

Règles d'Entreprise Contraignantes de SANOFI (BCR)

Pour le transfert de Données Personnelles

Table des matières

PART I. CONTEXTE ET CHAMP D'APPLICATION	3
1. Objectifs	4
2. Périmètre	4
PART II. ENGAGEMENTS DE SANOFI AU TITRE DES REGLES D'ENTREPRISE CONTRAIGNANTES	5
Section 1. Principes de traitement des Données Personnelles	5
1. Limitation de la finalité	5
2. Licéité du traitement	5
3. Loyauté et Transparence	7
4. Minimisation et exactitude	7
5. Sécurité, intégrité et confidentialité	8
6. Durée de conservation limitée des Données Personnelles	9
7. Responsabilité	9
8. Respect de l'obligation de notification d'une Violation de Données Personnelles	11
9. Information et droits des Personnes Concernées	11
10. Garantir une protection adéquate pour le transfert de Données Personnelles	14
11. Mesures en cas de législation nationale empêchant le respect des BCR de SANOFI	15
12. Conformité aux BCR de SANOFI	19
13. Restitution ou suppression des Données Personnelles	20
Section 2. Garanties d'effectivité, de mise en œuvre et d'application	21
14. Nature contraignante des BCR de SANOFI	21
15. Coopération avec les Autorités de Protection des Données	21
16. Réclamation d'une Personne Concernée	21
17. Procédure de mise à jour des BCR de SANOFI	22
18. Accessibilité aux BCR de SANOFI	22
19. Conflit de lois	22
20. Demande d'Accès aux Données Personnelles émanant d'une autorité gouvernementale	22
Section 3. Droits des Tiers Bénéficiaires	23
21. Droits des Tiers	23
22. Droit aux recours juridictionnels et à l'indemnisation	24
PART III. ANNEXES	26
ANNEXE 1. DEFINITIONS	26
ANNEXE 2. CHAMP MATERIEL DES BCR DE SANOFI	31
ANNEXE 3. Articles du RGPD ARTICLES DU RGPD	38

HISTORIQUE DES VERSIONS

Version	Date d'application	Description
1.0	2009	Version initiale
2.0	2026	Mise à jour générale alignée sur les recommandations du Comité Européen de la Protection des Données (CEPD) concernant les Règles d'Entreprise Contraignantes (art.47 GDPR)

Depuis 2009, Sanofi a mis en place des Règles d'Entreprise Contraignantes (BCR) pour assurer la protection des Données Personnelles dans ses activités à travers le monde. Ces règles sont régulièrement mises à jour afin de satisfaire aux exigences les plus exigeantes en matière de protection des données. Initialement approuvées par la CNIL, en sa qualité d'Autorité de Contrôle Chef de File, les BCR de SANOFI ont, à chaque mise à jour, fait l'objet de la procédure d'examen prévue par le règlement général sur la protection des données (RGPD). La version en vigueur a été approuvée par la CNIL, en concertation avec le Comité Européen de la Protection des Données (CEPD).

PART I. CONTEXTE ET CHAMP D'APPLICATION

Le Groupe SANOFI (ci-après « **SANOFI** ») mesure pleinement l'importance de la vie privée et de la protection des Données Personnelles à l'ère numérique. Il s'engage à garantir un niveau de protection adéquat des données pour toutes les personnes avec lesquelles il est en relation.

Cet engagement se traduit concrètement dans son Code d'éthique, publié sur son site internet¹, ainsi que dans ses Règles de Protection des Données Personnelles de SANOFI.

SANOFI a obtenu une première approbation de l'Autorité de Contrôle Compétente dès 2009, ses Règles d'Entreprise Contraignantes ont depuis été mises à jour à la suite de l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD), afin d'assurer une protection adéquate des Données Personnelles partagées au sein du groupe.

Les présentes Règles d'Entreprise Contraignantes et leurs Annexes (ci-après les « **BCR de SANOFI** ») formalisent l'engagement de SANOFI à garantir, à l'échelle de l'ensemble de son organisation, un niveau de protection adéquat des Données Personnelles conformément au Règlement Général Européen sur la Protection des Données (RGPD), pour les Activités de Traitement décrites au [2. Périmètre](#).

Les Règles d'Entreprise Contraignantes de SANOFI définissent les modalités selon lesquelles SANOFI se conformera au Droit Applicable s'agissant des traitements qu'il effectue en qualité de Responsable de Traitement.

Les termes utilisés dans ces Règles d'Entreprises Contraignantes ont des significations précises. Une liste complète des définitions est fournie à l'[Annexe 1](#). Lorsqu'un terme n'y est pas défini, il convient de se référer à la définition figurant dans le RGPD.

La présente version publique des Règles d'Entreprise Contraignantes de SANOFI est accessible à l'adresse www.sanofi.com et tenue à jour. Elle comprend l'intégralité des Principes de traitement des Données Personnelles ([Section 1](#). et des Droits des Tiers Bénéficiaires ([Section 3](#). ainsi qu'une sélection de dispositions tirées des Garanties d'effectivité, de mise en œuvre et d'application ([Section 2](#). pertinentes pour les Personnes Concernées, présentées de manière claire et accessible à leur intention.

Contact

- Formulaires de contact <https://www.sanofi.com/en/data-protection-contact> , ou,
- Courrier postal à: EBI - Data Privacy Office, 46 Avenue de la Grande Armée 75017 Paris, France.

¹ <https://www.codeofconduct.sanofi/fr/>

1. Objectifs

Les BCR de SANOFI ont pour objet de définir les principes auxquels l'ensemble des Entités Adhérentes s'engage à se conformer lors du traitement des Données Personnelles régi par le RGPD et d'assurer un niveau de protection adéquat lors du transfert de données à caractère personnel au sein du Groupe SANOFI entre les Importateurs de Données et les Exportateurs de Données.

La mise en œuvre des BCR de SANOFI constitue également l'un des instruments permettant de renforcer la culture et la sensibilisation aux Règles de Protection des Données de SANOFI au sein du Groupe SANOFI.

2. Périmètre

Les BCR de SANOFI couvrent l'ensemble des Activités de Traitement relevant du champ matériel d'application et qui sont réalisées par une Entité Adhérente agissant en qualité de Responsable de Traitement ou de Sous-Traitant pour le compte d'une autre Entité Adhérente, dans l'un quelconque des cas suivants :

- L'Entité Adhérente qui traite des Données Personnelles est établie dans l'Union européenne et/ou dans l'Espace Économique Européen (EEE) ;
- L'Entité Adhérente qui traite des Données Personnelles est établie dans un Pays Tiers et a reçu les Données Personnelles d'une Entité Adhérente établie dans l'Union européenne et/ou dans l'EEE ;
- Par convention entre Entités Adhérentes, quelle que soit la localisation de l'une ou l'autre entité, dans ou hors de l'EEE ;
- Les Transferts Ultérieurs de Données Personnelles entre Importateurs de Données.

Les BCR de SANOFI s'appliquent à l'ensemble des Affiliés SANOFI qui y adhèrent par la signature de l'Accord d'Acceptation des Règles d'Entreprise Contraignantes et qui agissent en qualité d'Exportateurs de Données ou d'Importateurs de Données, quelle que soit leur localisation et leur juridiction, lors du traitement de toute donnée à caractère personnel en qualité de Responsable de Traitement.

Les BCR de SANOFI s'appliquent à tout Traitement de Données Personnelles mis en œuvre par les Entités Adhérentes dans le contexte des activités suivantes :

- Gestion des Ressources Humaines et de la culture d'entreprise (People and Culture) ;
- Essais et études cliniques, études sur des données de vie réelle (Real-World Evidence) ;
- Systèmes de vigilance sanitaire.

Lorsqu'il est soumis à des transferts de données à caractère personnel :

- Par une Entité Adhérente individuellement soumise au Droit de l'Union Européenne ;
- Par une Entité Adhérente située dans un Pays Tiers.

Une description générale des catégories de Données Personnelles transférées régies par les BCR de SANOFI est incluse dans l'[Annexe 2](#). Cette description couvre les catégories de transferts de Données Personnelles, leurs finalités, leurs natures et la nature des Données Personnelles, les catégories des Personnes Concernées, ainsi que l'identification des pays dans lesquels se situent les Importateurs de Données.

SANOFI applique les présentes Règles d'Entreprises Contraignantes dans tous les cas où une Entité Adhérente traite des Données Personnelles de manière manuelle ou par des moyens automatisés.

Les BCR de SANOFI s'appliquent à l'ensemble des Personnes Concernées – quelle que soit leur localisation – dont les Données Personnelles sont transférées dans le cadre des Activités de Traitement relevant du champ matériel d'application susmentionné par une Entité Adhérente.

Les BCR de SANOFI ne régissent pas les Activités de Traitement et les transferts de Données Personnelles qui ne relèvent pas du champ matériel d'application défini. De tels transferts sont protégés par divers mécanismes légaux appropriés, tels que les clauses contractuelles types de l'Union Européenne et les exigences du Droit Applicable à la protection des données.

PART II. ENGAGEMENTS DE SANOFI AU TITRE DES REGLES D'ENTREPRISE CONTRAIGNANTES

Ces engagements s'appliquent quand les Filiales ayant adhéré aux présentes Règles d'Entreprise Contraignantes déterminent comment et pourquoi les Données Personnelles sont traitées. Dans ce cas, ces entités agissent en tant que Responsable de Traitement.

Ils établissent les principes fondamentaux de protection des données que toutes les entités Sanofi dans le monde, adhérentes aux Règles d'Entreprise Contraignantes, doivent respecter. Ces principes s'appliquent lors de la collecte, de l'utilisation et du transfert de Données Personnelles dans le cadre des BCR de SANOFI. Elles sont obligatoires pour toutes les Entités Adhérentes du Groupe SANOFI.

Elles définissent également les mesures que SANOFI a mises en place pour garantir le respect de ces règles au sein de toutes les Entités Adhérentes. Cela inclut les engagements pris par SANOFI auprès des Autorités de Protection des Données.

Enfin, elles détaillent les droits spécifiques dont disposent les Personnes Concernées au titre des présents BCR et la manière de les exercer. Ces droits s'appliquent quel que soit le lieu où les Données Personnelles sont traitées au sein des Entités Adhérentes.

Section 1. Principes de traitement des Données Personnelles

Les Importateurs de Données et les Exportateurs de Données veillent à ce que toutes les Activités de traitement réalisées au sein du Groupe SANOFI soient conçues, mises en œuvre et contrôlées conformément aux principes de protection des données à caractère personnel de SANOFI, tels qu'énoncés dans les Règles de Protection des Données Personnelles de SANOFI. En tout état de cause, les Données Personnelles sont traitées conformément au Droit Applicable à la protection des données.

En particulier, l'ensemble des Exportateurs de Données et des Importateurs de Données est tenu de respecter les principes suivants :

1. Limitation de la finalité

- 1.1 Les Entités Adhérentes veillent en tout temps à ce que le traitement des Données Personnelles soit effectué à des fins déterminées, explicites, légitimes, et limité à ce qui est strictement nécessaire.
- 1.2 Les Entités Adhérentes ne traitent les Données Personnelles qu'aux fins déterminées, explicites et légitimes susvisées et s'abstiennent de tout traitement ultérieur incompatible avec lesdites fins. Un traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques n'est pas réputé incompatible avec les finalités initiales, sous réserve de la mise en œuvre de garanties techniques et organisationnelles appropriées visant à protéger les droits et libertés des Personnes Concernées.

2. Licéité du traitement

- 2.1 Les Entités Adhérentes veillent en tout temps à ce que le traitement des Données Personnelles repose sur un fondement juridique licite, conformément au Droit Applicable à la Protection des Données Personnelles, y compris les lois régissant la protection des Données Personnelles dans le pays où ces données sont initialement collectées.
- 2.2 La licéité du traitement des Données à Personnelles implique que les Entités Adhérentes ne traitent des Données Personnelles relevant du champ d'application des présentes Règles d'Entreprise Contraignantes uniquement lorsqu'au moins l'une des conditions suivantes, telles qu'établies par le Droit de l'Union Européenne, est remplie :
 - La Personne Concernée a donné son consentement au traitement de ses Données Personnelles pour une ou plusieurs finalités spécifiques ;

- Le traitement des Données Personnelles est nécessaire à l'exécution d'un contrat auquel la Personne Concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la Personne Concernée ;
 - Le traitement des Données Personnelles est nécessaire au respect d'une obligation légale à laquelle le Responsable de Traitement est soumis en vertu du Droit Applicable à la Protection des Données Personnelles ;
 - Le traitement des Données Personnelles est nécessaire à la sauvegarde d'intérêts vitaux, tels que la vie, la santé ou la sécurité de la Personne Concernée ou d'une autre personne physique ;
 - Le traitement des Données Personnelles 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 de Traitement ;
 - Le traitement des Données à caractère personnel est nécessaire aux fins des intérêts légitimes poursuivis par le Responsable de Traitement ou par un Tiers, à moins que ne prévalent les intérêts ou les droits et libertés fondamentaux de la Personne concernée.
- 2.3 À cette fin, les Entités Adhérentes ne traitent les Données Personnelles qu'en s'appuyant sur l'un des fondements juridiques détaillés à l'[Annexe 2](#).
- 2.4 Lorsqu'une Activité de Traitement implique le traitement de Données Personnelles Sensibles, les Entités Adhérentes doivent :
- S'appuyer sur une base légale adéquate telle qu'énumérée au point [2.5](#),
 - Réaliser une Évaluation des Risques, si nécessaire, et prévoir les mesures appropriées visant à préserver les droits des individus, sans préjudice du respect des autres principes énoncés dans les BCR de SANOFI.
- 2.5 Le traitement des Données Personnelles Sensibles est soumis à des exigences supplémentaires en raison du risque plus élevé qu'il présente pour un individu en cas d'utilisation abusive ou de traitement incorrect. Lorsqu'une Entité Adhérente traite des Données Personnelles Sensibles, il ne peut le faire que si l'une des conditions suivantes est remplie :
- La Personne Concernée a donné son consentement explicite au traitement de ces Données Personnelles pour une ou plusieurs finalités déterminées, sauf lorsque le Droit de l'Union Européenne prévoit que l'interdiction du traitement des Données Personnelles Sensibles ne peut être levée par la Personne Concernée.
 - Le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres du Responsable du Traitement ou à la Personne Concernée en matière de droit du travail, de droit de la sécurité sociale et de protection sociale, dans la mesure où ce traitement est autorisé par le Droit de l'Union Européenne ou par une convention collective conclue en vertu du Droit de l'Union Européenne, prévoyant des garanties appropriées pour les droits fondamentaux et les intérêts de la Personne Concernée ;
 - Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la Personne Concernée ou d'une autre personne physique, dans le cas où la Personne Concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
 - Le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les Données Personnelles ne soient pas communiquées en dehors de cet organisme sans le consentement des Personnes Concernées ;
 - Le traitement porte sur des Données Personnelles Sensibles qui ont été manifestement rendues publiques par la Personne Concernée ;
 - Le traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice, ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
 - Le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du Droit de l'Union Européenne, lequel doit être proportionné à l'objectif poursuivi, respecter

l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la Personne Concernée ;

- Le traitement des Données Personnelles Sensibles est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du salarié, du diagnostic médical, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale, sur la base du Droit Applicable à la protection des données ou des règles établies par les organismes compétents d'un État membre de l'EEE ou de l'UE, ou par toute autre personne également soumise à une obligation de secret en vertu desdites lois ou règles ;
- Le traitement des Données Personnelles Sensibles est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du Droit Applicable qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la Personne Concernée, notamment le secret professionnel ;
- Le traitement de Données Personnelles Sensibles est nécessaire à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89(1) du RGPD, sur la base du Droit de l'Union Européenne, lequel doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la Personne Concernée ;
- Le traitement de condamnations pénales et d'infractions est strictement limité aux cas dans lesquels il est explicitement autorisé ou requis par le droit de l'EEE ou le Droit de l'Union Européenne.

- 2.6 Nonobstant toute disposition contraire des présentes, lorsque les lois applicables à l'Exportateur de Données prévoient une définition, un champ d'application ou un cadre réglementaire plus étendu concernant les Données Personnelles Sensibles, ces données sont qualifiées de Données Personnelles Sensibles, et les dispositions pertinentes des lois locales de l'Exportateur de Données prévalent sur toute disposition offrant un niveau de protection moindre.

3. Loyauté et Transparence

- 3.1 Chaque Activité de Traitement doit être mise en œuvre conformément au principe de transparence et être associée à une information appropriée décrivant ses spécificités, conformément aux mentions obligatoires listées au principe « Information et droits des Personnes Concernées » (voir [9.1](#) and [9.4](#)) des BCR de SANOFI. Cette information doit contenir des éléments appropriés concernant les transferts de Données Personnelles applicables ainsi que ceux relatifs aux droits des Personnes Concernées.
- 3.2 Lorsque le fondement juridique de l'Activité de Traitement est le consentement individuel des Personnes Concernées (par exemple, le traitement de Données Personnelles Sensibles), ce consentement doit être donné librement et doit être spécifique, éclairé et univoque, préalablement à sa mise en œuvre.

4. Minimisation et exactitude

- 4.1 Chaque Activité de Traitement doit reposer sur des Données Personnelles exactes, pertinentes et strictement nécessaires à la réalisation de la finalité pour laquelle elles sont collectées.
- 4.2 Les Entités Adhérentes ne collectent que les Données Personnelles strictement nécessaires à la poursuite de chaque finalité professionnelle déterminée, explicite et légitime, telle que décrite conformément au champ d'application matériel des BCR de SANOFI (voir [Annexe 2](#)).
- 4.3 Lorsque des Données Personnelles sont inexactes ou incomplètes, les Entités Adhérentes prennent toutes les mesures raisonnables pour les rectifier, les effacer ou les compléter.

- 4.4 Les Entités Adhérentes s'assurent, préalablement à toute collecte, que les Données Personnelles Sensibles sont effectivement nécessaires au regard de la finalité de traitement envisagée.
- 4.5 En règle générale, les Entités Adhérentes :
- S'abstiennent de traiter toute Donnée Personnelle relative à des condamnations pénales et des infractions, sauf lorsque ce traitement est explicitement autorisé ou requis par l'EEE ou le droit de l'Union Européenne ;
 - Examinent et évaluent la possibilité de recourir à des données anonymisées ou pseudonymisées, sous réserve que le coût et les efforts requis soient proportionnés à la finalité recherchée.

5. Sécurité, intégrité et confidentialité

- 5.1 L'Entité Adhérente est responsable de la mise en œuvre de mesures techniques et organisationnelles adéquates qui doivent être mises en place pour assurer la sécurité et la confidentialité des Données Personnelles traitées dans le cadre de chaque Activité de Traitement menée par les Entités Adhérentes, et est en mesure d'en démontrer la conformité. Ces mesures sont déterminées en tenant compte des risques pour les droits et libertés des personnes physiques associés à l'Activité de Traitement pour la Personne Concernée, et notamment s'agissant du traitement de Données Personnelles Sensibles.

A cette fin, les Entités Adhérentes :

- Se conforment aux politiques adoptées en matière de sécurité, de sûreté et de confidentialité de leurs systèmes, locaux et données, telles que révisées et mises à jour périodiquement.
- Mettent en œuvre toute autre procédure de sécurité applicable à l'un quelconque de leurs domaines ou fonctions afin de protéger les données contre tout accès ou utilisation illicite ou non autorisé, notamment afin de prévenir la survenance d'une Violation de Données Personnelles ;
- Conservent des preuves documentées de cette conformité et évaluent régulièrement l'efficacité de ces mesures ;
- S'assurent que tout Collaborateur ayant accès à des Données Personnelles n'agit que sur instruction d'une Entité Adhérente. Lorsqu'une Entité Adhérente agissant en qualité de Responsable du Traitement désigne un Tiers agissant en qualité de Sous-Traitant (par exemple, un prestataire de services), elle ne le fait qu'à la condition que ce dernier présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, y compris les mesures de sécurité régissant le traitement sous-traité de Données Personnelles à effectuer, et doit s'assurer du respect du Droit Applicable.

L'Entité Adhérente documente l'évaluation de ces garanties et conserve les justificatifs de l'ensemble des vérifications préalables effectuées.

- 5.2 Le traitement de Données Personnelles par un Sous-Traitant doit être régi par des clauses contractuelles écrites (c'est-à-dire par un Accord de Protection des Données). Les clauses contractuelles donnent instruction au Sous-Traitant et stipulent, en particulier, que celui-ci doit :
- Tenir et mettre à la disposition de l'Entité Adhérente une documentation complète démontrant sa conformité à ces obligations ;
 - N'agir que conformément aux instructions de l'Entité Adhérente lors du traitement des Données Personnelles, y compris en ce qui concerne les transferts, et informer sans délai l'Entité Adhérente s'il estime qu'une instruction constitue une violation du Droit de l'UE ou des dispositions du Droit Applicable ;
 - S'assurer que toute personne ayant accès aux Données Personnelles est soumise à une obligation de confidentialité ;
 - Ne recourir à un sous-traitant ultérieur que si l'Entité Adhérente a donné son autorisation écrite préalable spécifique ou générale, et à condition que l'accord avec le sous-traitant ultérieur protège les Données Personnelles selon le même niveau d'exigence requis du prestataire de services. En cas d'autorisation écrite générale, le

Sous-Traitant informe l'Entité Adhérente agissant en qualité de Responsable du Traitement de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants ultérieurs, donnant ainsi à ladite Entité Adhérente la possibilité de s'opposer à ces changements ;

- Assister l'Entité Adhérente pour garantir le respect de ses obligations en tant que Responsable du Traitement au titre du Droit Applicable, notamment en ce qui concerne la déclaration des incidents de sécurité des données et la réponse aux demandes des personnes souhaitant exercer leurs droits en matière de protection des données ;
- Compte tenu de la nature du traitement de Données Personnelles, assister l'Entité Adhérente par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour l'accomplissement des obligations de l'Entité Adhérente de donner suite aux demandes des Personnes Concernées d'exercer leurs Droits.
- Restituer ou supprimer les Données Personnelles ainsi que toute copie existante, au choix du Responsable du Traitement, dès lors qu'il a achevé ses prestations ; et
- Mettre à la disposition de l'Entité Adhérente toutes les informations dont elle pourrait avoir besoin afin de garantir le respect de ces obligations et contribuer aux audits, y compris les inspections, menés par le Responsable du Traitement ou par tout autre auditeur mandaté par le Responsable du Traitement. Le Sous-Traitant informe immédiatement le Responsable du Traitement si, selon lui, une instruction enfreint le droit de l'Union européenne ou d'autres Droits Applicables.
- Mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en tenant compte de l'état de l'art, des coûts de mise en œuvre, ainsi que de la nature, de la portée, du contexte et des finalités du traitement de Données Personnelles, de même que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.

6. Durée de conservation limitée des Données Personnelles

- 6.1 Chaque Activité de Traitement doit être mise en œuvre pour une durée déterminée ou déterminable de sorte que les Données Personnelles ne soient pas traitées et conservées au-delà de ce qui est strictement nécessaire à la réalisation de la finalité définie du traitement.
- 6.2 Chaque Entité Adhérente se conforme aux durées de conservation et à la Politique de Conservation de SANOFI ainsi qu'aux directives telles que révisées. Elle communique aux Personnes Concernées des informations adéquates sur la durée déterminée ou déterminable de conservation de leurs Données Personnelles.

7. Responsabilité

- 7.1 SANOFI garantit que chaque Activité de Traitement figure dans le Registre des Activités de Traitement du Système de Gestion de la Protection des données, soit par un nouvel enregistrement, soit par couverture d'une entrée existante, et que ce registre est tenu à jour conformément aux Règles de Protection des Données Personnelles de SANOFI applicables.
- 7.2 Chaque Entité Adhérente agissant en qualité de Responsable du Traitement, sous la supervision du Référent à la Protection des Données, tient un Registre des Activités de Traitement relevant de sa responsabilité. L'Entité Adhérente le met à la disposition des Autorités de Protection des Données sur demande. Le Registre des Activités de Traitement doit être tenu par écrit, y compris sous forme électronique. Ce registre doit contenir au moins les informations suivantes :
 - L'identité du ou des Entité(s) Adhérente(s) qui est (sont) le(s) Responsable(s) de Traitement ;
 - La ou les finalité(s) de l'Activité de Traitement ;
 - Les catégories de Personnes Concernées ;
 - Les catégories de Données Personnelles ;
 - Les catégories de Destinataires auxquels les données sont communiquées ;

- Les transferts de Données Personnelles et le(s) Pays Tiers vers le(s)quel(s) les Données Personnelles sont transférées, ainsi que le mécanisme juridique pertinent utilisé à cet effet ;
- Dans la mesure du possible, la durée de conservation envisagée et une description générale des mesures techniques et organisationnelles appliquées aux Activités de Traitement.

7.3 Chaque Entité Adhérente agissant en qualité de Sous-Traitant, quelle que soit sa localisation géographique, sous la supervision du Référent à la Protection des Données, tient un registre des Activités de Traitement qu'elle met en œuvre. L'Entité Adhérente le met à la disposition des Autorités de Protection des Données sur demande. Le Registre des Activités de Traitement doit être tenu par écrit, y compris sous forme électronique. Ce registre doit contenir au moins les informations suivantes :

- L'identité du ou des Entité(s) Adhérente(s) qui est (sont) le(s) Responsable(s) du Traitement ;
- Les catégories des Activités de Traitement ;
- Les transferts de Données Personnelles et le(s) Pays Tiers vers le(s)quel(s) les Données Personnelles sont transférées, ainsi que le mécanisme juridique pertinent utilisé à cet effet ;
- Dans la mesure du possible, la durée de conservation envisagée et une description générale des mesures techniques et organisationnelles appliquées aux Activités de Traitement.

7.4 Les Entités Adhérentes mettent en œuvre les principes de Protection des données *dès la conception* et de Protection des données *par défaut* pour tout nouveau projet (par exemple, systèmes et applications). À cette fin, chaque Activité de Traitement doit, par défaut, mettre en œuvre les paramètres les plus favorables à la protection des données en vue de réaliser l'objectif de protection des données par défaut. Les Entités Adhérentes mettent en place, au moment de la détermination des moyens du traitement et au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées qui sont conçues pour mettre en œuvre les Règles d'Entreprise Contraignantes de manière efficace et pour intégrer les garanties nécessaires dans le traitement. En outre, les Entités Adhérentes mettent en place des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les Données Personnelles nécessaires à chaque finalité spécifique du Traitement soient traitées.

7.5 Les Entités Adhérentes procèdent à une Évaluation des Risques en utilisant le module d'évaluation approprié en fonction de la nature de l'Activité de Traitement (général ou spécifique à l'activité), ainsi que de leur qualification respective au titre du Registre des Activités de Traitement (par exemple, Responsable du Traitement, Sous-Traitant ou Responsable Conjoint du Traitement). Cette évaluation porte sur l'impact des Opérations de Traitement envisagées sur la protection des Données Personnelles, en tenant compte de la nature, de la portée, du contexte et des finalités de l'Activité de Traitement.

Cette évaluation vise à traiter tout risque identifié et à déterminer des mesures de sécurité supplémentaires et/ou des mécanismes additionnels afin de garantir un niveau de protection approprié des droits et libertés des Personnes Concernées, y compris la mise en œuvre de mesures complémentaires telles que précisées au [Principe 11](#) le cas échéant. Elle porte sur l'impact des Opérations de Traitement envisagées sur la protection des Données Personnelles, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement.

7.6 Les Entités Adhérentes sollicitent l'avis du Référent à la Protection des Données et, lorsqu'une Évaluation des Risques indique que l'Activité de Traitement présenterait un risque élevé en l'absence de mesures prises pour atténuer le risque, SANOFI consulte l'Autorité de Contrôle Compétente préalablement à la mise en œuvre de ce traitement.

8. Respect de l'obligation de notification d'une Violation de Données Personnelles

- 8.1 Lorsqu'une Violation de Données Personnelles est détectée, l'incident est géré conformément au Processus de gestion relatif aux Violations de Données Personnelles de SANOFI.
- 8.2 La (les) Entité(s) Adhérente(s) et le(s) Référent(s) à la Protection des Données ainsi que l'Équipe Opérationnelle concernée(s) examinent la nature et la gravité de l'incident. Ils déterminent si, compte tenu des conséquences probables et/ou des risques pour les droits et libertés des Personnes Concernées, des mesures prises ou proposées pour atténuer les effets possibles, il est nécessaire au regard du Droit de l'Union Européenne de notifier la Violation des Données Personnelles (aux) Autorités de Contrôle Compétentes et/ou à l'Autorité de Contrôle Chef de File dans un délai de soixante-douze (72) heures et, le cas échéant, de communiquer sans retard injustifié aux Personnes Concernées.
- 8.3 Le(s) Référent(s) à la Protection des Données et l'Équipe Opérationnelle sont responsables :
- Le cas échéant, de garantir ladite notification à l'Autorité de Contrôle Compétente sans retard injustifié et au plus tard soixante-douze (72) heures après avoir pris connaissance de l'incident, sauf s'il est improbable qu'il en résulte un risque pour les droits et libertés des Personnes Concernées ;
 - De notifier sans retard injustifié toute Violation de Données Personnelles à (aux) Entité(s) Adhérente(s) Responsable(s) de concernée(s) ainsi qu'à l'Entité Adhérente agissant en qualité de Responsable du Traitement lorsque la Violation de Données Personnelles est identifiée par une Entité Adhérente agissant en qualité de Sous-Traitant ;
 - Le cas échéant, de garantir la notification aux Personnes Concernées affectées par la Violation de Données Personnelles si cet incident est susceptible d'engendrer un risque élevé pour leurs droits et libertés, conformément au Droit Applicable ;
 - De s'assurer que toutes les informations relatives à la Violation, à ses effets, aux mesures de remédiation et aux notifications sont documentées et mises à la disposition de la (ou des) l'Autorités Contrôle Compétentes et/ou de la (des) Autorités de Protection des Données Personnelles concernées sur demande.

9. Information et droits des Personnes Concernées

- 9.1 Lorsqu'une Entité Adhérente collecte des Données Personnelles directement auprès d'une Personne Concernée, elle l'informe sans délai des informations suivantes au moment de la collecte des données : l'identité du Responsable du Traitement et les coordonnées du Référent à la Protection des Données, les finalités et le fondement juridique du traitement, les Destinataires ou catégories de Destinataires, tout transfert envisagé, la durée de conservation, ainsi que de ses droits tels qu'énumérés à la section 9.4.

Cette obligation d'information ne s'applique pas lorsque la Personne Concernée dispose déjà de l'ensemble des informations susmentionnées.

- 9.2 Lorsqu'une Entité Adhérente obtient des Données Personnelles par des moyens autres que la collecte directe auprès de la Personne Concernée, elle informe cette personne des informations suivantes : l'identité du Responsable du Traitement et les coordonnées du Référent à la Protection des Données, les finalités et le fondement juridique du traitement, les catégories et les sources des Données Personnelles concernées, les Destinataires ou catégories de Destinataires, tout transfert de données envisagé, la durée de conservation, ainsi que les droits de la Personne Concernée tels qu'énumérés à la section 9.4. Ces informations sont fournies dans un délai raisonnable après l'obtention des Données Personnelles, au plus tard dans un délai d'un mois, ou au moment de la première communication avec la Personne Concernée ou de la première divulgation à un autre Destinataire.

- 9.3 L'Entité Adhérente agissant en qualité de Responsable du Traitement ne fournit pas ces informations à la Personne Concernée lorsqu'il existe un fondement légitime pour ne pas le faire (notamment les exigences de sécurité nationale ou de défense, la prévention ou la détection d'infractions pénales, les procédures judiciaires, les obligations de secret professionnel, les autorisations légales, ou lorsque la fourniture d'informations est impossible ou nécessiterait des efforts disproportionnés) et lorsque la personne a déjà reçu ces informations ou y a accès.

L'Entité Adhérente agissant en qualité de Responsable du Traitement est dispensée de fournir ces informations à la Personne Concernée dans les cas suivants :

- Lorsqu'il existe un fondement légitime pour ne pas le faire, notamment les exigences de sécurité nationale ou de défense, la prévention ou la détection d'infractions pénales, les procédures judiciaires, les obligations de secret professionnel ou toute autre autorisation légale ;
- Lorsque la fourniture de ces informations s'avère impossible ou nécessiterait des efforts disproportionnés ; ou
- Lorsque la Personne Concernée a déjà reçu ces informations ou y a accès.

- 9.4 Sur demande, toute Personne Concernée a le droit d'exercer les droits conférés par le Droit Applicable à l'encontre de toute Entité Adhérente. Dans les cas et dans la mesure où le Droit Applicable le prévoit, ou lorsque le Droit de l'UE s'applique conformément aux dispositions des présentes Règles d'Entreprise Contraignantes, chaque Personne Concernée dispose des droits suivants :

- Obtenir la confirmation qu'un Responsable du Traitement traite ou non des Données Personnelles les concernant et, le cas échéant, obtenir la communication de ces Données Personnelles ainsi que l'accès à celles-ci (*Droit d'Accès*).
- Exiger d'un Responsable du Traitement qu'il :
 - o Rectifie sans retard injustifié toute Donnée Personnelle inexacte et complète les données incomplètes, compte tenu de la finalité de l'Activité de Traitement (*Droit de Rectification*) ;
 - o Restreigne l'Activité de Traitement (*Droit à la Limitation du Traitement*) lorsque :
 - L'exactitude des Données Personnelles est contestée par la Personne Concernée, pendant une durée permettant au Responsable du Traitement de vérifier l'exactitude des Données Personnelles ;
 - Le traitement est illicite mais la Personne Concernée s'oppose à l'effacement et demande la limitation à la place ;
 - Le Responsable du Traitement n'a plus besoin des Données Personnelles mais celles-ci sont nécessaires à la Personne Concernée pour la constatation, l'exercice ou la défense de droits en justice ; ou
 - La Personne Concernée s'est opposée au traitement, en attendant la vérification de la question de savoir si les motifs légitimes du Responsable du Traitement prévalent sur ceux de la Personne Concernée.

Lorsque l'Activité de Traitement fait l'objet d'une limitation, les Données Personnelles concernées ne peuvent, à l'exception de leur conservation, être traitées que :

- Avec le consentement de la Personne Concernée ; 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
- Pour des motifs d'intérêt public important.
- o Efface les Données Personnelles (*Droit à l'Effacement*) sans retard injustifié lorsque :
 - La Personne Concernée s'oppose au traitement et il n'existe pas de motifs légitimes impérieux ;

- Le consentement est retiré et aucun autre fondement juridique n'existe ;
- L'Activité de Traitement est illicite ;
- L'effacement est requis en vertu d'une obligation légale à laquelle le Responsable du Traitement est soumis ;
- Les Données Personnelles ont été collectées dans le cadre de l'offre de services de la société de l'information à des enfants.

Le droit à l'effacement ne s'applique pas lorsque le traitement est nécessaire :

- À l'exercice du droit à la liberté d'expression et d'information ;
- Au respect d'une obligation légale qui requiert le traitement ;
- Pour des motifs d'intérêt public dans le domaine de la santé publique ;
- À des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit à l'effacement est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou
- À la constatation, à l'exercice ou à la défense de droits en justice.

Lorsque le Droit de Rectification, le Droit à la Limitation du Traitement ou le Droit à l'Effacement sont exercés, l'Entité Adhérente notifie à tous les Destinataires auxquels des Données Personnelles ont été communiquées la rectification, la limitation ou l'effacement effectué, sauf si cette notification s'avère impossible ou nécessite des efforts disproportionnés, et informe la Personne Concernée de ces Destinataires sur demande.

- S'opposer, à tout moment pour des motifs tenant à leur situation particulière, au traitement de leurs Données Personnelles fondé sur l'exécution d'une mission d'intérêt public ou sur les intérêts légitimes de l'Entité Adhérente ou d'un Tiers. L'Entité Adhérente cesse alors de traiter les Données Personnelles, à moins qu'elle ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts, droits et libertés de la Personne Concernée, ou pour la constatation, l'exercice ou la défense de droits en justice (*Droit d'Opposition*).
- Recevoir les Données Personnelles qui ont été traitées par une ou des Entités Adhérentes, dans un format structuré, couramment utilisé et lisible par machine, et transmettre ces informations à un autre Responsable du Traitement, si certaines conditions s'appliquent (*Droit à la Portabilité*).
- Retirer leur consentement à tout moment lorsque le traitement de Données Personnelles est fondé sur le consentement. Le retrait du consentement ne porte pas atteinte à la licéité du traitement fondé sur le consentement effectué antérieurement au retrait.
- Ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, qui produisent des effets juridiques les concernant ou les affectent de manière significative de façon similaire, le droit de contester la décision et d'exiger un examen humain de la décision (*Droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage*). Ce droit ne s'applique pas lorsque la décision :
 - o Est nécessaire à la conclusion ou à l'exécution d'un contrat entre la Personne Concernée et le Responsable du Traitement ;
 - o Est autorisée par le Droit de l'Union Européenne auquel l'Entité Adhérente agissant en qualité de Responsable du Traitement est soumise et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés ainsi que des intérêts légitimes de la Personne Concernée ;
 - o Est fondée sur le consentement explicite de la Personne Concernée.

Lorsque la prise de décision automatisée est autorisée, la Personne Concernée a le droit de :

- Obtenir l'intervention d'une personne physique de la part du Responsable du Traitement ;
- Exprimer son point de vue et de contester la décision ;
- Recevoir des informations utiles sur la logique sous-jacente au traitement automatisé, ainsi qu'une explication de la décision rendue et de la portée et des conséquences envisagées d'une telle Activité de Traitement pour la Personne Concernée.

Les décisions automatisées ne peuvent être fondées sur des Données Personnelles Sensibles que si l'une des conditions suivantes est remplie :

- La Personne Concernée a donné son consentement explicite pour une ou plusieurs finalités déterminées, sauf lorsque le Droit de l'Union Européenne prévoit que l'interdiction ne peut être levée par le consentement de la Personne Concernée ; ou
- L'Activité de Traitement est nécessaire pour des motifs d'intérêt public important sur la base du Droit de l'Union Européenne, lequel doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés ainsi que des intérêts légitimes de la Personne Concernée.

Chaque Entité Adhérente met en œuvre des mesures techniques et organisationnelles appropriées, y compris des garanties, afin d'assurer l'exactitude des Données Personnelles utilisées dans la prise de décision automatisée et de prévenir les effets discriminatoires.

9.5 Dans les cas et dans la mesure où le Droit Applicable le prévoit, ou lorsque le Droit de l'Union Européenne s'applique conformément aux dispositions de ces Règles d'Entreprise Contraignantes, chaque Personne Concernée dispose des droits suivants :

- Soumettre une Demande d'Exercice des Droits au traitement de Données Personnelles entrant dans le champ d'application des présentes Règles d'Entreprise Contraignantes. La demande est traitée conformément aux Règles de Protection des Données Personnelles de SANOFI par l'Entité Adhérente.
- Déposer une réclamation auprès de l'Autorité de Contrôle Compétente concernant le traitement de Données Personnelles entrant dans le champ d'application des présentes Règles d'Entreprise Contraignantes. La réclamation est traitée conformément aux Règles de Protection des Données Personnelles de SANOFI par l'Entité Adhérente.

10. Garantir une protection adéquate pour le transfert de Données Personnelles

10.1 *SANOFI ne transfère pas de Données Personnelles vers un Pays Tiers sans garantir une protection adéquate conformément aux normes établies par les présentes BCR SANOFI*

En principe, les transferts transfrontaliers de Données Personnelles vers un Pays Tiers et/ou un Tiers situé dans un Pays Tiers ne sont pas autorisés en l'absence d'un cadre approprié ou d'une justification prévue par le Droit Applicable, tels que, par exemple, la signature de clauses contractuelles types, lesquelles assurent la protection des Données Personnelles faisant l'objet du transfert.

Aucune Entité Adhérente ne peut transférer des Données Personnelles à l'international sans avoir préalablement et intégralement satisfait aux mesures requises par les lois régissant de tels transferts, y compris en ce qui concerne les Transferts Ultérieurs en provenance d'un Pays Tiers.

10.2 SANOFI garantit la protection adéquate de toute Donnée Personnelle susceptible d'être transférée ultérieurement en dehors de l'EEE

L'Entité Adhérente veille à ce que toute Donnée Personnelle transférée dans le cadre des BCR de SANOFI ne fasse l'objet d'un Transfert Ulérieur en dehors de l'EEE vers des Tiers que si l'une des conditions suivantes est remplie, conformément au Droit de l'Union Européenne :

- Le transfert est effectué vers un Pays Tiers reconnu par la Commission Européenne comme assurant un niveau de protection adéquate ; ou
- Le transfert est soumis à des garanties essentiellement équivalentes à celles offertes par le Droit de l'Union Européenne, compte tenu des circonstances spécifiques du Transfert Ulérieur.

Dans des circonstances exceptionnelles, lorsque le Transfert Ulérieur ne peut reposer sur une adéquation ou sur des garanties appropriées au titre du Droit Applicable, le transfert ne peut avoir lieu que si l'une des dérogations principales suivantes s'applique :

- La Personne Concernée a donné son consentement explicite au transfert envisagé après avoir été informée des risques éventuels ;
- Le transfert est nécessaire à l'exécution d'un contrat entre la Personne Concernée et l'Exportateur de Données, ou à la mise en œuvre de mesures précontractuelles ;
- Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la Personne Concernée entre l'Exportateur de Données et une autre partie ;
- Le transfert est nécessaire pour des motifs importants d'intérêt public reconnus par le Droit de l'Union Européenne ;
- Le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la Personne Concernée ou d'autres personnes, lorsque la Personne Concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- Le transfert a lieu au départ d'un registre qui, conformément au Droit de l'Union Européenne, est destiné à fournir des informations au public.

Ou, si aucune des dérogations susmentionnées ne s'applique, le transfert ne peut avoir lieu à titre exceptionnel que si :

- Le transfert n'est pas répétitif ;
- Il ne concerne qu'un nombre limité de Personnes Concernées ;
- Il est nécessaire aux fins d'intérêts légitimes impérieux poursuivis par l'Exportateur de Données ;
- Il comprend des garanties appropriées ; et
- L'Autorité de Protection des Données compétente en est informée.

Dans tous les cas, tout Transfert Ulérieur doit garantir une protection continue des Données Personnelles à un niveau essentiellement équivalent à celui garanti par le Droit de l'Union Européenne tout au long de la chaîne de transfert.

11. Mesures en cas de législation nationale empêchant le respect des BCR de SANOFI

11.1 Évaluation des lois et pratiques des Pays Tiers

Les Entités Adhérentes assurent une veille des évolutions dans les Pays Tiers susceptibles d'affecter l'évaluation du niveau de protection et les décisions qui en résultent concernant les transferts de Données Personnelles vers ces pays.

Avant de transférer des Données Personnelles vers un Pays Tiers, l'Entité Adhérente agissant en qualité d'Exportateur de Données évalue si les lois et pratiques de ce pays, y compris toute obligation de divulguer des Données Personnelles ou toute mesure autorisant l'accès par les autorités publiques, empêchent l'Entité Adhérente agissant en qualité d'Importateur de Données de remplir ses obligations au titre des présentes Règles d'Entreprise Contraignantes.

Cette évaluation repose sur le principe que les lois et pratiques d'un Pays Tiers qui respectent l'essence des droits et libertés fondamentaux et n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique ne contredisent pas les présentes Règles d'Entreprise Contraignantes

En outre, cette évaluation repose sur le principe que les lois et pratiques du Pays Tiers de destination respectent les droits et libertés fondamentaux de la Personne Concernée et n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour sauvegarder l'un des objectifs suivants :

- La sécurité nationale ;
- La défense ;
- La sécurité publique ;
- La prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- D'autres objectifs importants d'intérêt public général notamment un intérêt économique ou financier important, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ;
- La protection de l'indépendance de la justice et des procédures judiciaires ;
- La prévention, la détection, l'enquête et la poursuite de manquements à la déontologie des professions réglementées ;
- Une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés par les objectifs précédents ;
- La protection de la Personne Concernée ou des droits et libertés d'autrui ; et/ou
- L'exécution des demandes de droit civil

Les Entités Adhérentes documentent cette évaluation et la mettent à la disposition de l'Entité Adhérente Responsable concernée et, sur demande, de l'Autorité de Contrôle Compétente. Dans le cadre de l'évaluation des lois et pratiques d'un Pays Tiers susceptibles d'affecter le respect des engagements contenus dans les présentes Règles d'Entreprise Contraignantes, les Entités Adhérentes tiennent dûment compte, en particulier, des éléments suivants :

- Les circonstances spécifiques des transferts de Données Personnelles ou des ensembles de transferts de Données Personnelles, ainsi que les Transferts Ultérieurs envisagés au sein du même Pays Tiers ou vers un autre, notamment les finalités du transfert de Données Personnelles, les Entités Adhérentes et autres Destinataires impliqués, le secteur économique dans lequel s'effectue le transfert de Données Personnelles, les catégories et le format des données transférées, le lieu de l'Activité de Traitement et les canaux de transmission utilisés pour transférer les Données Personnelles ;
- Les lois et pratiques pertinentes du Pays Tiers au regard des circonstances du transfert de Données Personnelles, y compris toute obligation de divulguer des Données Personnelles aux autorités publiques et celles prévoyant l'accès aux données en transit, ainsi que les limitations et garanties applicables ; et
- Toute garantie contractuelle, technique ou organisationnelle pertinente susceptible de devoir être mise en œuvre en complément des présentes Règles d'Entreprise Contraignantes, y compris les mesures appliquées lors de la transmission et au traitement des Données Personnelles dans le pays de destination.

Si une Entité Adhérente agissant en qualité d'Importateur de Données a des raisons de croire qu'elle est soumise à des lois qui l'empêcheraient de remplir ses obligations au titre des présentes Règles d'Entreprise Contraignantes, y compris du fait d'une modification des lois d'un Pays Tiers ou d'une mesure indiquant une application de ces lois en pratique qui n'est pas conforme aux BCR de SANOFI, ladite Entité Adhérente en informe promptement :

- La(les) Entité(s) Adhérente(s) situées dans l'UE agissant en qualité d'Exportateur(s) des Données,

- Le *Data Privacy Office*, y compris le(s) Référent(s) la Protection des Données concerné(s),
- L'(les) Entités(s) Adhérente(s) concernée(s).

11.2 Identification et mise en œuvre de mesures supplémentaires devant être adoptées par les Entités Adhérentes agissant en qualité d'Exportateur(s) de Données et/ou d'Importateur(s) de Données afin de leur permettre de respecter leurs obligations au titre des BCR de Sanofi, conformément aux Recommandations 1/2022 du Comité Européen de la Protection des Données.

Lorsqu'il est nécessaire de mettre en œuvre des garanties ou des mesures supplémentaires (par exemple, des mesures techniques ou organisationnelles visant à assurer la sécurité et la confidentialité) en complément de celles prévues par les présentes Règles d'Entreprise Contraignantes, l'Entité Adhérente agissant en qualité d'Exportateur de Données informe l'Entité Adhérente Responsable agissant en qualité d'Importateur de Données ainsi que les Référents à la Protection des Données compétents des mesures identifiées devant être adoptées pour faire face à la situation.

Chaque Entité Adhérente faisant partie de l'Equipe Opérationnelle, avec le soutien du *Data Privacy Office* et du (des) Référent(s) à la Protection des Données concernés, évalue et documente les évaluations de manière appropriée, y compris les mesures supplémentaires sélectionnées et mises en œuvre.

Les Entités Adhérentes documentent cette évaluation et la mettent à la disposition de l'Entité Adhérente Responsable et, sur demande, de l'Autorité de Contrôle Compétente.

Le *Data Privacy Office* informe toutes les Entités Adhérentes des résultats de ladite évaluation, afin que toute mesure supplémentaire identifiée puisse être appliquée dans le cas où le même type de transferts de Données Personnelles serait effectué, ou lorsqu'il n'est pas possible de mettre en œuvre des mesures supplémentaires efficaces, les transferts de Données Personnelles en cause peuvent être suspendus ou interrompus. Après vérification de ces informations, l'Entité Adhérente agissant en qualité d'Importateur de Données s'engage à mettre en œuvre promptement les mesures supplémentaires définies ou à identifier des mesures additionnelles si nécessaire afin de respecter ses obligations au titre des présentes Règles d'Entreprise Contraignantes.

Les Entités Adhérentes agissant en qualité d'Importateurs de Données notifient promptement à l'Exportateur de Données concerné si, lors de l'utilisation des BCR de SANOFI comme instrument de transferts de Données Personnelles, elles ont des raisons de croire qu'elles sont soumises à des lois ou pratiques qui les empêcheraient de respecter leurs obligations au titre des présentes Règles d'Entreprise Contraignantes, y compris du fait de modifications des lois du Pays Tiers ou de mesures spécifiques (telles qu'une Demande de Divulgence de Données Personnelles).

Après vérification de cette notification, l'Entité Adhérente agissant en qualité d'Exportateur de Données, conjointement avec le *Data Privacy Office* et l'Entité Adhérente Responsable, s'engage à identifier promptement des mesures supplémentaires (par exemple, des mesures techniques ou organisationnelles visant à assurer la sécurité et la confidentialité) devant être adoptées respectivement par les Entités Adhérentes agissant en qualité d'Exportateur(s) de Données et d'Importateur(s) de Données, afin de leur permettre de respecter leurs obligations au titre des BCR de SANOFI. Il en va de même si une Entité Adhérente agissant en qualité d'Exportateur de Données a des raisons de croire qu'une Entité Adhérente agissant en qualité d'Importateur de Données ne peut plus respecter ses obligations au titre des présentes Règles d'Entreprise Contraignantes.

Lorsque l'Entité Adhérente agissant en qualité d'Exportateur de Données, conjointement avec les Référents à la Protection des Données concernés et l'Entité Adhérente Responsable, estime que l'Importateur de Données ne peut se conformer aux BCR de SANOFI, malgré les mesures supplémentaires mises en œuvre, ou lorsqu'elle en reçoit l'instruction d'une Autorité de Contrôle Compétente, elle doit immédiatement :

- Suspendre le transfert de Données Personnelles en cause ;
- Suspendre tous les autres transferts pour lesquels la même évaluation et le même

raisonnement conduiraient à un résultat similaire ;

- Maintenir cette suspension jusqu'à ce que la conformité soit à nouveau assurée ou que le transfert de Données Personnelles prenne fin.

Si la conformité aux BCR de SANOFI ne peut être rétablie dans un délai d'un (1) mois à compter de la suspension, l'Exportateur de Données met fin au transfert de Données Personnelles ou à l'ensemble de transferts de Données Personnelles. Toute Donnée Personnelle transférée avant cette suspension (ainsi que toute copie de celle-ci) doit (au choix de l'Exportateur de Données) être soit restituée, soit détruite.

Les Entités Adhérentes agissant en qualité d'Exportateurs de Données surveillent de manière continue, et le cas échéant en collaboration avec les Importateurs de Données concernés, les évolutions dans les Pays Tiers vers lesquels les Exportateurs de Données ont transféré des Données Personnelles susceptibles d'affecter l'évaluation initiale du niveau de protection et les décisions prises en conséquence concernant ces transferts de Données Personnelles.

En cas de doute quant à l'interprétation du Droit Applicable, le Référent Local à la Protection des données et/ou *Data Privacy Office* sollicite l'avis des Autorités de Protection des Données ou de conseils externes afin de garantir le respect des dispositions les plus strictes.

11.3 Gestion des Demandes d'Accès aux Données Personnelles par une autorité publique

Obligation de notifier. Sous réserve des lois applicables, l'Entité Adhérente agissant en qualité d'Importateur de Données notifie sans délai l'Exportateur de Données, le *Data Privacy Office* et, dans la mesure du possible, la Personne Concernée (avec l'aide de l'Exportateur de Données) si elle :

- Reçoit une demande juridiquement contraignante d'une autorité publique, en vertu des lois du pays de destination ou d'un autre Pays Tiers, aux fins de divulgation de Données Personnelles transférées en application des présentes Règles d'Entreprise Contraignantes (par exemple, une autorité chargée de l'application de la loi ou un organe de sécurité de l'État) ;
- Prend connaissance de tout accès direct par des autorités publiques aux Données Personnelles transférées en application des présentes Règles d'Entreprise Contraignantes ;
- Prend connaissance de la réception par un Tiers (c'est-à-dire des prestataires de services, fournisseurs ou partenaires) d'une demande juridiquement contraignante d'une autorité publique, en vertu des lois du pays dans lequel ce Tiers est établi, aux fins de divulgation d'informations et/ou de Données Personnelles transférées par une Entité Adhérente en application des garanties appropriées mises en œuvre dans le contrat ou tout autre document contraignant.

Contenu de la notification. Cette notification doit inclure toutes les informations dont dispose l'Importateur de Données concernant les Données Personnelles demandées, l'identité de l'autorité requérante, le fondement juridique de la demande et le projet de réponse.

S'il lui est interdit de notifier l'Exportateur de Données et/ou la Personne Concernée, l'Importateur de Données met tout en œuvre pour obtenir une levée de cette interdiction, en vue de communiquer le maximum d'informations dans les meilleurs délais. L'Importateur de Données documente ces efforts et en apporte la preuve sur demande de l'Exportateur de Données.

Dans la mesure où il reçoit des Demandes d'Accès aux Données Personnelles émanant d'une autorité publique, et selon ce qui est pertinent, l'Importateur de Données fournit périodiquement à l'Exportateur de Données des rapports détaillant l'ensemble des demandes reçues, en y incluant autant d'informations pertinentes que possible. S'il lui est interdit de communiquer ces informations, l'Importateur de Données en informe sans délai l'Exportateur de Données et le *Chief Privacy Officer* de cette restriction.

L'Importateur de Données conserve toutes les informations relatives aux demandes aussi longtemps que les Données Personnelles sont soumises aux BCR de SANOFI et les met à la disposition de l'Autorité de Contrôle Compétente sur demande.

Évaluation juridique. L'Importateur de Données examine la légalité de chaque Demande d'Accès aux Données Personnelles. Cet examen porte spécifiquement sur la question de savoir si la demande s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante. Après une évaluation approfondie, l'Entité Adhérente agissant en qualité d'Importateur de Données conteste la demande si elle a des motifs raisonnables de la considérer comme illicite au regard du droit local, des obligations internationales ou des principes de courtoisie internationale. Dans les mêmes conditions, elle explore les voies de recours disponibles et sollicite des mesures provisoires afin de suspendre les effets de la demande jusqu'à ce qu'une autorité judiciaire compétente se soit prononcée sur le fond. L'Importateur de Données ne divulgue pas les Données Personnelles demandées tant que les règles de procédure applicables ne l'y obligent pas.

L'Importateur de Données documente toutes les évaluations juridiques et contestations relatives aux demandes, met cette documentation à la disposition de l'Exportateur de Données et, sur demande, des Autorités de Contrôle Compétentes.

En aucun cas une Entité Adhérente ne transfère de Données Personnelles à une autorité publique d'un Pays Tiers de manière massive, disproportionnée et anarchiques au point d'excéder ce qui est nécessaire dans une société démocratique. En outre, lorsqu'il répond à une demande de divulgation, l'Importateur de Données fournit la quantité minimale d'informations autorisée, sur la base d'une interprétation raisonnable de la demande. Cette approche garantit que toute divulgation demeure proportionnée et limitée à ce qui est strictement nécessaire.

Pour les Entités Adhérentes situées dans l'EEE, tout jugement d'un tribunal ou toute décision d'une autorité administrative d'un Pays Tiers exigeant d'un Responsable du Traitement ou d'un Sous-Traitant qu'il transfère ou divulgue des Données Personnelles ne peut être reconnu ou exécuté que s'il est fondé sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le Pays Tiers requérant et l'Union européenne ou un État membre de l'EEE. Ceci est sans préjudice des autres fondements de transfert prévus au Chapitre V du RGPD.

Si une exigence légale à laquelle une Entité Adhérente est soumise dans un Pays Tiers est susceptible de compromettre significativement les garanties offertes par les présentes Règles d'Entreprise Contraignantes, l'Importateur de Données doit en informer sans délai le *Chief Privacy Officer* et l'Exportateur de Données. Le *Chief Privacy Officer* notifie alors l'Autorité de Contrôle Compétente et, dans la mesure du possible, les Personnes Concernées. Cela inclut notamment :

- Toute Demande d'Accès aux Données Personnelles juridiquement contraignante émanant d'une autorité publique aux fins de divulgation de Données Personnelles. Dans de tels cas, l'Autorité de Contrôle Compétente doit être clairement informée de la demande, y compris des détails concernant les données demandées, l'autorité requérante, le fondement juridique de la divulgation et la réponse fournie (sauf interdiction légale, telle qu'une interdiction de droit pénal visant à préserver la confidentialité d'une enquête répressive) ; et
- Tout accès direct par des autorités publiques aux Données Personnelles transférées en vertu des présentes Règles d'Entreprise Contraignantes conformément au Droit Applicable de l'Importateur de Données. Cette notification doit inclure toutes les informations disponibles (sauf interdiction légale, telle qu'une interdiction de droit pénal visant à préserver la confidentialité d'une enquête répressive).

12. Conformité aux BCR de SANOFI

- 12.1 Aucun transfert de Données Personnelles ne peut être effectué vers une Entité Adhérente agissant en qualité d'Importateur de Données à moins que cette entité ne soit effectivement liée par les BCR de SANOFI et soit en mesure d'en assurer le respect.
- 12.2 Une Entité Adhérente agissant en qualité d'Importateur de Données informe sans délai l'Exportateur de Données si elle est dans l'impossibilité de se conformer aux BCR de SANOFI, quelle qu'en soit la raison, y compris les raisons décrites au [Principe 11](#).
- 12.3 Lorsqu'il est constaté qu'un Importateur de Données a manqué aux BCR de SANOFI ou est dans l'impossibilité de s'y conformer, l'Entité Adhérente agissant en qualité d'Exportateur de Données suspend le transfert de Données Personnelles.

13. Restitution ou suppression des Données Personnelles

- 13.1. Une Entité Adhérente agissant en qualité d'Importateur de Données doit, au choix de l'Exportateur de Données, immédiatement restituer ou supprimer toutes les Données Personnelles en sa possession qui ont été transférées en vertu des présentes BCR SANOFI (y compris toute copie de celles-ci) si :
- L'Exportateur de Données a suspendu le transfert de Données Personnelles et que la conformité aux BCR de SANOFI n'est pas rétablie dans un délai raisonnable, et en tout état de cause dans un délai d'un (1) mois à compter de la décision de suspension ; ou
 - L'Importateur de Données commet un manquement substantiel ou persistant aux BCR de SANOFI ; ou
 - L'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 au titre des BCR de SANOFI.
- 13.2. Dans tous les cas, lorsqu'une Entité Adhérente agissant en qualité d'Importateur de Données cesse d'être en mesure de se conformer aux présents principes et aux BCR de SANOFI ou cesse d'y être liée, ou lorsque l'Entité Adhérente agissant en qualité d'Exportateur de Données en fait la demande, l'Importateur de Données :
- Informe l'Exportateur de Données sans délai ;
 - Sur instruction de l'Exportateur de Données, l'Importateur de Données peut conserver, cesser le traitement des Données Personnelles, restituer ou supprimer toutes les Données Personnelles ainsi que toute copie de celles-ci ;
 - S'assure que tout Tiers auquel les Données Personnelles ont été divulguées respecte les mêmes obligations concernant la restitution ou la suppression des Données Personnelles, y compris toute copie de celles-ci.
- 13.3. L'Importateur de Données doit :
- Certifier à l'Exportateur de Données la suppression des Données Personnelles et de toute copie de celles-ci ;
 - Fournir la documentation attestant des mesures prises pour garantir la suppression complète ou la restitution, selon le cas.
- 13.4. Jusqu'à ce que l'ensemble des Données Personnelles et de leurs copies aient été supprimées ou restituées, l'Importateur de Données continue de se conformer aux dispositions des BCR de SANOFI.
- 13.5. Lorsque des lois locales ou nationales dans le pays de l'Importateur de Données interdisent la restitution ou la suppression des Données Personnelles transférées ou de toute copie de celles-ci, sous réserve que ces lois et pratiques satisfassent *aux exigences énoncées au Principe 11.1 (Évaluation des lois et pratiques des Pays Tiers)*, l'Importateur de Données doit :
- Informer l'Exportateur de Données de cette exigence légale ;
 - Garantir qu'il continuera d'assurer le respect des BCR de SANOFI ;
 - Ne traiter les Données que dans la mesure et aussi longtemps que l'exigent les lois locales ou nationales de ce Pays Tiers ; et
 - Mettre en œuvre des mesures techniques et organisationnelles appropriées afin de limiter le traitement à ce qui est légalement requis.

14. Nature contraignante des BCR de SANOFI

- 14.1 Ces Règles d'Entreprise Contraignantes s'imposent juridiquement à toutes les entités de Sanofi qui ont formellement accepté d'y adhérer. Cet engagement obligatoire s'applique non seulement aux entités mais également à l'ensemble de leurs Collaborateurs, qui doivent respecter ces règles dans l'exercice de leur activité professionnelle.

15. Coopération avec les Autorités de Protection des Données

- 15.1 Sanofi coopère pleinement avec les Autorités de Protection des Données et respecte ses propres Règles de Protection des Données. Sanofi veille à ce que les décisions et lignes directrices de ces autorités soient reflétées afin de garantir le respect de ses Règles d'Entreprise Contraignantes. Cela inclut les lignes directrices du Comité Européen de la Protection des Données (CEPD), organe européen qui supervise la protection des données.
- 15.2 Lorsque les Autorités de Protection des Données inspectent ou auditent SANOFI, toutes les entités de SANOFI coopèrent pleinement. Cela signifie que SANOFI fournit toutes les informations nécessaires sur la manière dont les Données Personnelles sont traitées, y compris les résultats de ses propres audits internes, sur demande. Sanofi accueille favorablement les audits et inspections, y compris les visites de ses locaux, car ils contribuent à garantir les bonnes pratiques en matière de protection des données.
- 15.3 Si SANOFI est en désaccord avec une décision officielle d'une Autorité de Protection des Données, SANOFI peut la contester devant les tribunaux du pays concerné, conformément aux lois applicables. Tout désaccord portant sur la manière dont les Autorités de Protection des Données supervisent ces Règles d'Entreprise Contraignantes est tranché par les tribunaux du pays européen où l'autorité est établie, conformément au droit local en matière de protection des données.

16. Réclamation d'une Personne Concernée

- 16.1 Si une personne estime que ses droits ont été violés ou que sa demande concernant ses Données Personnelles a été rejetée, elle peut adresser une réclamation. Les réclamations doivent être soumises par écrit, selon l'une des modalités suivantes :
- En ligne via le formulaire disponible à <https://www.sanofi.com/en/data-protection-contact>,
 - Par courrier à : EBI - Data Privacy Office, 46 Avenue de la Grande Armée 75017 Paris, France.
- 16.2 SANOFI accuse réception de toutes les réclamations dans les cinq (5) jours ouvrables et y répond dans un délai d'un (1) mois à compter de sa réception. Pour les cas complexes, ce délai peut être prolongé de deux (2) mois supplémentaires maximum, auquel cas la personne sera informée avec une explication claire. La réclamation est d'abord traitée par l'équipe locale en charge de la protection des données. Si nécessaire, elle est transmise au *Chief Privacy Officer*. Après examen, Sanofi prend des mesures correctives ou fournit une explication détaillée.
- 16.3 Toute personne conserve le droit de porter sa réclamation devant d'autres instances, qu'elle ait ou non eu recours à la procédure interne de Sanofi ou l'ait menée à son terme. En particulier, toute personne peut :
- Porter plainte auprès des Autorités de Contrôle Compétentes (*voir Droits des Tiers*),
 - Introduire une action en justice devant les tribunaux compétents (*voir Droits des Tiers*),
 - Exercer un recours juridictionnel et obtenir réparation et indemnisation de tout dommage subi (*voir Droit aux recours juridictionnels et à l'indemnisation*).
- 16.4 Ces droits peuvent être exercés à tout moment, indépendamment du fait que la personne ait ou non utilisé la procédure interne de SANOFI.

17. Procédure de mise à jour des BCR de SANOFI

- 17.1 SANOFI peut mettre à jour ces Règles d'Entreprise Contraignantes à tout moment pour refléter les changements du Droit Applicable, les recommandations des autorités ou l'évolution de la structure du Groupe Sanofi, en maintenant le même niveau de protection pour vos Données et ses engagements obligatoires.
- 17.2 Toutes les mises à jour seront publiées sur le site de SANOFI à l'adresse www.sanofi.com
- 17.3 Sanofi conserve un registre détaillant toutes les modifications y compris les dates et les descriptions des changements.
- 17.4 Sanofi notifie annuellement toutes les modifications à l'Autorité de Contrôle Chef de File et sollicite son approbation préalable pour les modifications substantielles.
- 17.5 Toute nouvelle entité de SANOFI doit s'engager formellement à respecter ces règles avant de recevoir des Données Personnelles.

18. Accessibilité aux BCR de SANOFI

- 18.1 Les BCR de SANOFI sont accessibles au public et à jour sur le site internet de SANOFI : www.sanofi.com
- 18.2 Toutes les personnes dont les Données Personnelles sont traitées dans le cadre des BCR de SANOFI doivent être informées de leurs droits en qualité de Tiers Bénéficiaires, s'agissant du traitement de leurs Données Personnelles, ainsi que des moyens d'exercer ces droits.
- 18.3 Toute personne peut également obtenir une copie complète des BCR de SANOFI sur demande.

19. Conflit de lois

- 19.1 Les principes définis dans les BCR de SANOFI constituent le standard minimal de protection des données applicable à toutes les Entités Adhérentes, quelle que soit leur localisation géographique, pour l'ensemble des transferts de Données Personnelles entrant dans le champ d'application des BCR de SANOFI. Lorsque le Droit Applicable local est en conflit avec les présentes Règles d'Entreprise Contraignantes, l'Entité Adhérente doit toujours appliquer le niveau de protection le plus élevé pour les Personnes Concernées, sauf impossibilité légale. Dans tous les cas de conflit, l'Entité Adhérente doit informer sans délai le *Chief Privacy Officer* et se conformer aux exigences supplémentaires précisées au [Principe 11](#).

20. Demande d'Accès aux Données Personnelles émanant d'une autorité gouvernementale

- 20.1 Lorsque les autorités gouvernementales émettent une Demande d'Accès aux Données Personnelles, SANOFI suit une procédure pour s'assurer que toute divulgation reste strictement nécessaire et proportionnée. Cela s'applique quand SANOFI reçoit des demandes juridiquement contraignantes, prend connaissance d'un accès direct ou indirect formulé par des autorités, ou est informée de telles demandes reçues par des prestataires de services.
- 20.2 Si une Entité Adhérente agissant en tant qu'Importateur de Données reçoit une Demande d'Accès aux Données Personnelles, il en informe immédiatement le *Data Privacy Office*, l'Exportateur des Données et, dans la mesure du possible, les Personnes Concernées. Si les lois locales interdisent une telle notification, Sanofi documente ses efforts pour obtenir l'autorisation de procéder à une telle notification.
- 20.3 Chaque demande fait l'objet d'une évaluation juridique approfondie par le département juridique local et les experts en charge de la protection des données afin de garantir le respect des lois applicables et des présentes règles d'entreprise contraignantes.
- 20.4 En aucun cas Sanofi ne transfère de Données Personnelles à une autorité publique - telle qu'une autorité chargée de l'application de la loi, un organe de sécurité de l'État ou toute autre autorité gouvernementale dans un Pays Tiers - de manière massive, disproportionnée et anarchique au point d'excéder ce qui est nécessaire dans une société démocratique. Toute divulgation doit être strictement limitée à ce qui est légalement requis, et proportionnée à l'objectif légitime poursuivi.

Section 3. Droits des Tiers Bénéficiaires

21. Droits des Tiers

- 21.1 Les Personnes Concernées dont les Données Personnelles sont traitées dans l'EEE par une Entité Adhérente agissant en qualité de Responsable du Traitement (c'est-à-dire l'Exportateur de Données) et sont transférées à une Entité Adhérente située dans un Pays Tiers en vertu des BCR de SANOFI (c'est-à-dire l'Importateur de Données) peuvent faire valoir les présentes Règles d'Entreprise Contraignantes en qualité de Tiers Bénéficiaires.
- 21.2 Ces droits ne s'étendent pas aux éléments des BCR de SANOFI relatifs aux mécanismes internes mis en œuvre au sein du Groupe SANOFI.
- 21.3 Les Personnes Concernées disposent des droits suivants au titre des BCR de SANOFI :
- Le droit de se prévaloir des BCR de SANOFI en qualité de Tiers Bénéficiaires, y compris celui d'invoquer ce statut en lui-même ;
 - L'ensemble des principes de protection des données et de la vie privée, ainsi que les exigences de licéité du traitement, tels qu'énoncés à la [Section 1.](#) des présentes Règles d'Entreprise Contraignantes ;
 - Les mesures de sécurité et les obligations de notification des Violations de Données Personnelles ([Section 1.5](#)) ;
 - Les restrictions applicables aux Transferts Ultérieurs vers des Tiers extérieurs au Groupe SANOFI ([Section 1.10.](#)) ;
 - La transparence et l'accès facile aux BCR de SANOFI ([Voir Accessibilité aux BCR de SANOFI](#)) ;
 - Les obligations de SANOFI en cas de lois et pratiques locales affectant la conformité aux BCR de SANOFI ou en cas de demande d'accès gouvernementale ([Section 1.11](#)) ;
 - Les obligations de coopération de SANOFI avec les Autorités de Protection des Données ([Voir Coopération avec les Autorités de Protection des Données](#)) ;
 - Les droits d'information, d'accès, de rectification, d'effacement, de limitation, de notification relative à la rectification, à l'effacement ou à la limitation, d'opposition au traitement et le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, ainsi que le droit de déposer une réclamation via la procédure interne de réclamation de SANOFI ([Section 1.9](#)) ;
 - Le droit d'être informé dans les meilleurs délais de toute mise à jour des BCR de SANOFI et de la liste des Entités Adhérentes ([voir Procédure de mise à jour des BCR de SANOFI](#)) ;
 - Le droit de déposer une réclamation conformément à la Procédure de Gestion des Réclamations ([voir Droit aux recours juridiques et à l'indemnisation](#)), ainsi que le droit de saisir l'Autorité de Contrôle Chef de File, l'Autorité de Contrôle Compétente ou toute Autorité de Contrôle Compétente dans la juridiction de leur résidence habituelle, de leur lieu de travail ou du lieu de l'infraction alléguée ;
 - Le droit à un recours juridique et à réparation en cas de violation de leurs droits au titre des présentes BCR SANOFI résultant du traitement de leurs Données Personnelles en violation des présentes BCR SANOFI ([voir Droit aux recours juridiques et à l'indemnisation](#)) ;
 - Le droit à indemnisation pour toute Personne Concernée ayant subi un préjudice matériel ou moral résultant d'une violation des BCR de SANOFI, laquelle dispose du droit de recevoir une indemnisation de la part de SANOFI ([voir Droit aux recours juridiques et à l'indemnisation](#)) ;
 - Le droit d'engager une procédure judiciaire pour faire respecter les BCR de SANOFI devant les juridictions compétentes d'un État Membre de l'EEE (soit la juridiction dans laquelle le Responsable du Traitement est établi), devant l'Autorité de Contrôle Chef de File ou dans la juridiction de la résidence habituelle de la Personne Concernée ([voir Droit aux recours juridiques et à l'indemnisation](#)) ;
 - Le droit de représentation permettant aux Personnes Concernées de mandater un organisme, une organisation ou une association à but non lucratif, dûment constitué conformément au Droit de l'Union Européenne.

Les procédures détaillées pour l'exercice de ces droits en tant que Personne Concernée, y compris la gestion des réclamations, les voies de recours judiciaires et l'indemnisation, sont précisées à la [Section 3. Droit aux recours juridiques et à l'indemnisation](#).

- 21.4 Toute demande relative aux Droits des Tiers doit être adressée à l'Entité Adhérente concernée via le formulaire de Demande d'Exercice des Droits et sera gérée par le Référent à la Protection des Données compétent et l'Équipe Opérationnelle.
- 21.5 L'Entité Adhérente concernée doit informer dans les meilleurs délais la Personne Concernée du résultat de sa demande, et ce au plus tard dans un délai d'un (1) mois à compter de sa réception. Cette notification doit inclure, le cas échéant, les motifs de l'absence de suite donnée à la demande ainsi que les options disponibles pour déposer une réclamation auprès de l'Autorité de Contrôle Compétente ou pour exercer un recours juridique. Le délai d'un (1) mois peut être prolongé de deux (2) mois supplémentaires si nécessaire, eu égard à la complexité et au volume des demandes.
- 21.6 Le Référent à la Protection des Données compétent doit notifier à la Personne Concernée toute prolongation de ce délai dans un délai d'un (1) mois à compter de la réception de la demande, en indiquant les motifs du délai supplémentaire.
- 21.7 L'ensemble des communications, actions et informations fournies en réponse à une Demande d'Exercice des Droits sont gratuites. Si les demandes de la Personne Concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, l'Entité Adhérente concernée peut soit :
- Mettre à la charge de la Personne Concernée des frais raisonnables correspondant aux coûts administratifs liés à la fourniture des informations ou communications ou à l'exécution de l'action demandée ; soit
 - Refuser de donner suite à la demande.
- 21.8 L'Entité Adhérente concernée doit démontrer que la demande est manifestement infondée ou excessive.

22. Droit aux recours juridiques et à l'indemnisation

- 22.1 La présente section définit le cadre et les mécanismes permettant de faire valoir les Droits des Tiers tels que décrits à la [Section 3. Droits des Tiers Bénéficiaires](#). Elle expose les différentes voies de recours disponibles pour les Personnes Concernées ainsi que les mécanismes d'exécution destinés à garantir une protection effective de leurs droits, tout en établissant des principes clairs de responsabilité au sein du Groupe SANOFI.
- 22.2 **Compétence juridique et responsabilité.** En cas de violation des BCR de SANOFI par un Importateur de Données, les Personnes peuvent engager une procédure à l'encontre de SANOFI devant les juridictions compétentes ou d'autres autorités judiciaires, y compris les Autorités de Contrôle Compétentes dans l'EEE et l'Autorité de Contrôle Chef de File, lorsque :
- L'Entité Adhérente dispose d'un établissement ;
 - La personne a sa résidence habituelle, son lieu de travail ou le lieu de l'infraction alléguée ;
 - L'Autorité de Contrôle Chef de File est établie ;
 - Les personnes disposent des droits et voies de recours à l'encontre de l'Entité Adhérente Responsable concernée comme si la violation avait été commise par cette dernière en France, indépendamment du fait que la violation ait été effectivement commise par l'Importateur de Données ou l'Exportateur de Données.
- 22.3 **Indemnisation.** Les Personnes Concernées peuvent, à tout moment, solliciter une indemnisation auprès de l'Entité Adhérente Responsable concernée pour tout préjudice matériel ou moral subi à la suite d'une violation des BCR de SANOFI, telle que constatée par une juridiction ou toute autre autorité compétente.
- 22.4 **Charge de la preuve.** Lorsqu'une Personne Concernée est en mesure de démontrer qu'elle a subi un préjudice et d'établir des faits permettant de présumer que ce préjudice résulte d'une violation des BCR de SANOFI, la charge de la preuve incombe à l'Entité Adhérente Responsable. Celle-ci doit démontrer que l'Entité Adhérente située en dehors de l'EEE n'était pas responsable de la violation à l'origine de ces préjudices, ou qu'aucune violation de cette nature n'a eu lieu.

22.5 Si l'Entité Adhérente Responsable concernée apporte une telle preuve, elle ne peut être tenue responsable du préjudice invoqué par la Personne Concernée.

Les Règles d'Entreprise Contraignantes de SANOFI prennent effet dès leur approbation par l'Autorité de Contrôle Chef de File et s'appliquent aux Filiales dès la signature de l'Accord d'Acceptation des Règles d'Entreprise Contraignantes.

Aucune Donnée Personnelle ne peut être transférée à une Filiale de SANOFI à moins que celle-ci ne soit soumise aux présentes Règles d'Entreprise Contraignantes et au Cadre de Transfert de SANOFI. Lorsqu'un Importateur de Données n'est plus lié par les BCR de SANOFI, il doit immédiatement restituer ou supprimer l'ensemble des Données Personnelles (y compris toute copie) transférées en vertu des présentes Règles d'Entreprise Contraignantes. Toutefois, l'Importateur de Données peut conserver les Données Personnelles transférées s'il prend des engagements juridiquement contraignants visant à protéger ces données conformément au Chapitre V du RGPD.

PART III. ANNEXES

Annexe 1. Définitions

Le contenu des Règles d'Entreprise Contraignantes de SANOFI doit être interprété conformément aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des Données Personnelles et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (le « RGPD »).

Les termes ou expressions commençant par une lettre majuscule ont le sens qui leur est attribué dans le RGPD, les Recommandations 1/2022 relatives à la demande d'approbation ainsi qu'aux éléments et principes devant figurer dans les Règles d'Entreprise Contraignantes pour les Responsables du Traitement (art. 47 du RGPD) du CEPD (les « Recommandations 1/2022 du CEPD »). En cas de contradiction, les définitions du RGPD prévalent.

Aux fins des présentes Règles d'Entreprise Contraignantes SANOFI, les termes suivants ont le sens qui leur est attribué ci-après :

Accord d'Acceptation des Règles d'Entreprise Contraignantes	Accord conclu au sein du groupe SANOFI par lequel les Filiales s'engagent à se conformer aux Règles d'Entreprise Contraignantes de SANOFI.
Accord de Protection des Données	Tout contrat, annexe ou ensemble de clauses contractuelles conclu entre une ou plusieurs Filiale(s) de SANOFI et un ou plusieurs Tiers, régissant spécifiquement une Activité de Traitement conformément au Droit Applicable (incluant, sans s'y limiter, les Accords de Traitement des Données entre un Responsable de Traitement et un Sous-Traitant, les accords de responsabilité conjointe et les accords entre Responsables de traitement indépendants).
Activité de Traitement	Activité spécifique de SANOFI menée à des fins déterminées ou à un ensemble de finalités cohérentes, impliquant ou nécessitant une ou plusieurs Opérations de Traitement de Données Personnelles, devant être enregistrée dans le(s) Registre(s) des Activités de Traitement et soumise à une Évaluation des Risques de protection des données à caractère personnel.
Autorité de Contrôle Chef de File	L'autorité de protection des données française désignée par le Groupe SANOFI comme son autorité chef de file en vertu du RGPD. Il s'agit de la Commission Nationale de l'Informatique et des Libertés (CNIL).
Autorité de Contrôle Compétente	L'autorité de protection des données établie dans l'Espace Économique Européen (EEE) ayant compétence pour superviser le traitement des Données Personnelles effectué par une Entité Adhérente dans le cadre des Règles d'Entreprise Contraignantes de SANOFI, conformément au Droit de l'Union Européenne.
Autorité de Protection des Données	Entité publique investie du pouvoir de contrôler et d'assurer le respect des lois relatives à la protection des données à caractère personnel sur son territoire, qu'il s'agisse d'un pays, d'une région, d'un État ou de tout autre ressort territorial.
Business Process Owner	Tout Collabora de SANOFI en charge de projets, d'actifs (par exemple, logiciels, matériels, systèmes, etc.) ou d'activités impliquant le traitement de Données Personnelles dans le cadre de sa mission professionnelle pour le compte d'une ou plusieurs fonctions, division (BU), pays et/ou Filiale de SANOFI pour une ou plusieurs fonctions, entités opérationnelles ou pays.
Cadre de Transfert de SANOFI	L'ensemble constitué par les BCR de SANOFI, de l'accord intragroupe de transfert de données, les déclarations d'adhésion signées, ainsi que tout autre document adopté ou tout autre accord conclu par SANOFI afin d'encadrer les transferts de Données Personnelles conformément au Droit Applicable

Data Privacy Office	L'équipe composée des Référents à la Protection des Données de l'Équipe <i>Privacy Legal Advisory</i> et de l'Équipe <i>Privacy Operations</i>, placée sous la supervision du <i>Chief Privacy Officer</i>. Elle est chargée au sein de SANOFI de : • Informer et conseiller SANOFI et ses collaborateurs au niveau du groupe sur leurs obligations légales au regard des Droit Applicable, • Contrôler la conformité de SANOFI aux Droit Applicable et aux Règles de Protection des Données Personnelles de SANOFI, et • Coordonner le réseau des Référents à la Protection des Données locaux et fonctionnels.
Demande d'Accès aux Données Personnelles	Toute demande d'accès formulée par une autorité publique en vertu des lois du pays de destination, ou d'un autre Pays Tiers, visant la divulgation de Données Personnelles traitées par SANOFI.
Demande d'Exercice des Droits	Toute demande présentée par un individu qui souhaite exercer ses Droits en qualité de Personne Concernée.
Destinataire	Personne physique ou morale (ex. une Filiale de SANOFI), une autorité publique, un organisme ou toute autre entité à qui des Données Personnelles sont communiquées.
Données de Santé	Toute information relative à la santé physique ou mentale d'une Personne Concernée, qu'elle soit pseudonymisée ou non. Cela inclut les données relatives aux pathologies, maladies, traitements, médicaments, antécédents médicaux, résultats d'analyses de laboratoire, informations génétiques, ainsi que toute autre donnée collectée dans le cadre de la prestation de soins de santé, y compris dans le contexte d'essais et d'études cliniques. Les Données de Santé peuvent également englober des informations sur le mode de vie, telles que l'alimentation, l'exercice physique et les habitudes, ainsi que les données provenant d'appareils connectés ou d'applications de santé.
Données Personnelles	Toute information traitée par SANOFI ou pour son compte, relative à une Personne Concernée identifiée ou identifiable (notamment le nom et le prénom, les coordonnées, le numéro de sécurité sociale, les informations financières, les données médicales et les Données de Santé, la formation professionnelle, etc.). Une Personne Concernée peut être identifiée ou identifiable indirectement, en particulier (i) par référence à un identifiant tel qu'un numéro d'identification, un numéro de patient, un pseudonyme ou un identifiant en ligne, ou (ii) par le croisement de plusieurs données (ex. le genre, la date de naissance et l'adresse), ou (iii) par des éléments propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale.
Données Personnelles Sensibles	La notion de Données Personnelles Sensibles, qui peut varier selon les pays, comprend au minimum les informations relatives à l'origine raciale ou ethnique d'une personne, à ses opinions politiques, à ses convictions religieuses ou philosophiques, à son appartenance syndicale, ses données génétiques, ses données biométriques, ses Données de Santé, ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique aux fins de l'identifier de manière unique, ainsi que ses condamnations pénales et infractions.

<i>Droit Applicable (à la protection des données)</i>	Lois, règles et réglementations en matière de protection des données à caractère personnel qui garantissent un niveau de protection au moins équivalent à celui prévu par le Droit de l'UE applicable aux Activités de Traitement, dans leur version en vigueur. En cas de transfert vers des Entités Adhérentes établies dans des Pays Tiers, les lois relatives à la protection des données à caractère personnel de l'Exportateur de Données (y compris le droit de l'Union Européenne lorsque l'Exportateur de Données y est soumis) sont réputées applicables aux Données Personnelles transférées.
<i>Droit de l'Union Européenne</i>	Le Règlement général sur la protection des données ((UE) 2016/679) (le « RGPD ») et, le cas échéant, les lois locales et nationales relatives à la protection des Données Personnelles et au traitement de celles-ci, mettant en œuvre le RGPD dans un État Membre de l'EEE concerné.
<i>Droits de la Personne Concernée</i>	Les droits que le Droit de l'Union Européenne reconnaît aux Personnes Concernées et qu'elles peuvent exercer auprès du Responsable de Traitement, du Sous-traitant ou de l'Exportateur de Données, l'Importateur de Données ou du Destinataire.
<i>Entité Adhérente</i>	Toute Filiale, succursale, représentation ou autre entité juridique du Groupe SANOFI qui adhère aux Règles d'Entreprise Contraignantes de SANOFI et qui est liée par l'Accord d'Acceptation des Règles d'Entreprise Contraignantes.
<i>Entité Adhérente Responsable</i>	SANOFI WINTHROP INDUSTRIE ou SANOFI-AVENTIS RECHERCHE ET DÉVELOPPEMENT, société établie au sein de l'Union Européenne, qui accepte la responsabilité, dans le champ d'application matériel tel que défini à Annexe 2 de tout manquement à ces Règles d'Entreprise Contraignantes commis par un ou plusieurs Membres établis hors de l'Union Européenne et s'engage à prendre les mesures appropriées pour remédier à ces manquements ainsi qu'à verser une indemnisation pour tout dommage en résultant au nom de l'Entité Adhérente concernée en violation de ces Règles d'Entreprise Contraignantes.
<i>Equipe Opérationnelle</i>	Collaborateurs de SANOFI, personnel temporaire et personnel externe tenus de se conformer aux Processus de Protection des Données conformément aux Règles de la Protection des données de SANOFI, y compris les instructions du Référent à la Protection des Données.
<i>Espace Économique Européen</i>	Zone géographique qui comprend les États Membres de l'Union Européenne ainsi que les pays de l'Association européenne de libre-échange (AELE).
<i>Évaluation des Risques (en matière de protection des Données)</i>	Une évaluation interne de SANOFI à effectuer pour un projet, afin d'évaluer les risques associés à l'Activité de Traitement, de conseiller le <i>Business Process Owner</i> sur les mesures à mettre en œuvre pour assurer une protection adéquate des Données Personnelles et de documenter les projets menés en lien avec une Activité de Traitement figurant dans le(s) Registre(s) de SANOFI.
<i>Exportateur de Données</i>	Toute Entité Adhérente, quelle que soit sa localisation géographique, qui transfère des Données Personnelles à une autre Entité Adhérente agissant en qualité d'Importateur de Données, dans le champ d'application matériel des BCR de SANOFI. Cette définition inclut, sans s'y limiter, les Entités Adhérentes établies dans l'Espace Économique Européen (EEE) qui transfèrent des Données Personnelles à des Entités Adhérentes situées en dehors de l'EEE. Elle couvre également les Transferts Ultérieurs de Données Personnelles.

Filiale	Toute entité juridique qui, directement ou indirectement, contrôle la Société Mère SANOFI, est contrôlée par elle ou est placée sous un contrôle commun avec elle. Au sens de la présente définition, le « contrôle » d'une entité juridique s'entend de la détention, directe ou indirecte, de plus de cinquante pour cent (50 %) de son capital conférant le droit de vote ou le pouvoir d'en diriger les affaires.
Groupe SANOFI	L'ensemble des sociétés constitué par les Filiales.
Importateur de Données	Toute Entité Adhérente qui reçoit des Données Personnelles d'une autre Entité Adhérente agissant en qualité d'Exportateur de Données, dans le champ d'application matériel des Règles d'Entreprise Contraignantes de SANOFI. Au regard du Droit de l'Union Européenne, cette définition vise les entités établies en dehors de l'Espace Économique Européen (EEE). Pour l'application du cadre interne de protection des données à caractère personnel de SANOFI, par convention entre les Entités Adhérentes, ce terme couvre également toute Entité Adhérente qui reçoit des Données Personnelles d'une autre Entité Adhérente, que l'une ou l'autre de ces entités soit établie au sein ou en dehors de l'EEE.
Opération(s) de Traitement des Données Personnelles	Toute opération effectuée sur des Données Personnelles, telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
Pays Tiers	Tout pays situé en dehors de l'Espace Économique Européen (EEE).
Personne(s) Concernée(s)	Personne physique identifiée ou identifiable à laquelle se rapportent les Données Personnelles traitées par SANOFI ; une personne physique identifiable est celle qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments propres à son identité physique, physiologique, mentale, économique, culturelle ou sociale.
Processus de Protection des Données Personnelles	L'ensemble des processus inclus dans la Procédure Opérationnelle Globale (GOP) de protection des données à caractère personnel décrivant les actions mises en œuvre par SANOFI pour assurer la conformité aux obligations découlant du Droit Applicable.
Référent à la Protection des Données	Personne désignée par le <i>Chief Privacy Officer</i> comme étant responsable de la gestion du programme de protection des données à caractère personnel et de la conformité au niveau fonctionnel, régional ou local.
Règles de Protection des Données Personnelles de SANOFI	Le corpus de règles internes (politiques, pratiques, lignes directrices, recommandations et avis) que le Groupe SANOFI adopte et diffuse afin de protéger les Données Personnelles qu'il collecte, traite, conserve et transmet. Ce corpus comprend notamment les BCR de SANOFI, la Politique Globale de Protection des Données (<i>Global Privacy Policy</i>) et la Procédure Opérationnelle Globale de Protection des Données (<i>Privacy Global Operating Procedure</i>).

Registre(s) des Activités de Traitement	Registres tenus par le <i>Data Privacy Office</i> dans le Système de Gestion de la Protection des Données, recensant l'ensemble des Activités de Traitement effectuées par SANOFI et lui permettant d'assurer le suivi et la traçabilité de sa conformité au Droit de l'Union Européenne. Ces registres sont déclinés : • Au niveau des Divisions mondiales (GBU) et des Fonctions Transverses (GF) dans le Registre des Activités de Traitement principale (MRoPA) ; • Au niveau régional ou national dans le Registre des Activités de Traitement locales (LROPA).
Responsable Conjoint de Traitement	Le Responsable de Traitement qui détermine conjointement avec un ou plusieurs autres Responsables de Traitement les finalités et les moyens d'une Activité de Traitement et dont les rôles et responsabilités sont régis par un accord de responsabilité conjointe.
Responsable de Traitement	Personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données Personnelles.
Société Mère SANOFI	La société de droit français immatriculée au Registre du commerce et des sociétés de Paris sous le numéro 395 030 844.
Sous-Traitant	Personne physique ou morale (ex. une Filiale de SANOFI), l'autorité publique, le service ou tout autre organisme qui traite des Données Personnelles pour le compte du Responsable de Traitement.
Système de Gestion de la Protection des Données Personnelles	La plateforme numérique utilisée par les membres du <i>Data Privacy Office</i> pour gérer certains aspects de la conformité aux principes de protection des données, y compris les Processus de Protection des Données Personnelles associés.
Tiers	Toute personne physique ou morale, autorité publique, organisme ou entité qui n'est pas une Entité Adhérente et qui n'est pas soumise aux Règles d'Entreprise Contraignantes de SANOFI.
Transfert Ulérieur	Un transfert subséquent de Données Personnelles initialement reçues par une Entité Adhérente (agissant en qualité d'Importateur de Données) vers une autre Entité Adhérente ou vers un Tiers, situé dans un autre pays. Cela inclut : - Les transferts entre Entités Adhérentes situées en dehors de l'EEE ; - Les transferts d'une Entité Adhérente située en dehors de l'EEE vers un Tiers.
Violation de Données Personnelles	Tout incident résultant d'une atteinte à la sécurité ou à la confidentialité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, le vol, la divulgation non autorisée de Données Personnelles ou l'accès non autorisé à celles-ci, et pouvant impliquer l'obligation d'envoyer une notification spécifique aux Autorités de Contrôle Compétentes et une communication aux Personnes Concernées affectées, le cas échéant.

Annexe 2. Champ matériel des BCR de Sanofi

Les BCR de SANOFI établissent un cadre pour le transfert des Données Personnelles entre les Entités Adhérentes.

Ce document présente le champ d'application matériel des BCR de SANOFI. Il décrit les transferts ou l'ensemble de transferts, en précisant la nature et les catégories de Données Personnelles, la nature des traitements et les finalités poursuivies, les Personnes Concernées.

1. Gestion des Ressources Humaines et de la Culture d'Entreprise

<i>Qui transfère les Données Personnelles ?</i>	Chaque Entité Adhérente située au sein de l'Espace Économique Européen (EEE) peut transférer les Données Personnelles qu'elle contrôle, décrites dans la présente section, à toute autre Entité Adhérente située à l'intérieur comme à l'extérieur de l'EEE. Chaque Entité Adhérente située hors de l'EEE peut également transférer les Données Personnelles qu'elle contrôle, décrites dans la présente section, à toute Entité Adhérente située à l'intérieur comme à l'extérieur de l'EEE.
<i>Qui reçoit ces Données Personnelles ?</i>	Chaque Entité Adhérente située hors de l'EEE peut recevoir les Données Personnelles décrites dans la présente section qui lui sont transmises par d'autres Entités Adhérentes situées à l'intérieur comme à l'extérieur de l'EEE. Chaque Entité Adhérente située au sein de l'EEE peut également recevoir les Données Personnelles décrites dans la présente section qui lui sont transmises par d'autres Entités Adhérentes situées à l'intérieur comme à l'extérieur de l'EEE.
<i>Quelles sont les catégories de Personnes Concernées dont les Données Personnelles sont transférées ?</i>	Collaborateurs Candidats
<i>Quelle est l'Entité Adhérente Responsable ?</i>	SANOFI WINTHROP INDUSTRIE
<i>Quelles catégories de Données Personnelles sont transférées ?</i>	• Données d'identification – Nom, genre, photographie, date de naissance, identifiants salariés. • Coordonnées – Adresse personnelle et professionnelle, numéros de téléphone/adresses électroniques, coordonnées de la personne à contacter en cas d'urgence. • Données relatives à l'emploi – Intitulé du poste/fonction, lieu de travail, contrat de travail, évaluations professionnelles et sanctions disciplinaires, procédures de traitement des réclamations, arrêts de travail/congés. • Données relatives à la vie professionnelle – Formation au titre des emplois antérieurs et actuels. • Données de localisation – Localisation géographique des Personnes Concernées telle que résultant des badges, données de géolocalisation, informations de déplacement, réservations de salles de réunion, flex office, aménagements des locaux. • Informations relatives au parcours – Diplômes/qualifications professionnelles, formation, CV. • Identifiants nationaux – Carte d'identité nationale/passeport, statut d'immigration/visa, numéros de sécurité sociale. • Situation familiale – Informations relatives au conjoint et aux personnes à charge, situation matrimoniale. • Informations financières – Coordonnées bancaires, informations fiscales, retenues, salaire, avantages, notes de frais, indemnités de l'entreprise, attributions d'actions et de titres. • Informations informatiques – Informations nécessaires pour permettre l'accès aux systèmes et réseaux informatiques de SANOFI, telles que les adresses IP, fichiers journaux et informations de connexion. • Toute autre information communiquée volontairement par les Salariés sur leurs profils d'entreprise.

	• Informations statistiques relatives aux Salariés de SANOFI. • Enquêtes préalables (telles que les antécédents judiciaires) lorsque cela est justifiée et conformément au Droit Applicable en matière de protection des données. • Données de Santé – <i>Lorsqu'elles sont liées au travail.</i>
Quelles catégories de Données Personnelles Sensibles (le cas échéant) sont transférées ?	En règle générale, SANOFI ne transfère aucune Donnée Personnelle Sensible relative à ses Collaborateurs, sauf lorsque le Droit Applicable en matière de protection des données l'y contraint. Dans un tel cas, SANOFI peut, à titre exceptionnel, transférer certaines informations relatives à : • L'origine raciale/ethnique d'un Collaborateur ; • La religion ; • Sexe et aux handicaps, aux fins du suivi de l'égalité des chances, du respect des lois anti-discrimination et des obligations de déclaration aux autorités publiques ; ou • L'état de santé physique ou mentale d'un Salarié, afin de mettre en place des aménagements liés au travail, des prestations de santé et d'assurance (<i>par exemple, la gestion des absences</i>).
Pourquoi ces Données Personnelles sont-elles transférées et comment seront-elles utilisées ?	SANOFI peut transférer ces Données Personnelles au sein du groupe afin de gérer les ressources humaines à l'échelle du groupe, ainsi qu'aux fins d'autres activités de Traitement telles que le respect du Droit Applicable en matière de protection des données et de la réglementation, la formation et le développement des compétences, les services et la sécurité informatiques, l'audit et les enquêtes nécessaires, la fiscalité et la comptabilité, ainsi que la gestion générale de l'entreprise. Les Données Personnelles pourront notamment être utilisées aux fins suivantes : - Recrutement ; - Gestion des talents et développement organisationnel (<i>par exemple, optimisation des ressources</i>) ; - Paie, traitements et salaires, analyse comparative des rémunérations, primes, attributions d'actions (<i>par exemple, pour l'administration des plans d'actionnariat et d'avantages</i>) ; - Administration des prestations de santé, de rémunération, des programmes d'incitation et autres avantages ; - Accidents et maladies liés au travail, absences, y compris la gestion de la santé et de la sécurité des Salariés ainsi que des situations de handicap ; - Gestion de carrière, entretiens d'évaluation et gestion de la performance ; - Mobilité internationale (<i>par exemple, relocalisation</i>) ; - Formation et développement des compétences, e-learning ; - Gestion administrative et services d'accompagnement des Salariés (<i>par exemple, téléphones mobiles, ordinateurs</i>) ; - Gestion des déplacements professionnels et remboursement des notes de frais ; - Procédure de continuité d'activité en cas d'urgence ; - Gestion de la flotte automobile de l'entreprise ; services d'assistance informatique et sécurité/gestion informatique ; - Enregistrements téléphoniques aux fins de formation des Salariés de SANOFI et de qualité de service ; - Comptabilité, planification financière, audit interne, enquêtes et statistiques internes ;

	- Questions disciplinaires, enquêtes internes, ligne d'alerte anonyme (<i>par exemple</i>, dispositif d'alerte professionnelle) ; - Aide à la conduite des activités de SANOFI de manière plus efficace et plus efficiente (<i>par exemple</i>, aux fins de gestion générale des ressources humaines à l'échelle mondiale) ; - Respect des obligations légales ou réglementaires et réponse aux demandes des autorités administratives ou judiciaires ; - Assurance de la sécurité physique des personnes, des biens et des actifs de Sanofi (<i>par exemple</i>, contrôle d'accès, entrée/sortie des bâtiments) ; - Gestion de la gouvernance d'entreprise et des obligations de conformité (<i>par exemple</i>, audit, délégations de pouvoir, listes d'initiés, conflits d'intérêts) ; - Évaluation et réalisation d'opérations et de transactions commerciales (<i>par exemple</i>, ventes, achats, accords) ; - Réalisation de communications externes et internes à l'occasion d'événements.
Où ces Données Personnelles sont-elles traitées ?	Les Données Personnelles décrites dans la présente section peuvent être traitées dans tout territoire où sont établies les Entités Adhérentes ou leurs Sous-traitants internes ou externes.
Sur quelle(s) base(s) légale(s) les Données Personnelles sont-elles traitées ?	Le Traitement des Données Personnelles est nécessaire sur le fondement : - De l'exécution d'un contrat (<i>c'est-à-dire le contrat</i> de travail et tout autre contrat pertinent) ; - Du respect d'obligations légales (notamment les obligations résultant du droit du travail) ; - Des intérêts légitimes de SANOFI ; - Du consentement préalable du Collaborateur dans des cas limités et lorsqu'ils ont clairement exprimé leur accord au Traitement de leurs Données Personnelles par SANOFI.

2. Système de vigilance sanitaire

Qui transfère les Données Personnelles ?	Chaque Entité Adhérente située au sein de l'Espace Économique Européen (EEE) peut transférer les Données Personnelles qu'elle contrôle, décrites dans la présente section, à toute autre Entité Adhérente située à l'intérieur comme à l'extérieur de l'EEE. Chaque Entité Adhérente située hors de l'EEE peut également transférer les Données Personnelles qu'elle contrôle, décrites dans la présente section, à toute Entité Adhérente située à l'intérieur comme à l'extérieur de l'EEE.
Qui reçoit ces Données Personnelles ?	Chaque Entité Adhérente située hors de l'EEE peut recevoir les Données Personnelles décrites dans la présente section qui lui sont transmises par d'autres Entités Adhérentes situées à l'intérieur comme à l'extérieur de l'EEE. Chaque Entité Adhérente située au sein de l'EEE peut également recevoir les Données Personnelles décrites dans la présente section qui lui sont transmises par d'autres Entités Adhérentes situées à l'intérieur comme à l'extérieur de l'EEE.
Quelles sont les catégories de Personnes Concernées dont les Données Personnelles sont transférées ?	Personne exposée à un événement sanitaire indésirable Personne ayant procédé à la notification de l'événement sanitaire indésirable (<i>c'est-à-dire</i> patient exposé à l'événement sanitaire indésirable, proche du patient, Professionnels de Santé, membre d'une association, membre d'une autorité de santé...) Professionnels de Santé (PS) (<i>c'est-à-dire</i> susceptibles d'apporter toute clarification utile).
Quelle est l'Entité Adhérente Responsable ?	SANOFI-AVENTIS RECHERCHE ET DEVELOPPEMENT
Quelles catégories de Données Personnelles sont transférées ?	• Données d'identification – Nom, genre, photographie, date de naissance, âge, numéro d'identification (<i>par exemple</i>, code numérique ou alphabétique) • Coordonnées – Adresse postale, numéro de téléphone/adresse électronique • Données de Santé – Traitements administrés, résultats d'examen, nature du ou des événements indésirables, antécédents personnels ou familiaux, maladies ou événements associés, facteurs de risque
Quelles catégories de Données Personnelles Sensibles (le cas échéant) sont transférées ?	• Données de Santé
Pourquoi ces Données Personnelles sont-elles transférées et comment seront-elles utilisées ?	SANOFI peut transférer des Données Personnelles au sein du groupe afin de gérer les finalités suivantes : - Enregistrement - Analyse - Suivi - Documentation - Transmission aux autorités de santé
Où ces Données Personnelles sont-elles traitées ?	Les Données Personnelles décrites dans la présente section peuvent être traitées dans tout territoire où sont établies les Entités Adhérentes ou leurs Sous-traitants internes ou externes.
Sur quelle(s) base(s) légale(s) les Données Personnelles sont-elles traitées ?	Le Traitement des Données Personnelles est nécessaire sur le fondement du respect d'obligations légales (au titre des mécanismes locaux ou régionaux de vigilance sanitaire).

3. Essais cliniques et études, Études sur des données de vie réelle (Real-World Evidence)

Qui transfère les Données Personnelles ?	Chaque Entité Adhérente située au sein de l'Espace Économique Européen (EEE) peut transférer les Données Personnelles qu'elle contrôle, décrites dans la présente section, à toute autre Entité Adhérente située à l'intérieur comme à l'extérieur de l'EEE. Chaque Entité Adhérente située hors de l'EEE peut également transférer les Données Personnelles qu'elle contrôle, décrites dans la présente section, à toute Entité Adhérente située à l'intérieur comme à l'extérieur de l'EEE.
Qui reçoit ces Données Personnelles ?	Chaque Entité Adhérente située hors de l'EEE peut recevoir les Données Personnelles décrites dans la présente section qui lui sont transmises par d'autres Entités Adhérentes situées à l'intérieur comme à l'extérieur de l'EEE. Chaque Entité Adhérente située au sein de l'EEE peut également recevoir les Données Personnelles décrites dans la présente section qui lui sont transmises par d'autres Entités Adhérentes situées à l'intérieur comme à l'extérieur de l'EEE.
Quelles sont les catégories de Personnes Concernées dont les Données Personnelles sont transférées ?	Patients (c'est-à-dire participants) Professionnels de Santé (PDS) impliqués dans l'essai clinique ou l'étude
Quelle est l'Entité Adhérente Responsable ?	SANOFI-AVENTIS RECHERCHE ET DEVELOPPEMENT
Quelles catégories de Données Personnelles sont transférées ?	• Données d'identification – Nom, genre, photographie, enregistrement vidéo, enregistrement vocal, date de naissance, âge, numéro d'identification (<i>par exemple</i>, code numérique ou alphabétique), origine ethnique • Coordonnées – Adresse postale, numéro de téléphone/adresse électronique • Données de Santé – <i>Par exemple</i>, informations médicales, données biologiques, poids, taille, antécédents personnels ou familiaux, données génétiques... • Situation familiale • Informations relatives au parcours – diplômes/qualifications professionnelles, formation • Informations financières – coordonnées bancaires, remboursement de frais, montant des indemnités et rémunérations perçues. • Informations informatiques – informations nécessaires pour permettre l'accès aux systèmes et réseaux informatiques
Quelles catégories de Données Personnelles Sensibles (le cas échéant) sont transférées ?	• Données de Santé • Vie sexuelle • Origine raciale/ethnique.
Pourquoi ces Données Personnelles sont-elles transférées et comment seront-elles utilisées ?	SANOFI peut transférer des Données Personnelles au sein du groupe afin de gérer les finalités suivantes : - Évaluer la sécurité et l'efficacité des médicaments expérimentaux, - Promouvoir les soins de santé, se conformer aux exigences réglementaires, commercialiser ou poursuivre la commercialisation de produits et soutenir les activités de remboursement,

	- Conduire des études axées sur une pathologie ou des études cliniques exploratoires, telles que des études de validation de méthodologie de dosage, des modèles pharmacologiques ou physiologiques de médecine expérimentale, - Évaluer la sécurité et l'efficacité de produits expérimentaux déjà commercialisés, menées aux fins du développement de connaissances biologiques, scientifiques ou médicales, et dans le cadre desquelles l'ensemble des procédures sont réalisées et les produits utilisés de manière habituelle dans le cadre de la pratique médicale courante, - Les Données Personnelles seront traitées par le biais d'activités d'enregistrement, d'analyse, de surveillance, de documentation, de transmission et de conservation. Les Données Personnelles traitées seront compilées dans un rapport d'étude (<i>par exemple</i>, un rapport d'étude clinique) aux fins de soumission aux autorités de santé.
<i>Où ces Données Personnelles sont-elles traitées ?</i>	Les Données Personnelles décrites dans la présente section peuvent être traitées dans tout territoire où sont établies les Entités Adhérentes ou leurs Sous-traitants internes ou externes.
<i>Sur quelle(s) base(s) légale(s) les Données Personnelles sont-elles traitées ?</i>	Le Traitement des Données Personnelles est nécessaire sur le fondement : - Des intérêts légitimes de SANOFI dans le domaine de la santé publique, tels que la garantie de normes élevées de qualité et de sécurité des médicaments ou des dispositifs médicaux (art. 9.2.i) du RGPD), - Lorsque la réglementation locale l'exige, une autre base juridique peut justifier le Traitement des Données Personnelles (<i>c'est-à-dire</i> le consentement), - Du respect d'obligations légales (<i>c'est-à-dire</i> en matière de sécurité).

Annexe 3. Articles du RGPD

Article 37, RGPD

Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

- a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
- b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
- c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

2. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

3. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

4. Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

5. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.

6. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

7. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

Article 39, RGPD

Missions du délégué à la protection des données

1. Les missions du délégué à la protection des données sont au moins les suivantes :

- a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;
- b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

- c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;
 - d) coopérer avec l'autorité de contrôle;
 - e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.
2. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Article 89(1), RGPD

Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

1. Le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au présent règlement, à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière.