

<b>GROUPE AXA</b> <b>Règles internes d'entreprise ou Binding Corporate Rules (BCR)</b>
---

### Contexte

Le Groupe AXA s'engage à assurer la protection des données obtenues dans le cadre de ses activités et à se conformer aux lois et réglementations applicables en matière de Traitement de Données à Caractère Personnel ainsi que des Catégories particulières de Données.

Le Groupe AXA est doté d'une gouvernance/organisation relative à la protection des Données à Caractère Personnel au niveau international avec (i) un modèle de gouvernance en matière de Données à Caractère Personnel approuvé par le Management Committee, (ii) un Chargé de la Protection des Données Groupe, (iii) un Comité de pilotage AXA BCR de la protection des données (iv) un réseau mondial de Chargés de la Protection des Données coordonné par le Chargé de la Protection des Données Groupe et (v) une politique au niveau du Groupe relative à la protection des Données à Caractère Personnel.

Le Groupe AXA a décidé d'adopter un ensemble de Règles internes d'entreprise (Binding Corporate Rules - « BCR ») afin de définir des garanties adéquates pour s'assurer que les Données à Caractère Personnel sont protégées au sein du Groupe AXA lors de leur Transfert d'une Entité AXA établie dans un Pays Adéquat (comme défini à l'article I ci-après) vers une Entité AXA établie dans un autre pays lorsque la loi applicable ne permet pas un tel transfert, et qu'un Transfert ultérieur de ces données n'est pas autorisé par la loi applicable.

### **ARTICLE I - DÉFINITIONS**

Lorsqu'ils sont utilisés dans les BCR, les annexes et l'Accord de Groupe, les expressions, acronymes et termes suivants comportant une majuscule emporteront le sens qui leur est donné ci-après :

« **Accord de Groupe** » ou « **AG** » désigne l'accord sur les BCR joint à l'Annexe 1 ainsi que tout Accord d'acceptation des Règles internes d'entreprise (décrit dans l'Annexe B de l'Annexe 1) portant sur les Règles internes d'entreprise du Groupe AXA signé par les Entités AXA BCR ou que celles-ci doivent signer.

« **Autorité de contrôle** » ou « **Autorité de protection des données** » ou « **APD** » désigne l'autorité administrative officielle en charge de la protection des Données à Caractère Personnel dans chaque Pays Adéquat où est présent le Groupe AXA (par exemple en France, il s'agit de la Commission Nationale de l'Informatique et des Libertés, en Espagne de l'Agencia Española de Protección de Datos, etc.). Afin d'éviter toute ambiguïté, le terme « **Autorité de contrôle** » désigne toute autorité de substitution succédant à une Autorité de protection des données.

« **Catégories Particulières de Données** » désigne les données décrites au paragraphe 2 de l'article IV.

« **Chargés de la Protection des Données** » ou « **CPD** » désigne la personne, au sein des Entités AXA, responsable de la coordination avec le CPDG et chargée de s'assurer que les Entités AXA respectent les Règles internes d'entreprise et la législation/réglementation en vigueur.

«**Chargé de la Protection des Données Groupe**» ou «**CPDG**» désigne la personne en charge du contrôle d'ensemble des présentes Règles internes d'entreprise par le biais d'un réseau de Chargés de la Protection des Données.

«**Clauses européennes types**» désigne les clauses contractuelles types publiées par la Commission européenne offrant les garanties suffisantes requises par la Réglementation européenne concernant le Transfert de Données à Caractère Personnel vers des pays Tiers qui ne garantissent pas un niveau de protection des données suffisant selon la Commission européenne.

«**Collaborateurs AXA**» désigne les salariés des Entités AXA, y compris les administrateurs, stagiaires, apprentis et autre fonction assimilée.

«**Comité de pilotage AXA BCR**» désigne un comité spécialement dédié aux Règles internes d'entreprise, composé de représentants de l'équipe dirigeante du Groupe AXA et de responsables de la protection des données d'Entités AXA BCR sélectionnées.

«**Comité européen de la protection des données**» désigne l'organe de l'Union composé des présidents des autorités nationales de chaque État membre et du Contrôleur européen à la protection des données.

«**Données à Caractère Personnel**» désigne les données se rapportant à une personne (personne physique) identifiée ou identifiable à partir de celles-ci ou à partir de données conjointement à d'autres informations.

«**EEE**» ou «**Espace économique européen**» désigne l'Espace économique européen qui comprend les pays de l'Union européenne et les pays membres de l'AELE (l'Association européenne de libre-échange). En 2012, l'EEE regroupait l'Autriche, la Belgique, la Bulgarie, Chypre, la République tchèque, le Danemark, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Irlande, l'Italie, la Lettonie, le Liechtenstein, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Norvège, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, l'Espagne, la Suède et le Royaume-Uni.

«**Entités AXA**» désigne :

(i) AXA, société anonyme à conseil d'administration, ayant son siège social 25, avenue Matignon, 75008 Paris, immatriculée au registre du commerce et des sociétés de Paris sous le numéro B 572 093 920;

(ii) toute société contrôlée par, ou contrôlant AXA, une société étant considérée comme en contrôlant une autre :

a. lorsqu'elle détient directement ou indirectement une fraction du capital lui conférant la majorité des droits de vote dans les assemblées générales de cette société ; ou

b. lorsqu'elle dispose seule de la majorité des droits de vote dans cette société en vertu d'un accord conclu avec d'autres associés ou actionnaires et qu'il n'est pas contraire à l'intérêt de la société ; ou

c. lorsqu'elle détermine en fait, par les droits de vote dont elle dispose, les décisions dans les assemblées générales de cette société ; ou

d. en tout état de cause, lorsqu'elle dispose, directement ou indirectement, d'une fraction des droits de vote supérieur à 40 % et qu'aucun autre associé ou actionnaire ne détient directement ou indirectement une fraction supérieure à la sienne.

(iii) tout groupement d'intérêt économique dans lequel AXA et/ou une ou plusieurs Sociétés du Groupe AXA participent à hauteur de 50 % au moins aux frais de fonctionnement.

(iv) Dans les cas où la loi applicable à une société limite les droits de vote ou le contrôle (tel que défini ci-dessus), cette société sera réputée être une Société du Groupe AXA, si les droits de vote dans les assemblées générales ou le contrôle détenu(s) par une Société du Groupe AXA atteignent le maximum fixé par la dite loi applicable.

(V) L'ensemble des Sociétés du Groupe AXA constitue le “ Groupe AXA ”.

« **Entités AXA BCR** » désigne toutes les Entités AXA ayant signé l'Accord de Groupe soit en tant qu'Exportateurs de données, soit en tant qu'Importateurs de données.

« **Exportateur de données** » désigne un Responsable du traitement établi dans un Pays Adéquat ou un Sous-traitant établi dans un Pays Adéquat qui traite des Données à Caractère Personnel pour le compte d'un Responsable du traitement qui transfère des Données à Caractère Personnel en dehors du Pays Adéquat où il est établi (que ce soit par le biais d'un Sous-traitant ou d'un Sous-traitant Tiers ou non) et qui a signé l'Accord de Groupe.

« **Exportateur de données de l'EEE** » désigne un Responsable du traitement établi dans l'EEE ou un Sous-traitant établi dans l'EEE qui traite des Données à Caractère Personnel pour le compte d'un Responsable du traitement qui transfère des Données à Caractère Personnel en dehors de l'EEE (que ce soit par le biais d'un Sous-traitant ou d'un Sous-traitant Tiers ou non) et qui a signé l'Accord de Groupe.

« **Groupe AXA** » désigne, ensemble, AXA SA et toutes les Entités AXA.

« **Hubs AXA BCR** » désigne les principales Entités AXA locales et/ou transversales ou d'autres groupes d'entreprises AXA participant à la mise en œuvre des Règles internes d'entreprise en collaboration avec le CPDG afin de préserver les Données à Caractère Personnel au sein du Groupe AXA et dans le cadre du transfert de Données à Caractère Personnel d'un état membre de l'Espace économique européen (« EEE ») vers l'EEE ou hors de l'EEE.

« **Importateur de données** » désigne un Responsable du traitement ou un Sous-traitant qui traite des Données à Caractère Personnel pour le compte d'un Responsable du traitement qui reçoit des Données à Caractère Personnel de l'Exportateur de données dans le cadre d'un Transfert concerné ou d'un Transfert ultérieur et qui a signé l'Accord de Groupe.

« **Pays Adéquat** » désigne tout pays faisant partie de l'EEE ainsi que la Principauté d'Andorre, la Suisse, les Îles Féroé, Guernesey, l'Île de Man et Jersey.

« **Personne concernée** » désigne toute personne physique, qui peut être identifiée, directement ou indirectement, par des moyens qui pourraient être raisonnablement utilisés par toute personne physique ou morale, en particulier par référence à une identification, comme un nom, un numéro d'identification, des données sur un lieu, un identifiant en ligne ou un ou plusieurs facteurs spécifiques à l'aspect physique, physiologique, génétique, mental, économique, culturel ou social de cette personne.

« **Personne concernée de l'EEE** » désigne une personne concernée qui résidait dans un État membre de l'EEE lorsque les Données à Caractère Personnel la concernant ont été recueillies.

« **Personne concernée d'un Pays Adéquat** » désigne une personne concernée qui résidait dans un Pays Adéquat lorsque les Données à Caractère Personnel la concernant ont été recueillies.

« **Règles internes d'entreprise** » ou « **BCR** » (**Binding Corporate Rules**) désigne les présentes Règles internes d'entreprise établies par et entre AXA SA et toutes les autres Entités AXA BCR.

« **Réglementation européenne** » désigne les règles et réglementations en vigueur, actuelles et futures, qui se rapportent à la protection des Données et s'appliquent dans les pays membres de l'EEE.

« **Responsable du traitement** » désigne une Entité AXA BCR qui, seule ou conjointement avec d'autres Entités AXA, détermine les finalités, conditions et moyens affectés au Traitement de Données à Caractère Personnel.

« **Sous-traitant** » désigne une Entité AXA BCR qui traite les Données à Caractère Personnel sur instruction d'un Responsable du traitement.

« **Tiers** » désigne la personne physique ou morale (y compris les Entités AXA / Entités AXA BCR), l'autorité publique, l'organe ou tout autre organisme que la Personne concernée, le Responsable du traitement, le Sous-traitant et les personnes qui, placées sous l'autorité directe du Responsable du traitement ou du Sous-traitant, sont habilitées à assurer le Traitement de Données à Caractère Personnel d'une Personne concernée.

« **Transfert concerné** » désigne un transfert de Données à Caractère Personnel (dans la mesure où lesdites Données n'ont pas déjà fait l'objet d'un Transfert concerné ou d'un Transfert ultérieur) :

- (i) d'une Entité AXA BCR qui est un Exportateur de données vers une autre Entité AXA BCR établie dans un pays qui (dans le cadre de l'application des Règles internes d'entreprise) n'offre pas le niveau de protection suffisant requis par la législation en matière de protection des données dans le Pays Adéquat de l'Exportateur de données ; et
- (ii) non assujetti aux dérogations autorisées ou conditions prévues par la législation relative à la protection de la vie privée du Pays Adéquat concerné (qui peuvent inclure le consentement de la Personne concernée, les protections contractuelles existantes, l'adhésion au *Privacy Shield* et/ou l'établissement dans un Pays Adéquat approuvé par la Commission européenne en vertu de la Réglementation européenne).

« **Transfert ultérieur** » désigne le transfert ultérieur de Données à Caractère Personnel précédemment exportées dans le cadre d'un Transfert concerné ou d'un Transfert en vertu du *Privacy Shield*, dans chaque cas :

- (i) vers une autre Entité AXA BCR établie dans un pays qui (dans le cadre de l'application des Règles internes d'entreprise) n'offre pas un niveau de protection adéquat exigé par la législation en matière de protection des données du Pays Adéquat concernée à l'origine du Transfert concerné d'origine ; et
- (ii) qui n'est pas assujetti aux dérogations autorisées ou conditions prévues par la législation relative à la protection des données de la Juridiction compétente concernée (qui peuvent inclure le consentement de la Personne concernée, les protections contractuelles existantes, l'adhésion au *Privacy Shield* et/ou l'établissement dans un pays approuvé par la Commission européenne en application de la Réglementation européenne).

« **Traitement** » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la séparation, le croisement, la fusion, la mise à disposition, la divulgation, 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.

« **Violation de données** » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de

données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

## **ARTICLE II -FINALITÉ**

Les BCR visent à garantir un niveau de protection adéquat à la Personne concernée dans le cadre d'un Transfert concerné ou d'un Transfert ultérieur entre une Entité AXA située dans un Pays Adéquat et une Entité AXA située dans un autre pays.

## **ARTICLE III - CHAMP D'APPLICATION**

### **1. Champ d'application géographique**

Le Groupe AXA est présent dans plus de 50 pays et plus de 150 000 Collaborateurs et distributeurs d'AXA s'engagent à servir des millions de clients.

Les présentes BCR s'appliquent exclusivement aux Transferts concernés d'Exportateurs de données établis dans un Pays Adéquat à des Importateurs de données établis dans un autre pays, ainsi qu'aux Transferts ultérieurs. Les recours en cas de violation des dispositions relatives aux droits de Tiers bénéficiaires, aux plaintes et aux dispositions prévues par les présentes BCR en matière de responsabilité (articles VII, VIII et IX des présentes) sont limités aux Personnes concernées établies dans un Pays Adéquat.

Les BCR ne s'appliquent pas aux Données à Caractère Personnel non soumises à une législation sur la protection des données personnelles d'un Pays Adéquat, autrement dit qui ne sont pas transférées depuis un Pays Adéquat. Par exemple,

- si une Entité AXA établie aux États-Unis transfère des Données à Caractère Personnel la concernant à une Entité AXA établie en Inde, ledit Transfert et le Traitement s'y rattachant ne relèveront pas des BCR ; ou
- si une Entité AXA établie au Japon transfère les Données à Caractère Personnel la concernant à une Entité AXA située à Singapour, ledit Transfert et le Traitement s'y rattachant ne relèveront pas des BCR.

### **2. Champ d'application matériel**

#### **a. Champ d'application pour les Entités AXA BCR et opposabilité aux Collaborateurs AXA**

Les présentes BCR lient toutes les Entités AXA ayant signé un Accord de Groupe portant sur l'acceptation des BCR, comme indiqué à l'Annexe A de l'Annexe 1, ou en accédant à l'Accord de Groupe. Chaque Entité AXA qui signe un AG devient une Entité AXA BCR à compter de la date de signature ou (si cette date intervient ultérieurement) à la date d'entrée en vigueur précisée dans l'AG en vigueur.

Conformément au droit du travail en vigueur, les présentes BCR engagent et s'appliquent aux Collaborateurs AXA de l'ensemble des Entités AXA BCR par l'un des moyens suivants, au niveau de chaque Entité AXA BCR :

- le respect des politiques internes contraignantes d'AXA, ou
- le respect du règlement intérieur, ou
- le respect d'une clause du contrat de travail, ou

- tout autre moyen permettant de rendre les BCR obligatoires pour les Collaborateurs AXA du pays concerné.

En application du droit du travail, du règlement intérieur et des contrats de travail en vigueur, chaque Entité AXA BCR peut prendre des mesures disciplinaires à l'encontre de ses Collaborateurs AXA, notamment dans les cas suivants :

- non-respect des présentes BCR de la part d'un Collaborateur AXA,
- non-respect des recommandations et conseils émis par les Chargés de la protection des données (« CPD ») suite à un contrôle de conformité,
- défaut de coopération dans le cadre du contrôle de conformité aux BCR effectué par les CPD ou par les Autorités de protection des données compétentes.

#### **b. Champ d'application des Données à Caractère Personnel et des Traitements**

Les Transferts de Données à Caractère Personnel et le Traitement assuré après ces Transferts visent à soutenir et faciliter les activités commerciales d'AXA.

Les domaines d'expertises d'AXA s'expriment à travers une offre de produits et de services adaptés à chaque client dans trois grands domaines d'activité : l'assurance dommages, l'assurance vie et la gestion d'actifs:

- l'activité dommages regroupe les assurances des biens et les assurances responsabilité civile. Elle couvre un large éventail de produits et de services destinés à nos clients particuliers et entreprises, notamment des services d'assistance et d'assurance internationale pour les grandes entreprises, dans les secteurs de la marine et de l'aéronautique, par exemple.
- l'activité d'assurances vie individuelles et collectives comprend d'une part des produits d'épargne et de retraite, d'autre part d'autres produits de prévoyance et d'assurance santé. Les produits épargne et retraite répondent au besoin de constitution d'un capital pour financer l'avenir, un projet d'avenir ou la retraite. La prévoyance couvre les risques liés à l'intégrité physique, à la santé ou la vie d'une personne. AXA offre également à ses clients particuliers, dans certains pays, une gamme simple de produits et de services bancaires complémentaires à notre offre d'assurance.
- l'activité gestion d'actifs place et gère les investissements des sociétés d'assurance du Groupe et de leurs clients, ainsi que ceux de tiers, particuliers ou entreprises.

Le service des activités métiers d'AXA inclut:

- Vision (définition de la vision à long terme de la société, définition de la stratégie commerciale, gestion d'un projet stratégique, suivi de l'évolution)
- Conception (définition de la stratégie en termes de produits, définition de la politique relative aux risques, étude, développement et lancement de produits, préservation du portefeuille de produits existants)
- Distribution (définition de la stratégie de distribution, gestion et contrôle des réseaux de distribution, exécution des opérations marketing, gestion des relations avec les clients, personnalisation de l'offre, vente, valorisation des performances commerciales)
- Production (souscription, administration d'une police, recouvrement des primes, suivi du portefeuille de polices)
- Service (gestion de catastrophe, traitement des sinistres, service client, gestion des auxiliaires, détection des fraudes, gestion des subrogations, recouvrement des fonds de réassurance, gestion de la récupération d'épaves, contrôle de la gestion des sinistres)
- Gestion financière (planification et contrôle des finances, gestion des investissements, gestion des finances de l'entreprise, saisie des opérations, gestion des immobilisations, analyse financière, gestion de trésorerie, gestion des opérations)

de trésorerie, gestion de la fiscalité, respect des réglementations, gestion des réassurances)

- Gestion des technologies de l'information (gestion des relations avec les clients de l'informatique, fourniture et maintenance de solutions, gestion des services informatiques et assistance, gestion du système informatique, gestion de l'organisation informatique, gestion de la sécurité informatique)
- Développement et gestion des ressources humaines (administration des ressources humaines, gestion des ressources humaines, communication dans le domaine des ressources humaines, gestion des partenaires sociaux et comités d'entreprises)
- Gestion des achats (gestion des fournisseurs et des contrats, achat, réception de biens et services, gestion des factures fournisseurs, validation des règlements, rapport sur l'approvisionnement et analyse des performances)
- Gestion des risques (gestion des risques financiers, gestion des risques d'investissements, gestion du risque opérationnel, projection, calcul de la rentabilité ajustée au risque)
- Autres fonctions de soutien (communication externe, assistance juridique, gestion des améliorations et des changements, audit interne, fonctions centrales).

Tous les types et toutes les catégories de Données à Caractère Personnel traitées par les Entités AXA BCR dans le cadre de leurs activités commerciales entrent dans le champ d'application des présentes BCR. Ces types et catégories comprennent entre autres : les Données à Caractère Personnel recueillies auprès de clients, prospects, demandeurs, Collaborateurs AXA, candidats à un poste, agents, fournisseurs et autres Tiers.

Les catégories de Données à Caractère Personnel traitées par les Entités AXA BCR devant ou pouvant les collecter localement conformément à la législation applicable incluent celles qui suivent :

- état civil/identité/données d'identification,
- vie professionnelle,
- vie personnelle,
- données de connexion,
- données de localisation,
- numéro de sécurité sociale,
- informations d'ordre économique et financier,
- infractions, condamnations, mesures de sûreté,
- opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciale,
- données biométriques,
- données génétiques,
- décès des personnes,
- appréciation sur les difficultés sociales des personnes,
- données de l'assurance maladie

Les BCR s'appliquent aussi bien aux Traitements automatisés que manuels.

## **ARTICLE IV - PRINCIPES RELATIFS AU TRAITEMENT**

Les principes relatifs au Traitement définis ci-après s'appliquent au Traitement de Données à Caractère Personnel visées à l'Article III- CHAMP D'APPLICATION.

### **1. Principes de base**

Chaque Entité AXA BCR s'engage à respecter les obligations requises par la législation en vigueur et par l'Autorité de protection des données compétente concernant le Traitement

initial des Données à Caractère Personnel transférées ultérieurement dans le cadre d'un Transfert concerné ou d'un Transfert ultérieur dans le cadre des BCR.

Chaque Entité AXA BCR s'engage à ce que le Traitement de Données à Caractère Personnel effectué sous son contrôle, y compris les Transferts de données, continue à être assurés conformément aux dispositions des présentes BCR, en particulier selon les principes généraux relatifs à la protection des données minimum suivants :

- Les Données à Caractère Personnel doivent être recueillies de manière loyale, licite et transparente et en respect du droit à l'information de la Personne concernée, sauf dans le cas où ladite information n'est pas nécessaire en vertu d'exceptions légales, et ne doivent être traitées que si la Personne concernée a donné son accord explicite ou si le Traitement est autorisé en application de la législation en vigueur.
- Les Données à Caractère Personnel doivent exclusivement être recueillies à des fins précises, explicites et légitimes et ne doivent pas subir de Traitement ultérieur incompatible avec ces finalités. Les Données à Caractère Personnel seront uniquement communiquées à des Tiers pour ces finalités ou à toute autre finalité autorisée par la législation en vigueur.
- Des contrôles appropriés ainsi que des procédures techniques et d'organisation doivent être mis en place afin de garantir la sécurité des Données à Caractère Personnel et les protéger contre l'accès ou la diffusion non autorisé(e) et les préjudices potentiels pouvant résulter d'une altération de Données, d'une destruction accidentelle ou illicite ou d'une perte accidentelle de Données, ainsi que contre toute autre forme de Traitement illicite. Compte tenu des obligations légales, des bonnes pratiques et des coûts inhérents à leur mise en œuvre, les mesures de sécurité doivent assurer un niveau de sécurité approprié en regard des risques présentés par le Traitement et de la nature des Données à Caractère Personnel à protéger.
- Des mesures techniques et organisationnelles appropriées doivent être prises, au moment de la détermination des moyens de traitement et au moment du traitement lui-même, afin de mettre en œuvre les principes relatifs à la protection des données de façon effective et d'intégrer les garanties nécessaires dès la conception aux fins de répondre aux exigences de la Réglementation européenne et de protéger les droits de la personne concernée.
- Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre en vue de garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.
- Les Données à Caractère Personnel recueillies doivent être exactes, complètes pour les finalités en question et, au besoin, mises à jour.
- Les Données à Caractère Personnel recueillies doivent être réduites au minimum, c'est-à-dire adéquates, pertinentes et limitées à ce qui est réellement nécessaire au regard des finalités pour lesquelles elles sont recueillies et/ou traitées ultérieurement.
- Les Données à Caractère Personnel ne doivent pas être conservées plus longtemps que nécessaire par rapport aux finalités pour lesquelles elles ont été recueillies, sauf disposition contraire prévue par la loi en vigueur. De plus amples informations concernant les durées de conservation des données pertinentes sont disponibles



dans la politique en matière de conservation des données applicable au sein de chaque Entité AXA BCR.

- Des procédures doivent être mises en place de manière à garantir une réponse rapide aux demandes formulées par les Personnes concernées afin que celles-ci puissent exercer pleinement leur droit d'accès, de rectification, d'effacement de leurs Données à Caractère Personnel et leurs droits de limitation et d'opposition au Traitement (sauf disposition contraire prévue par la loi en vigueur) et de retrait du consentement quand le Traitement dépend de ce fondement juridique.

Les Données à Caractère Personnel doivent être uniquement traitées si ledit Traitement est légitime, notamment pour les cas où:

- la Personne concernée a donné son consentement ; ou
- le Traitement 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 celle-ci; ou
- le Traitement est nécessaire au respect d'une obligation légale à laquelle le Responsable du Traitement est soumis ; ou
- le Traitement est nécessaire à la sauvegarde de l'intérêt vital de la Personne concernée ; ou
- le Traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le Responsable du Traitement ou le Tiers auquel les Données à Caractère Personnel sont communiquées ; ou
- le Traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le Responsable du Traitement ou par le ou les Tiers auquel/auxquels les Données à Caractère Personnel sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la Personne concernée.

Si le Traitement de Données à Caractère Personnel est uniquement fondé sur un Traitement automatisé de Données, y compris le profilage, et produit des effets juridiques pour les Personnes concernées ou les affecte de manière significative, les Personnes concernées ont le droit de ne pas faire l'objet d'une telle décision, à moins que ledit Traitement :

- ne soit nécessaire 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 et de contester la décision, garantissent la sauvegarde de son intérêt légitime ; ou
- soit autorisé par une loi qui précise également les mesures garantissant la sauvegarde de l'intérêt légitime de la Personne concernée ; ou
- ne soit fondé sur le consentement explicite de la Personne concernée,

étant entendu qu'il existe des mesures appropriées pour la sauvegarde de ses intérêts légitimes, telles que la possibilité d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision.

Chaque Responsable du Traitement tiendra un registre de toutes les catégories des activités de traitement effectuées sur les Données à Caractère Personnel des Personnes concernées de l'EEE et mettra le registre à disposition de l'Autorité de protection des données coordinatrice et de toute autre Autorité de protection des données pertinente sur demande.

Chaque Responsable du Traitement effectuera des Analyses d'Impact relatives à la Protection des Données des opérations de traitement susceptibles de constituer un risque élevé pour les droits et libertés des Personnes concernées de l'EEE. Si une Analyse d'Impact relative à la

Protection des Données indique que le traitement constituerait un risque élevé en l'absence de mesures prises par l'Entité AXA BCR pour atténuer le risque, l'Autorité de protection des données coordinatrice ou toute autre Autorité de protection des données pertinente devra être consultée.

## **2. Catégories Particulières de Données à Caractère Personnel**

Aux fins des présentes BCR, les Catégories Particulières de Données concernent notamment les Données à Caractère Personnel portant sur :

- l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques de la Personne concernée ;
- l'appartenance à une organisation syndicale ;
- la santé physique ou mentale ou les conditions ou la vie ou l'orientation sexuelle de la Personne Concernée, les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique ;
- des informations particulières réputées être des Catégories Particulières de Données en vertu de la législation et des réglementations en vigueur (par exemple des données médicales) ;
- la commission ou la commission présumée de condamnations pénales et infractions par la Personne concernée ; ou
- l'infraction ou la présomption d'infraction pénale commise par la Personne concernée ; ou toutes poursuites engagées pour une infraction commise ou présumée commise par la Personne Concernée, la soumission de telles poursuites ou la décision de toute juridiction dans le cadre de telles poursuites.

La liste des Catégories Particulières de Données ci-dessus n'est en aucun cas exhaustive, la législation locale pouvant inclure d'autres catégories que l'Exportateur de données et l'Importateur de données doivent, dans certains cas et le cas échéant, considérer comme des Catégories Particulières de Données.

Le Traitement de Catégories Particulières de Données est interdit, sauf dans les cas où :

1. la Personne concernée a donné son consentement exprès au Traitement de Catégories Particulières de Données en question, et ledit consentement est considéré comme valable en vertu de la législation et des réglementations en vigueur ; ou
2. le Traitement est nécessaire à des fins de respect des obligations et droits spécifiques du Responsable du Traitement ou de la Personne Concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où il est autorisé par une législation en vigueur prévoyant des garanties adéquates ; ou
3. 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 serait dans l'incapacité physique ou juridique de donner son consentement ; ou
4. le Traitement est effectué par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale dans le cadre de leurs activités légitimes et avec des garanties appropriées et à condition que le Traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers en rapport avec les objectifs poursuivis par celui-ci et que les Données à Caractère Personnel ne soient pas communiquées à des Tiers sans le consentement des Personnes concernées ; ou
5. le Traitement porte sur des Catégories Particulières de Données rendues publiques par la Personne concernée ; ou

6. le Traitement de Catégories Particulières de Données est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ; ou
7. le Traitement est nécessaire pour des motifs d'intérêt public, sur la base du droit de l'Union ou du droit d'un État membre qui 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 ; ou
8. le Traitement de Catégories Particulières de Données est nécessaire à des fins de médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, 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 de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de santé et soumis aux conditions et garanties si ces données sont traitées :
  - o par un professionnel de la santé soumis à une obligation de secret professionnel, ou
  - o par une autre personne également soumise à une obligation de secret ; ou
9. le Traitement est nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique selon le droit de l'Union ou le droit d'un État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la Personne concernée, notamment le secret professionnel ;
10. le Traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à la Réglementation européenne, sur la base du droit de l'Union ou du droit d'un État membre qui 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 ;
11. le Traitement est autorisé en vertu de la législation en vigueur dans le pays où est établi l'Exportateur de données.

### **3. Sous-traitance**

Dans le cas où le Traitement est assuré par un Sous-traitant pour le compte d'un Importateur de données, ce dernier est tenu d'obtenir l'autorisation écrite préalable de l'Exportateur de Données, de choisir un Sous-traitant donnant des garanties suffisantes quant à la mise en œuvre de mesures de sécurité technique et de mesures organisationnelles appropriées afin d'assurer un Traitement conforme aux BCR, et l'Importateur de données doit veiller à ce que le Sous-traitant respecte ces mesures. L'Importateur de données qui choisit le Sous-traitant doit s'assurer que ce dernier accepte lesdites mesures de sécurité technique et organisationnelle en signant un contrat écrit conformément à la Réglementation européenne stipulant notamment que le Sous-traitant ne doit agir que sur les seules instructions de l'Importateur de données.

### **4. Transferts de données**

#### **1. Transferts de données au sein du Groupe AXA**

Aucune donnée à Caractère Personnel ne doit être transférée à un Importateur de données établi dans un pays en dehors de l'EEE (ou dans le cas d'exportations d'un autre Pays Adéquat) tant que l'Exportateur de données n'a pas établi que l'Importateur de données était lié :

- par les présentes BCR, ou
- par d'autres mesures autorisant le transfert de Données à Caractère Personnel en vertu de la législation en vigueur (par exemple, les Clauses européennes types).

Comme mentionné dans les définitions de « Transfert concerné » et « Transfert ultérieur », les BCR s'appliquent uniquement aux Transferts qui ne sont pas déjà visés par d'autres mesures autorisant les transferts, sauf accord écrit contraire entre l'Exportateur de données et l'Importateur de données.

## **2. Transferts de données en dehors du Groupe AXA**

Pour les Transferts vers une société tierce au Groupe AXA établie en dehors de l'EEE (dans le cas d'exportations depuis l'EEE et vers un pays non qualifié de Pays Adéquat), chaque Importateur de données s'engage à :

- lors d'un Transfert vers un Sous-traitant, signer un contrat de Traitement de données avec le Sous-traitant Tiers afin que celui-ci s'engage à protéger les Données traitées de manière appropriée conformément aux normes européennes, en se basant par exemple sur les Clauses européennes types en vigueur proposées par la Commission européenne, ou sur un contrat équivalent; ou
- prendre toutes les autres garanties nécessaires au Transfert de Données à Caractère Personnel conformément à la législation en vigueur (par exemple les Clauses européennes types).

## **5. Violation de Données**

En cas de Violation de Données à Caractère Personnel des Personnes Concernées d'un Pays Adéquat, les Entités AXA BCR concernées notifieront la Violation de Données au(x) CPD des Entités AXA BCR affectées dans les meilleurs délais, et quand plus de 1 000 Personnes Concernées d'un Pays Adéquat sont concernées, elles le notifieront également au CPDG.

Les Entités AXA BCR qui sont des Responsables du Traitement impliqués dans une Violation de Données susceptible d'engendrer un risque élevé pour les droits et libertés des Personnes Concernées d'un Pays Adéquat le notifieront également directement aux Personnes Concernées d'un Pays Adéquat.

Toute notification d'une Violation de Données sera documentée et doit inclure au moins :

- les faits afférents à la Violation de Données,
- les conséquences probables de la Violation de Données,
- les mesures prises pour remédier à la Violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Cette documentation sera mise à la disposition de l'Autorité de protection des données coordinatrice et de toute autre Autorité de protection des données compétente sur demande.

## **ARTICLE V - DROITS D'INFORMATION, D'ACCÈS, DE RECTIFICATION, DE SUPPRESSION ET D'OPPOSITION DES DONNÉES**

Dans le cas d'un Traitement de Données à Caractère Personnel par un Importateur de données, les Personnes concernées d'une Juridiction compétente sont en droit, moyennant une demande écrite :

- d'obtenir, sur demande et dans un délai raisonnable, une copie de la version publique des présentes BCR depuis le site Internet d'AXA, le site Intranet d'AXA ou auprès des CPD ;

- de demander des informations au sujet des Données à Caractère Personnel conservées les concernant, notamment les informations relatives à la collecte des Données à Caractère Personnel ;
- d'obtenir la liste des destinataires ou des catégories de destinataires auxquels/auxquelles les Données à Caractère Personnel les concernant sont transférées ;
- d'obtenir des informations concernant les finalités pour lesquelles les Données à Caractère Personnel les concernant sont recueillies et transférées ;
- d'obtenir la rectification des Données à Caractère Personnel les concernant dans les meilleurs délais si celles-ci sont inexactes ;
- de s'opposer, pour des motifs tenant à leur situation particulière, à ce que des Données à Caractère Personnel les concernant fassent l'objet d'un Traitement, sauf disposition contraire prévue la loi en vigueur ;
- de demander l'effacement des Données à Caractère Personnel les concernant dans les meilleurs délais pour des motifs précisés par la Réglementation européenne et si cela est possible sur le plan juridique ;
- d'obtenir la restriction du traitement conformément à la Réglementation européenne ;
- d'obtenir toute autre information requise en vertu de la législation nationale,

dans chaque cas, sauf dans la mesure autorisée par la législation en matière de protection de données du Pays Adéquat où la Personne concernée résidait au moment de la collecte des Données à Caractère Personnel la concernant.

## **ARTICLE VI - ACTIONS EN VUE DE L'APPLICATION DES REGLES INTERNES D'ENTREPRISE**

### **1. Programme de formation**

Les Entités AXA BCR s'engagent à mettre en place des programmes de formation sur la protection des Données à Caractère Personnel destinés aux Collaborateurs AXA participant au Traitement de Données à Caractère Personnel et au développement d'outils utilisés pour traiter les Données à Caractère Personnel conformément aux principes énoncés dans les présentes BCR.

Les principes généraux en termes de formation et de sensibilisation seront définis au niveau central et des exemples concrets seront partagés. Le développement et la mise en œuvre finale des sessions de formation et de sensibilisation (apprentissage à distance, session en présentiel ,...) seront toutefois à la charge de chaque Entité AXA BCR, conformément aux procédures et à la législation en vigueur.

Chaque Entité AXA BCR doit définir les modalités de suivi des formations. Chacune d'elles doit, en outre, déterminer la fréquence des sessions à laquelle les Collaborateurs doivent suivre la formation, la formation sur la protection des Données à Caractère Personnel dispensée aux nouveaux Collaborateurs AXA dans le cadre de la journée d'accueil qu'ils doivent suivre après avoir été embauchés au sein d'une Entité AXA BCR, ainsi que la formation dédiée aux Collaborateurs AXA manipulant des Données à Caractère Personnel.

### **2. Gouvernance des BCR**

### **3. Responsabilités concernant les BCR et le programme de contrôle de leur application**

#### **4. Accès et communication des BCR aux Personnes concernées d'un Pays Adéquat**

Les Personnes concernées d'un Pays Adéquat n'ayant pas accès au site Intranet d'AXA, comme les clients, les personnes assimilées (demandeurs, victimes d'accidents et autres bénéficiaires d'une police d'assurance ne l'ayant pas souscrite), candidats à un poste et fournisseurs peuvent trouver des informations sur les BCR en consultant la version publique des BCR disponible sur le site institutionnel Internet d'AXA.

Les Personnes concernées d'un Pays Adéquat ayant accès au site Intranet d'AXA, comme les Collaborateurs AXA et les personnes assimilées (agents, représentants,...), peuvent trouver des informations sur les BCR en consultant la version publique des BCR disponibles sur le site Intranet d'AXA.

D'autres sources d'information sont mises à la disposition des clients, des fournisseurs et des Collaborateurs AXA. Des courriers/notes d'informations sur différents sujets peuvent être adressé(e)s aux clients. Ces derniers peuvent recevoir des informations par l'intermédiaire d'une agence (par exemple par le biais de l'accès des agents au site Intranet). Les Collaborateurs AXA peuvent recevoir des informations par l'intermédiaire des comités d'entreprise ou de tout autre organisme compétent représentant le personnel. Dans la majorité des cas, il n'est pas possible (car ceci est extrêmement difficile et coûteux) d'adresser un courrier à tous les clients, comme les demandeurs, victimes d'accidents ou bénéficiaires de polices qui ne sont pas assurés ou qui ne les ont pas souscrites.

#### **ARTICLE VII - DROITS DE TIERS BÉNÉFICIAIRES**

Tous les Exportateurs de données acceptent d'accorder aux Personnes concernées d'un Pays Adéquat des droits de Tiers bénéficiaires au titre des présentes BCR en ce qui concerne les Transferts concernés et les Transferts ultérieurs. Tout Exportateur de données reconnaît et convient donc expressément que les Personnes concernées d'un Pays Adéquat sont autorisées à exercer leurs droits relatifs aux Transferts concernés et aux Transferts ultérieurs en vertu des dispositions visées aux articles IV.1, IV.2, IV.4, IV 5, V, VII, VIII, IX, X, XII.3 et XIII des présentes BCR et que tout manquement aux obligations incombant à l'Exportateur de données au titre des dits articles donne droit à un recours dans ces cas et, au besoin, dans les limites autorisées par la législation en vigueur, à des droits à réparation (selon le cas en fonction du manquement commis et du préjudice subi) pour la Personne concernée d'un Pays Adéquat, affectée par ce préjudice.

Il est expressément prévu que les droits accordés à des Tiers, comme précisé ci-dessus, sont strictement réservés aux Personnes concernées d'un Pays Adéquat en ce qui concerne les Transferts concernés et les Transferts ultérieurs et ne doivent en aucun cas être étendus ou être interprétés comme s'étendant aux Personnes concernées d'un pays non soumis à réglementation ou à d'autres Transferts de Données à Caractère Personnel.

#### **ARTICLE VIII - PLAINTES**

Les Entités AXA BCR sont tenues de mettre en place une procédure interne de Traitement des plaintes. En cas de litige, les Personnes concernées d'une Juridiction compétente sont habilitées à déposer une plainte, en ayant recours à la procédure locale appropriée, en cas de Traitement illicite ou non conforme de Données à Caractère Personnel les concernant qui ne serait pas conforme, de quelque façon que ce soit, aux présentes BCR auprès :

- du Chargé de la Protection des Données,

- de l'Autorité de protection des données compétente qui sera, soit l'Autorité de protection des données dans le Pays Adéquat de sa résidence habituelle au moment où les Données à Caractère Personnel impliquées dans la réclamation ont été collectées, soit du lieu où la violation aurait été commise, et
- des juridictions compétentes d'un pays de l'EEE au choix de la Personne Concernée : la Personne Concernée peut choisir d'agir par-devant les tribunaux du pays de l'EEE dans lequel l'Exportateur de données est établi ou par-devant les tribunaux du pays de l'EEE où la Personne Concernée avait sa résidence habituelle au moment où les Données à Caractère Personnel impliquées dans la réclamation sont collectées.

Afin d'éviter toute ambiguïté, il est entendu que si la Personne concernée d'un Pays Adéquat n'est pas satisfaite des réponses du Chargé de la Protection des Données, celle-ci est en droit de déposer une plainte auprès de l'Autorité de protection des données compétente et/ou des juridictions nationales compétentes conformément aux dispositions visées au paragraphe précédent.

Chaque Entité AXA BCR doit mettre en place sur son site Internet des outils permettant aux Personnes concernées d'un Pays Adéquat de déposer une plainte, et notamment par au moins l'un des éléments suivants :

- Un lien vers un formulaire de plainte
- Une adresse e-mail
- Un numéro de téléphone
- Une adresse postale.

À moins qu'il ne s'avère particulièrement difficile de trouver les informations nécessaires pour répondre à la plainte, les plaintes doivent être examinées dans un délai d'un (1) mois à compter du dépôt de la plainte. En cas de difficulté particulière et en tenant compte de la complexité et du nombre de demandes, cette durée d'un (1) mois peut être prolongée au maximum de deux (2) mois supplémentaires, auquel cas, les Personnes Concernées d'un Pays Adéquat en seront informées.

## **ARTICLE IX - RESPONSABILITÉ**

### **1. Disposition générale**

Chaque Entité AXA BCR assume l'entière responsabilité en cas de manquements aux BCR qui relèveraient de sa responsabilité à l'égard, selon le cas, d'autres Entités AXA BCR, des Autorités de protection des données compétentes dans un Pays Adéquat et des Personnes concernées d'un Pays Adéquat, dans tous les cas dans les limites autorisées par la législation et la réglementation en vigueur.

Dans les limites autorisées par la législation et la réglementation en vigueur et en application des articles IX(2) et IX(3), chaque Exportateur de données est responsable individuellement de tout préjudice causé à une Personne concernée d'un Pays Adéquat à la suite d'un manquement aux BCR qui lui est reproché ou qui a été commis par un Importateur de données ayant reçu les Données à Caractère Personnel transférées depuis un Pays Adéquat, dans le cadre d'un Transfert concerné ou d'un Transfert ultérieur effectué par l'Exportateur de Données en question.

Dans les limites autorisées par la législation et la réglementation en vigueur et en application des articles IX(2) et IX(3), si les Données à Caractère Personnel d'une Personne concernée située dans l'EEE proviennent d'un Exportateur de données établi dans l'EEE, chaque Exportateur de données établi dans l'EEE est responsable individuellement de tout préjudice

causé à une Personne concernée d'un Pays Adéquat suite à un manquement aux BCR qui lui est reproché ou qui a été commis par un Importateur de données ayant reçu les Données à Caractère Personnel depuis un Pays Adéquat, dans le cadre d'un Transfert concerné ou d'un Transfert ultérieur effectué par l'Exportateur de Données en question.

En application des articles IX(2) et IX (3), chaque Entité AXA BCR est responsable des pertes ou des préjudices résultant d'un manquement aux BCR qui lui est imputable, dans les limites autorisées par la législation et la réglementation en vigueur. Aucune Entité AXA BCR ne pourra être tenue responsable d'un manquement commis par une autre Entité AXA BCR, sauf dans le cas d'un manquement de la part d'un Importateur de données pour lequel l'Exportateur de données peut être tenu d'indemniser dans un premier temps la Personne concernée d'un Pays Adéquat (au titre des articles IX(2) et (3)) et peut ensuite demander un remboursement à l'Importateur de données. Par exemple, si un Importateur de données ne respecte pas les BCR et si l'Exportateur de données doit indemniser la Personne concernée d'un Pays Adéquat au titre dudit manquement, l'Importateur de données est tenu de rembourser l'Exportateur de données. De même, si un Exportateur de données ne respecte pas les BCR et si l'Importateur de données indemnise la Personne concernée d'un Pays Adéquat, l'exportateur de données est tenu de rembourser l'Importateur de données.

L'Exportateur de données, dont la responsabilité est engagée suite à un manquement de la part d'un Importateur de données, est habilité à prendre toutes les mesures nécessaires afin de remédier aux actes commis par l'Importateur de données et, pour compenser le manquement et le préjudice subi par la Personne concernée d'un Pays Adéquat, s'engage à indemniser cette dernière conformément à la législation et à la réglementation locale en vigueur. L'Exportateur de données est ensuite en droit de demander réparation à l'Importateur de données au titre du manquement aux BCR qui lui est reproché. La responsabilité de l'Exportateur de données peut être partiellement ou totalement dérogée s'il est en mesure d'apporter la preuve qu'il n'est pas responsable du préjudice subi.

Une Personne concernée d'un Pays Adéquat est en droit de demander la réparation du préjudice subi, causé par un Importateur de données et se rapportant à des Données à Caractère Personnel transférées par l'Exportateur de données, en contrepartie du manquement reproché, conformément à la législation et à la réglementation locales en vigueur et en fonction du préjudice subi (prouvé). Dans les limites autorisées par la législation en vigueur, une Personne concernée d'un Pays Adéquat peut déposer plainte auprès de l'Autorité de protection des données ou des juridictions compétentes du pays où est établi l'Exportateur de données. Si ce dernier n'est pas établi dans l'EEE mais assure le Traitement des Données à Caractère Personnel dans l'EEE de Personnes concernées de pays membres de l'EEE, la juridiction compétente est le pays où le Traitement est assuré. Si les Données à Caractère Personnel de Personnes concernées établies dans l'EEE proviennent d'un Exportateur de données établi dans l'EEE, la juridiction compétente est le lieu d'établissement du premier Exportateur de données dans l'EEE.

## **2. Dispositions complémentaires applicables à un Importateur de données agissant en qualité de Responsable du Traitement**

Les dispositions suivantes s'appliquent seulement si un Importateur de données agit en qualité de Responsable du Traitement et elles définissent les conditions dans lesquelles une plainte peut être déposée par une Personne concernée d'un Pays Adéquat à l'encontre de l'Importateur de données en question.

Dans le cas où des plaintes seraient déposées relative à un manquement présumé de la part de l'Importateur de données à ses obligations au titre des BCR, la Personne concernée d'un Pays Adéquat doit dans un premier temps demander que l'Exportateur de données concerné prenne des mesures raisonnables afin d'examiner l'affaire et (si un manquement est avéré)



remédier au préjudice résultant du manquement présumé et subi par la Personne concernée d'un Pays Adéquat ainsi que de faire valoir ses droits à l'encontre de l'Importateur de données ayant enfreint les BCR. Si l'Exportateur de données ne prend pas lesdites mesures dans un délai raisonnable (en règle générale 1 mois), la Personne concernée d'un Pays Adéquat est alors en droit de faire valoir ses droits directement à l'encontre de l'Importateur de données. Une Personne concernée d'un Pays Adéquat est également habilitée à intenter directement une action à l'encontre d'un Exportateur de données qui n'aurait pas pris les mesures raisonnables afin de déterminer si l'Importateur de données est en mesure de respecter ses obligations dans le cadre des présentes BCR dans les limites autorisées par la législation en vigueur et conformément à ladite législation.

### **3. Dispositions complémentaires concernant un Importateur de données agissant en qualité de Sous-traitant**

Les dispositions suivantes s'appliquent uniquement dans le cas où un Importateur de données agit en qualité de Sous-traitant et elles définissent les conditions dans lesquelles une plainte peut être déposée par une Personne concernée d'un Pays Adéquat à l'encontre d'un Importateur de données ou de son Sous-traitant.

Si une Personne concernée d'un Pays Adéquat n'est pas en mesure d'intenter une action en réparation à l'encontre de l'Exportateur de données, suite à un manquement de la part de l'Importateur de données ou de son Sous-traitant à une quelconque de ses obligations au titre des présentes BCR, en raison du fait que l'Exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'Importateur de données convient que la Personne concernée d'un Pays Adéquat peut exercer un recours à l'encontre de l'Importateur de données comme si celui-ci était l'Exportateur de données, à moins que l'entité qui lui succède n'assume toutes les obligations légales de l'Exportateur de données, par contrat ou par effet de loi, auquel cas la Personne concernée d'un Pays Adéquat peut exercer ses droits à l'encontre de l'entité en question. L'Importateur de données ne peut pas se prévaloir d'un manquement de la part d'un Sous-traitant à ses obligations dans le but de s'exonérer de ses propres responsabilités.

Si une Personne concernée d'un Pays Adéquat n'est pas en mesure d'exercer un recours à l'encontre de l'Exportateur de données ou de l'Importateur de données, suite à un manquement de la part d'une Entité AXA BCR Sous-traitante à une quelconque de ses obligations au titre des présentes BCR, en raison du fait que l'Exportateur de données et l'Importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolubles, l'Entité AXA BCR Sous-traitante convient que la Personne concernée d'un Pays Adéquat peut exercer un recours à son encontre se rapportant à ses propres opérations de Traitement comme si celle-ci était l'Exportateur de données ou l'Importateur de données, à moins que l'entité qui lui succède n'assume toutes les obligations légales de l'Exportateur de données ou de l'Importateur de données, par contrat ou par effet de loi, auquel cas la Personne concernée d'un Pays Adéquat peut exercer ses droits à l'encontre de l'Entité en question. La responsabilité de l'Entité AXA BCR Sous-traitante est limitée à ses propres opérations de Traitement de Données à Caractère Personnel.

## **ARTICLE X - ENTRAIDE ET COOPÉRATION AVEC LES AUTORITÉS DE PROTECTION DES DONNÉES**

### **1. Coopération avec les Autorités de protection des données**

Les Entités AXA BCR travailleront en collaboration avec leur Autorité de protection des données compétente sur toute question relative à l'interprétation des BCR dans les limites

autorisées par la législation et la réglementation en vigueur et sans renoncer aux exceptions et/ou droits de recours dont le Responsable du traitement peut se prévaloir :

- en mettant à disposition le personnel nécessaire pour dialoguer avec les Autorités de protection de données,
- en examinant et étudiant activement les décisions prises par les Autorités de protection de données et les conclusions du Comité européen de la protection des données concernant les BCR,
- en informant les Autorités de protection des données concernées de toute modification importante des BCR,
- en répondant aux demandes d'information ou plaintes adressées par les Autorités de protection des données,
- en appliquant les recommandations ou les conseils des Autorités de protection des données compétentes en ce qui concerne le respect des BCR par les Entités AXA BCR.

Les Entités AXA BCR conviennent d'appliquer les décisions officielles de l'Autorité de protection des données compétente concernant l'interprétation et l'application des BCR dans la mesure autorisée par la législation et les réglementations en vigueur et sans renoncer aux exceptions et/ou droits de recours dont le Responsable du traitement peut se prévaloir.

## **2. Liens entre la législation nationale et les règles d'entreprise contraignantes**

Les Entités AXA BCR doivent toujours respecter la législation locale en vigueur. En l'absence de droit en matière de protection des données, les Données à Caractère Personnel seront traitées conformément aux BCR. Si la législation locale prévoit un niveau de protection des Données à Caractère Personnel supérieur à celui des BCR, la législation locale prévaudra. Dans le cas où la législation locale prévoirait un niveau de protection des Données à Caractère Personnel inférieur à celui des BCR, ces dernières prévaudront.

Si une Entité AXA BCR a des raisons de penser que les exigences légales/réglementaires en vigueur ne lui permettent pas d'appliquer les BCR, l'Entité AXA BCR s'engage à en informer sans délai son CPD, qui informe à son tour le CPD de l'Exportateur de données et le CPDG.

Dans la mesure où certaines clauses des présentes BCR seraient en contradiction avec les exigences légales/réglementaires en vigueur, ces dernières prévaudront jusqu'à l'obtention d'une solution adéquate et conforme à la législation locale en vigueur. Le CPDG et/ou le CPD peut/vent contacter l'Autorité de protection des données compétente afin de discuter des solutions éventuelles.

## **3. Demande de divulgation émanant des organes d'application des lois**

Quand une Entité AXA BCR reçoit une demande juridiquement contraignante de divulgation de Données à Caractère Personnel émanant d'une autorité d'application des lois ou d'un organe de sûreté de l'État susceptible d'avoir des effets négatifs sur les garanties fournies par les BCR, l'Autorité de protection des données compétente en sera informée par le CPD ou le CPDG, sauf disposition contraire des lois locales applicables. Les informations communiquées à l'APD doivent inclure des informations concernant les données demandées, l'organe ayant fait la demande et le fondement juridique de la divulgation.

Si la notification des demandes de divulgation est interdite en vertu des lois locales applicables, l'Entité AXA BCR ayant reçu la demande fera tout son possible pour renoncer à cette interdiction. Si, bien qu'elle ait fait son possible, il ne peut être renoncé à l'interdiction, l'Entité AXA BCR ayant reçu la demande doit fournir des informations générales annuelles à l'Autorité de protection des données compétente concernant les demandes qu'elle a reçues.

Dans tous les cas, la divulgation des Données à Caractère Personnel par une Entité AXA BCR à toute autorité publique doit être conforme aux principes de traitement indiqués à l'article IV et ne peut être massive, disproportionnée et discriminante d'aucune manière qui dépasserait ce qui est nécessaire au sein d'une société démocratique.

## **ARTICLE XI - DATE D'ENTRÉE EN VIGUEUR ET DURÉE DES REGLES D'ENTREPRISE CONTRAIGNANTES**

Les BCR prennent effet le 15 janvier 2014 pour une durée indéterminée.

Chaque Entité AXA BCR est tenue d'appliquer les BCR à compter de la date d'entrée en vigueur de l'AG conclu au titre des présentes BCR. Une Entité AXA BCR concernée cessera d'appliquer les BCR dès lors que (i) les BCR sont résiliées moyennant préavis écrit adressé par le CPDG à l'Autorité de protection des données coordinatrice (la CNIL) et à chaque Entité AXA BCR ; ou que (ii) l'AG conclu a été résilié conformément aux conditions définies dans celui-ci.

## **ARTICLE XII - LOI APPLICABLE - JURIDICTION COMPETENTE**

### **1. Loi applicable**

Les présentes BCR (y compris les AG) sont régies et interprétées en vertu du droit français.

### **2. Litige entre l'Importateur de données et l'Exportateur de données**

Le règlement de tout litige entre l'Importateur de données et l'Exportateur de données dans le cadre des BCR relève de la juridiction compétente du pays de l'Exportateur de données, à moins que la législation en vigueur du pays n'en dispose autrement.

### **3. Autres litiges entre des Entités AXA BCR**

Le règlement de tout autre litige entre les Entités AXA BCR dans le cadre des BCR (y compris des Accords sur les BCR) relève de la compétence des tribunaux de Paris de la juridiction compétente, sauf autre disposition obligatoire prévue par la législation en vigueur.

### **4. Litiges avec des Personnes concernées d'un Pays Adéquat**

Dans les limites autorisées par la législation en vigueur et les dispositions relatives aux droits des Tiers prévues dans les présentes BCR, une Personne concernée d'un Pays Adéquat est en droit d'exercer un recours à l'encontre d'une Entité AXA BCR :

- (i) devant les juridictions compétentes d'un pays de l'EEE au choix de la Personne Concernée : la Personne Concernée peut choisir d'agir par-devant les tribunaux du pays de l'EEE dans lequel l'Exportateur de données est établi ou par-devant les tribunaux du pays de l'EEE où la Personne Concernée avait sa résidence habituelle au moment où les Données à Caractère Personnel impliquées dans la réclamation sont collectées ; ou
- (ii) devant les tribunaux de Paris.

## **ARTICLE XIII - MISE À JOUR DES RÈGLES**

Le CPDG est tenu de contrôler et d'actualiser régulièrement les BCR, par exemple suite à des changements importants au niveau de la structure de l'entreprise et du cadre réglementaire.

Toutes les Entités AXA BCR reconnaissent et acceptent que :

- Des modifications importantes, ayant pour effet de renforcer de manière significative les obligations incombant aux Entités AXA BCR, soient apportées aux BCR suite à une décision du **Comité de pilotage AXA BCR** dans un délai d'un (1) mois à compter de la consultation par e-mail des Entités AXA BCR par le biais d'e-mails adressés par les CPD reconnus par le CPDG ; et
- Des modifications peu importantes, autrement dit toutes les autres modifications, soient apportées aux BCR suite à une décision du **Comité de pilotage AXA BCR** sans nécessaire consultation préalable des Entités AXA BCR.

Le CPDG sera chargé d'établir la liste des Entités AXA BCR et d'enregistrer toutes les modifications apportées aux BCR et aux Entités AXA BCR. Le CPDG communiquera chaque année sur demande les changements au niveau des Entités AXA BCR et tout changement substantiel apporté aux BCR à l'Autorité de protection des données coordinatrice ainsi qu'à toute autre Autorité de protection des données compétente. Le CPDG communiquera sans tarder tout changement qui affecterait de manière significative le niveau de protection proposé par les BCR ou affecterait de manière significative les BCR à l'Autorité de protection des données coordinatrice. Le CPD doit être en mesure de mettre à disposition de la Personne concernée d'un Pays Adéquat ladite version actualisée des BCR, sur demande.

#### LISTE DES ANNEXES :

Annexe 1 : AG

Annexe 2 : Programme de contrôle de l'application des règles