

Déclaration publique sur les règles internes d'entreprise (BCR) de GSK

Introduction

Les activités en matière de ressources humaines (RH) 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 de ces données personnelles au niveau international. Nous nous sommes engagés à respecter des normes élevées d'intégrité dans le traitement des données personnelles et avons adopté des règles internes d'entreprise (BCR) pour nous permettre d'effectuer des transferts internationaux de données personnelles au sein du groupe de sociétés GSK conformément aux lois en vigueur sur la protection des données de l'Union européenne, notamment le Règlement général sur la protection des données (règlement 2016/679) (RGPD).

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

Les BCR de GSK comprennent un certain nombre de documents, y compris la Politique de protection des données personnelles et d'autres politiques en vigueur dans ce domaine, un accord intragroupe entre les sociétés GSK ainsi que la présente déclaration publique. Nos règles internes d'entreprise sont étayées par des formations et des audits. La présente Déclaration publique a été conçue aux fins d'expliquer ces BCR et de s'assurer que les individus dont nous traitons les données personnelles dans le cadre de nos activités RH et R&D (vous-même) 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 avez besoin de plus de détails à ce sujet, vous pourrez obtenir un exemplaire des BCR de GSK en contactant notre délégué EU à la protection des données à l'adresse suivante : EU.DPO@GSK.com.

Champ d'application des BCR de GSK

Les BCR de GSK s'appliquent aux données à caractère personnel vous concernant recueillies dans le cadre de nos activités RH et R&D, comme indiqué plus en détail ci-après, et qui font l'objet d'un transfert international par une société GSK soumise à la législation britannique ou européenne en matière de protection des données, dans les pays de l'Union européenne approuvés à cet effet, vers un pays situé hors de l'Espace économique européen (EEE) où les lois applicables n'offrent pas un niveau adéquat de protection des données personnelles.

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

Nos activités RH : celles-ci incluent l'administration et la gestion de nos effectifs ; les activités de recrutement et de sélection ; l'établissement d'une relation d'emploi ; l'administration des salaires et des avantages sociaux ; la formation, le développement et la performance ; la gestion des procédures disciplinaires et des griefs ; la communication avec les employés et la fourniture des références ; la communication avec les employés en cas d'urgence ; l'exploitation du processus de communication « [Speak Up](#) » pour soulever ou signaler les problèmes en interne ; la prise en charge de la continuité des activités et de l'assurance que les employés peuvent accéder aux systèmes et assumer leur rôle ; l'examen et la surveillance des communications des employés ; la conformité aux exigences légales, réglementaires et autres applicables à GSK, y compris celles concernant la fiscalité, la santé et la sécurité, l'anti-discrimination, la protection des données personnelles, les lois et réglementations relatives à l'immigration, les obligations en matière de conservation de pièces et de reporting, ainsi que les obligations d'audit et les inspections gouvernementales ; et la réponse aux procédures légales, l'exercice des droits et des recours judiciaires, la prise en charge de la défense en cas de litige et la gestion des plaintes et des réclamations internes. Les données personnelles traitées comprennent les données relatives aux employés et prestataires ou intérimaires (voir glossaire) actuels, anciens et futurs de GSK aussi bien qu'à leurs conjoints et personnes à charge, selon le cas.

Nos activités de R&D : celles-ci comprennent des études cliniques interventionnelles et non interventionnelles, individuellement ou collectivement lancées, gérées et financées par nos soins ainsi que la conformité réglementaire

qui y est associée, telle que la surveillance de la sécurité et le signalement d'effets indésirables. Les données personnelles 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 personnelles par le biais de 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 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 du Royaume-Uni ou de l'Union européenne sur la protection des données.

Sociétés GSK couvertes par les BCR : nos règles internes d'entreprise sont contraignantes pour toutes les sociétés du groupe ayant signé l'accord intragroupe mentionné ci-dessus. 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 règles internes d'entreprise, y compris à la nécessité de remédier aux éventuels manquements à celles-ci.

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

1. Nous traitons les données personnelles de manière loyale et légale

Nous respecterons les lois locales applicables en matière de traitement des données personnelles. En cas de conflit entre ces BCR et les lois applicables, et lorsque cela risque d'entraîner des effets négatifs importants, cela doit être signalé à l'autorité de protection des données.

Finalités du traitement : nous procédons au traitement des données personnelles uniquement lorsque cela sert l'entreprise à des fins légitimes qui ne peuvent être réalisées sans procéder à ce traitement. 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 décrites pour traiter les données personnelles. Le traitement n'est réalisé que s'il est nécessaire :

- (i) pour exécuter un contrat dont vous êtes partie prenante ou prendre des mesures à votre demande avant la passation d'un contrat ;
- (ii) pour se conformer à nos obligations légales ;
- (iii) pour l'exécution par nos soins d'une tâche effectuée dans l'intérêt public ;
- (iv) pour protéger vos intérêts vitaux ; ou
- (v) pour la réalisation de l'intérêt légitime poursuivi 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 :

- (i) lorsqu'il est nécessaire en vue de remplir nos obligations légales et d'exercer nos droits en matière de droit du travail ;
- (ii) lorsqu'il est nécessaire pour protéger vos intérêts vitaux si vous êtes physiquement ou légalement incapable d'accorder votre consentement ;
- (iii) lorsque le traitement porte sur des données à caractère personnel manifestement rendues publiques par vous-même ;
- (iv) lorsqu'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- (v) lorsqu'il est nécessaire pour un motif d'intérêt public important ; ou
- (vi) 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 praticien de la santé. Dans ces circonstances, le traitement sera effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalent.

Nous obtiendrons votre consentement sans équivoque pour traiter les données personnelles et les catégories

particulières de données vous concernant seulement si la loi l'exige ou si nous nous trouvons dans l'impossibilité de nous fonder sur l'une des bases juridiques susmentionnées.

2. Nous recueillons et conservons le minimum de données personnelles à des fins spécifiques et légitimes nécessaires à la poursuite des objectifs commerciaux de l'entreprise

Nous recueillons le minimum de données personnelles nécessaires à la poursuite des différents objectifs commerciaux légitimes de l'entreprise. Nous nous efforçons de faire en sorte que les données à caractère personnel soient appropriées, pertinentes et non excessives eu égard aux finalités pour lesquelles nous les avons recueillies et/ou ultérieurement traitées. Dans la mesure du possible, nous utilisons des données rendues anonymes plutôt que des données à caractère personnel pour atteindre nos objectifs. Nous vérifions que les données personnelles sont correctes et, si nécessaire, à jour.

Nous conservons les données à caractère personnel seulement aussi longtemps que nécessaire à la réalisation de nos objectifs commerciaux légitimes. Nous veillons ensuite à supprimer, détruire ou rendre anonymes les données personnelles.

3. Nous vous expliquons comment nous comptons utiliser les données personnelles 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 fournissons les données requises par les lois applicables, au moment de la collecte des données personnelles. Nous fournissons au minimum les données minimales requises en vertu des articles 13 et 14 du RGPD. Lorsque nous obtenons des données personnelles par l'entremise de tiers plutôt qu'en nous adressant directement à vous, nous pourrions (sous réserve de la loi applicable) ne pas vous fournir ces données si cela s'avère être impossible ou impliquer un effort disproportionné de notre part.

Gestion des droits individuels nous vous permettons d'exercer vos droits en vertu du RGPD, y compris :

- (i) le droit d'accéder à vos données personnelles ;
- (ii) le droit de faire corriger vos données personnelles ;
- (iii) le droit d'effacer vos données personnelles ;
- (iv) le droit de restreindre ou de suspendre le traitement des données personnelles vous concernant ;
- (v) le droit de fournir une copie de vos données personnelles à vous-même ou à un tiers ;
- (vi) le droit de ne pas prendre de décisions automatisées à votre encontre (voir ci-dessous) ;
- (vii) le droit de retirer votre consentement ; et
- (viii) le droit de vous opposer à la réception de communications marketing.

En outre, nous nous conformons aux lois applicables dans les pays qui vous accordent d'autres droits en ce qui a trait à vos données personnelles. Nous pouvons restreindre votre droit d'accéder aux données personnelles vous concernant afin de protéger les droits d'autrui (tels que le droit à la vie privée d'une autre personne).

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

- (i) lorsqu'elle est nécessaire pour conclure ou exécuter un contrat entre nous et vous ;
- (ii) lorsqu'elle est autorisée dans le cadre d'une loi spécifique de l'Union européenne ou d'un État membre, et si les protections requises conformément à cette loi ont bien été mises en place ; ou
- (iii) lorsque vous nous en avez explicitement donné l'autorisation.

4. Nous n'utilisons pas de données personnelles à d'autres fins incompatibles avec le but pour lequel elles ont été initialement recueillies

Limitation des finalités : nous ne traiterons les données personnelles que d'une manière compatible avec l'objectif commercial légitime pour lequel elles ont été initialement collectées. Nous vous aviserons de toute nouvelle finalité de traitement applicable aux données personnelles vous concernant.

5. Nous utilisons des garanties de sécurité appropriées

Protection de la 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 ou l'accès aux données personnelles, de nature accidentelle ou illégale. 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 aviserons l'autorité de protection des données de toute violation des données à caractère personnel vous concernant, 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 de présenter des risques importants au regard de vos droits et libertés et (à notre discrétion) dans certaines autres circonstances particulières. Nous maintenons un inventaire des cas de violation de données personnelles, qui comprend des détails sur les violations de données personnelles et leurs effets (le cas échéant) sur vous, sur nous ou sur toute autre tierce partie, ainsi que les mesures correctives prises à cet effet. Nous mettrons ces dossiers à la disposition de l'autorité de protection des données, à sa demande.

6. Nous contrôlons minutieusement la divulgation de données personnelles aux tiers.

Gestion de la protection des données personnelles en relation avec les tiers nous divulguons des données personnelles en dehors de notre groupe de sociétés lorsque cela est requis par la loi, dans le cadre de procédures judiciaires et dans d'autres circonstances limitées prévues par la loi. 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 personnelles. Nous exigeons de ces parties tierces qu'elles acceptent toutes les dispositions énoncées à l'article 28 du RGPD. Si nous découvrons qu'une tierce partie traite les données personnelles de façon incompatible avec les exigences que nous lui avons imposées ou avec les lois applicables, nous prendrons toutes les mesures raisonnables pour veiller à ce que les lacunes relevées soient comblées le plus rapidement possible.

Transferts ultérieurs à des tiers : lorsque nous effectuons des transferts internationaux de données personnelles à des tiers situés dans des pays hors de l'EEE 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 approuvées, dont vous trouverez les détails en cliquant [ici](#) ou nous nous prévalons d'une autre exception prévue par la loi pour le transfert des données personnelles.

Démarches réglementaires : Lorsque la législation applicable en matière de protection des données en vigueur dans l'État membre concerné l'exige, nous notifions l'autorité de protection des données ou obtenons son consentement en ce qui concerne le traitement des données personnelles (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 réclamation 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 des données personnelles sur notre page [Speak Up](#).

Activités RH : pour les employés et autres personnes dont les données sont traitées dans le cadre des activités RH, une plainte relative à la protection des données personnelles peut être déposée auprès de votre supérieur hiérarchique (dans le cas des employés GSK), du responsable Compliance local, du service RH 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'au Centre d'excellence de Protection des données personnelles. 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 personnelles sont traitées dans le cadre d'activités de R&D, si vous êtes un sujet de recherche (voir glossaire), vous devrez contacter le clinicien ou le chercheur responsable de l'étude, qui transmettra votre plainte au Centre d'excellence de Protection des données personnelles. Si vous êtes un chercheur externe (voir glossaire), vous pourrez déposer une plainte relative à la protection des données personnelles 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 de la plainte relative à la protection des données personnelles, si celle-ci ne peut être résolue, elle sera transmise : (i) au conseiller national à la protection des données personnelles, dont les coordonnées sont publiées sur notre site Web que vous pouvez consulter en cliquant [ici](#) ; ou (ii) ultérieurement au délégué EU à la protection des données personnelles de GSK, qui peut être contacté à l'adresse e-mail EU.DPO@GSK.com. Le délégué EU à la protection des données 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 également contacter directement notre délégué EU à la protection des données.

Dépôt de plainte auprès de l'autorité de protection des données personnelles ou d'un tribunal : vous pouvez déposer une plainte auprès des autorités suivantes : (i) l'autorité compétente en matière de protection des données personnelles dans le pays où vous avez votre résidence principale ou votre lieu de travail ou dans lequel l'infraction présumée aurait eu lieu ; (ii) le commissaire à l'information du Royaume-Uni ou les tribunaux britanniques (en tant que lieu d'implantation de GlaxoSmithKline plc) ; (iii) les tribunaux du pays de l'EEE à partir duquel vos données personnelles ont été transférées par nos soins ; et (iv) les tribunaux du pays de l'EEE où vous avez votre résidence principale. 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.

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 nos BCR, il nous faudra prouver qu'il n'y a pas eu violation de nos BCR. Si l'autorité de protection des données personnelles ou un tribunal compétent rend une ordonnance 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 du tribunal 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

Les « 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.

Les « données anonymisées » désignent les données personnelles rendues anonymes de telle sorte que l'individu auxquelles elles se rapportent ne soit pas ou plus identifiable.

Les « données personnelles » sont toutes les données qui se rapportent à une personne identifiée ou identifiable.



Un « chercheur externe » est un médecin externe ou un professionnel de santé qui participe ou est susceptible de participer aux activités de R&D.

Un « employé prestataire ou 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.

Un « 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 personnelles dans un contexte de pharmacovigilance. Les sujets de recherche incluent les participants externes et internes à GSK.

[Juin 2018]