

Règles d'entreprise contraignantes de GSK

Déclaration de politique publique de GSK

Novembre 2022



Introduction

Les activités en matière de ressources humaines (**HR**) et de recherche et développement (**R&D**) de GSK (« nous », « notre », « nos ») impliquent le traitement de « données à caractère personnel » (voir glossaire), y compris le transfert international de ces données à caractère personnel. Nous nous sommes engagés à respecter des normes élevées d'intégrité dans le traitement des données à caractère personnel et avons adopté des Règles d'entreprise contraignantes (**BCR**) pour nous permettre d'effectuer des transferts internationaux de données à caractère personnel au sein du groupe de sociétés GSK, conformément aux lois en vigueur sur la protection des données de l'Union européenne et du Royaume-Uni, notamment le Règlement général sur la protection des données (règlement 2016/679) (**RGPD**) et son équivalent au Royaume-Uni.

Que sont les règles d'entreprise contraignantes (BCR) ?

Les BCR de GSK comprennent un certain nombre de documents, y compris la Politique de protection des données personnelles et la Norme de protection des données personnelles en vigueur dans ce domaine, un accord intragroupe entre les sociétés GSK ainsi que la présente Déclaration de politique publique. Nos règles d'entreprise contraignantes sont étayées par des formations et des audits. La présente Déclaration de politique publique a été conçue aux fins d'expliquer ces BCR et de s'assurer que les individus (**vous-même**), dont nous traitons les données à caractère personnel dans le cadre de nos activités HR et R&D, connaissent bien leurs droits en vertu de ces BCR et savent les exercer.

Un glossaire des termes utilisés à cet effet figure à la fin du présent document. Si vous souhaitez obtenir des informations complémentaires, veuillez contacter notre délégué UE/Royaume-Uni à la protection des données à l'adresse suivante : EU.DPO@GSK.com.

Champ d'application des BCR de GSK

Le Royaume-Uni ayant cessé d'être un État membre de l'UE, GSK dispose de deux types de BCR, les **BCR de l'UE** et les **BCR du Royaume-Uni**. Toutes les références aux BCR de GSK figurant dans cette déclaration concernent les BCR de l'UE et les BCR du Royaume-Uni. Toutes les références au RGPD figurant dans cette déclaration signifient, eu égard aux BCR du Royaume-Uni de GSK, les lois équivalentes sur la protection des données au Royaume-Uni, notamment la Loi sur la protection des données du Royaume-Uni de 2018 et le RGPD, qui fait partie de la loi du Royaume-Uni (connue sous le nom de « UK GDPR » [RGPD du Royaume-Uni]).

Les **BCR de l'UE** s'appliquent aux données à caractère personnel collectées dans le cadre des activités HR et R&D de GSK (décrites ci-après), lorsqu'elles font l'objet d'un transfert international :

- par une société GSK soumise à la législation de l'EEE en matière de protection des données, dans les pays de l'EEE identifiés ci-après ;
- vers un pays hors de l'Espace économique européen (**EEE**), où les lois applicables n'offrent pas un niveau adéquat de protection des données à caractère personnel.

Pays de l'EEE dans lesquels l'approbation a été obtenue : les BCR de GSK ont été approuvées dans les pays suivants : Allemagne, Autriche, Belgique, Bulgarie, Croatie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pologne, Pays-Bas, Portugal, République tchèque, Roumanie (R&D uniquement), Slovaquie, Slovénie, Suède et Suisse.

Les **BCR du Royaume-Uni** s'appliquent aux données à caractère personnel collectées dans le cadre des activités HR et R&D de GSK (décrites ci-après), lorsqu'elles font l'objet d'un transfert international :

- par une société GSK soumise à la législation du Royaume-Uni en matière de protection des données ;
- vers un pays hors du Royaume-Uni, où les lois applicables n'offrent pas un niveau adéquat de protection des données à caractère personnel.

Nos activités HR : elles comprennent (i) gérer le processus de recrutement, notamment toute la sélection, les contrôles des antécédents et du casier judiciaire ; (ii) gérer nos effectifs, notamment l'administration des salaires et des avantages sociaux ; gérer les soins de santé, les retraites, l'assistance aux employés, les congés, les régimes d'assurance et les plans d'épargne ; gérer les maladies, la santé et le bien-être, l'inclusion et la diversité ; gérer les relations entre employés et les questions disciplinaires et licenciements ; fournir un logement ou des prestations de santé et d'assurance liés à votre emploi ; répondre aux questions et requêtes ; et gérer les dossiers et activités post-emploi ; (iii) maintenir la continuité des activités en affectant des actifs et des ressources, mener la planification



stratégique et la gestion de projets, créer des budgets et des états financiers, conserver les pistes d'audit et maintenir les dossiers ; (iv) analyser nos effectifs afin de mieux utiliser et affecter les actifs et les ressources humaines de l'entreprise ; (v) gérer la vente d'actifs, les fusions, acquisitions et réorganisations ; (vi) communiquer avec le personnel, y compris dans une situation d'urgence et créer du contenu, tel que des enregistrements, vidéos ou photos à des fins de communication interne et éducatives ; (vi) gérer la formation, le développement, les performances et les talents ; (vii) gérer les produits, services, réseaux IT et canaux de communication de GSK, notamment permettre au personnel de les utiliser, gérer les droits d'accès et leur utilisation acceptable, créer des sauvegardes et collecter des données statistiques sur leur utilisation ; (viii) activités juridiques et de conformité, qui incluent le respect des exigences juridiques et réglementaires et d'autres exigences, telles que les lois et règlements sur l'emploi, la sécurité sociale et la santé au travail, l'impôt sur le revenu et les déductions d'assurance nationale, le respect des obligations en matière de conservation de pièces et de compte-rendu ; assurer le suivi de l'égalité des chances et de générer des rapports à cet égard ; réaliser des audits et assurer la gestion des risques ; se conformer aux inspections gouvernementales ; répondre aux procédures légales, exercer des droits et des recours judiciaires, assurer la défense en cas de litige et gérer les plaintes ou réclamations internes ; respecter les politiques et les procédures internes ; et surveiller les activités dans la mesure autorisée et/ou exigée par la législation locale ; (ix) surveiller l'utilisation des ressources GSK IT et les enquêtes de l'entreprise ; (x) activités liées à la santé, à la sûreté et à la sécurité ; et (xi) exploiter le processus de communication « Speak Up » pour soulever ou signaler les problèmes en interne.

Nos activités de R&D : elles comprennent des études cliniques interventionnelles et non interventionnelles, individuellement ou collectivement lancées, gérées ou financées par nos soins ainsi que la conformité réglementaire qui y est associée, telle que la surveillance de la sécurité et la déclaration des effets indésirables. Les données à caractère personnel traitées dans ce cadre comprennent les données liées aux « chercheurs externes » et aux « sujets de recherche » (voir glossaire).

Ce qui ne relève pas du champ d'application des BCR : nos BCR ne régissent ni le traitement ni le transfert de données à caractère personnel par nos divisions commerciales (par exemple, les données à caractère personnel concernant nos clients ou les individus liés aux fournisseurs de nos divisions commerciales). Ces données sont protégées par d'autres mécanismes juridiques. Nos BCR de l'UE ne couvrent pas les transferts de données à caractère personnel par les sociétés GSK situées en dehors de l'EEE, où celles-ci ne sont pas soumises aux lois de l'Union européenne sur la protection des données. Nos BCR du Royaume-Uni ne couvrent pas les transferts de données à caractère personnel par les sociétés GSK situées en dehors du Royaume-Uni, où celles-ci ne sont pas soumises aux lois du Royaume-Uni sur la protection des données.

Sociétés GSK couvertes par les BCR : nos BCR sont contraignantes pour toutes les sociétés du groupe ayant signé l'accord intragroupe mentionné ci-dessus. Ces sociétés du groupe doivent fournir sur demande aux autorités de contrôle, des informations détaillées sur les audits liés aux données à caractère personnel traitées dans le cadre de ces BCR et permettre à ces autorités de contrôle de les auditer afin de prouver la conformité à ces BCR.

Pour les BCR de l'UE : GlaxoSmithKline (Ireland) Limited, une société irlandaise, a la responsabilité globale de veiller à ce que toutes les sociétés du groupe à travers le monde se conforment aux BCR de l'UE, y compris à la nécessité de remédier aux éventuels manquements à celles-ci.

Pour les BCR du Royaume-Uni : GlaxoSmithKline plc, une société du Royaume-Uni, a la responsabilité globale de veiller à ce que toutes les sociétés du groupe à travers le monde se conforment aux BCR du Royaume-Uni, y compris à la nécessité de remédier aux éventuels manquements à celles-ci.

Nos règles (telles que reflétées dans notre Norme de protection des données personnelles)

1. Nous traitons les données à caractère personnel de manière loyale et légale

Nous respectons les lois locales applicables en matière de traitement des données à caractère personnel. En cas de conflit entre ces BCR et les lois applicables, et lorsque cela risque d'avoir des effets négatifs substantiels, y compris toute demande juridiquement contraignante de divulgation des données à caractère personnel par une autorité chargée de l'application des lois ou un organisme de sûreté de l'état, ce conflit doit être signalé à GlaxoSmithKline (Ireland) Limited (pour les BCR de l'UE) ou à GlaxoSmithKline plc (pour les BCR du Royaume-Uni), ainsi qu'à l'autorité de contrôle compétente. Lorsque la loi en vigueur interdit à la société du groupe concernée d'effectuer une telle notification à l'autorité de contrôle compétente, GSK déploie tous les efforts possibles pour obtenir une dérogation à cette interdiction.



Si ces efforts sont infructueux, la société du groupe fournit à l'autorité de contrôle compétente, pour chaque période de 12 mois, des informations générales concernant les requêtes qu'elle a reçues desdites autorités, notamment le nombre de demandes de divulgations, le type de données requises et, si possible, l'identité de l'organisme effectuant la requête.

Toute société du groupe ne doit en aucun cas fournir des données à caractère personnel à des entités gouvernementales de tout pays sans distinction, de manière disproportionnée ou à grande échelle, d'une façon qui va au-delà de ce qui est nécessaire dans une société démocratique.

Raison du traitement : nous procédons au traitement des données à caractère personnel uniquement pour une finalité légitime de l'entreprise et si un tel traitement est nécessaire à cette finalité. Tous les traitements sont fondés sur une base juridique au titre du RGPD.

Base juridique du traitement : nous nous appuyons sur les bases juridiques ci-après pour traiter les données à caractère personnel. Le traitement n'est réalisé que s'il est nécessaire :

- pour exécuter un contrat dont vous êtes partie prenante ou prendre des mesures à votre demande avant la passation d'un contrat ;
- pour se conformer à nos obligations légales ;
- pour l'exécution par nos soins d'une tâche effectuée dans l'intérêt public ;
- pour protéger vos intérêts vitaux ; ou
- pour la réalisation des intérêts légitimes poursuivis par GSK ou par un tiers, à condition que ces intérêts ne soient pas supplantés par vos propres intérêts, droits et libertés.

Catégories particulières de données : compte tenu de la nature des « catégories particulières de données » (voir glossaire), des garanties supplémentaires s'appliquent. Nous procédons au traitement des catégories particulières de données uniquement dans les cas suivants :

- lorsqu'il est nécessaire en vue de remplir nos obligations légales et d'exercer nos droits en matière de droit du travail ;
- lorsqu'il est nécessaire pour protéger vos intérêts vitaux si vous êtes physiquement ou légalement incapable d'accorder votre consentement ;
- lorsque le traitement porte sur des données à caractère personnel manifestement rendues publiques par vous-même ;
- lorsqu'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- lorsqu'il est nécessaire pour un motif d'intérêt public important ; ou
- aux fins de la médecine préventive ou de la médecine du travail, pour l'évaluation de la capacité de travail d'un de nos employés, le diagnostic médical, la fourniture de services de santé ou de services sociaux ou de traitement ou la gestion de systèmes de soins de santé et de services sociaux, que ce soit en vertu des lois applicables ou en vertu d'un contrat avec un professionnel de la santé. Dans ces circonstances, le traitement sera effectué par un professionnel de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalent.

Lorsque la loi l'exige ou lorsque nous nous trouvons dans l'impossibilité de nous fonder sur l'une des bases juridiques susmentionnées pour traiter vos données à caractère personnel, nous obtiendrons votre consentement sans équivoque. Lors du traitement des catégories particulières de données, nous ne procédons audit traitement que lorsque nous avons obtenu explicitement un tel consentement. Si vous donnez votre consentement, vous êtes libre de le retirer à tout moment. Si tel est le cas, veuillez-nous en informer en nous contactant de la façon indiquée dans la notice de protection des données personnelles, disponible [ici](#).

2. Nous collectons et conservons le minimum de données à caractère personnel nécessaire aux finalités spécifiques, explicites et légitimes de l'entreprise

Nous collectons le minimum de données à caractère personnel nécessaire aux finalités spécifiées, explicites et légitimes de l'entreprise. Nous nous efforçons de faire en sorte que les données à caractère personnel soient appropriées, pertinentes et limitées aux finalités pour lesquelles nous les avons collectées et/ou ultérieurement traitées. Lorsque nous avons connaissance que des données à caractère personnel sont inexactes, nous prenons toutes les mesures raisonnables pour les effacer ou les rectifier sans délai. Dans la mesure du possible, nous utilisons des « données anonymisées » (voir le glossaire) plutôt que des données à caractère personnel pour atteindre nos objectifs. Nous vérifions que les données à caractère personnel sont correctes et, si nécessaire, à jour.



Nous tenons un registre de toutes les activités de traitement de vos données à caractère personnel que nous réalisons, que nous mettons à disposition des autorités de contrôle, sur demande. Ce registre contient des informations détaillées sur les personnes à contacter dans chaque société de GSK qui traite des données à caractère personnel, les objectifs du traitement de vos données à caractère personnel (la raison pour laquelle nous utilisons vos données à caractère personnel), les catégories de personnes, les types de données à caractère personnel, les catégories de destinataires auxquels nous communiquons vos données à caractère personnel, les transferts internationaux de vos données à caractère personnel et l'instrument juridique pertinent que nous utilisons à cette fin, et si possible, les limites de rétention envisagées ainsi qu'une description générale des mesures de sécurité appliquées aux activités de traitement.

Lorsque notre utilisation de données à caractère personnel risque de menacer gravement vos droits et vos libertés, avant leur traitement, nous réalisons une évaluation de l'impact du traitement sur la protection de vos données à caractère personnel. Nous menons ces évaluations de l'impact sur la protection des données à caractère personnel en collaboration avec le délégué à la protection des données de l'UE/du Royaume-Uni, afin d'éliminer tout risque lors du traitement et d'identifier les mesures de sécurité et les autres mécanismes garantissant la protection de vos données à caractère personnel.

Nous conservons les données à caractère personnel seulement aussi longtemps que nécessaire à la finalité légitime de l'entreprise. Nous veillons ensuite à supprimer, détruire ou rendre anonymes les données à caractère personnel.

3. Nous vous expliquons comment nous comptons utiliser les données à caractère personnel vous concernant et vous énonçons vos droits y afférents

Transparence : nous agissons en toute transparence en ce qui concerne le traitement des données à caractère personnel que nous détenons. Nous garantissons que, conformément à la législation en vigueur, les informations concernant les activités de traitement vous sont fournies, généralement au moment de la collecte des données à caractère personnel. Pour toute information sur la manière dont GSK utilise vos données à caractère personnel, veuillez consulter la notice de protection des données personnelles, disponible [ici](#). Au minimum, nous fournissons ou garantissons la fourniture des informations ci-après.

Informations concernant GSK :

- l'identité et les coordonnées de la personne de la société GSK qui agit en tant que « responsable du traitement » (voir le glossaire) de vos données à caractère personnel et, le cas échéant, du représentant du responsable du traitement ;
- les coordonnées de notre délégué à la protection des données (le délégué à la protection des données de l'UE/du Royaume-Uni) ;

Informations sur la façon dont nous utilisons vos données à caractère personnel :

- comment et pourquoi nous sommes autorisés, conformément à la législation en vigueur, à collecter et à utiliser vos données à caractère personnel, y compris les objectifs du traitement auquel les données à caractère personnel sont destinées ;
- si nous utilisons vos données à caractère personnel pour une finalité légitime de l'entreprise, informations sur cet intérêt légitime ;
- informations sur les personnes auxquelles nous communiquons vos données à caractère personnel, y compris les destinataires ou catégories de destinataires, le cas échéant ;
- dans quelles circonstances nous transférons vos données à caractère personnel en dehors de votre pays de résidence (ou en dehors de l'EEE, si votre lieu de résidence se situe dans l'EEE) ;
- si nous nous basons sur ces BCR ou sur un autre mécanisme légal pour le transfert international de vos données à caractère personnel (vers un pays ou une organisation qui ne sont pas considérés comme adéquats, selon la législation en vigueur) : informations sur ces BCR ou le mécanisme légal, et façon dont vous pouvez obtenir une copie des BCR ou d'un autre mécanisme légal ;
- combien de temps nous gardons vos données à caractère personnel, notamment la période pendant laquelle les données à caractère personnel seront stockées ou, si ce n'est pas possible, les critères utilisés pour déterminer cette période ;



Informations sur vos droits concernant vos données à caractère personnel :

- informations sur vos droits, notamment le droit de demander l'accès, la rectification ou l'effacement de vos données à caractère personnel, ou la limitation du traitement de vos données à caractère personnel ou votre opposition à celui-ci, ou encore le droit de demander le transfert par GSK de vos données à caractère personnel à une autre organisation ;
- comment vous pouvez, à tout moment, retirer votre consentement à notre traitement de vos données à caractère personnel ;
- votre droit de déposer une plainte auprès de l'autorité de contrôle ;

Informations sur les activités de traitement particulières :

- s'il est nécessaire pour nous d'utiliser vos données à caractère personnel conformément à la loi ou pur remplir un contrat avec vous et les conséquences pour vous si vous ne nous autorisez pas à utiliser ces données ;
- si nous prenons des décisions sur votre utilisation de vos données à caractère personnel par des processus automatisés sans intervention humaine (également appelé « prise de décision automatisée », notamment pour prédire le comportement ou évaluer les caractéristiques d'une personne (connu sous le nom de « profilage ») ;
- si nous effectuons des prises de décision automatisées ou des profilages, informations concernant notre approche, l'importance de ce traitement et les conséquences du traitement pour vous, en tant qu'individu ; et
- lorsque nous avons l'intention d'utiliser vos données à caractère personnel pour d'autres finalités (autres que celles qui vous ont été communiquées), informations sur ces autres finalités.

Lorsque nous obtenons des données à caractère personnel par l'entremise de tiers plutôt qu'en nous adressant directement à vous, nous pourrions (sous réserve de la loi en vigueur) ne pas vous fournir les données ci-dessus si cela est impossible ou implique un effort disproportionné de notre part.

Gestion des droits individuels : nous vous permettons d'exercer vos droits en vertu du RGPD, notamment les droits décrits ci-après (qui peuvent être soumis à certaines restrictions en fonction de votre cas) :

- (i) **droit d'accès à vos données à caractère personnel** - en particulier le droit d'obtenir la confirmation de notre part du traitement ou non de vos données à caractère personnel, et, lorsque c'est le cas, d'accéder à vos données à caractère personnel et aux informations suivantes :
- les finalités du traitement ;
 - Les catégories de données à caractère personnel concernées ;
 - les destinataires ou les catégories de destinataires auxquels vos données à caractère personnel ont été, ou seront, révélées, dont les destinataires dans de pays tiers ou d'organisations internationales ;
 - lorsque c'est possible, la période prévue pendant laquelle vos données à caractère personnel seront stockées ou, si ce n'est pas possible, les critères utilisés pour déterminer cette période ;
 - l'existence de votre droit à nous demander la rectification ou l'effacement de vos données à caractère personnel ou la limitation du traitement des données à caractère personnel vous concernant, ou d'opposition à un tel traitement ;
 - votre droit de déposer une plainte auprès de l'autorité de contrôle ;
 - lorsque vos données à caractère personnel ne sont pas collectées auprès de vous, toute information disponible quant à leur source ;
 - l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour vous ;
 - lorsque vos données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, vous avez le droit d'être informé des garanties appropriées.

Nous vous fournissons une copie des données à caractère personnel vous concernant faisant l'objet d'un traitement. Nous pouvons exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire que vous demandez, ou lorsqu'une demande est manifestement infondée ou excessive, en particulier en raison de son caractère répétitif. Lorsque vous présentez votre demande par voie électronique, les informations vous sont fournies sous une forme électronique d'usage courant. Votre droit d'obtenir une copie de vos données à caractère personnel ne porte pas atteinte aux droits et libertés d'autrui.



- (ii) **droit de rectification (correction) de vos données à caractère personnel** - vous avez en particulier le droit d'obtenir de notre part, dans les meilleurs délais, la rectification de vos données à caractère personnel qui sont inexactes. Compte tenu des finalités du traitement, vous avez le droit d'obtenir que vos données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.
- (iii) **droit à l'effacement de vos données à caractère personnel** - vous avez en particulier le droit d'obtenir de notre part l'effacement, dans les meilleurs délais, de données à caractère personnel vous concernant et nous avons l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :
- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
 - vous retirez le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
 - vous vous opposez au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;
 - vos données à caractère personnel ont fait l'objet d'un traitement illicite ;
 - vos données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle nous sommes soumis ; et
 - les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information.

Lorsque nous avons rendu publiques les données à caractère personnel et que nous sommes tenus de les effacer, compte tenu des technologies disponibles et des coûts de mise en œuvre, nous prenons des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que vous avez demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

Le droit à l'effacement ne s'applique pas dans la mesure où ce traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale qui requiert le traitement prévue par la loi à laquelle nous sommes soumis, ou pour exécuter une mission d'intérêt public ;
- pour des motifs d'intérêt public dans le domaine de la santé publique ;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ; ou à la constatation, à l'exercice ou à la défense de droits en justice.

- (iv) **droit de limitation du traitement de vos données à caractère personnel ou d'opposition à celui-ci.** En particulier, vous avez le droit d'obtenir de notre part la limitation du traitement de vos données à caractère personnel lorsque l'un des éléments suivants s'applique :
- l'exactitude des données à caractère personnel est contestée par vous, pendant une durée nous permettant de vérifier l'exactitude des données à caractère personnel ;
 - le traitement est illicite et vous vous opposez à leur effacement et exigez à la place la limitation de leur utilisation ;
 - nous n'avons plus besoin des données à caractère personnel aux fins du traitement mais celles-ci nous sont encore nécessaires pour la constatation, l'exercice ou la défense de droits en justice ;
 - vous vous êtes opposé au traitement pendant la vérification portant sur le point de savoir si les motifs légitimes que nous poursuivons prévalent sur les vôtres.

Lorsque le traitement a été limité, ces données à caractère personnel ne peuvent, à l'exception de la conservation, être traitées qu'avec votre consentement, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public en vertu de la législation de l'UE ou d'un État membre de l'EEE (pour les transferts de l'EEE), ou de la législation du Royaume-Uni (pour les transferts du Royaume-Uni). Lorsque vous avez obtenu la limitation du traitement, vous êtes informé par nous avant que la limitation du traitement ne soit levée.

- (v) **droit à la portabilité des données** - pour vous fournir ou à un tiers, une copie de vos données à caractère personnel, en particulier : vous avez le droit de recevoir les données à caractère personnel vous concernant que vous nous avez fournies, dans un format structuré, couramment utilisé et lisible par machine, et avez le droit de transmettre ces données à un autre responsable du traitement sans que nous y fassions obstacle, lorsque :



- le traitement est fondé sur votre consentement ; et
- le traitement est effectué à l'aide de procédés automatisés.

Lorsque vous exercez votre droit à la portabilité des données, vous avez le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible. Le droit visé ne porte pas atteinte aux droits et libertés de tiers.

- (vi) **droit de ne pas faire l'objet de décisions automatisées.** En particulier, vous avez le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques vous concernant ou l'affectant de manière significative de façon similaire. Ce droit ne s'applique pas lorsque la décision :
- est nécessaire à la conclusion ou à l'exécution d'un contrat entre vous et nous ;
 - est autorisée par le droit auquel nous sommes soumis et qui prévoit également des mesures appropriées pour la sauvegarde de vos droits et libertés et de vos intérêts légitimes ; ou
 - est fondée sur votre consentement explicite.

Nous mettons en œuvre des mesures appropriées pour la sauvegarde de vos droits et libertés et de vos intérêts légitimes, au moins de votre droit d'obtenir une intervention humaine de notre part, d'exprimer votre point de vue et de contester la décision.

- (vii) **droit de retrait de votre consentement** - lorsque vous nous avez donné votre consentement au traitement de vos données à caractère personnel.
- (viii) **droit d'opposition au traitement conduit dans un intérêt légitime.** En particulier, vous avez le droit de vous opposer à tout moment au traitement de vos données à caractère personnel pour les intérêts légitimes du responsable du traitement ou d'un tiers, ou si le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
- (ix) **droit de vous opposer à la réception de communications marketing et de la refuser.** En particulier, vous avez le droit de vous opposer à tout moment au traitement de vos données à caractère personnel à des fins de marketing.

En outre, nous nous conformons aux lois en vigueur dans les pays qui vous accordent d'autres droits en ce qui a trait à vos données à caractère personnel. Nous pouvons limiter votre droit d'accès à vos données à caractère personnel afin de protéger les droits d'autrui (tels que le droit à la vie privée d'une autre personne) ou de respecter nos obligations légales.

Prise de décisions automatisée : nous faisons un usage limité des procédures de prise de décision automatisée lors du traitement des données à caractère personnel. Nous avons recours à la prise de décision automatisée dans les cas suivants :

- lorsqu'elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre nous et vous ;
- lorsqu'elle est autorisée par une loi spécifique de l'Union européenne ou d'un État membre (en lien avec les BCR de l'UE) ou du Royaume-Uni (en lien avec les BCR du Royaume-Uni), et si les sauvegardes requises par cette loi ont bien été mises en place ; ou
- lorsque vous avez donné votre consentement explicite.

Si vous souhaitez exercer l'un de vos droits, veuillez-nous en informer en nous contactant de la façon indiquée dans la Notice de protection des données personnelles. Lorsque vous choisissez d'exercer l'un de vos droits, nous nous efforcerons de fournir des informations sur la mesure que nous avons prise en réponse, dans un délai d'un mois calendaire. En fonction de la complexité de votre demande et du nombre d'autres demandes que nous devons traiter, il se peut que nous ayons besoin de deux mois supplémentaires pour vous fournir cette information. Nous vous indiquerons dans le mois qui suit votre demande si notre réponse sera retardée.

4. Nous n'utilisons pas de données à caractère personnel à d'autres fins incompatibles avec la finalité pour laquelle elles ont été initialement collectées

Limitation des finalités : nous ne traitons les données à caractère personnel que d'une manière compatible avec la finalité spécifiée, explicite et légitime de l'entreprise pour laquelle elles ont été initialement collectées. Nous vous aviserons de toute nouvelle finalité de traitement de vos données à caractère personnel.



5. Nous utilisons des garanties de sécurité appropriées

Protection de votre vie privée : nous mettons en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour empêcher la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Ces mesures sont adaptées aux risques associés à l'utilisation de données à caractère personnel et intègrent des technologies de pointe.

Gestion des incidents et des violations : nous avisons les autorités de contrôle de toute violation des données à caractère personnel (voir glossaire), dans les meilleurs délais et en tout état de cause, dans les 72 heures après en avoir pris connaissance, à moins que ces violations ne risquent pas de porter atteinte à vos droits et libertés. Nous vous informerons des violations de vos données à caractère personnel, si de telles violations sont susceptibles d'engendrer un risque élevé pour vos droits et libertés et (à notre discrétion) dans certaines autres circonstances. Nous tenons un registre des violations de données à caractère personnel, qui comprend les faits sur la violation de données à caractère personnel, ses effets (le cas échéant), ainsi que les mesures correctives prises pour y remédier. Nous mettons ces registres à la disposition des autorités de contrôle, sur demande de leur part.

6. Nous contrôlons minutieusement la divulgation de données à caractère personnel à des tiers

Gestion de la protection de la vie privée par des tiers : nous divulguons des données à caractère personnel en dehors de notre groupe de sociétés lorsque la loi l'exige, dans le cadre de procédures judiciaires et dans d'autres circonstances légales limitées. Nous pouvons également transférer des données à caractère personnel à l'extérieur de notre groupe de sociétés vers : (a) des tiers agissant en notre nom, y compris des fournisseurs ; ou (b) d'autres tiers indépendants, tels que des partenaires de recherche, des partenaires commerciaux ou des organismes de régulation.

Lorsque nous avons recours aux services de tiers pour le traitement de données à caractère personnel en notre nom, nous mettons en place des contrôles contractuels, organisationnels et opérationnels appropriés avec ces derniers en vue de garantir la confidentialité et la sécurité de vos données à caractère personnel. Nous exigeons de ces tiers qu'ils acceptent toutes les dispositions énoncées à l'article 28 du RGPD. Si nous découvrons que le traitement de données à caractère personnel par un tiers est contraire aux exigences que nous lui avons imposées ou aux lois en vigueur, nous prendrons toutes les mesures raisonnables pour veiller à ce que les manquements relevés soient corrigés le plus rapidement possible.

Transferts ultérieurs à des tiers : lorsque nous effectuons des transferts internationaux de données à caractère personnel au départ de l'EEE ou le Royaume-Uni vers des tiers situés dans des pays où les lois sur la protection des données n'offrent pas un niveau adéquat de protection des données à caractère personnel, nous mettons en œuvre des clauses contractuelles types avec le destinataire de ces données à caractère personnel. Il s'agit de protections contractuelles qui figurent dans un formulaire prescrit approuvé par la Commission européenne (pour les transferts au départ de l'EEE) ou par le secrétaire d'État ou l'ICO (pour les transferts au départ du Royaume-Uni), le cas échéant, (des informations détaillées sur ces clauses sont consultables ici : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en et <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/>). Vous êtes habilité à recevoir une copie de ces clauses contractuelles types et en faire la demande à l'adresse suivante : EU.DPO@GSK.com. Ces clauses contractuelles types requièrent que tant GSK, en tant qu'expéditeur, que le tiers, en tant que destinataire, de vos données à caractère personnel, acceptent de satisfaire aux exigences contractuelles strictes concernant le traitement de vos données à caractère personnel, afin de garantir qu'elles sont adéquatement protégées. Vous, en tant que personne concernée par les données, avez la possibilité de former un recours, en vertu des clauses contractuelles types pertinentes, si GSK ou le destinataire viole ces exigences.

Assurer un niveau de protection essentiellement équivalent : nous pouvons divulguer des données à caractère personnel au sein de notre groupe de sociétés et à des tiers situés dans des pays hors de l'EEE ou du Royaume-Uni où les lois sur la protection des données ne sont pas considérées par la Commission européenne (pour les transferts au départ de l'EEE) ou par le secrétaire d'État (pour les transferts au départ du Royaume-Uni) comme offrant un niveau adéquat de protection des données à caractère personnel. Avant la divulgation de données à caractère personnel à des destinataires situés dans ces pays, nous procédons à une évaluation en plusieurs



étapes afin de déterminer si nos protections contractuelles (parmi lesquelles les BRC et les clauses contractuelles types pour les transferts ultérieurs) offrent des garanties adéquates qui assurent une protection appropriée des données à caractère personnel :

- Nous évaluons si les lois et pratiques du pays du destinataire affaiblissent les mesures de protection des données existantes, notamment si les destinataires des données à caractère personnel peuvent remplir leurs obligations en matière de protection des données à caractère personnel. Pour ce faire, nous évaluons si les lois et pratiques du pays impliquent la divulgation par le destinataire de données à caractère personnel aux, ou l'accès aux données à caractère personnel par les autorités publiques, dans une mesure qui excède ce qui est nécessaire et proportionné.
- Si cette évaluation indique que les BCR risquent de ne pas offrir les garanties appropriées concernant les données à caractère personnel, nous déterminons si nous pouvons imposer des mesures supplémentaires pour le transfert des données à caractère personnel, afin de garantir un niveau de protection essentiellement équivalent. Nous pouvons être amenés à appliquer des mesures de sécurité techniques.
- Le délégué à la protection des données de l'UE/du Royaume-Uni, ainsi que GlaxoSmithKline (Ireland) Limited (pour les transferts au départ de l'EEE) et GlaxoSmithKline plc (pour les transferts au départ du Royaume-Uni), participeront à cette évaluation.
- Nous informerons d'autres sociétés GSK du résultat de cette évaluation et leur demanderons d'appliquer ces mesures de sécurité supplémentaires aux transferts similaires.
- Lorsque nous considérons que nous sommes dans l'incapacité d'identifier des mesures de sécurité supplémentaires appropriées offrant un niveau de protection essentiellement équivalent des données à caractère personnel, ou si une autorité de contrôle compétente le requiert, nous informerons d'autres sociétés GSK et mettrons fin au transfert de telles données à caractère personnel ou le suspendrons.

Démarches réglementaires : lorsque la législation en vigueur en matière de protection des données en vigueur dans un État membre de l'EEE ou au Royaume-Uni l'exige, nous notifions l'autorité de contrôle pertinente ou obtenons son consentement en ce qui concerne le traitement des données à caractère personnel (y compris les transferts internationaux de données à caractère personnel) et veillons à ce que les notifications ou les soumissions d'approbation soient toujours mises à jour en fonction des changements susceptibles d'intervenir.

7. Nous appliquons une procédure de plainte et respectons votre droit de recours

Dépôt de plainte : si vous pensez que nous n'avons pas respecté les règles établies dans nos BCR, vous avez la possibilité de nous faire part de vos préoccupations et de nous soumettre directement une plainte qui sera évaluée dans le cadre de notre procédure interne de règlement des plaintes. Nous vous encourageons à soumettre toute éventuelle plainte relative à la protection de la vie privée sur notre page [Speak Up](#).

Activités HR : pour les employés et autres personnes dont les données sont traitées dans le cadre des activités HR, une plainte relative à la protection de la vie privée peut être déposée auprès de votre supérieur hiérarchique (dans le cas des employés GSK), du responsable de la mise en conformité local, du service HR ou du représentant juridique local, ou de leurs homologues régionaux respectifs, qui sont tous tenus de signaler la plainte à la chaîne de traitement des plaintes qui acheminera celle-ci au service Compliance de l'unité fonctionnelle concernée ainsi qu'à l'équipe chargée de la protection de la vie privée. La ligne de conduite appropriée en réponse à votre plainte sera évaluée de manière indépendante via ces différentes voies de recours.

Activités de R&D : pour les personnes dont les données à caractère personnel sont traitées dans le cadre d'activités de R&D, si vous êtes un « sujet de recherche » (voir glossaire), vous devez contacter le clinicien ou le chercheur responsable de l'étude, qui transmettra votre plainte à l'équipe chargée de la protection de la vie privée. Si vous êtes un « chercheur externe » (voir glossaire), vous pourrez déposer une plainte relative à la protection de la vie privée auprès du responsable Compliance local de GSK, du représentant juridique local de GSK ou de leurs homologues régionaux respectifs, qui sont tous tenus de signaler la plainte à la chaîne de traitement des plaintes au sein de GSK. La ligne de conduite appropriée en réponse à votre plainte sera évaluée de manière indépendante via ces différentes voies de recours.

Remontée de l'information : quel que soit le lieu de dépôt des plaintes relatives à la protection de la vie privée, elles seront transmises : (i) à un contact responsable de la protection de la vie privée, dont les coordonnées sont publiées sur notre site Web que vous pouvez consulter en cliquant [ici](#) ; ou (ii) au délégué à la protection des données à caractère personnel de GSK dans l'UE/le Royaume-Uni, qui peut être contacté à l'adresse e-mail : EU.DPO@GSK.com. Le délégué à la protection des données de l'UE/du Royaume-Uni représente la dernière voie de recours au sein de GSK pour le règlement des plaintes relatives à nos BCR. Nous nous efforçons de



résoudre les plaintes qui nous parviennent le plus rapidement possible et, sauf circonstances exceptionnelles, GSK vous contactera par écrit dans un délai d'un mois à compter de la date de réception de votre plainte. Vous recevrez à cet effet une communication qui devra soit : (a) vous indiquer notre position en ce qui concerne la plainte ainsi que toute mesure que nous aurions prise, ou que nous comptons prendre, en réponse à votre plainte ; ou (b) vous indiquer la date à laquelle vous serez informé de notre position, qui devra intervenir deux mois au plus tard après cette notification. Si vous le souhaitez, vous pouvez contacter directement notre délégué à la protection des données de l'UE/du Royaume-Uni.

Dépôt de plainte auprès de l'autorité de contrôle ou de tribunaux :

Pour les BCR de l'UE : vous pouvez déposer une plainte en lien avec nos BCR de l'UE auprès de : (i) l'autorité de contrôle compétente dans le pays de l'EEE où vous avez votre résidence habituelle, votre lieu de travail ou dans lequel l'infraction présumée aurait eu lieu ; (ii) le Data Protection Commissioner irlandais ou les tribunaux irlandais (en tant que lieu d'implantation de GlaxoSmithKline [Ireland] Limited) ; (iii) les tribunaux du pays de l'EEE à partir duquel vos données à caractère personnel ont été transférées par nos soins ; et (iv) les tribunaux du pays de l'EEE où vous avez votre résidence habituelle.

Pour les BCR du Royaume-Uni : vous pouvez déposer une plainte en lien avec nos BCR du Royaume-Uni à l'Information Commissioner du Royaume-Uni ou aux tribunaux du Royaume-Uni (en tant que lieu d'implantation de GlaxoSmithKline plc).

Le respect de notre procédure interne de règlement des plaintes ne préjuge en aucune manière de votre droit d'utiliser librement l'une de ces options.

Vous êtes en droit d'obtenir réparation et, dans certains cas, une indemnisation pour violation des BCR. Si vous déposez une plainte et que vous êtes en mesure de démontrer que vous avez subi des dommages matériels ou immatériels très probablement en raison d'une violation de l'une de nos BCR (de l'UE ou du Royaume-Uni) ou des deux, il nous faudra prouver qu'il n'y a pas eu violation des BCR concernées.

Si une autorité de contrôle de l'EEE ou un tribunal d'un pays de l'EEE rend une ordonnance en lien avec nos BCR de l'UE à l'encontre d'une société GSK située en dehors de l'EEE, et si la société GSK en question ne peut ou ne veut, pour une raison quelconque, ni payer les dommages, ni se conformer à l'ordonnance dans un délai de grâce applicable, GlaxoSmithKline (Ireland) Limited vous paiera directement les dommages qui vous sont accordés ou veillera à ce que la société GSK concernée se conforme à l'ordonnance.

Si l'Information Commissioner du Royaume-Uni (ou son successeur ou remplaçant) ou un tribunal du Royaume-Uni rend une ordonnance en lien avec nos BCR du Royaume-Uni à l'encontre d'une société GSK située en dehors du Royaume-Uni, et si la société GSK en question ne peut ou ne veut, pour une raison quelconque, ni payer les dommages, ni se conformer à l'ordonnance dans un délai de grâce applicable, GlaxoSmithKline plc vous paiera directement les dommages qui vous sont accordés ou veillera à ce que la société GSK concernée se conforme à l'ordonnance.

Glossaire

- « délégué à la protection des données de l'UE/du Royaume-Uni » désigne le délégué à la protection des données qui contrôle la conformité à nos BCR et qui est chargé de contrôler la conformité aux lois sur la protection des données de l'UE et du Royaume-Uni. Le délégué à la protection des données de l'UE/du Royaume-Uni peut être contacté à l'adresse suivante : EU.DPO@GSK.com.
- « catégories particulières de données » désignent un sous-ensemble de données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
- « chercheur externe » fait référence à un médecin externe ou un autre professionnel de santé qui participe ou est susceptible de participer aux activités de R&D.
- « collaborateur intérimaire » au sein de GSK s'entend de toute personne, à l'exclusion des employés de GSK, qui fournit des services pour GSK ou en son nom, y compris les travailleurs occasionnels sur et hors site, les consultants professionnels, le personnel temporaire, les fournisseurs et les prestataires de service.
- « donnée anonymisée » désigne une donnée à caractère personnel rendue anonyme de telle sorte que l'individu auquel elle se rapporte ne soit pas ou plus identifiable.



- « données à caractère personnel » désigne toute information se rapportant à une personne physique identifiée ou identifiable.
- « protection adéquate » ou « niveau adéquat de protection » signifie un niveau de protection des données dans un pays hors de l'EEE (pour les transferts au départ de l'EEE) ou du Royaume-Uni (pour les transferts au départ du Royaume-Uni) qui, en vertu des lois sur la protection des données, est considéré comme offrant un niveau adéquat de protection des droits et libertés des personnes dans le cadre de la protection des données à caractère personnel.
- « responsable du traitement » désigne une personne physique ou morale qui, seul ou conjointement avec d'autres, détermine les finalités et moyens du traitement des données à caractère personnel.
- « sujet de recherche » fait référence à une personne participant à des activités de recherche ou à tout éventuel candidat à ce type d'activité, ou à un individu qui prend des produits ou des traitements GSK et dont nous traitons les données à caractère personnel dans le cadre de la pharmacovigilance. Les sujets de recherche incluent les participants externes et internes à GSK.
- « violation des données à caractère personnel » signifie toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel, ou l'accès non autorisé à de telles données.

Novembre 2022