**ADDENDUM SUR LE RESPONSABLE CONJOINT DU TRAITEMENT**

**Date de révision : 12 mars 2024**

Aux fins du présent Addendum sur le responsable conjoint du traitement (« Joint Controller Addendum », « JCA »), l'entité ou la société affiliée de Merck Sharp et Dohme LLC qui exécute le contrat ou toute autre forme d'accord faisant référence au présent JCA (l'« Accord ») sera désignée par le terme « Société » et toutes les autres parties à cet Accord seront collectivement désignées par le terme « Fournisseur ». La Société et le Fournisseur sont chacun une « Partie » et ensemble les « Parties ».

Contexte

1. Les Parties ont conclu cet Accord et peuvent parallèlement conclure un ou plusieurs bons de commande ou ordres de tâches, accords de projet, annexes au plan de projet, énoncés de travail, ordres de travail ou autres conditions de service (chacun étant un « Énoncé de tâche »), régissant les services envisagés dans l'Accord (l'« Objectif conjoint »).
2. Les Parties souhaitent compléter les termes de l'Accord pour s'assurer que tout partage de données personnelles dans le cadre de l'Accord est effectué en conformité avec la loi sur la protection des données, et pour clarifier leurs rôles en tant que responsables conjoints du traitement de ces données.

Les Parties conviennent de ce qui suit :

1. *Activités conjointes de Traitement*. En ce qui concerne les informations personnelles traitées dans le cadre de l'accord, l'objet, la nature, la finalité et la durée du partage, les catégories de personnes concernées et les catégories de données personnelles sont précisés dans l'annexe à l'Accord intitulée « Détails du traitement des données ».
2. *Applicabilité*. Les conditions du présent JCA s'appliquent à chaque Énoncé de tâche prévu par l'Accord, sauf indication contraire dans cet Énoncé de tâche.
3. *Obligations*. En ce qui concerne les Données personnelles traitées dans le cadre de l'Accord, les deux Parties s'engagent à :
   1. se conformer à la Loi sur la protection des données et à leurs obligations respectives en vertu du présent JCA et, dans le cas où l'une des Parties n'est pas en mesure de respecter ces obligations, en informer immédiatement l'autre Partie et prendre toutes les mesures raisonnables et appropriées nécessaires pour remédier à la non-conformité.
   2. traiter les Données personnelles uniquement comme spécifié dans le présent JCA et dans l'Accord, sauf en cas de consentement écrit de l'autre Partie et également dans le cas où :
      1. cette Partie a obtenu le consentement préalable valide de la personne concernée, tel que requis par la loi applicable en matière de protection des données ;
      2. lorsqu'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le cadre de procédures administratives, réglementaires ou judiciaires spécifiques ;
      3. lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
      4. la loi applicable exprime d'autres exigences, auquel cas, la Partie affectée doit en informer l'autre Partie, à moins que la loi applicable ne l'interdise, et s'efforcera de limiter la nature et la portée de toute divulgation requise et ne divulguera que la quantité minimale de Données personnelles nécessaires pour se conformer à la loi applicable.
   3. ne pas divulguer ou transférer de Données personnelles à un tiers sans que ce tiers ne conclue un accord écrit assorti de conditions qui garantissent une protection des Données personnelles au moins équivalente à celle assurée par les obligations énoncées dans le présent JCA et dans l'Accord.
   4. ne pas vendre, partager, conserver, utiliser ou divulguer des Données personnelles autres que celles spécifiées dans l'Accord ou autorisées en vertu du présent JCA.
   5. être entièrement responsable de tous les actes ou omissions de ses employés, sociétés affiliées, agents, sous-traitants et autres représentants.
   6. mettre en œuvre et maintenir des programmes écrits relatifs à la sécurité de l'information et à la confidentialité raisonnables et appropriés, lesquels doivent incorporer des mesures physiques, techniques et organisationnelles proportionnelles à la nature des Données personnelles traitées dans le cadre de l'Accord, qui respectent ou dépassent les bonnes pratiques de l'industrie et qui protègent raisonnablement contre une violation des Données personnelles, ce qui inclut la formation de l'ensemble du personnel chargé du Traitement des Données personnelles d'une façon qui permet de satisfaire les exigences du présent JCA, et le cas échéant :
      1. la pseudonymisation et le chiffrement des Données personnelles ;
      2. la capacité d'assurer constamment la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de Traitement ;
      3. la capacité de rétablir la disponibilité et l'accès aux Données personnelles en temps opportun en cas d'incident physique ou technique ;
      4. un processus permettant de tester, d'évaluer et d'apprécier régulièrement l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du Traitement ; et
      5. la capacité de confirmer dans les 72 heures suivant la détection si un événement constitue une Violation de données personnelles.
   7. en cas de violation réelle ou légitimement soupçonnée de Données personnelles, la Partie à l'origine de cette découverte doit en informer l'autre Partie dans les plus brefs délais (en tout état de cause dans les 24 heures suivant la découverte de la violation des Données personnelles) et coopérer avec l'autre Partie pour décider d'un plan d'action approprié.
   8. en informer l'autre Partie dans les plus brefs délais et, en tout état de cause, dans les 24 heures suivant :
      1. toute plainte, enquête, demande ou préoccupation d'une autorité compétente en matière de protection des données ou autre autorité réglementaire concernant les Données personnelles liées à l'Accord ;
      2. toute plainte, demande, requête ou préoccupation de la part de la personne concernée au sujet des Données personnelles en lien avec le contrat, y compris toute demande visant à exercer des droits en vertu de la loi sur la protection des données ou de la politique de confidentialité de l'une ou l'autre des Parties, telles qu'accéder, rectifier, modifier, corriger, partager, supprimer ou cesser le Traitement de ses Données personnelles.
   9. se conformer à toutes les mesures raisonnables et appropriées demandées par l'autre partie et qui sont nécessaires pour que les deux parties puissent se conformer à leurs obligations respectives en vertu de la loi sur la protection des données et du présent JCA.
   10. ne pas conserver les Données personnelles au-delà du délai nécessaire pour atteindre l'Objectif conjoint, sauf si la loi applicable l'exige autrement.
   11. maintenir l'exactitude et l'intégrité des Données personnelles soumises au présent JCA.
   12. informer, conformément aux termes de l'Accord, toute personne concernée dont les Données personnelles sont recueillies dans le cadre de l'Accord, et obtenir son consentement à cet égard.
   13. conserver tous les documents nécessaires afin de pouvoir démontrer que les Données personnelles ont été traitées uniquement conformément aux avis, consentements, autorisations et droits applicables et tel que permis par le présent JCA, et pour que chaque Partie se conforme à la loi sur la protection des données.
   14. dans la mesure où l'une des deux Parties doit traiter des Données personnelles concernant des personnes concernées de tout pays ou région avec des restrictions sur le transfert transfrontalier de Données personnelles, les deux Parties ne le feront qu'en conformité avec la Loi sur la protection des données, ce qui peut inclure, sans s'y limiter, la conclusion de Clauses contractuelles types ou de mécanismes similaires destinés à protéger les transferts de Données personnelles.
   15. à l'exception des modifications apportées conformément au respect d'une norme supérieure de l'industrie ou d'une Loi sur la protection des données, les deux Parties doivent maintenir leurs pratiques respectives en matière de confidentialité et de sécurité des données en vigueur, les appliquer de manière cohérente et les divulguer à l'autre Partie dans le cadre de toute diligence raisonnable récemment exercée par l'autre Partie sur ces pratiques au sein de l'Accord.
   16. chaque Partie reconnaît et accepte que l'exécution du présent JCA constitue sa certification qu'il comprend les restrictions énoncées dans le JCA et qu'il s'y conformera.
4. *Définitions*
   1. La « Loi sur la protection des données » désigne toute loi applicable en matière de protection des données, de sécurité des données ou de confidentialité, y compris le Règlement général sur la protection des données de l'UE et toute législation nationale de mise en œuvre s'y rapportant, la législation HIPAA (Health Insurance Portability and Accountability Act), la loi californienne sur la protection de la vie privée des consommateurs (California Privacy Rights Act) et toute autre loi nationale, étatique, fédérale, provinciale ou régionale relative à la protection des données, à la sécurité des données ou à la vie privée.
   2. Les « Données personnelles » désignent toutes les données liées à l'Accord concernant une personne identifiée ou identifiable, y compris les données qui identifient une personne ou qui pourraient être utilisées pour identifier, localiser, suivre ou contacter une personne. Les Données personnelles comprennent à la fois des informations directement identifiables, telles qu'un nom, un numéro d'identification ou un intitulé de poste unique, et des informations indirectement identifiables telles que la date de naissance, l'identifiant unique d'un appareil mobile ou portable, des informations qui pourraient être utilisées pour identifier un foyer, un numéro de téléphone, des données codées par clé, des identifiants en ligne tels que des adresses IP, ou des activités, comportements ou préférences personnels, et comprennent toutes les données qui constituent des « Données personnelles » en vertu de la Loi sur la protection des données.
   3. Le « Traitement » désigne l'exécution de toute opération ou ensemble d'opérations sur des Données personnelles ou des ensembles de Données personnelles, que ce soit par le biais (ou non) de moyens automatisés, tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'accès, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l'évaluation, l'analyse, la création de rapports, le partage, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction.
   4. La « Violation de Données personnelles » désigne la destruction, la perte, l'altération, la divulgation, l'utilisation ou l'accès non autorisés accidentels ou illégaux à des Données personnelles, transmises, stockées ou traitées de toute autre manière.
   5. Les « Clauses contractuelles types » désigne les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers qui n'ont pas été évalués par la Commission européenne comme offrant un niveau adéquat de protection des données à caractère personnel, telles que publiées par la Commission européenne le 4 juin 2021, qui peuvent être mises à jour de temps à autre.
   6. Dans le cas où ces définitions restreignent ou réduisent la portée des définitions connexes en vertu de la Loi sur la protection des données, la définition doit être élargie pour correspondre à la définition de ladite Loi sur la protection des données.
   7. En l'absence d'une définition en vertu de la présente section, un terme doit être interprété d'une manière conforme à la loi applicable en matière de protection des données.
5. Interprétation.
   1. Les mots « inclure » et « y compris » doivent être interprétés comme signifiant « y compris, mais sans s'y limiter ».
   2. Dans le cadre de l'Objectif conjoint et en vertu de l'Accord, les deux Parties peuvent traiter les Données personnelles d'une ou de plusieurs sociétés affiliées de l'autre Partie. Dans un tel cas, l'une de ces sociétés affiliées de la Société sera considérée comme un « Contrôleur » des Données personnelles et comme un tiers bénéficiaire du présent JCA et autorisée à s'appuyer sur tous les droits et protections accordés à la Société en vertu du présent JCA, que cette société affiliée soit désignée ou non comme partie à l'Accord ou au présent JCA.
   3. Dans l'exécution de leurs obligations en vertu de l'Accord de Services et de ce JCA, les Parties reconnaissent que la politique d'entreprise de MSD et de ses Affiliés exige que les activités de MSD soient menées dans l'esprit et la lettre de toute loi applicable en matière de protection des données, y compris le Règlement général sur la protection des données de l'UE. Dans le cas où les deux Parties ne seraient pas soumises aux mêmes Lois de protection des données, il est attendu que les deux Parties respectent toutes les normes de protection des données raisonnablement pertinentes contenues dans ces lois.
   4. Le présent JCA est par la présente incorporé à l'Accord et en fait partie intégrante.
   5. En cas de conflit entre les dispositions de l'Accord et celles du présent JCA, les dispositions du présent JCA prévalent, sauf si les dispositions de l'Accord protègent davantage les Données personnelles traitées dans le cadre de l'Accord, auquel cas les dispositions les plus protectrices de l'Accord prévalent.
   6. En cas de conflit entre les dispositions du présent JCA et les Clauses contractuelles types, les dispositions des Clauses contractuelles types prévalent.
   7. Sauf modification expresse des présentes, les dispositions de l'Accord restent pleinement en vigueur.
   8. Si le présent JCA est rédigé en anglais et dans une autre langue, en cas de différences entre le texte en anglais et le texte dans cette autre langue, le texte en anglais prévaut.
   9. Les sections et autres titres du présent JCA ont pour seul but de faciliter les références et ne font pas partie intégrante du présent JCA et n'en affectent pas le sens ou l'interprétation.
   10. Les appendices et les annexes du présent JCA sont réputés faire partie intégrante du présent JCA dans la même mesure que s'ils avaient été énoncés textuellement dans le présent JCA.
   11. Chaque disposition du présent JCA est indépendante. Si une phrase, une clause ou une disposition est invalide ou inapplicable en tout ou en partie, cette invalidité ou inapplicabilité n'affecte que cette phrase, cette clause ou cette disposition, et le reste du JCA reste pleinement en vigueur.
   12. Le présent JCA peut être conclu en plusieurs exemplaires, qui, ensemble, constituent un seul et même accord. Toute Partie peut conclure le présent JCA en signant l'exemplaire approprié.
   13. Le présent JCA constitue l'intégralité de l'accord entre les Parties en ce qui concerne l'objet du présent JCA et (dans la mesure où la loi le permet) remplace toutes les déclarations antérieures ou tous les accords oraux ou écrits entre les Parties en ce qui concerne cet objet, à condition que rien dans le présent JCA ni aucune des Parties ne tente d'exclure toute responsabilité en cas de déclarations frauduleuses.
   14. Les dispositions de l'Accord relatives à la loi applicable et à la juridiction compétente s'appliquent au présent JCA.
6. *Limites des mises à jour*.
7. Lorsque les Parties renouvellent, modifient, émettent un nouveau Cahier des Charges sous, ou modifient de quelque manière que ce soit l'Accord ou tout Cahier des Charges sous l'Accord (un "Événement Déclencheur"), le document le plus récent sous "Joint Controller Addendum" situé à <https://www.msdprivacy.com/privacyterms/> remplacera et supplantera les termes de cet Addendum jusqu'au prochain Événement Déclencheur, à moins qu'une objection ne soit formulée dans les 30 jours suivant la survenue de l'événement déclencheur. Nonobstant ce qui précède, il peut y avoir des situations nécessitant une modification immédiate des termes de cet Addendum, qui ne se produira que pour des raisons articulées dans 6(b), et ne sera faite de bonne foi et après avoir assuré que les nouveaux termes ou termes modifiés sont limités à ceux nécessaires pour se conformer à la nouvelle loi applicable en matière de protection des données, à la jurisprudence, ou aux orientations émises par les autorités compétentes en matière de protection des données.
8. Dans l'éventualité où l'un des scénarios suivants se produit, les Parties conviennent immédiatement des termes les plus récents publiés à l'adresse ci-dessus, à moins qu'une objection ne soit formulée dans les 30 jours suivant la notification par l'Entreprise des nouveaux termes fournis à toutes les entités ayant demandé à recevoir une notification à [privacy\_updates@merck.com](mailto:privacy_updates@merck.com):
   * 1. la loi applicable en matière de protection des données a été mise à jour de manière à ce que les termes contractuels existants de cet Addendum soient insuffisants pour satisfaire aux exigences de la loi mise à jour,
     2. il y a un changement dans la loi applicable en matière de protection des données et les Parties ont un intérêt raisonnable et légitime à modifier ces termes en raison du changement de loi, par exemple et sans limitation, en supprimant les exigences qui ne sont plus nécessaires, ou
     3. il y a une nouvelle jurisprudence ou des orientations émises par les autorités compétentes en matière de protection des données qui ont un effet comparable à un changement de loi décrit en (i) ou en (ii) ci-dessus.
9. *Applicabilité des annexes*. Les Clauses contractuelles types jointes aux présentes en Annexe 2 et les addenda joints en Annexe 3 ne s'appliquent que dans la mesure où elles sont requises par la Loi sur la protection des données applicable. Les Parties conviennent de se conformer à ces clauses et addenda uniquement dans la mesure où ils sont conformes aux exigences de la loi applicable en matière de protection des données dans chaque juridiction et sont requis par celles-ci.
10. *Avis*. Les avis émis en vertu du présent JCA (chacun étant un « Avis ») doivent l'être par écrit. Les Avis émis en vertu du présent JCA doivent l'être conformément aux dispositions relatives aux avis de l'Accord applicable, et une copie doit être envoyée à la Société par courrier électronique à l'adresse [msd\_privacy\_office@msd.com](mailto:msd_privacy_office@msd.com), avec pour objet « Avis JCA du Fournisseur » ou, dans le cas d'une Violation de données personnelles, « Urgent : Avis de violation de données personnelles ».

**ANNEXE 1 - Mesures de sécurité IT**

1. Définitions – Lorsqu'elles sont utilisées dans cette Annexe, chacun des termes définis suivants aura la définition donnée ci-dessous pour ce terme. Les termes définis utilisés dans cette Annexe mais non définis ici auront la signification spécifiée ailleurs dans le Contrat.
   1. “Information de l'Entreprise” désigne toute information de l'Entreprise ou de l'un de ses Affiliés ou de leurs fournisseurs respectifs, clients ou autres partenaires commerciaux fournis à, obtenus par, créés ou générés par ou autrement traités par le Fournisseur ou l'un de ses prestataires de services tiers en relation avec l'un des Services et toute autre information à traiter comme confidentielle en vertu du Contrat.
   2. “Violation de Données” signifie une destruction, perte, altération, utilisation, transmission ou divulgation accidentelle ou non autorisée de ou l'accès à toute Information de l'Entreprise.
   3. “Point d'Extrémité” désigne tout ordinateur, y compris tout ordinateur portable ou de bureau, appareil mobile, équipement de laboratoire, serveur ou autre appareil sur les Systèmes du Fournisseur, y compris tout hébergé sur un site tiers externe (par exemple, fournisseur de cloud).
   4. “Événement de Notification” désigne tout événement, y compris une Violation de Données, qui nécessite la notification des individus ou des entités en vertu de toute Loi.
   5. “Événement de Sécurité” désigne toute A) Violation de Données, (B) Événement de Notification, (C) accès non autorisé à ou interférence avec les opérations des Systèmes du Fournisseur ou (D) violation des obligations de sécurité du Fournisseur en vertu de cette Annexe, du Contrat ou de toute Loi.
   6. “Logiciel Sujet” désigne tout logiciel fourni ou utilisé en relation avec l'un des Services, y compris tout logiciel livré à, ou installé sur tout ordinateur, y compris tout ordinateur portable ou de bureau, appareil mobile, équipement de laboratoire, serveur, autre appareil ou autre composant de, ou connecté à, les systèmes d'information de, l'Entreprise ou l'un de ses Affiliés.
   7. “Systèmes du Fournisseur” désigne les réseaux du Fournisseur et tous les systèmes, y compris le Logiciel Sujet, (A) fournis ou utilisés en relation avec l'un des Services, (B) sur lesquels toute Information de l'Entreprise ou livrables ou travail en cours pour l'Entreprise ou ses Affiliés, est stocké ou autrement traité ou à partir duquel ils sont accessibles, (C) connecté à l'information, au réseau ou à d'autres systèmes de l'Entreprise ou de ses Affiliés ou à partir duquel l'information, le réseau ou d'autres systèmes de l'Entreprise ou de ses Affiliés peuvent être accessibles, ou (D) auquel l'un des éléments précédents peut être connecté ou à partir duquel l'un des éléments précédents peut être accessible.
2. Sécurité du Réseau - Le Fournisseur maintiendra des politiques, des procédures et des contrôles de sécurité du réseau et effectuera des activités de sécurité du réseau, conformément aux meilleures pratiques de l'industrie du Fournisseur, mais qui incluent au minimum la fourniture de pare-feu de réseau, les contrôles de détection et de prévention d'intrusion, les contrôles de protection contre les attaques par déni de service distribué (DDoS) et les évaluations de vulnérabilité et les tests de pénétration effectués régulièrement, conformément aux meilleures pratiques de l'industrie du Fournisseur (mais pas moins fréquemment qu'annuellement). En aucun cas, les politiques, procédures ou contrôles de sécurité du réseau du Fournisseur appliqués à la protection de l'Information de l'Entreprise et des Systèmes du Fournisseur ne seront moins rigoureux et protecteurs que ceux appliqués par le Fournisseur à la protection de ses propres informations et de ses autres systèmes de nature similaire.
3. Sécurité des applications - En fonction de la nature des services fournis, le cas échéant, le Fournisseur doit disposer de processus et de contrôles de cycle de vie de développement de logiciels ("Processus SDLC") régissant le développement et les modifications de tout logiciel du Fournisseur, y compris les mises à jour, les améliorations, les correctifs, les améliorations, les corrections de bugs, les modifications, les améliorations, les corrections, les révisions, les versions et autres modifications. Le processus SDLC doit, au minimum, inclure des pratiques reconnues et comparables de développement de logiciels sécurisés selon les normes de l'industrie. Le Fournisseur doit suivre un processus de gestion des correctifs qui garantit que les systèmes d'information du Fournisseur sont à jour avec une sécurité et une fonctionnalité appropriées. Le Fournisseur doit, en temps opportun, en fonction du risque, et dans les délais prévus dans les politiques et procédures du Fournisseur, remédier et retester toute vulnérabilité identifiée.
4. Sécurité des données - En fonction de la nature des services fournis, le cas échéant, le Fournisseur doit gérer, stocker et traiter les informations de l'entreprise, conformément aux pratiques et normes de l'industrie reconnues et comparables, telles que celles énoncées au paragraphe 11 (y compris PCI DSS, le cas échéant) et conformément à toutes les lois. Le Fournisseur doit établir et maintenir des protections raisonnables contre une violation de données. En plus de et sans limiter aucune autre obligation du Fournisseur, le Fournisseur doit stocker toutes les informations de l'entreprise conformément aux meilleures pratiques de l'industrie du Fournisseur et en conformité avec toutes les lois, et doit utiliser des mesures de sécurité qui répondent aux meilleures pratiques de l'industrie du Fournisseur, y compris le cryptage et les pare-feu, pour protéger les informations de l'entreprise contre une violation de données. Lorsque le Fournisseur stocke des informations de l'entreprise dans une installation hors site, le Fournisseur doit avoir respecté toutes les conditions de l'Accord ou de tout accord exécuté en relation avec l'Accord, lié à la divulgation des informations de l'entreprise à des tiers ou à l'engagement d'autres tiers pour fournir ou aider à fournir des produits ou des services, et le Fournisseur doit utiliser une installation de stockage hors site raisonnablement acceptable pour l'entreprise qui doit, sans limiter ce qui précède, être en pleine conformité avec toutes les dispositions de cette Annexe. De plus, le fournisseur de cette installation de stockage hors site doit être lié par un accord de confidentialité écrit entre le Fournisseur et ce fournisseur, qui contient des conditions pas moins strictes que celles de l'Accord ou de tout accord exécuté en relation avec l'Accord et qui protège toutes les informations de l'entreprise stockées à l'intérieur.
5. Stockage des données - En fonction de la nature des services fournis, le cas échéant, toutes les informations de l'entreprise seront gérées, stockées et traitées uniquement sur les ressources informatiques et de stockage désignées du Fournisseur. Les informations de l'entreprise ne seront gérées, stockées ou traitées sur un ordinateur portable ou un appareil mobile que si (A) il s'agit d'un ordinateur portable ou d'un appareil mobile du Fournisseur, (B) le Fournisseur crypte toutes les informations de l'entreprise sur cet ordinateur portable ou cet appareil mobile conformément aux normes de cryptage du paragraphe 7 ci-dessous et (C) cet ordinateur portable ou cet appareil mobile est soumis à des contrôles de point de terminaison conformes aux pratiques et normes de l'industrie reconnues et comparables, telles que celles énoncées au paragraphe 11. Les informations de l'entreprise ne seront pas gérées, stockées ou traitées sur un appareil portable, sauf comme prévu dans la phrase immédiatement ci-dessus. Le Fournisseur doit stocker toutes les sauvegardes des informations de l'entreprise dans le cadre de ses processus de sauvegarde et de récupération désignés, et ces sauvegardes des informations de l'entreprise doivent être cryptées conformément à cette Annexe, y compris les exigences de ce paragraphe 5 et du paragraphe 7 ci-dessous.
6. Transmission de données - En fonction de la nature des services fournis, le cas échéant, toute transmission ou échange électronique d'informations de l'entreprise doit se faire par des moyens sécurisés (utilisant HTTPS ou SFTP ou équivalent) conformes aux pratiques et normes industrielles reconnues et comparables, telles que celles énoncées au paragraphe 11, et uniquement conformément au paragraphe 7 ci-dessous.
7. Chiffrement des données - En fonction de la nature des services fournis, le cas échéant, en plus de et sans limiter les autres obligations du fournisseur, le fournisseur accepte que toute information de l'entreprise composée d'informations personnelles soumises à protection en vertu de toute loi ou composée d'informations soumises à protection en vertu de la norme de protection des données de l'industrie des cartes de paiement en vigueur, y compris toutes les données de sauvegarde de l'entreprise, soit conservée sous forme cryptée, en utilisant une solution de cryptage commercialement supportée. Le fournisseur accepte que des solutions de cryptage soient déployées qui cryptent les informations de l'entreprise conformément aux pratiques et normes industrielles reconnues et comparables, telles que celles énoncées au paragraphe 11, mais avec au moins une clé de 128 bits pour le cryptage symétrique et une clé de 2048 (ou plus) bits pour le cryptage asymétrique.
8. Réutilisation des données - En fonction de la nature des services fournis, le cas échéant, le fournisseur doit utiliser toutes les informations de l'entreprise uniquement aux fins de la prestation des services. Le fournisseur ne doit pas distribuer, réutiliser ou partager entre autres applications, environnements ou unités commerciales du fournisseur toute information de l'entreprise.
9. Gestion des données en fin de contrat - En fonction de la nature des services fournis, le cas échéant, en plus de et sans limiter les autres obligations du fournisseur, à la demande de l'entreprise et sauf disposition contraire dans le contrat, à l'expiration ou à la résiliation anticipée du contrat, toutes les informations de l'entreprise en la possession ou sous le contrôle du fournisseur ou de l'un de ses affiliés, sous-traitants, prestataires de services, agents ou autres consultants doivent être détruites ou restituées, selon le choix de l'entreprise.
10. Notification de violation de sécurité - En plus de et sans limiter les autres obligations du fournisseur, le fournisseur doit informer l'entreprise d'un événement de sécurité réel ou raisonnablement suspecté dans les 24 heures suivant la prise de conscience de cet événement de sécurité réel ou raisonnablement suspecté. Le fournisseur doit informer l'entreprise de cet événement de sécurité réel ou raisonnablement suspecté en contactant l'équipe de sécurité de l'entreprise par téléphone (+1-704-345-6700 – Choisissez l'option 1) et par e-mail au Centre d'opérations mondial [globalopscnt@merck.com](mailto:globalopscnt@merck.com). Le fournisseur fournira des informations et une assistance que l'entreprise peut raisonnablement demander concernant un événement de sécurité, y compris des informations sur la cause première.
11. Normes de l'industrie - Les normes de l'industrie généralement reconnues incluent mais ne sont pas limitées aux normes et benchmarks actuels établis et maintenus par les suivants :
    1. Centre pour la sécurité de l'Internet - voir [http://www.cisecurity.org](http://www.cisecurity.org/)
    2. Industrie des cartes de paiement / Normes de sécurité des données (PCI/DSS) – voir <http://www.pcisecuritystandards.org/>
    3. Institut national des normes et de la technologie - voir [http://csrc.nist.gov](http://csrc.nist.gov/)
    4. Loi fédérale sur la gestion de la sécurité de l'information (FISMA) - voir [http://csrc.nist.gov](http://csrc.nist.gov/)
    5. Série ISO/IEC 27000 - voir <http://www.iso27001security.com/>
    6. Organisation pour l'avancement des normes d'information structurées (OASIS) – voir <http://www.oasis-open.org/>
    7. Le projet de sécurité des applications Web ouvertes (OWASP) – voir [http://www.owasp.org](http://www.owasp.org/)
    8. La CWE (Common Weakness Enumeration) - voir [http://cwe.mitre.org](http://cwe.mitre.org/) ou CWE/SANS Top 25 Programming Errors - <http://cwe.mitre.org/top25/>
    9. L'Institut SANS - voir [http://www.sans.org](http://www.sans.org/)
    10. Les erreurs logicielles les plus dangereuses <http://www.sans.org/top25-programming-errors/>

Sur demande raisonnable de l'entreprise, le fournisseur permettra à l'entreprise d'auditer la conformité du fournisseur avec les exigences énumérées ci-dessus. Le fournisseur corrigera toute défaillance à se conformer aux exigences, dès que raisonnablement possible.

**ANNEXE 2**

Dans le cas où la Société ou le Fournisseur exporte des Données personnelles d'une manière qui nécessite le Module 1 des Clauses contractuelles types, les conditions suivantes s'appliquent :

*Le corps du texte du Module 1 (Contrôleur à Contrôleur) des Clauses contractuelles types jointes à la décision d'application (UE) 2021/914 de la Commission du 4 juin 2021 est intégré par référence. Les aspects facultatifs sont décrits ci-dessous :*

1. *La clause 7 (clause d'adhésion) est omise.*
2. *Pour la clause 11, le texte facultatif est omis.*
3. *Pour la clause 17, l'option 1 est choisie, l'État membre étant les Pays-Bas.*
4. *Pour la clause 18, le choix du forum est les Pays-Bas.*

**APPENDICE 1 À L'ANNEXE 2**

**A. LISTE DES PARTIES**

*Voir l'Accord*

**B. DESCRIPTION DU TRANSFERT**

*Voir l'annexe à l'Accord intitulée « Détails du traitement des données ».*

**C. AUTORITÉ DE CONTRÔLE COMPÉTENTE**

****Commission Nationale de l'Informatique et des Libertés - CNIL****  
3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07  
Tel. +33 1 53 73 22 22  
Fax +33 1 53 73 22 00  
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**APPENDICE 2 À L'ANNEXE 2 – MESURES TECHNIQUES ET ORGANISATIONNELLES**

Voir l'Annexe 1 du JCA auquel ces Clauses sont jointes. En outre, l'Importateur de données doit s'assurer que toutes les Données personnelles sont pseudonymisées et cryptées le cas échéant. En outre, lorsqu'ils reçoivent une demande d'une autorité gouvernementale relative aux Données personnelles faisant l'objet des présentes Clauses, l'Importateur de données et ses Sociétés affiliées garantissent que (i) les demandes d'accès des services de renseignement ou des autorités similaires aux États-Unis ou ailleurs aux Données personnelles décrites à l'annexe 1B, et (ii) toute « obligation de divulgation » de ces données seront contestées par l'Importateur de données et ses sociétés affiliées conformément aux lois et réglementations applicables avant l'extraction.

**ANNEXE 3**

**Exigences légales supplémentaires en termes d'État, de pays, de région et de province**

**ADDENDUM DU ROYAUME-UNI : Loi sur la protection des données de 2018**

La présente Annexe 3 incorpore par référence l'Addendum sur le transfert international des données aux Clauses contractuelles types de la Commission européenne, version B1.0, en vigueur depuis le 21 mars 2022, et doit être considérée comme appliquée intégralement par les deux Parties de l'Accord de façon à couvrir l'ensemble des transferts applicables en vertu du JCA et comprenant toutes les Clauses obligatoires de la partie 2.

**ADDENDUM SUR LA SUISSE : FADP**

1. Dans la mesure où les transferts de données décrits dans l'Annexe 2 sont soumis au FADP, les références au RGPD doivent s'entendre comme des références à la loi fédérale suisse sur la protection des données (« FADP »).
2. Aussi longtemps que l'exige le FADP, les données personnelles des personnes morales sont protégées conformément aux présentes Clauses de la même manière que les personnes concernées.
3. Clause 13 : Supervision parallèle
   1. Lorsque le transfert de données est régi par le FADP : le Préposé fédéral à la protection des données et à la transparence (« FDPIC ») est l'organe de surveillance compétent ;
   2. Lorsque le transfert de données est régi par le GDPR : les critères de la Clause 13, point a), s'appliquent.
4. Clause 18(c) : Choix du forum et de la juridiction : une personne concernée, ayant sa résidence habituelle en Suisse, peut également intenter une action en justice contre l'exportateur de données et/ou l'importateur de données devant les tribunaux suisses.

**ADDENDUM SUR LE CANADA : Loi 25 du Québec**

* + - 1. Tout avis requis en vertu du présent JCA en relation avec une Violation de Données personnelles, et tout avis similaire requis en vertu de l'Accord seront également requis pour tout événement constituant une violation ou une tentative de violation du présent JCA par le Fournisseur.
      2. Si cela est exigé pour recueillir le consentement relatif aux conditions du présent JCA, le Fournisseur est également dans l'obligation de conserver l'ensemble des preuves de consentement pendant les trois (3) ans suivant la fin de l'Accord.

**ADDENDA DES ÉMIRATS ARABES UNIS : Loi fédérale n° 45 de 2021 sur la protection des données personnelles**

1. Dans la mesure où les transferts de données décrits à l'annexe 2 sont soumis à la loi fédérale n° 45 de 2021 des Émirats arabes unis sur la protection des données personnelles (« PDPL »), à moins et jusqu'à ce que l'Office des données des EAU émette ses propres clauses contractuelles types pour légitimer le transfert d'informations personnelles en dehors des Émirats arabes unis et que les parties aient conclu de telles clauses contractuelles types, les parties conviennent que les clauses contractuelles types jointes aux présentes en tant qu'annexe 2 s'appliqueront, mutatis mutandis, à ces transferts pour fournir des garanties appropriées pour les informations personnelles et les personnes concernées. À ces fins : a. Les références au « Règlement (UE) 2016/679 », au « 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 (Règlement général sur la protection des données) » et à « ce règlement » sont toutes remplacées par « PDPL ». b. Les références à des articles spécifiques du « Règlement (UE) 2016/679 » sont remplacées par l'article ou la section équivalente du PDPL. c. Les références à l'« Union européenne », « Union », « UE », « État membre de l'UE », « État membre » et « UE ou État membre » sont toutes remplacées par « Émirats arabes unis ». d. L'« autorité de contrôle compétente » et l'« autorité de contrôle » sont toutes deux remplacées par l'« Office des données ». e. Tout litige découlant des clauses contractuelles types sera régi par les lois des Émirats arabes unis et résolu par les tribunaux des Émirats arabes unis. Les parties conviennent de se soumettre à la juridiction de ces tribunaux. f. En cas d'incohérence ou de conflit entre le PDPL et les clauses contractuelles types jointes aux présentes en tant qu'annexe 2, le PDPL s'applique. g. Si le sens des clauses contractuelles types jointes aux présentes en tant qu'annexe 2 est ambigu dans la mesure où il s'applique aux transferts d'informations personnelles en dehors des EAU, ou s'il existe plus d'un sens, le sens qui correspond le plus au PDPL s'applique.
2. Si l'Office des données des EAU émet ses propres clauses contractuelles types pour légitimer le transfert d'informations personnelles en dehors des Émirats arabes unis, les parties négocieront de bonne foi en vue de convenir et de mettre en œuvre les clauses contractuelles types dès que cela est raisonnablement possible. Lorsque les parties concluent des clauses contractuelles types conformément à la phrase précédente, ces clauses contractuelles types remplaceront, en ce qui concerne les transferts d'informations personnelles soumises au PDPL en dehors des Émirats arabes unis, les clauses contractuelles types jointes aux présentes en tant qu'annexe 2 en tant que garanties appropriées mises en œuvre pour fournir des garanties appropriées pour les informations personnelles et les personnes concernées en ce qui concerne les transferts.
3. La société peut révoquer son accord d'être liée par les clauses contractuelles types jointes aux présentes en tant qu'annexe 2 sur notification écrite au fournisseur lorsque l'Office des données adopte une décision d'adéquation couvrant le transfert d'informations personnelles auxquelles les clauses contractuelles types s'appliquent, ou lorsque la société détermine autrement que d'autres garanties appropriées s'appliquent en ce qui concerne le transfert. À compter de la date de toute notification signifiée par la société conformément à la phrase précédente, les clauses contractuelles types jointes aux présentes en tant qu'annexe 2 cesseront de s'appliquer aux transferts d'informations personnelles soumises au PDPL en dehors des Émirats arabes unis.

**ANNEXE BRÉSIL : LGPD - Clauses contractuelles types**

Les Clauses Contractuelles Types brésiliennes (« CCT ») en vertu de la Loi Générale sur la Protection des Données (Lei Geral de Proteção de Dados – « LGPD ») doivent être respectées lorsque les données des résidents brésiliens sont traitées, ou lorsqu'un transfert de données nécessite leur application. Les parties conviennent d'adopter les CCT dans leur intégralité, telles qu'émises par l'Autorité Nationale de Protection des Données du Brésil (« ANPD »), sauf modification permise expressément par les clauses. Ces CCT sont intégrées par référence dans l'Accord, avec les sélections suivantes faites lorsque plus d'une option de texte est présentée :

OPTION B est sélectionnée pour la Section 3.1. L'Importateur peut effectuer un Transfert Ultérieur de Données Personnelles soumis au Transfert International de Données régi par ces Clauses, dans les cas et selon les conditions décrites ci-dessous et les dispositions de la CLAUSE 18.

OPTION A est sélectionnée pour la Section 4.1. Sans préjudice de l'obligation d'assistance mutuelle et des obligations générales des Parties, la Partie Désignée ci-dessous sera principalement responsable du respect des obligations définies dans ces Clauses :

a) Responsable de la publication du document prévu dans la CLAUSE 14 :

[x] Exportateur [ ] Importateur

b) Responsable de répondre aux demandes des personnes concernées traitées dans la CLAUSE 15 :

[x] Exportateur [ ] Importateur

c) Responsable de notifier l'incident de sécurité prévu dans la CLAUSE 16 :

[x] Exportateur [ ] Importateur

**ANNEXE ARABIE SAOUDITE : PDPL - Clauses contractuelles types**

Les Clauses Contractuelles Types de l'Arabie Saoudite (« CCT ») en vertu de la Loi sur la Protection des Données Personnelles (« PDPL ») doivent être intégrées lorsque les données des résidents saoudiens sont traitées, lorsqu'un transfert de données est soumis à la juridiction saoudienne, ou lorsque la loi saoudienne exige le respect des CCT saoudiennes. La version des CCT alignée avec le modèle décrit dans l'Annexe 2 est applicable dans son intégralité et est incorporée par référence dans l'Accord.