Les bâtiments d'Olympus sont fermés et surveillés à chaque issue. Les employés peuvent uniquement entrer dans les bâtiments avec leur carte d'identification personnelle. Les visiteurs ne peuvent entrer dans les bâtiments qu'en passant par la réception et accompagnés par un membre du personnel. L'accès au bâtiment est refusé à toute personne non- autorisée. Les mesures de sécurité suivantes sont mises en place : - Badges pour les employés/visiteurs - Contrôle d'accès, lecteur de carte, transpondeur, cartes magnétiques ou à puce - Accueil/réceptionniste/portier - Touches (contrôlées)/affectation de touches - Verrouillage de porte (ouverture de porte électrique, portes avec bouton extérieur, etc.) - Sécurité, portier - Système de surveillance, système d'alarme, surveillance vidéo/TV
b) Contrôle d'accès - systèmes	Tous les systèmes sont installés dans des centres de données sécurisés et protégés par des cartes d'identification personnelles associées à un code PIN.

	Les mesures de sécurité suivantes sont mises en œuvre : - Procédure de mot de passe sécurisée (incluant des caractères spéciaux, une longueur minimale, des changements réguliers de mot de passe) - Mécanismes de verrouillage automatique (par exemple, mot de passe ou interrupteur de pause, verrouillage automatique du bureau) - Instructions pour le verrouillage manuel du bureau - Création et gestion d'un profil utilisateur et d'un dossier principal - Pare-feu, logiciel antivirus pour les serveurs et les postes clients - Utilisation d'un VPN pour l'accès à distance - Politique relative aux appareils mobiles
c) Contrôle de l'accès – gestion des droits : autorisation de lecture et d'édition	Gestion des droits systématique pour l'utilisation des systèmes informatiques mise en place. Accès au système uniquement possible avec le nom et le mot de passe des utilisateurs. Les autorisations diffèrent entre les droits de lecture et d'écriture. Les mesures de sécurité suivantes sont mises en place : - Concept d'autorisation différenciée et droits d'accès fondés sur une information à connaître (profils, rôles, transactions et objets)
d) Contrôle de la séparation Systèmes informatiques internes d'Olympus	La maintenance à distance est effectuée séparément pour chaque client. Les mesures de sécurité suivantes sont mises en œuvre : - Capacité multi-clients des applications concernées - earmarking/affectation dédiée - Séparation fonctionnelle entre l'environnement de production et l'environnement de test - Séparation physique des systèmes, bases de données et supports de données

	- Définition des droits d'accès aux bases de données
a) Chiffrement	Une communication chiffrée est privilégiée. La méthode de chiffrement utilisée est conforme à l'état de l'art.
2. NTÉGRITÉ	
a) Contrôle des transferts Systèmes informatiques internes d'Olympus	Les mesures de sécurité suivantes sont mises en œuvre : - Le chiffrement des courriels est possible au sein du réseau - Aucune lecture, copie, modification ou suppression non autorisée au sein du système - Utilisation d'un VPN, ainsi que mise à disposition via des connexions chiffrées telles que SFTP, HTTPS
b) Contrôle des entrées	Les modifications apportées aux systèmes sont enregistrées. Les mesures de sécurité suivantes sont mises en œuvre : - Journalisation des accès - Systèmes d'analyse des journaux et traçabilité des saisies, modifications et suppressions de données par noms d'utilisateurs individuels - Attribution des droits via des comptes utilisateurs personnalisés - Gestion documentaire
3. DISPONIBILITÉ ET RÉSILIENCE	
a) Contrôle de la disponibilité ; mesures de protection des données Systèmes informatiques internes d'Olympus	Les données à caractère personnel sont sécurisées. Une protection contre la destruction ou la perte accidentelle ou intentionnelle est assurée, ainsi qu'un contrôle de la disponibilité des données. Les mesures de sécurité suivantes sont mises en œuvre : - Procédure de sauvegarde : description de la fréquence et du support de sauvegarde, durée de conservation et lieu de stockage (en ligne/hors ligne, sur site/hors site) - Disques durs en miroir, par exemple via une procédure RAID - Alimentation électrique sans interruption (UPS)

	- Stockage ou partition séparée pour les systèmes d'exploitation et les données - Protection antivirus et pare-feu - Canaux de signalement et plans d'urgence - Extincteurs et systèmes d'alarme dans les bâtiments, notamment dans la salle des serveurs, où la température et l'humidité sont également surveillées, et où des blocs multiprises avec protection sont installés
b) Récupération rapide	La récupération des données relève de la responsabilité du responsable du traitement.
4. PROCÉDURES RÉGULIÈRES DE RÉVISION, D'ÉVALUATION ET D'EXAMEN	
a) Contrôle des commandes Systèmes informatiques internes d'Olympus	L'efficacité des mesures prises est régulièrement contrôlée. Le contrôle des commandes est vérifié de manière aléatoire. Les mesures de sécurité suivantes sont mises en œuvre : - Conception claire des contrats - Formalisation des commandes - Sélection du prestataire sur la base de critères de diligence raisonnable (en matière de protection des données et de sécurité) - Conclusion des accords nécessaires relatifs au traitement de données pour le compte d'autrui ou des clauses contractuelles types de l'UE - Instructions données au prestataire par écrit ou sous forme de texte - Obligation pour les employés du prestataire au respect de la confidentialité des données - Obligation pour le prestataire de désigner un délégué à la protection des données si une telle obligation s'applique - Accord sur des droits de contrôle effectifs à l'égard du prestataire - Dispositions encadrant le recours à des sous-traitants supplémentaires - Garantie de la destruction des données à l'issue de la prestation - Vérification continue du prestataire et de son niveau de protection

b) Protection de la vie privée et gestion des réponses aux incidents	- Documentation centralisée de l'ensemble des procédures et règles en matière de protection des données, accessible aux employés selon leurs besoins/autorisations - Responsable interne de la sécurité de l'information et de la protection des données - Formation régulière des employés et engagement au respect de la confidentialité/vie privée - Processus documenté pour l'identification et le signalement des incidents de sécurité / violations de données (y compris en ce qui concerne les obligations de notification aux autorités de contrôle) - Procédure documentée de gestion des incidents de sécurité et des violations de données - Analyse d'impact sur la vie privée formalisée et procédure de traitement des demandes d'accès ou d'information des personnes concernées

ANNEXE III

LISTE DES SOUS-TRAITANTS

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

Nom et adresse	**Nom de la personne à contacter, fonction et coordonnées**	**Description du traitement**	**Le cas échéant : garanties pour les transferts vers des pays tiers**
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hambourg Allemagne	Stefan Limbacher Responsable de la protection des données EMEA privacy@olympus.com	Assistance de 2e niveau pour les réparations, la maintenance et la maintenance à distance des logiciels et dispositifs médicaux	n/a, sous-traitant basé à Hambourg, Allemagne
Olympus Surgical Technologies Europe **Olympus Winter & Ibe GmbH** Kuehnstraße 61 22045 Hambourg Allemagne	privacy@olympus.com	Interface entre l'assistance de 1er et de 3e niveau pour la logistique et le traitement du matériel.	n/a, sous-traitant basé à Hambourg, Allemagne
Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi Tokyo 192-8507 Japon	privacy@olympus.com	Traitement des réclamations, y compris les enquêtes sur les dysfonctionnements et les erreurs imprévues.	Décision d'adéquation (UE) 2019/419 de la Commission européenne

Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 États-Unis	privacy@olympus.com	Traitement des réclamations, y compris les enquêtes sur les dysfonctionnements et les erreurs imprévues.	Clauses contractuelles standard
Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Allemagne	privacy@olympus.com	Prestataire d'infrastructures et de services informatiques	n/a, sous-traitant basé à Francfort, Allemagne
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Allemagne	privacy@teamviewer.com	Surveillance et contrôle informatiques	n/a, Sub-Processors is located in Göppingen, Germany
ImageStreamMedical One Monarch Drive Littleton, MA 01460 États-Unis	privacy@cision.com	Assistance de niveau 3 pour la réparation, la maintenance et la maintenance à distance des logiciels	Clauses contractuelles standard
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521 Irlande	privacy@microsoft.com	Divers services d'informatique en nuage	n/a, sous-traitant basé en Irlande

RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH Royaume-Uni et Irlande du Nord	privacy@realvnc.com	Fournisseur de logiciels de contrôle à distance pour SPiN Planning Laptop Workstation – Aucun stockage de données, uniquement partage d'écran crypté	Décision d'adéquation pour le Royaume-Uni