Règles d'entreprise contraignantes (BCR) de Novartis

(Règles d'entreprise contraignantes pour le Transfert de Données à caractère personnel en dehors de l'EEE+ en vertu de l'article 47 du RGPD et de l'article 16 (2) (e) de la LPD)

Les termes commençant par une majuscule dans ces Règles d'entreprise contraignantes (« BCR ») sont définis dans ces BCR, dans le Glossaire (Annexe 2) et dans l'Annexe 1 relative aux Personnes concernées visées par ces BCR.

Introduction

Chez Novartis, notre mission est de découvrir de nouvelles solutions afin d'améliorer et d'allonger la vie des personnes. Nous exploitons l'innovation scientifique permettant de résoudre certaines problématiques les plus complexes de la société en terme de santé. Nous découvrons et développons des traitements révolutionnaires et trouvons des moyens innovants de les offrir au plus grand nombre de personnes possible.

Notre Code d'éthique contient les principes et engagements fondamentaux concernant la conduite éthique des affaires, y compris l'engagement à l'égard du droit à la vie privée et de la protection des Données à caractère personnel de nos Employés et des autres Personnes concernées, y compris celles qui participent à la recherche biomédicale telles que définies à l'Annexe 1.

La Politique relative à l'utilisation éthique des données et de la technologie de Novartis, en vigueur depuis le 1er novembre 2024, et la documentation qui l'accompagne, établissent une norme commune sur la protection appropriée des Données à caractère personnel au sein de Novartis et de ses filiales (« Novartis », « Groupe Novartis » ou, le cas échéant, « Sociétés Novartis »). Elle énonce des principes généraux concernant le droit des individus à la vie privée et à des mesures de protection raisonnables de leurs Données à caractère personnel. Nous Traitons les Catégories spéciales de données, y compris les données médicales, avec une attention particulière.

Ces BCR complètent la Politique actuelle de Novartis relative à l'utilisation éthique des données et de la technologie, ainsi que la documentation qui l'accompagne et les procédures opérationnelles standard. Ces documents sont mis en place conformément au Droit applicable à la protection des données de l'EEE+. En cas de contradiction entre les termes des BCR et les directives de Novartis relatives aux Transferts de données transfrontaliers, les présentes BCR prévaudront pour les Sociétés Novartis qui sont liées par ces BCR.

1. Objet et champ d'application

L'objet des BCR est d'assurer un niveau de protection adéquat concernant les Transferts de Données à caractère personnel au sein du Groupe Novartis, d'une Société Novartis agissant en tant que Responsable du traitement à une Société Novartis agissant en tant que Responsable du traitement ou en tant que Sous-traitant.

Ces BCR s'appliquent au Transfert de Données à caractère personnel soumis au Droit applicable à la protection des données de l'EEE+ (ou qui était soumis au Droit applicable à la protection des données de l'EEE+ avant le Transfert de ces Données à caractère personnel à une Société Novartis en dehors de l'EEE+) vers une Société Novartis établie dans un pays pour lequel il n'existe pas de Décision d'adéquation.

Ces BCR s'appliquent aux Données à caractère personnel des Employés, des Consommateurs, des Clients professionnels et des autres Parties prenantes, des Fournisseurs et des Partenaires commerciaux, ainsi que des Personnes participant ou contribuant à la Recherche et à la pharmacovigilance, tels que définis dans le Glossaire de l'Annexe 2 et visés à l'Annexe 1.

2. Garanties d'application

2.1. Caractère contraignant vis-à-vis des Sociétés Novartis

Ces BCR constituent des Règles d'entreprise contraignantes pour le Transfert de Données à caractère personnel en dehors de l'EEE+ en vertu de l'article 47 du RGPD et de l'article 16 (2) (e) de la LPD et sont juridiquement contraignantes et s'appliquent à toutes les Sociétés Novartis qui ont signé l'Accord inter-entreprises BCR (Annexe 3), y compris leurs Employés.

Chaque Société Novartis qui signe l'Accord inter-entreprises BCR est responsable de l'administration et de la supervision de la mise en œuvre de ces BCR au sein de ses organisations respectives, y compris de rendre ces BCR contraignantes pour ses Employés.

Aucun Transfert de Données à caractère personnel ne doit être effectué à une Société Novartis, à moins que cette Société ne soit liée par ces BCR et puisse en assurer le respect.

Toute Société Novartis agissant en tant qu'Importateur de données qui, pour quelque raison que ce soit, n'est pas en mesure de se conformer à ces BCR, ou qui enfreint ces BCR, doit en informer sans délai la Société Novartis agissant en tant qu'Exportateur de données. Dans ce cas, la Société Novartis agissant en tant qu'Exportateur de Données doit suspendre le Transfert. En outre, la Société Novartis agissant en tant qu'Importateur de données doit, au choix de l'Exportateur de données, restituer ou supprimer immédiatement les Données à caractère personnel qui ont été Transférées en vertu des BCR dans leur intégralité, lorsque :

i. La Société Novartis agissant en tant qu'Exportateur de données a suspendu le Transfert, et le respect de ces BCR 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 ; ou

ii. La Société Novartis agissant en tant qu'Importateur de données est en violation substantielle ou persistante de ces BCR ; ou

iii. La Société Novartis agissant en tant qu'Importateur de données ne se conforme pas à une décision contraignante d'un tribunal compétent ou d'une Autorité de contrôle compétente concernant ses obligations en vertu de ces BCR.

La Société Novartis, agissant en tant qu'Importateur de données, doit certifier la suppression des données et de toute copie de celles-ci à la Société Novartis agissant en tant qu'Exportateur de données.

Jusqu'à ce que les Données à caractère personnel soient supprimées ou renvoyées, la Société Novartis agissant en tant qu'Importateur de données doit continuer à assurer le respect de ces BCR.

Dans le cas où le Droit local applicable à la protection des données à la Société Novartis agissant en tant qu'Importateur de données interdit le retour ou la suppression des Données à caractère personnel Transférées, la Société Novartis agissant en tant qu'Importateur de données doit continuer à assurer le respect de ces BCR et ne Traitera les Données à caractère personnel que dans la mesure et aussi longtemps que l'exige cette législation locale.

2.2. Disponibilité des BCR

Les Personnes concernées ont le droit d'accéder facilement aux BCR. Chaque Société Novartis qui signe l'Accord inter-entreprises BCR est responsable de mettre à la disposition des Personnes concernées des informations sur les droits des Personnes concernées tels qu'ils sont couverts par les BCR, y compris les moyens d'exercer ces droits. Les BCR seront publiées sur le site internet et l'intranet de Novartis.

2.3. Caractère contraignant vis-à-vis des Employés

Les Employés sont liés par ces BCR et ont le devoir de se conformer aux obligations énoncées dans les présentes.

Les Employés qui enfreignent ces BCR peuvent faire l'objet de procédures disciplinaires, telles que définies par la Société Novartis concernée.

2.4. Rôle de Novartis Pharma S.A.S.

Novartis a désigné Novartis Pharma S.A.S. (« Novartis France ») en tant que Société Novartis au sein de l'EEE+ ayant des responsabilités déléguées en matière de protection des données aux fins de ces BCR. Ces responsabilités comprennent la surveillance, la coordination et la mise en œuvre des BCR, ainsi que l'acceptation de la responsabilité en cas de violation des BCR par les Sociétés Novartis en dehors de l'EEE+, comme décrit plus en détail à la section 7 de ces BCR.

3. Principes applicables au Traitement des Données à caractère personnel

3.1. Obligations des Responsables du traitement

Une Société Novartis agissant en tant que Responsable du traitement doit se conformer aux principes suivants lors du Traitement des Données à caractère personnel :

i. **Transparence :**

   a. Collecter et Traiter les Données à caractère personnel de manière équitable, légale et transparente (légalité, équité et transparence) ;

   b. Information : Veiller à ce que les Personnes concernées soient informées du Traitement et du Transfert de leurs Données à caractère personnel (transparence) conformément au Droit applicable à la protection des données de l'EEE+ et obtenir le consentement de la Personne concernée, le cas échéant. La notice d'information doit comporter les informations requises par les articles 13 et 14 du RGPD et l'article 19 de la LPD, y compris, le cas échéant :

      i. L'identité et les coordonnées du ou des Responsables du traitement ;

      ii. Les coordonnées du Délégué à la protection des données du Groupe (ou de tout autre délégué à la protection des données compétent) ;

      iii. Pour quelles finalités et sur quelle base juridique les Données à caractère personnel seront Traitées et Transférées ;

iv. Lorsque le Traitement est fondé sur l'intérêt légitime du Responsable du traitement, la description de l'intérêt poursuivi ;

v. Les destinataires ou les catégories de destinataires des Données à caractère personnel ;

vi. Le cas échéant, le fait que le Responsable du traitement a l'intention d'effectuer un Transfert de Données à caractère personnel en dehors de l'EEE+, et si la destination du Transfert est couverte par une Décision d'adéquation, ou l'existence de garanties appropriées, telles que les Clauses contractuelles types, et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;

vii. La durée pendant laquelle les Données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

viii. Des informations sur les droits des Personnes concernées en vertu des BCR, y compris les droits des tiers bénéficiaires, et les moyens d'exercer ces droits ;

ix. Lorsque le Traitement est fondé sur le consentement des Personnes concernées, le droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du Traitement ou la licéité du Traitement non fondé sur le consentement ;

x. Le droit d'introduire une réclamation auprès de l'Autorité de contrôle compétente en vertu de la section 7.2 ;

xi. Si la fourniture de Données à caractère personnel est une exigence légale ou contractuelle, ou une exigence nécessaire à la conclusion d'un contrat, des informations sur la question de savoir si la Personne concernée est tenue de fournir les Données à caractère personnel et les conséquences éventuelles de la non-fourniture de ces Données à caractère personnel ;

xii. L'existence d'une prise de décision automatisée, y compris le profilage, et des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues d'un tel Traitement pour la Personne concernée ;

xiii. Lorsque les Données à caractère personnel n'ont pas été obtenues directement auprès de la Personne concernée, la description des catégories de Données à caractère personnel et la source des Données à caractère personnel.

ii. **Traitement légitime et licite :**

a. Traiter uniquement des Données à caractère personnel qui sont pertinentes et non excessives au regard des finalités (minimisation des données) ;

b. S'assurer que les Données à caractère personnel sont Traitées légalement en s'assurant qu'il existe une base juridique appropriée en vertu du Droit applicable à la protection des données de l'EEE+, conformément à la Politique relative à l'utilisation éthique des données et de la technologie de Novartis et à tout document spécifique

pertinent et à la ou aux procédures opérationnelles standard locales, le cas échéant ; et

c. S'assurer que le Traitement de Catégories spéciales des données répond à l'une des exceptions prévues par le Droit applicable à la protection des données de l'EEE+, et que les Données à caractère personnel relatives aux condamnations pénales et aux infractions ne seront Traitées que conformément au Droit applicable à la protection des données de l'EEE+ applicable, et conformément aux règles et orientations pertinentes de la Politique relative à l'utilisation éthique des données et de la technologie de Novartis, dans tout autre document pertinent et de la ou les procédures opérationnelles standard locales.

iii. **Traitement responsable et durable :**

a. Traiter et Transférer des Données à caractère personnel uniquement pour des finalités professionnelles ou règlementaires spécifiques, explicites et légitimes et ne pas poursuivre le Traitement des Données à caractère personnel d'une manière incompatible avec ces finalités (limitation des finalités) ;

b. Protection des données dès la conception et par défaut (Privacy by design et Privacy by default) : Prendre en compte le droit à la protection des données au moment du développement et de la conception des produits, services et applications (protection des données dès la conception) et assurer que, par défaut, seules les Données à caractère personnel qui sont nécessaires pour chaque finalité spécifique du Traitement soient effectivement Traitées (protection des données par défaut) ;

c. Exactitude : S'assurer que les Données à caractère personnel sont exactes, complètes et, si cela est nécessaire, mises à jour ;

d. Droits des Personnes concernées : Établir une procédure pour prévoir les droits des Personnes concernées en vertu du Droit applicable à la protection des données de l'EEE+. Cela inclut le droit d'accès, de rectification, d'effacement, de limitation, d'information relative à la rectification ou l'effacement ou la limitation des données, la portabilité des données, l'opposition au Traitement, le droit de demander à une autorité indépendante la protection judiciaire et le droit de ne pas faire l'objet de décisions uniquement fondées sur un Traitement automatisé, y compris le profilage ;

e. Transferts : Ne communiquer des Données à caractère personnel qu'à d'autres Sociétés Novartis et à des tiers qui se sont soit engagés à respecter ces BCR (applicables uniquement aux Sociétés Novartis), soit qui sont établis dans des pays disposant d'un niveau adéquat de protection des données tel que défini par une Décision d'adéquation, soit répondant à tout autre moyen juridique de Transfert de Données à caractère personnel tel que prévu par le Droit applicable à la protection des données de l'EEE+ ;

f. Sous-traitants : Préalablement à la communication de Données à caractère personnel à une Société Novartis agissant en tant que Sous-traitant ou à un tiers agissant en tant que Sous-traitant, communiquer au Sous-traitant des instructions concernant le Traitement des Données à caractère personnel ; conclure des contrats écrits qui incluent les exigences établies par le Droit applicable à la protection des données de l'EEE+ et le paragraphe 3.2 de ces BCR ;

g. Tiers : S'assurer que des procédures sont en place afin que les Sociétés Novartis ou les tiers, autorisés à avoir accès aux Données à caractère personnel, y compris les Sous-traitants, respectent et maintiennent la confidentialité et la sécurité des Données à caractère personnel de manière appropriée et se conforment aux principes énoncés dans ces BCR ;

h. Prise de décision automatisée : En cas de prise de décision reposant exclusivement sur le fondement d'un Traitement automatisé qui affecte de manière significative la Personne concernée, y compris le profilage, définir des mesures de protection adéquates visant à protéger les droits et libertés et les intérêts légitimes de la Personne concernée, et accorder à la Personne concernée le droit de faire réviser manuellement la décision et de faire valoir ses observations.

iv. **Sécurité, Intégrité et Qualité :**

a. Novartis ne donnera à ses Employés et aux autres membres du personnel l'accès aux Données à caractère personnel que dans la mesure nécessaire pour effectuer le Traitement et effectuer leur travail. Novartis imposera des obligations de confidentialité aux Employés et aux autres membres du personnel ayant accès aux Données à caractère personnel.

b. Compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du Traitement ainsi que du risque de probabilité et de gravité variables pour les droits et libertés de la Personne concernée, Novartis prend des mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel contre toute destruction accidentelle ou illicite, perte, altération, divulgation, accès ou autre Traitement non autorisés (« **Violation de la sécurité** »), inclut, le cas échéant, des mesures renforcées pour assurer la sécurité des Catégories spéciales de données (intégrité et confidentialité) ;

c. Gestion des Violations de sécurité : Mettre en place une procédure permettant de documenter les Violations de sécurité, de mettre cette documentation à la disposition de l'Autorité de contrôle compétente sur demande (y compris les faits, les effets et les mesures correctives), et de faire remonter les Violations de sécurité dans les meilleurs délais en interne à la Société Novartis responsable, au Délégué à la protection des données du Groupe ainsi qu'à la Société Novartis agissant en tant que Responsable du traitement lorsqu'une Société Novartis agissant en tant que Sous-traitant prend connaissance de la Violation de sécurité, et, si le Droit applicable à la protection des données de l'EEE+ l'exige, notifier les Autorités de contrôle compétentes dans les meilleurs délais et, si possible, au plus tard 72 heures après avoir pris connaissance de la Violation de sécurité, et dans les meilleurs délais aux Personnes concernées, lorsque la Violation de sécurité est susceptible d'entraîner un risque élevé pour leurs droits et libertés conformément aux exigences de l'article 34 du RGPD.

v. **Durée de conservation limitée :** S'assurer que les Données à caractère personnel ne sont conservées qu'aussi longtemps que nécessaire pour les finalités pour lesquelles elles sont Traitées, à moins que des échéanciers globaux de conservation légaux ou internes prépondérants n'exigent une période de conservation plus longue ou plus courte (limitation de la conservation).

3.2. Sous-traitants

Les Transferts à des Sous-traitants tiers, ainsi qu'à des Sous-traitants internes, par un Responsable du traitement Novartis doivent se faire sur la base d'un contrat écrit valablement conclu et conforme aux exigences du Droit applicable à la protection des données de l'EEE+ (« **Contrat de sous-traitance** »). Le Contrat de sous-traitance doit inclure les dispositions suivantes :

i. Le Sous-traitant ne Traitera les Données à caractère personnel que pour les finalités autorisées par le Responsable du traitement et sur instruction documentée de ce dernier, y compris en ce qui concerne les Transferts de Données à caractère personnel à des Sous-traitants non couverts par une Décision d'adéquation, à moins que le Sous-traitant ne soit tenu d'y procéder en vertu des exigences impératives applicables au Sous-traitant et notifiées à Novartis ;

ii. Le Sous-traitant doit préserver la confidentialité des Données à caractère personnel et imposer des obligations de confidentialité au personnel ayant accès aux Données à caractère personnel ;

iii. Le Sous-traitant doit prendre des mesures de sécurité techniques, physiques et organisationnelles appropriées pour protéger les Données à caractère personnel ;

iv. Le Sous-traitant n'autorisera les Sous-traitants ultérieurs à Traiter les Données à caractère personnel dans le cadre de ses obligations envers le Responsable du traitement (a) qu'avec l'autorisation écrite préalable, spécifique ou générale, du Responsable du traitement et (b) sur la base d'un contrat écrit ou électronique valablement conclu avec le Sous-traitant ultérieur, qui impose des obligations de Traitement liées à la protection des données similaires à celles imposées au Sous-traitant en vertu du Contrat de sous-traitance et à condition que le Sous-traitant demeure pleinement responsable devant le Responsable du traitement de l'exécution par les Sous-traitants ultérieurs de leurs obligations conformément aux termes du Contrat de sous-traitance. Dans le cas où le Responsable du traitement donne une autorisation écrite générale pour l'implication de Sous-traitants ultérieurs, le Sous-traitant informera le Responsable du traitement de tout changement prévu concernant ses Sous-traitants ultérieurs et donnera au Responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements sur la base de motifs raisonnables ;

v. Le Responsable du traitement doit être en mesure de vérifier les mesures de sécurité susmentionnées prises par le Sous-traitant (a) par l'obligation du Sous-traitant de soumettre ses installations pertinentes utilisées pour Traiter les Données à caractère personnel à des audits et inspections par le Responsable du traitement, un tiers pour le compte du Responsable du traitement ou toute autorité publique compétente ; ou (b) au moyen d'une déclaration émise par un expert tiers indépendant qualifié pour le compte du Sous-traitant certifiant que les installations du Sous-traitant utilisées pour le Traitement des Données à caractère personnel sont conformes aux exigences du Contrat de sous-traitance ;

vi. Le Sous-traitant informera immédiatement le Responsable du traitement de tout incident de sécurité impliquant des Données à caractère personnel ;

vii. Le Sous-traitant gèrera immédiatement et de manière appropriée :

   a. Les demandes pour obtenir les informations nécessaires pour démontrer la conformité du Sous-traitant à remplir ses obligations en vertu du Contrat de sous-

traitance et informera le Responsable du traitement si des instructions du Responsable du traitement à cet égard constituent une violation du Droit applicable à la protection des données ;

b. Les demandes et les plaintes des Personnes concernées, conformément aux instructions du Responsable du traitement ;

c. Les demandes d'assistance du Responsable du traitement dans la mesure où cela est raisonnablement nécessaire pour assurer la conformité du Traitement des Données à caractère personnel avec le Droit applicable à la protection des données de l'EEE+, et le Sous-traitant doit aider le Responsable du traitement à assurer le respect des obligations relatives à la sécurité des Données à caractère personnel, à la notification des Violations de sécurité, à l'analyse d'impact relative à la protection des données, en tenant compte de la nature du Traitement et des informations dont dispose le Sous-traitant ; et

d. À la résiliation du Contrat de sous-traitance, le Sous-traitant doit, selon le choix du Responsable du traitement, renvoyer les Données à caractère personnel et les copies de celles-ci au Responsable du traitement ou supprimer de manière sécurisée ces Données à caractère personnel, sauf dans la mesure où le Contrat de sous-traitance ou le Droit applicable à la protection des données de l'EEE+ en dispose autrement.

Une Société Novartis qui souhaite Transférer des Données à caractère personnel à un Sous-traitant tiers doit sélectionner un tiers offrant des garanties suffisantes de sa capacité à assurer la sécurité des Données à caractère personnel.

3.3. Transferts à des tiers situés dans un pays en dehors de l'EEE+ pour lequel il n'existe pas de Décision d'adéquation

La Société Novartis qui souhaite Transférer des Données à caractère personnel à un tiers situé dans un pays établi en dehors de l'EEE+ pour lequel il n'existe pas de Décision d'adéquation, doit mettre en œuvre des garanties appropriées pour les Transferts en vertu du Droit applicable à la protection des données de l'EEE+, par exemple (i) en concluant des Clauses contractuelles types appropriées, ou (ii) si la conclusion de Clauses contractuelles types n'est pas possible, s'appuyer sur une dérogation en vertu du Droit applicable à la protection des données de l'EEE+, avant le Transfert de toute Donnée à caractère personnel.

4. Programme de sensibilisation et de formation

Novartis s'engage à fournir une formation de base relative à la vie privée et à la protection des données, incluant les exigences des BCR, à ses Employés, ainsi que des formations spécifiques aux Employés qui ont un accès régulier aux Données à caractère personnel et les Traitent, ainsi qu'à ceux en charge du développement des outils et systèmes d'information en lien avec les Traitements des Données à caractère personnel. Le cas échéant, la formation sera également dispensée à d'autres personnes qui Traitent des Données à caractère personnel dans le cadre de leurs fonctions ou responsabilités respectives utilisant les systèmes de technologie de l'information de Novartis ou travaillant principalement dans les locaux de Novartis. La formation ciblée appréhende les normes et

les exigences de protection des données spécifiques en lien avec la nature de leur activité. Les formations doivent être organisées conformément aux termes du programme de formation à la protection des données visé en Annexe 4 des présentes.

5. Programme de conformité, de surveillance et d'audit

5.1. Organisation relative à la protection des Données à caractère personnel

L'approche de Novartis en matière de gestion de la protection des données est fondée sur le principe de responsabilité (« Accountability »). Les Sociétés Novartis sont responsables du respect de la conformité à ces BCR, aux lois et réglementations locales en matière de protection des données, et sont responsables de la mise en œuvre du programme de protection des données du Groupe Novartis (« Programme de protection des données du Groupe ») au niveau national. Le Programme de protection des données du Groupe vise à accompagner les activités locales et à s'assurer de la conformité des projets transfrontaliers, ceci incluant les Transferts internationaux de données en lien avec des activités d'externalisation ainsi qu'avec le déploiement de bases de données mondiales.

Dans le but d'assurer la conformité avec les lois, les règlementations et nos procédures en matière de protection des données, nous nous efforçons d'intégrer les principes et exigences en matière de protection des données dans nos processus métiers et nos systèmes d'information ainsi que de promouvoir le principe de responsabilité au sein du Groupe Novartis, et ce au travers de programmes de sensibilisation et de formation.

Novartis a établi une organisation globale de protection des données DPDAI (Protection des données, Digital et Intelligence Artificielle) au sein de la fonction Éthique, Risque & Conformité, composée de Responsables DPDAI au niveau national, rapportant indirectement au Responsable Global DPDAI, dans les conditions décrites à l'Annexe 6.

5.2. Programme de surveillance et d'audit

Novartis s'engage à réaliser de manière régulière des contrôles de conformité en matière de protection des données, et ce afin de s'assurer que les principes de protection des données, y compris ceux inclus dans ces BCR, sont effectivement respectés. Ces contrôles peuvent être réalisés de différentes manières :

i. Tel que requis par les procédures internes, les Sociétés Novartis réaliseront des analyses d'impact relatives à la protection des données lorsqu'un Traitement est susceptible d'entraîner un risque élevé pour les droits et libertés d'une Personne concernée. Lorsque l'évaluation montre que, malgré les mesures d'atténuation prises par Novartis, le Traitement présente toujours un risque élevé résiduel pour les droits et libertés des Personnes concernées, l'Autorité de contrôle compétente sera consultée avant que ce Traitement n'ait lieu.

ii. Chaque Société Novartis qui Traite des Données à caractère personnel sera régulièrement soumise à des contrôles prédéfinis liés à la protection des données sous la direction de l'équipe Corporate DPDAI. Les résultats, incluant un plan de remédiation, seront documentés et communiqués au Responsable Global DPDAI. Les résultats de ces contrôles de protection des données et du plan de remédiation doivent être communiqués, en cas de demande, à l'Autorité de contrôle compétente.

iii. L'équipe Audit Interne de Novartis vérifiera les activités professionnelles à intervalles

réguliers sur la base de l'évaluation des risques, et en tout cas au moins une fois tous les trois ans, les procédures et les systèmes d'information impliquant le Traitement de Données à caractère personnel pour s'assurer qu'ils sont conformes aux BCR. L'indépendance de l'équipe Audit Interne de Novartis sera garantie quant à la réalisation de ces audits. Ces audits couvrent tous les aspects des BCR, y compris les méthodes permettant de s'assurer que des mesures correctives seront prises. Les audits doivent être effectués dans le cadre des activités régulières d'audit interne de Novartis, telles qu'approuvées par le Comité d'audit et de conformité (ACC) ou à la demande du Responsable Global DPDAI. Le Responsable Global DPDAI peut demander qu'un audit tel que spécifié dans la présente section soit effectué par un auditeur externe accrédité qui se verra garantir l'indépendance dans l'exercice de ses fonctions. Les résultats de ces audits, incluant un plan de remédiation, doivent être communiqués à la direction, au niveau du groupe, de la Division et de l'entreprise, incluant le Comité exécutif de Novartis, l'ACC, ainsi que le Responsable Global DPDAI. Une copie des résultats complets de l'audit relatifs au respect des BCR doit être fournie à l'Autorité de contrôle compétente sur demande.

iv. Novartis a mis en place une fonction Revue & Remédiation DPDAI rattachée à l'équipe Ethique, Risque & Conformité Assurance Corporate, qui effectue des revues de surveillance périodiques des différentes unités organisationnelles de Novartis afin d'identifier et de superviser la correction des non-conformités potentielles dans la mise en œuvre du Programme de protection des données de Novartis et des BCR.

v. Novartis tient des registres des activités de Traitement facilement accessibles conformément aux exigences du Droit applicable à la protection des données de l'EEE+, et en particulier de l'article 30.1 du RGPD. Ces registres comprendront (i) le nom et les coordonnées de la Société Novartis qui est le Responsable du traitement des Données à caractère personnel, (ii) les finalités du Traitement, (iii) une description des catégories de Données à caractère personnel et des catégories de Personnes concernées, (iv) des informations sur les Transferts de Données à caractère personnel et, dans la mesure du possible, (v) les durées de conservation, et (vi) une description générale des mesures de sécurité. Une copie de ces informations sera fournie à l'Autorité de contrôle compétente sur demande. Novartis tient également des registres des activités de Traitement facilement accessibles pour les Sociétés Novartis agissant en tant que Sous-traitants, conformément aux exigences du Droit applicable à la protection des données de l'EEE+, et en particulier de l'article 30.2 du RGPD. Ces registres comprendront (i) le nom et les coordonnées du ou des Sous-traitants et de chaque Responsable du traitement pour le compte duquel le Sous-traitant agit, (ii) les catégories de Traitements effectués pour le compte de chaque Responsable du traitement, (iii) le cas échéant, les Transferts de Données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées, (iv) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées dans le RGPD.

6. Procédure de gestion des plaintes

Si une Personne concernée considère qu'il y a eu violation de ces BCR, elle doit le signaler à l'équipe DPDAI (global.privacy_office@novartis.com), désignée par Novartis conformément à l'article 37 du RGPD, et ce dans les conditions prévues par la procédure définie en Annexe 5.

7. Responsabilité et droits des tiers bénéficiaires

7.1. Droits des tiers bénéficiaires

Les droits contenus dans la présente section s'ajoutent à tout autre droit ou recours que les Personnes concernées peuvent autrement avoir en vertu du Droit applicable à la protection des données de l'EEE+ ou des lois applicables, et ne portent pas préjudice à ceux-ci.

Si Novartis en tant que Responsable du traitement, enfreint ces BCR en ce qui concerne le Traitement des Données à caractère personnel d'une Personne concernée, la Personne concernée peut, en tant que tiers bénéficiaire, faire appliquer les sections 2.2, 3, 6, 7, 8.2, 9, 10.2, 10.3 et l'Annexe 5 de ces BCR, en se référant si nécessaire aux informations incluses dans les Annexes 1, 2 et 7.

Les Personnes concernées sont encouragées à suivre d'abord la procédure de gestion des plaintes, qui les aidera à adresser toute plainte relative à la protection des données en interne. Les Personnes concernées sont toutefois libres d'introduire une réclamation directement auprès des Autorités de contrôle compétentes ou d'introduire une action en justice devant les tribunaux compétents en vertu de la section 7.2 à tout moment.

7.2. Juridiction et responsabilité

Dans le cas où une Personne concernée a une revendication en vertu de la section 7.1, la Personne concernée peut, selon son choix, soumettre une plainte en vertu de la présente section auprès de l'Autorité de contrôle de l'État membre de sa résidence habituelle, de son lieu de travail ou du lieu de l'infraction présumée, ou introduire une action en justice devant les tribunaux compétents (le cas échéant) :

i. Dans le pays de l'EEE+ où la Société Novartis est établie en tant que Responsable du traitement des Données à caractère personnel concernées, à l'encontre de cette Société ;

ii. Dans le pays de l'EEE+ où la Personne concernée a sa résidence habituelle ou son lieu de travail ;

iii. En France, contre Novartis France. Novartis France s'assurera que des mesures adéquates sont prises pour remédier aux violations de ces BCR par une Société Novartis. Novartis France se conformera à l'avis des Autorités de contrôle compétentes émis sur l'interprétation et l'application de ces BCR.

Les Personnes concernées ont le droit d'être représentées par un organisme, une organisation ou une association à but non lucratif si, et dans la mesure où le Droit applicable le permet.

Novartis France accepte la responsabilité d'une violation par une Société Novartis située en dehors de l'EEE+, bien que Novartis France puisse faire valoir toute défense que cette Société Novartis ou le Sous-traitant tiers aurait pu faire valoir.

7.3. Droit de réclamer des dommages et intérêts et charge de la preuve

Dans le cas où une Personne concernée a une revendication en vertu de la section 7.1, cette Personne concernée a droit à une indemnisation pour les dommages matériels et moraux subis par la

Personne concernée résultant d'une violation de ces BCR dans la mesure prévue par le Droit applicable à la protection des données de l'EEE+, conformément à la section 7.2.

Afin d'introduire une demande de dommages et intérêts, la Personne concernée doit démontrer qu'elle a subi les dommages correspondants et établir des faits qui montrent qu'il est plausible que le dommage soit survenu en raison d'une violation de ces BCR. Novartis doit alors prouver que les dommages subis par cette Personne concernée ne sont pas imputables à Novartis ou à un Sous-traitant ou faire valoir d'autres moyens de défense applicables.

8. Assistance mutuelle et coopération

8.1. Assistance mutuelle

Les Sociétés Novartis liées par les BCR s'engagent à coopérer et à s'assister mutuellement pour gérer de manière appropriée :

i. Les demandes émanant des Autorités de contrôle compétentes concernant l'application des BCR ;

ii. Les demandes et enquêtes émanant d'autres autorités publiques lorsque cela peut avoir un impact sur l'application des BCR ;

iii. Les demandes et réclamations des Personnes concernées.

La Société Novartis qui est responsable du Traitement auquel se rapporte une demande, une réclamation ou une plainte, supportera tous les frais occasionnés et remboursera Novartis France.

8.2. Coopération avec les Autorités de contrôle compétentes

Les Sociétés Novartis liées par les BCR s'engagent à coopérer avec les Autorités de contrôle compétentes, en particulier en répondant de manière diligente et dans des délais raisonnables à toute demande qui pourrait émaner de leur part en lien avec l'interprétation et l'application des BCR et à prendre en compte leurs conseils et recommandations à cet égard.

Les Sociétés Novartis qui sont liées par les BCR s'engagent à accepter d'être inspectées et/ou auditées, y compris, le cas échéant, sur site, par les Autorités de contrôle compétentes pour vérifier le respect de ces BCR. Elles s'engagent également à fournir à l'Autorité de contrôle compétente, sur demande, toute information sur les Traitements couverts par les BCR.

Novartis se conformera aux décisions de l'Autorité de contrôle compétente sur les questions liées aux BCR. Tout litige relatif à l'exercice par l'Autorité de contrôle compétente du contrôle du respect des BCR sera résolu par les tribunaux de l'État membre de cette Autorité de contrôle.

9. Mises à jour des BCR

Novartis se réserve la possibilité de mettre à jour les BCR si cela est justifié par un Objectif Professionnel Légitime, si les lois, réglementations et orientations réglementaires applicables en matière de protection des données de l'EEE+, ainsi que la jurisprudence, ont changé, ou si les Autorités de contrôle ont demandé que certaines modifications soient apportées. Les décisions seront prises par l'équipe de direction DPDAI.

Les modifications significatives qui ont un impact significatif sur la protection offerte par ces BCR ou

sur les BCR elles-mêmes seront communiquées rapidement par le Responsable DPDAI Région Europe aux Sociétés Novartis liées par les BCR et à l'Autorité de contrôle chef de file. Le Responsable DPDAI Région Europe sera également chargé de coordonner les réponses de Novartis aux questions de l'Autorité de contrôle chef de file à ce sujet. Lorsqu'elle signale tout changement à l'Autorité de contrôle chef de file, Novartis inclura une brève explication des raisons justifiant les changements. Les autres modifications mineures apportées aux BCR ou à la liste des Sociétés Novartis liées par les BCR seront signalées dans les meilleurs délais aux Sociétés Novartis, et une fois par an à l'Autorité de contrôle chef de file, avec une brève explication de ces modifications. Novartis publiera sur son site internet dans les meilleurs délais toute version actualisée des BCR et la liste des membres des BCR figurant à l'Annexe 7.

En outre, Novartis a pris des mesures pour qu'un Responsable national DPDAI soit nommé pour assumer la responsabilité de tenir à jour une liste des Sociétés Novartis liées par les BCR, de suivre et d'enregistrer les mises à jour des BCR et de s'assurer que les informations nécessaires sont fournies aux Personnes concernées et à l'Autorité de contrôle compétente sur demande.

10. Règlementation applicable

10.1. Règlementation applicable

Les Personnes concernées ont le droit de faire valoir tous les droits et recours dont elles peuvent disposer en vertu des lois locales applicables. Lorsque la loi locale applicable offre plus de protection que ces BCR, la loi locale s'applique. Lorsque ces BCR offrent une protection supérieure à celle de la loi locale applicable ou prévoient des garanties, des droits ou des recours supplémentaires pour les Personnes concernées, ces BCR prévaudront.

10.2. Conflit avec les lois locales applicables

Les Sociétés Novartis n'utiliseront les BCR comme outil pour les Transferts que si elles ont évalué que la législation et les pratiques du pays de destination en dehors de l'EEE+ s'appliquent au Traitement des Données à caractère personnel par la Société Novartis agissant en tant qu'Importateur de données, y compris toute exigence de divulgation de Données à caractère personnel ou toute mesure autorisant l'accès par les autorités publiques, n'empêchent pas la Société Novartis importatrice de remplir ses obligations en vertu de ces BCR. Ces exigences s'appliquent également aux Transferts ultérieurs, qui sont des Transferts d'un Importateur de données vers un autre Importateur de données ou un tiers établi dans un pays non-membre de l'EEE+.

Lors de l'évaluation des lois et pratiques du pays non-membre de l'EEE+ susceptibles d'affecter le respect des engagements contenus dans ces BCR, les Sociétés Novartis doivent tenir dûment compte, en particulier, des éléments suivants :

i. Les circonstances spécifiques des Transferts, y compris :

   a. Les finalités pour lesquelles les Données à caractère personnel sont Transférées et Traitées ;

   b. Les types d'entités impliquées dans le Traitement ;

   c. Le secteur économique dans lequel le Transfert a lieu ;

d. Les catégories et le format des Données à caractère personnel Transférées ;

e. Le lieu du Traitement, y compris le stockage ; et

f. Les canaux de transmission utilisés.

ii. Les lois et pratiques du pays de destination hors EEE+ pertinentes à la lumière des circonstances du Transfert, y compris celles exigeant la divulgation des données aux autorités publiques, et celles prévoyant l'accès à ces données pendant le transit entre le pays de la Société Novartis agissant en tant qu'Exportateur de données et le pays de la Société Novartis agissant en tant qu'Importateur de données, ainsi que les limitations et mesures de protection applicables, ou autorisant l'accès par ces autorités et celles qui prévoient l'accès à ces Données à caractère personnel.

iii. Toutes les garanties contractuelles, techniques ou organisationnelles pertinentes mises en place pour compléter les garanties prévues par ces BCR, y compris les mesures appliquées lors de la transmission et du Traitement des Données à caractère personnel dans le pays de destination.

Lorsque des garanties supplémentaires à celles prévues par les BCR doivent être mises en place, Novartis France et le Responsable Global DPDAI concerné seront informés et impliqués dans cette évaluation.

Novartis documentera de manière appropriée cette évaluation, ainsi que les mesures supplémentaires sélectionnées et mises en œuvre. Elle devra mettre cette documentation à la disposition des Autorités de contrôle compétentes sur demande.

Toute Société Novartis agissant en tant qu'Importateur de données doit informer rapidement l'Exportateur de données si elle a des raisons de croire que l'Importateur de données est ou est devenu soumis à des lois ou à des pratiques qui l'empêcheraient de remplir ses obligations en vertu des BCR, y compris à la suite d'une modification des lois du pays tiers ou d'une mesure (telle qu'une demande de divulgation). Ces informations doivent également être fournies à Novartis France. Dans ce cas, la Société Novartis agissant en tant qu'Exportateur de données, ainsi que Novartis France et le Responsable Global DPDAI ou la Fonction concernés, doivent s'engager à identifier rapidement les mesures supplémentaires (par exemple, des mesures techniques ou organisationnelles visant à assurer la sécurité et la confidentialité) à adopter par la Société Novartis agissant en tant qu'Exportateur de données et/ou Importateur de données, afin de lui permettre de remplir ses obligations en vertu des BCR. Il en va de même si une Société Novartis agissant en tant qu'Exportateur de données a des raisons de croire qu'une Société Novartis agissant en tant qu'Importateur de données ne peut plus remplir ses obligations en vertu de ces BCR.

Lorsque la Société Novartis agissant en tant qu'Exportateur de données, avec Novartis France et le Responsable DPDAI concerné, estime que les BCR ne peuvent être respectées pour un Transfert ou un ensemble de Transferts, ou sur instruction des Autorités de contrôle compétentes, elle s'engage à suspendre le Transfert ou l'ensemble des Transferts en cause, ainsi que tous les Transferts pour lesquels la même appréciation et le même raisonnement conduiraient à un résultat similaire, jusqu'à ce que la conformité soit à nouveau assurée ou que le Transfert soit terminé. À la suite d'une telle suspension, la Société Novartis agissant en tant qu'Exportateur de données doit mettre fin au Transfert ou à l'ensemble des Transferts si les BCR ne peuvent être respectées et si la conformité aux BCR n'est pas rétablie dans un délai d'un mois à compter de la suspension. Dans ce cas, les Données à caractère personnel qui ont été Transférées avant la suspension, ainsi que toute copie de

celles-ci, doivent, au choix de la Société Novartis agissant en tant qu'Exportateur de données, lui être restituées ou être détruites dans leur intégralité.

Le Responsable DPDAI compétent informera toutes les autres Sociétés Novartis de l'évaluation effectuée et de ses résultats, afin que des mesures supplémentaires identifiées soient appliquées dans le cas où le même type de Transferts est effectué par une Société Novartis ou, lorsque des mesures supplémentaires efficaces n'ont pas pu être mises en place, que les Transferts en question sont suspendus ou être terminés.

Les Sociétés Novartis agissant en tant qu'Exportateurs de données doivent surveiller, de manière continue et, le cas échéant, en collaboration avec les Sociétés Novartis agissant en tant qu'Importateurs de données, l'évolution de la situation dans les pays tiers vers lesquels les Exportateurs de données ont Transféré des Données à caractère personnel qui pourrait affecter l'évaluation initiale du niveau de protection et les décisions prises en conséquence concernant ces Transferts.

En cas de conflit entre la loi locale applicable et ces BCR, y compris lorsqu'une exigence légale de Transfert de Données à caractère personnel entre en conflit avec le Droit applicable à la protection des données de l'EEE+, le Responsable Global DPDAI doit être consulté pour déterminer comment se conformer à ces BCR et résoudre le conflit dans la mesure du possible compte tenu des exigences légales applicables à la Société Novartis concernée. Le Responsable Global DPDAI peut demander l'avis de l'Autorité de contrôle chef de file ou d'une autre autorité publique compétente.

10.3. Accès gouvernemental aux Données à caractère personnel

Sous réserve du paragraphe suivant, une Société Novartis agissant en tant qu'Importateur de données informera rapidement la Société Novartis agissant en tant qu'Exportateur de données et, si possible, les Personnes concernées, si Novartis : (i) reçoit une demande juridiquement contraignante en vertu des lois du pays de destination, ou d'un autre pays non-membre de l'EEE+, pour la divulgation de Données à caractère personnel de la part d'une autorité chargée de l'application de la loi ou d'un organisme de sécurité de l'État (« **Demande de divulgation** ») ; ou (ii) prend connaissance d'un accès direct par les autorités publiques aux Données à caractère personnel Transférées en vertu de ces BCR (« **Accès** »). La Société Novartis agissant en tant qu'Importateur de données fournira à la Société Novartis agissant en tant qu'Exportateur de données autant d'informations pertinentes que possible sur l'Accès ou la Demande de divulgation à intervalles réguliers. Les notifications d'une Demande de divulgation doivent inclure des informations sur les données demandées, l'organisme demandeur, la base juridique de la divulgation et la réponse fournie. Si la Société Novartis agissant en tant qu'Importateur de données se voit ou va se voir interdire partiellement ou totalement de fournir les informations susmentionnées, elle fera ses meilleurs efforts pour obtenir une levée de cette interdiction, en vue de communiquer autant d'informations que possible et dans les meilleurs délais, et documentera ses meilleurs efforts afin de pouvoir les démontrer à la demande de la Société Novartis agissant en tant qu'Exportateur de données.

L'Importateur de données conservera les informations susmentionnées aussi longtemps que les Données à caractère personnel sont soumises aux garanties prévues par les BCR, et les mettra à la disposition des Autorités de contrôle compétentes sur demande.

La Société Novartis agissant en tant qu'Importateur de données fournira à la Société Novartis agissant en tant qu'Exportateur de données, à intervalles réguliers, autant d'informations pertinentes

que possible sur les demandes reçues (en particulier, le nombre de demandes, le type de données demandées, l'autorité ou les autorités requérantes, si les demandes ont été contestées et l'issue de ces contestations, etc.). Si la Société Novartis agissant en tant qu'Importateur de données se voit interdire partiellement ou totalement de fournir les informations susmentionnées à la Société Novartis agissant en tant qu'Exportateur de données, elle en informera dans les meilleurs délais la Société Novartis agissant en tant qu'Exportateur de données.

Novartis examinera la légalité de la Demande de divulgation et la contestera si, après une évaluation minutieuse, elle conclut qu'il existe des motifs raisonnables de considérer que la demande est illégale, et elle poursuivra les possibilités d'appel. Lorsqu'elle conteste la demande, Novartis demandera des mesures provisoires en vue de suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se soit prononcée sur son bien-fondé. Novartis ne divulguera pas les Données à caractère personnel demandées tant qu'elle n'aura pas été tenue de le faire en vertu des règles de procédure applicables. Novartis documentera son évaluation juridique et toute contestation de la Demande de divulgation et, dans la mesure permise par les lois du pays de destination, mettra la documentation à la disposition de la Société Novartis agissant en tant qu'Exportateur de données. Sur demande, la Société Novartis agissant en tant qu'Importateur de données mettra également la documentation à la disposition de l'Autorité de contrôle compétente.

Novartis fournira la quantité minimale d'information permise lorsqu'elle répond à une Demande de divulgation, en fonction d'une interprétation raisonnable de la demande. Quoi qu'il en soit, le partage de Données à caractère personnel par Novartis en réponse à une Demande de divulgation ne sera pas massif, disproportionné ou indiscriminé d'une manière qui irait au-delà de ce qui est nécessaire dans une société démocratique.

Cette section ne s'applique pas aux demandes reçues par Novartis d'autres organismes gouvernementaux dans le cours normal de ses activités, que Novartis peut continuer à fournir conformément à la loi applicable.

11. Entrée en vigueur et Résiliation

Les BCR sont entrées en vigueur le 3 juillet 2012 et ont ensuite été mises à jour en 2018, 2019 et 2024. Les BCR sont applicables aux Sociétés Novartis dès la signature de l'Accord inter-entreprises BCR (Annexe 3).

Toute modification ou mise à jour des BCR entrera en vigueur après avoir été approuvée par l'équipe de direction DPDAI, communiquée aux Sociétés Novartis concernées et publiée sur le site internet et l'intranet de Novartis.

Toute demande, réclamation ou plainte d'une Personne concernée impliquant les BCR sera jugée à l'aune de la version des BCR telle qu'elle était en vigueur au moment où l'événement à l'origine de la demande, de la réclamation ou de la plainte, s'est produit.

Une Société Novartis agissant en tant qu'Importateur de données qui cesse d'être liée par ces BCR parce qu'elle ne fait plus partie du Groupe de Sociétés Novartis doit demander à Novartis des instructions sur la restitution ou la suppression des Données à caractère personnel en sa possession.

Si la Société Novartis agissant en tant qu'Exportateur de données et la Société Novartis agissant en tant qu'Importateur de données conviennent que les données peuvent être conservées par la Société Novartis agissant en tant qu'Importateur de données, la protection doit être maintenue conformément

au chapitre V du RGPD.

12. Annexes

Les Annexes ci-jointes font partie intégrante des BCR.

Annexe 1 : Catégories de Personnes concernées et finalités du Traitement couvertes par les BCR

Annexe 2 : Glossaire des termes de protection des données utilisés aux fins des BCR et de leur application

Annexe 3 : Modèle d'Accord inter-entreprises BCR

Annexe 4 : Programme de formation en matière de protection des données relatif aux BCR

Annexe 5 : Procédure de gestion des plaintes en lien avec les BCR

Annexe 6 : Organisation globale Protection des données, Digital et IA Compliance chez Novartis

Annexe 7 : Liste des membres BCR

Auteur et propriétaire des BCR : Responsable Protection des données, Digital et IA, Région Europe

Revue par : Équipe de direction Protection des données, Digital et IA

Historique des versions

Date d'entrée en vigueur	Propriétaire	Version	CNIL
3 juillet 2012	Groupe Protection des données	1.0	3 juillet 2012
3 septembre 2018	Groupe Protection des données	2.0	3 septembre 2018
20 décembre 2024	Responsable Protection des données, Digital et IA Compliance Région Europe	3.0	20 décembre 2024