Version publique des Règles contraignantes d'entreprise (BCR) d'Amgen

Traduction française des BCRs

Introduction :

Amgen est une société leader dans le domaine des biotechnologies qui s'engage à servir les patients atteints de maladies graves.

Les règles contraignantes d'entreprise (en anglais « Binding Corporate Rules » ou « BCR ») témoignent de l'engagement d'Amgen envers la protection des données et la vie privée, en s'efforçant d'assurer un niveau de protection adéquat aux transferts et au traitement des données à caractère personnel entre les entités Amgen.

Toutes les entités juridiques au sein d'Amgen et tous les membres du personnel s'engagent à respecter les BCR. Leur non respect peut entraîner d'actions disciplinaires conforméent à la loi locale applicable.

Le Responsable de la conformité (Chief Compliance Officer), en liaison avec le Responsable de la protection des données (Chief Privacy Officer), veille à faire appliquer les règles décrites.

Les BCR ont été adoptées en référence aux textes européens actuellement en vigueur sur la protection des données à caractère personnel, qui sont les Directives européennes 95/46/CE et 2002/58/CE.

1 – Champ d'application

Les BCR Amgen s'appliquent aux transferts et au traitement, automatisé ou manuel, de toutes les données à caractère personnel des employés, des clients, des fournisseurs, des actionnaires, des patients et de toutes les autres personnes concernées, réalisés par une société participante d'Amgen, et ce lorsqu'elles exercent à titre de responsable du traitement l'un des cas suivants:

a) la société participante d'Amgen qui traite les données à caractère personnel est établie dans un pays réglementé ; ou

b) la société participante d'Amgen qui traite les données à caractère personnel n'est pas établie dans un pays réglementé (« importateur de données ») et a reçu les données à

caractère personnel de la part d'une société participante Amgen établie dans un pays réglementé comme défini à l'article 2 (« exportateur de données »).

Ces BCR s'appliquent également aux transferts ultérieurs de données à caractère personnel d'importateurs de données vers des importateurs de données.

2 – Définitions

Termes	Définitions
Données à caractère personnel	Informations se rapportant à une personne dont l'identité est apparente, ou peut être constatée, à partir de telles informations, par moyen direct ou indirect. Par ailleurs, les données à caractère personnel peuvent être considérées comme des informations qui peuvent, soit seules soit associées à d'autres informations, identifier ou être utilisées afin de contacter ou de localiser une personne déterminée. Les données à caractère personnel peuvent par exemple inclure les suivantes, selon les législations locales relatives à la protection des données et de la vie privée : • Nom, adresse, numéro de sécurité sociale, numéro de permis de conduire, numéros de compte bancaire, informations relatives à la familialles ou données médicales d'une personne, • Nom, formation professionnelle, et pratiques de prescription d'un médecin, • Adresse e-mail, et autres informations d'identification fournies par une personne visitant un site internet Amgen. La liste ci-dessus est donnée à titre d'exemple uniquement et n'est pas exhaustive.
Données à caractère personnel sensibles	Informations se rapportant à la personne concernée telles que : • Problèmes médicaux ou de santé (physiques ou mentaux) • Informations financières • Origine raciale ou ethnique • Opinions politiques • Convictions religieuses ou philosophiques • Appartenance syndicale • Orientation sexuelle • Condamnations pénales ou antécédents d'incarcération Amgen se réfère aux données sensibles comme étant des données pouvant être utilisées pour commettre un vol d'identité tel qu'un numéro de sécurité sociale, un numéro de permis de conduire, une carte de crédit ou d'autres informations de comptes bancaires.
Personne concernée	La personne à qui les données personnelles se rapportent. Une personne concernée peut être (parmi d'autres) un : • Patient / client / sujet participant à un essai clinique • Professionnel de santé (par ex. médecin ou infirmier(-ière)) • Employé (actuel, ancien ou retraité) • Sous-traitant / entrepreneur individuel / fournisseur / consultant

Responsable du traitement (Responsable du traitement des données)	Toute entité qui émet des décisions à l'égard de la collecte et du traitement des données à caractère personnel, y compris des décisions sur les finalités pour lesquelles, et les modalités par lesquelles les données à caractère personnel sont traitées.
Sous-traitant	Personne ou entité qui traite les données à caractère personnel au nom d'un responsable du traitement.
Traitement	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'affichage, l'accès, la conservation, l'enregistrement, l'organisation, 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, le verrouillage, l'effacement ou la destruction.
Tiers	Une personne physique ou morale, une autorité publique, une agence ou un organisme autre que la personne concernée, le responsable du traitement et les personnes qui, placées sous l'autorité directe du responsable du traitement, sont autorisées à traiter les données à caractère personnel. Chez Amgen, un fournisseur est considéré comme un tiers.
Fournisseur	Toute personne, entreprise ou organisation qui fournit des biens et/ou services à Amgen, résultant d'une relation contractuelle, et/ou est destinataire des données à caractère personnel transmises par Amgen requises dans le cadre de ces biens et/ou services.
Autorités de protection des données (DPA)	Une ou plusieurs autorités publiques chargées de contrôler la mise en application au sein de leur territoire des dispositions adoptées par les États membres conformément à la Directive 95/46. Ces autorités agissent en indépendance complète dans l'exercice des fonctions qui leur sont confiées.
Pays réglementé	Pays de l'Espace Économique Européen (EEE) ou pays avec un niveau adéquat de protection des données comme l'a estimé la Commission européenne par décision ou tout autre pays reconnaissant les BCR comme des procédés légitimes pour le transfert les données à caractère personnel en dehors de leur juridiction ; ces pays sont l'Andorre, l'Argentine, le Canada, les Iles Féroé, Guernesey, l'ile de Man, Israël, Jersey, la Nouvelle Zélande, la Suisse et l'Uruguay.
Exportateur de données	Une entité d'Amgen exerçant à titre de responsable du traitement établie dans un pays réglementé qui transfère des données à caractère personnel vers une autre entité d'Amgen qui n'est pas établie dans un pays réglementé (importateur de données).
Importateur de données	Une entité d'Amgen qui n'est pas établie dans un pays réglementé qui reçoit des données à caractère personnel d'un exportateur de données.

Mesures de sécurité techniques et organisationnelles	Mesures visant à protéger les données à caractère personnel contre la destruction accidentelle ou illicite ou la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données par un réseau, ainsi que contre toute autre forme de traitement illicite.
Société participante	Une entité légale appartenant au groupe Amgen qui est liée par les BCR.
Consentement	Toute manifestation de volonté, libre, spécifique et éclairée d'une personne concernée, par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'une collecte et d'un traitement.
Délégué à la protection des données (DPO)	Membre du personnel de l'entreprise qui a été identifié et nommé par une filiale ou une division opérationnelle comme étant chargé de la surveillance de la protection des données et de la vie privée au niveau local, ainsi que de la mise en place de contrôles adéquats et requis. Il est appelé DPO (Data Protection Officer).

Amgen interprète les termes des BCR conformément aux Directives 95/46/CE et 2002/58/CE de l'Union européenne, auxquelles il est fait référence ci-dessous sous le nom de Directive européenne.

3 – Limitation des finalités

Les données à caractère personnel seront traitées à des fins explicites, déterminées et légitimes conformément à l'Article 6.1(b) de la Directive 95/46.

Les données à caractère personnel ne seront pas traitées de manière incompatible avec les finalités légitimes pour lesquelles les données à caractère personnel ont été collectées. Les importateurs de données sont obligés d'adhérer aux finalités d'origine lors de la conservation et/ou du traitement ultérieur ou de l'utilisation des données qui leur sont transférées par une autre société participante. La finalité du traitement des données peut uniquement être modifiée avec le consentement de la personne concernée ou dans la limite autorisée par la loi locale à laquelle l'exportateur de données transférant les données est soumis.

Des précautions supplémentaires snt prévues pour les données sensibles, comme le prévoit la Directive européenne 95/46/CE.

4 - Qualité des données et proportionnalité

Les données à caractère personnel doivent être correctes dans les faits et, si nécessaire, tenues à jour. Toutes les mesures adéquates doivent être prises pour que les données qui sont inexactes ou incomplètes soient rectifiées ou effacées.

Les données à caractères personnel seront adéquates et pertinentes, conformément à l'article 6.1(c) de la Directive 95/46.

Le traitement des données sera guidé par l'objectif delimiter la collecte, le traitement et/ou l'utilisation des données à caractère personnel à ce qui est strictement nécessaire , c'est-à-dire à une quantité de données aussi limitée que possible. Le recours possible à des données anonymes

ou pseudonymes doit être exploité, si tant est que le coût et les efforts consentis pour ce faire soient proportionnels à l'objectif fixé.

Toutes les données à caractère personnel qui ne sont plus nécessaires aux activités de l'entreprise pour lesquelles elles avaient initialement été recueillies et conservées doivent être supprimées suivant le tableau de conservation des documents (« Record Retention Schedule ») d'Amgen. Dans le cas où des durées obligatoires de conservation des données sont prévues par la loi, les données seront verrouillées et non supprimées. Au terme de la période de conservation ou de mise en suspens juridique, les données seront supprimées.

5 – Fondement juridique du traitement des données à caractère personnel

Le traitement des données à caractère personnel n'est permis que si au moins l'une des conditions suivantes est remplie :

- La personne concernée a donné son consentement éclairé, libre et univoque
- Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou est liée par une relation de confiance similaire ou afin de prendre des mesures à l'exécution de mesures précontractuelles prises à la demande de celle-ci Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou est stipulé ou permis par les lois ou réglementations applicables
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, tels que de vie, de santé ou de sécurité de la personne concernée
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou un tiers auquel les données sont divulguées
- Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par le tiers ou les parties auxquelles les données sont divulguées, à condition que ne prévalent pas les intérêts légitimes ou droits fondamentaux et libertés de la personne concernée

6 – Traitement des données sensibles

Si Amgen doit traiter des données sensibles pour une finalité déterminée et légitime, Amgen le fera uniquement si :

- La personne concernée a donné son consentement explicite au traitement de ces données sensibles, sauf dans les cas où les lois applicables interdisent un tel traitement
- Le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates
- Le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne 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 avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant

avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées

- Le traitement porte sur des données sensibles manifestement rendues publiques par la personne concernée
- Le traitement des données sensibles est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice
- Le traitement des données sensibles est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, et le traitement de ces données sensibles est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente

7 – Transparence et droit à l'information

Toutes les sociétés participantes traiteront les données à caractère personnel d'une manière transparente.

Amgen s'engage à mettre les BCR à la disposition de chaque personne concernée, y compris les informations de contact, et à informer les personnes concernées du transfert et du traitement de leurs données à caractère personnel.

Pour ce faire, Amgen utilisa divers moyens de communication, tels que les sites Internet d'entreprise, y compris les sites internes et bulletins d'informations, les contrats, et les mentions d'information spécifiques ajoutées aux supports adéquats.

Les personnes concernées dont les données personnelles sont traitées par une société participante doivent recevoir les informations suivantes :

- l'identité du ou des responsables du traitement et, le cas échéant, de son représentant ;
- les finalités du traitement auquel les données sont destinées ;
- l'origine des données (à moins que les données personnelles aient été collectées directement auprès de la personne concernée)
- toute information supplémentaire telle que :

  i) les destinataires ou les catégories de destinataires des données,

  ii) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données, dans la mesure où ces informations supplémentaires sont nécessaires, compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données.

Lorsque les données n'ont pas été collectées auprès de la personne concernée, l'obligation d'informer la personne concernée ne s'applique pas si l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données.

8 – Droits d'accès, de rectification, d'effacement et de blocage des données

Chaque personne concernée a le droit d'obtenir sans contrainte à des intervalles raisonnables une communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données. La suite apportée à cette

demande, y compris la possibilité d'une indemnisation ou le délai de réponse à une telle demande, sera soumise aux lois applicables et communiquée de manière adéquate à la personne concernée lorsqu'ilelle soumet sa demande.

Chaque personne concernée a le droit d'obtenir la rectification, l'effacement ou le blocage des données, notamment lorsque les données sont incomplètes ou inexactes.

Chaque personne concernée a le droit de s'opposer, à tout moment, pour des raisons impérieuses et légitimes tenant à sa situation particulière, à ce que les données personnelles la concernant fassent l'objet d'un traitement, à moins que ce traitement soit requis par des obligations légales ou réglementaires. En cas d'opposition justifiée, ce traitement doit cesser.

Chaque personne concernée a le droit de s'opposer (gratuitement) au traitement des données personnelles la concernant à des fins de prospection directe.

Chaque personne concernée a le droit d'obtenir la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément à l'article 12(c) de la Directive 95/46.

Chaque personne concernée a le droit de connaître la logique qui sous-tend tout traitement automatisé des données, en vertu de l'article 12(a) de la Directive 95/46.

9 – Décisions individuelles automatisées

Les procédures automatisées sont uniquement utilisées comme outil du processus de décision. Aucune évaluation ou décision concernant une personne concernée qui l'affecte de manière significative ne se base uniquement sur le processus automatisé de ses données, sauf si une telle décision :

- est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime ; ou
- est autorisée par une loi qui prévoit également des mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

10 – Sécurité et confidentialité

Amgen met en œuvre des mesures de sécurité technique et organisationnelles adéquates afin de détecter et protéger Amgen contre une destruction accidentelle ou illicite, une perte, une altération, une diffusion ou un accès non autorisé aux données personnelles, notamment lorsque le traitement comporte des transmissions de données sur un réseau public, ainsi que contre toute autre forme potentielle de traitement illicite. Un dispositif international tel que ISO/CEI 27002 est utilisé par Amgen afin de déterminer de telles mesures de sécurité.

Des processus sont en place chez Amgen afin d'assurer que les incidents potentiels relatifs à la vie privée soient soumis à une déclaration, à un suivi et à des mesures correctives adéquates, si nécessaire.

Des évaluations du risque lié à la sécurité des informations sont utilisées afin d'identifier les menaces potentielles aux données à caractère personnel sensibles, et des contrôles de sécurité supplémentaires sont mis en œuvre, si nécessaire.

Ces mesures seront mises en œuvre en tenant compte de l'état de l'art, conformément à l'article 17.1 de la Directive 95/46.

Le Responsable de la sécurité des systèmes d'information (Chief Information Security Officer) travaille conjointement avec le Responsable de la conformité (Chief Compliance Officer) afin d'assurer la sécurité et la confidentialité des données à caractère personnel.

11 – Relations avec les sous-traitants (importateur de données d'Amgen ou fournisseur)

Le responsable du traitement choisira soigneusement un sous-traitant qui peut être soit une société participante d'Amgen soit un fournisseur. Le sous-traitant doit apporter des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer, et doit veiller au respect de ces mesures.

Lorsqu'il est jugé nécessaire de sous-traiter une activité après évaluation des besoins de l'activité et des risques d'une telle sous-traitante, le processus de sélection du fournisseur inclura une évaluation des facteurs de risque liés à la confidentialité des données et comparera les besoins de l'activité et les risques potentiels.

Le responsable du traitement, en ayant recours à un instrument contractuel écrit, instruira notamment le fournisseur, conformément à la loi applicable, que :

i) le sous-traitant n'agit que sur la seule instruction du responsable du traitement, et que le traitement des données pour les besoins propres du sous-traitant ou pour les besoins d'un tiers est interdit ; et

ii) les règles se rapportant à la sécurité et à la confidentialité doivent incomber au sous-traitant.

Le responsable du traitement veille à ce que le sous-traitant se conforme en tous points aux mesures de sécurité technique et organisationnelles.

Le responsable du traitement reste chargé de la légitimité des traitements et reste responsable des droits de la personne concernée.

Afin de prévoir de telles obligations contractuelles, un document-modèle contractuel intitulé Data Privacy Schedule est fourni. En cas de situation contractuelle spécifique, le responsable du traitement peut négocier une disposition différente, mais cette dernière respectera néanmoins les obligations mentionnées précédemment.

12 – Limitations concernant les transferts et les transferts ultérieurs

Les fournisseurs agissant en qualité de sous-traitants sont tenus par des accords écrits stipulant que le fournisseur n'agit que sur seule instruction du responsable du traitement et qu'il est responsable de la mise en œuvre des mesures de sécurité et de confidentialité adéquates.

Tous les transferts de données vers des fournisseurs établis en dehors de l'UE se conforment aux règles européennes concernant les flux transfrontaliers de données, soit par recours aux clauses contractuelles standard de l'UE approuvées par la Commission européenne, soit par d'autres moyens contractuels adéquats conformément aux articles 25 et 26 de la Directive européenne.

Tous les transferts de données vers des fournisseurs agissant en qualité de sous-traitants établis en dehors de l'UE se conforment aux règles de la Directive européenne à l'égard des sous-traitants en plus des règles relatives aux flux transfrontaliers de données.

13 – Programme de formation

Amgen forme tous les membres du personnel sur les principes de la protection des données et notamment sur les BCR à. Cette formation inclut également des informations concernant les conséquences en matière de droit criminel et de droit du travail pour les employés ne respectant pas les BCR.

La formation est obligatoire et renouvelée chaque année. La participation réussie à cette formation sera documentée.

Des formations spécifiques seront apportées au cas par cas aux membres du personnel disposant d'un accès permanent ou régulier aux données à caractère personnel, ou qui sont impliqués dans la collecte de données personnelles ou dans le développement d'outils utilisés pour le traitement des données à caractère personnel.

En outre, le Département de la protection des données (« Privacy Office ») d'Amgen apporte des informations et des ressources en matière de protection des données appropriées, notamment sur le portail Intranet d'Amgen et sur d'autre vecteurs d'information.

14 – Programme d'audit et de surveillance

Lors de la mise en oeuvre des règles d'entreprise contraignantes (BCR), les audits de conformité se poursuivront et le programme de conformité d'Amgen sera mis à jour pour incorporer les BCR. En outre, Amgen continuera d'effectuer une surveillance régulière de la protection des données au niveau local par l'intermédiaire des délégués à la protection des données (DPO) agissant dans leur rôle de responsables de la conformité locale.

Le programme d'audit couvre tous les aspects des BCR, y compris les méthodes visant à veiller à la mise en œuvre des mesures correctives.

Ces audits sont réalisés régulièrement par l'équipe d'audit interne habilitée.

Le programme d'audit est développé et validé par concertation entre le Responsable des audits et le Responsable de la conformité (Chief Compliance Officer).
Le Responsable de la protection des données (Chief Privacy Officer), le Responsable de la conformité (Chief Compliance Officer)et le Responsable des systèmes d'information peuvent initier des audits liés aux BCR *ad hoc*, à tout moment.

Tous les rapports d'audit sur les BCR sont communiqués au Responsable de la conformité (Chief Compliance Officer)et au Responsable de la protection des données (Chief Privacy Officer) dans un délai convenable. Les résumés et conclusions d'audit des BCR, ainsi que d'autres informations pertinentes, font l'objet de synthèses régulières dont il est rendu compte au Conseil d'administration, par l'intermédiaire des comités adéquats (par ex. le Comité de la responsabilité d'entreprise et de la conformité et/ou le Comité d'audit du Conseil d'administration).

Les autorités de protection des données peuvent, sur demande, recevoir un exemplaire des rapports d'audit se rapportant aux BCR.

Chaque société participante comprend qu'elle peut faire l'objet d'un audit par les autorités de protection des données et qu'elles appliqueront les conseils émis par celles-ci concernant toute question liée aux BCR. Chaque entité faisant l'objet d'un audit doit informer le Responsable de la protection des données (Chief Privacy Officer) lorsqu'il est informé d'un audit.

15 – Conformité et contrôle de la conformité

Amgen nomme les membres du personnel adéquats, y compris un réseau de délégués à la protection des données, avec le soutien de la direction, afin de surveiller et d'assurer le respect des règles.

Chez Amgen, les responsabilités du Responsable de la protection des données (Chief Privacy Officer)incluent entre autres :

- conseiller le Conseil d'administration,
- veiller au respect de la protection des données à un niveau global
- communiquer régulièrement sur le respect de la protection des données, et
- collaborer sur les enquêtes menées par les autorités de protection des données

Le Responsable de la protection des données (Chief Privacy Officer)est responsable du « Global Privacy Office » qui est une équipe apportant un soutien expert aux entités Amgen du monde entier.

Au niveau local, les délégués à la protection des données sont responsables de la gestion des demandes locales en matière de protection des données provenant des personnes concernées, en vue de veiller à la conformité du point de vue local, avec le soutien du Privacy Office, et de notifier les problèmes majeurs en matière de confidentialité auprès du Responsable de la protection des données (Chief Privacy Officer). Amgen assure le maintien d'un réseau de délégués à la protection des données (DPO) et veille à ce qu'un DPO soit nommé ou attribué à chaque pays où Amgen (la société participante) détient une entité juridique. Cette désignation est effectuée en accord avec le supérieur hiérarchique local du DPO et le service des ressources humaines local.

Généralement, les délégués à la protection des données (DPO) sont les responsables locaux de la conformité qui rendent compte au service de Conformité mondiale et éthique de l'entreprise (« Worldwide Compliance and Business Ethics »). Le Privacy Office rend compte également au service de Conformité mondiale et éthique de l'entreprise. Dans de rares cas, en raison de la spécificité d'une entité Amgen ou de circonstances particulières, le délégué à la protection des données (DPO) peut provenir d'une autre fonction, par exemple réglementaire. Quoi qu'il en soit, le Privacy Office veille à ce que les délégués à la protection des données soient formés

adéquatement et aient un niveau suffisant de gestion et d'expertise afin de remplir leur rôle de délégué à la protection des données. En outre, les délégués à la protection des données disposent de moyen de communication direct avec Responsable de la protection des données (Chief Privacy Officer), ainsi que le personnel du Privacy Office, dans l'éventualité où ils ont besoin de conseils supplémentaires.

16 – Actions en cas de législation nationale empêchant le respect des BCR

Lorsqu'un membre du groupe a des raisons de croire que la législation applicable empêche l'entreprise de remplir ses obligations en vertu des BCR et a un impact significatif sur les garanties prévues par les BCR, il en informera immédiatement le Responsable de la protection des données (Chief Privacy Officer) (à moins que cela ne soit interdit par une autorité chargée d'assurer le respect de la loi, comme, par exemple, une interdiction prévue par le code pénal visant à préserver le secret d'une enquête policière).

En cas de conflit entre la législation nationale et les engagements pris en vertu des BCR, le Responsable de la protection des données (Chief Privacy Officer)en liaison avec le responsable juridique local et le délégué à la protection des données local (DPO) déterminera l'action à entreprendre sur le plan légal. Si nécessaire, le Responsable de la protection des données (Chief Privacy Officer) consultera également les autorités de protection des données compétentes.

17 – Mécanismes internes de gestion des plaintes

Amgen étendra et exploitera son système existant de traitement des plaintes afin d'incorporer le traitement de toutes plaintes ou problèmes liés aux BCR.

Toute personne concernée peut, à tout moment, introduire une plainte indiquant qu'une société participante ne respecte pas les BCR. Ces plaintes seront traitées par le Privacy Office sous la direction du Responsable de la protection des données (Chief Privacy Officer)et en coopération avec le délégué à la protection des données local concerné.

Amgen recommande que ces plaintes soient émises par écrit, soit par courrier postal soit par e-mail adressé directement au Privacy Office ou à la filiale. Les Personnes concernées peuvent de même, lorsque cela est acceptable du point de vue des lois applicables, utiliser le service d'assistance en matière d'alertes professionnelles (la « Business Conduct Hotline ») afin de signaler une plainte relative aux BCR.

Si la plainte est reçue localement, le DPO la traduira si nécessaire et la transmettra sans délai au Privacy Office.

Une première réponse sera fournie à la personne concernée l'informant que sa plainte est en cours d'instruction et qu'elle recevra une réponse dans un délai de deux mois maximum.

Si le Privacy Office découvre une faute individuelle, des mesures disciplinaires appropriées seront prises, qui peuvent aller jusqu'au licenciement immédiat, dans la limite autorisée par la loi applicable.

Dans un délai de deux mois maximum, la personne concernée recevra une réponse l'informant de l'issue de sa plainte.

La personne concernée sera informée que si elle n'est pas satisfaite de la réponse d'Amgen, elle pourra introduire une plainte auprès du tribunal compétent ou de l'autorité de protection des données.

Ce système de traitement des plaintes sera rendu public par la publication des BCR, comme mentionné dans la section 7.

18 - Droits et responsabilités du tiers bénéficiaire

Une personne concernée dont les données personnelles émanent d'un pays réglementé, et qui invoque un manquement à l'une des obligations visées dans les BCR, a le droit de faire appliquer les règles en tant que tiers bénéficiaire. Ces droits recouvrent les recours juridictionnels en cas de violation des droits garantis, et le droit à un dédommagement. Le cas échéant, la responsabilité est limitée au dommage réel subi.

Dans la limite autorisée par la juridiction applicable, les personnes concernées peuvent choisir d'introduire des plaintes auprès de :

- la juridiction de l'exportateur de données, et si les données personnelles de la personne concernée émanent d'un exportateur de données de l'EEE, la juridiction compétente sera le lieu d'établissement de l'exportateur de données de l'EEE, ou
- les autorités de protection des données compétentes.

Toute personne concernée ayant subi un dommage du fait d'un manquement aux obligations visées dans les BCR par l'exportateur de données ou l'importateur de données a le droit d'obtenir un dédommagement de la part de l'exportateur de données pour le préjudice subi. Si l'exportateur de données ou l'importateur de données est tenu pour responsable d'un manquement, dans la mesure où celui-ci est responsable, il dédommagera l'autre partie de tout coût, charge, dommage, dépense ou perte encouru.

Chaque exportateur de données et importateur de données peut être exempt de responsabilité en vertu des BCR, s'il prouve que le membre du groupe établi en dehors de l'UE n'a pas violé les BCR ou n'est pas responsable des dommages causés à la personne concernée. Toutefois, la charge de la preuve incombe toujours à l'exportateur de données ou à l'importateur de données.

L'importateur de données agissant en qualité de responsable du traitement ne peut invoquer un manquement par un sous-traitant ultérieur à ses obligations pour échapper à ses propres responsabilités. Si une personne concernée souhaite déposer une plainte à l'encontre de l'exportateur de données, à la suite d'un manquement aux BCR, mais n'en est pas capable parce que l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, la personne concernée peut faire valoir ses droits contre l'importateur de données directement. Si l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données ont été transférées à un successeur légal, par contrat ou par effet de la loi, la personne concernée peut faire valoir ses droits contre ce successeur. La responsabilité de l'importateur de données doit être limitée à ses propres activités de traitement conformément aux BCR.

19 – Assistance mutuelle et coopération avec les autorités de protection des données

Les sociétés participantes sont obligées de coopérer et de s'entraider pour traiter une demande ou une plainte déposée par une personne concernée ou une investigation ou une enquête menée par les autorités de protection des données.

Les sociétés participantes répondront, en collaboration avec le Responsable de la protection des données (Chief Privacy Officer), aux demandes liées aux BCR provenant de l'autorité de protection des données dans un délai convenable et de manière convenable, et se soumettront aux conseils et décisions de l'autorité de protection des données compétente concernant la mise en œuvre des BCR.

20 – Mises à jour et modifications apportées aux BCR

Amgen se réserve le droit de modifier et/ou mettre à jour ces BCR à tout moment. Une telle mise à jour des BCR peut être nécessaire notamment à la suite de changements dans les obligations légales, de changements importants apportés à la structure du groupe Amgen ou d'exigences officielles imposées par les autorités de protection des données compétentes.

Amgen rendra compte de toute modification significative apportée aux BCR ou à la liste des sociétés participantes à toutes les autres sociétés participantes et aux autorités de protection des données, visant à prendre en compte les modifications de l'environnement réglementaire et de la structure d'entreprise.

Certaines modifications pourraient nécessiter une nouvelle autorisation de la part des autorités de protection des données.

Le Responsable de la protection des données (Chief Privacy Officer)tiendra une liste mise à jour des sociétés participantes aux BCR, des pays réglementés qui peuvent être protégés en vertu des BCR,suivra les mises à jour apportées aux BCR, et transmettra les informations nécessaires aux personnes concernées ou aux autorités de protection des données sur demande.

Amgen s'engage à ce qu'aucun transfert ne soit effectué vers une nouvelle société participante en vertu des garanties contenues dans les BCR tant que la nouvelle société participante n'est pas effectivement liée par les BCR et en mesure de garantir le respect des BCR.

Toute modification apportée aux BCR ou à la liste des sociétés participantes, assortie d'un bref exposé des motifs justifiant cette mise à jour, sera notifiée une fois par an aux autorités de protection des données délivrant les autorisations de transfert.

Les modifications substantielles apportées aux règles seront également communiquées aux personnes concernées par quelque moyen que ce soit conformément à l'article 7 des BCR.

21 – Lien entre les législations nationales et les BCR

Si la législation locale exige un degré supérieur de protection des données personnelles, celle-ci prévaut sur les BCR. Si la législation locale applicable exige un degré inférieur de protection des données personnelles par rapport aux BCR, les BCR s'appliqueront.

En cas de conflit entre les obligations découlant de la loi locale applicable et les BCR, la société participante informera le Responsable de la protection des données (Chief Privacy Officer)sans délai indu.

Quoi qu'il en soit, les données personnelles seront traitées conformément à la loi applicable prévue par l'article 4 de la Directive 95/46/CE et la législation locale applicable.