Nos engagements RGPD

AXA France – Mai 2021

Règlement Général sur la Protection des données

Madame, Monsieur,

Avec l'entrée en vigueur du Règlement européen sur la Protection des Données (RGPD), vous vous posez légitimement des questions sur la mise en conformité de notre société.

Ce document est là pour vous donner la transparence nécessaire sur les différentes mesures déployées et réaffirmer la volonté d'AXA France de protéger vos données.

1. Une activité d'assureur fortement réglementée.

Les activités d'AXA France sont réglementées par de nombreux textes.

Outre la loi française dite « Informatique et Libertés », connue pour avoir très tôt été particulièrement protectrice des données personnelles, et aujourd'hui le RGPD, AXA France est également soumise à des normes et réglementations de protection particulièrement exigeantes pour le secteur de l'assurance (code des assurances, code monétaire et financier, recommandations de l'Autorité de contrôle prudentiel et de résolution…).

Ces différents textes encadrent et sécurisent notre activité.

Comme assureur, réassureur ou co-assureur, AXA France est donc, plus que les entreprises d'autres secteurs, particulièrement sensibilisée et responsabilisée sur la protection des données personnelles.

2. Un statut de responsable de traitement du fait de la spécificité de notre métier.

Par la spécificité de ses activités, AXA France, lorsqu'elle intervient en tant qu'assureur, se positionne comme responsable de traitement au sens de l'article 4 du RGPD, à savoir celui qui « détermine les finalités et les moyens du traitement ».

Elle remplit effectivement l'ensemble des critères en ce sens, lorsqu'elle intervient comme assureur, tels que détaillés par l'avis 1/2010 du G29, toujours d'actualité dans la mesure où l'article 4 du RGPD n'a pas modifié la définition de responsable de traitement, comme :

- être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres,

- le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables que cette visibilité peut susciter chez ces dernières,

- la détermination des «moyens» englobe donc à la fois des questions techniques et d'organisation, auxquelles les sous-traitants peuvent tout aussi bien répondre (par exemple, « quel matériel informatique ou logiciel utiliser ? »), et des aspects essentiels qui sont traditionnellement et intrinsèquement réservés à l'appréciation du responsable du traitement, tels que « quelles sont les données à traiter ? », « pendant combien de temps doivent-elles être traitées ? », « qui doit y avoir accès », etc.,

- la détermination de la finalité du traitement est réservée au responsable du traitement. Toute personne qui prend cette décision est donc un responsable du traitement (de fait).

Appliqué à un contrat d'assurance, c'est bien AXA France, assureur, qui détermine la finalité principale du traitement d'assurance (assurance, adhésion, gestion, lutte contre le blanchiment, lutte contre la fraude…) et les moyens essentiels pour la réalisation de ces traitements (sélection des données nécessaires, durée de conservation…).

Dans ce cadre, à titre d'exemple, une entreprise qui souhaiterait souscrire un contrat d'assurance collectif au bénéfice de ses salariés, interviendrait quant à elle en tant que responsable du traitement des données de ses salariés : ce traitement ayant pour finalité la gestion du contrat de travail, incluant notamment la souscription par l'entreprise d'un contrat d'assurance collective au bénéfice de ses salariés. Dans ce contexte cette entreprise pourrait être amenée à transférer les données de ses salariés à AXA France, assureur. Il s'agirait donc d'un transfert de données de responsable de traitement dont la finalité est la gestion des ressources humaines à responsable de traitement dont la finalité est la gestion du contrat d'assurance.

Ainsi, par la spécificité du métier d'assureur, celui-ci n'est pas assimilable à un fournisseur ou prestataire de service qui aurait vocation à participer à tout ou partie d'un traitement de données personnelles comme sous-traitant. Il ne lui est pas délégué une tâche ou fonction qu'une entreprise souscriptrice de produits d'assurance pourrait exercer elle-même mais aurait choisi de lui confier.
Cela parce que l'assurance, la réassurance ou la co-assurance est qui plus est un métier qui exige un agrément et une expertise bien particulière.

Dans ce contexte, AXA France est légitime, en tant que responsable de traitement, à collecter, traiter et conserver, aussi longtemps que nécessaire, les données à caractère personnel dont elle a besoin pour exercer ses activités et remplir ses obligations.
L'article 28 du RGPD relatif au sous-traitant lui est ainsi inapplicable et il ne peut être exigé l'insertion des mentions et droits décrits à cet article au contrat d'assurance, comme des normes particulières d'audit ou de sécurité, ou un questionnaire détaillé à compléter qui aurait pour objet la sous-traitance.
Toutefois, nous vous confirmons qu'en tant que responsable de traitement, AXA France assure évidemment la sécurité et la conformité de ses traitements avec la réglementation en vigueur et notamment le RGPD et la production de cette note a vocation à vous apporter les éléments nécessaires pour en juger.

3. Un DPO et un Chief IT Security Officer, alliant la double compétence data et sécurité.

AXA France a fait le choix d'un Data Protection Officer (DPO) qui exerce en même temps comme Chief Security Officer (CSO) de niveau 2 , assisté par un Chief IT Security Officer (CITSO) avec des équipes dédiées.
De ce fait, la fonction bénéficie des leviers et compétences qui sont les miennes tant sur les aspects de protection des données personnelles que sur les aspects de de sécurité physique et logique de ces dernières.

Le DPO nommé auprès de la CNIL est le garant de la conformité d'AXA France en matière de protection des données personnelles. A ce titre, ses missions sont notamment de :

- tenir à jour la liste des traitements de données à caractère personnel et en contrôler la conformité,
- conseiller les différentes entités de l'entreprise,
- garantir les droits de l'ensemble des assurés (droits d'accès, derectification, d'opposition...),
- veiller à la conformité continue d'AXA France au RGPD
- assurer la sensibilisation et la formation des différentes parties prenantes.

Le CSO est le garant de la sécurité d'AXA France sur les trois piliers fondamentaux : Sécurité du SI – dont cybersécurité, Résilience Opérationnelle et Sécurité Physique avec les missions principales suivantes :

- garantir un niveau de sécurité adapté à la stratégie du Groupe et d'AXA France, effectif et conforme à la réglementation,
- conseiller le management de l'entreprise sur la stratégie de sécurité à mettre en place sur les trois fonctions,
- identifier et analyser les risques de sécurité en lien avec l'évolution du contexte business et cyber, évalue leur impact possible, définit les plans d'action de réduction des risques et en supervise l'exécution pour garantir l'atteinte des objectifs d'AXA France,
- définir et exécuter les plans de sensibilisation et de formation des différentes parties prenantes à la sécurité
- superviser l'utilisation des budgets affectés à la sécurité,
- superviser la gestion de la confidentialité et l'intégrité du Système d'Information,
- s'assurer du traitement effectif des incidents de sécurité.

Le C.IT.SO assiste le CSO sur le volet sécurité du SI. Ses missions sont notamment de :

- gérer et traiter les risques liés à la disponibilité, confidentialité et l'intégrité du système d'information (SI) et des informations qu'il contient,
- définir et assurer la mise en œuvre des règles de sécurité à prendre en compte lors de la conception,
le déploiement et la gestion de chaque activité d'AXA France,
- gérer les incidents de sécurité et identifier et traiter les causes qui en sont à l'origine.

Pour garantir la bonne fin des missions qui nous ont été confiées, AXA France s'est imposé des politiques rigoureuses, à jour du RGPD, comme sa politique générale de sécurité des systèmes d'information et sa politique relative à la protection des données à caractère personnel.

4. Des contrôles internes et externes réguliers.

AXA France fait par ailleurs l'objet de contrôles réguliers, qui garantissent une continuité et une qualité permanente de son niveau de protection des données :

- AXA France est auditée chaque année par ses Commissaires aux Comptes (Mazars et PWC) sur la gestion des droits d'accès à nos systèmes, ainsi que sur d'autre sujets de sécurité,

- tous les sites web d'AXA France sont testés au moins une fois par an (tests d'intrusion) par des auditeurs externes tels que Ernst & Young, Deloitte ou Devoteam, qui sont régulièrement remis en concurrence pour éviter toute connivence,

- le département d'audit du groupe AXA vérifie régulièrement le niveau de sécurité d'AXA France (à titre d'exemple, nous avons répondu en 2018 à un audit sur « La Politique et la gestion des données à caractère personnel », un second sur « La gestion des droits d'accès des collaborateurs » et un troisième sur « La Gouvernance de la sécurité »),

- l'autorité de tutelle des assureurs, l'ACPR, est venue auditer la gestion du groupe AXA en matière de gouvernance de la sécurité,

- le DPO du groupe AXA réalise au moins trois fois dans l'année une revue de l'effectivité de la protection des données à caractère personnel mise en place par AXA France.

5. Un programme de mise en conformité complet

AXA France a, comme toute entreprise européenne, mené un programme de mise en conformité au RGPD dès 2016.

Parmi les nombreux chantiers de ce programme, il y a notamment :

- l'envoi d'une notice d'information à l'ensemble des assurés pour leur expliquer leurs nouveaux droits,
- le déploiement d'une nouvelle mention conforme à l'article 13 du RGPD dans nos documents à destination des assurés,
- la révision des contrats avec nos prestataires sous-traitants pour y insérer une nouvelle clause type et une annexe dédiée avec les mentions requises par l'article 28 du RGPD, ou encore
- une procédure de détection et de notification des violations de données à caractère personnel de l'article 33 du RGPD.

Ce programme a bénéficié des débats conduits au sein de la Fédération Française des Assureurs auxquels participent l'ensemble des assureurs de la place et leurs experts en RGPD.

6. Un engagement de tout le Groupe AXA sur la protection des données

Le groupe AXA s'est engagé depuis longtemps dans la protection des données personnelles, avec des standards d'exigence déployés au sein de toutes ses sociétés et publiquement affichés, qui anticipaient sur le RGPD.

Le groupe AXA a également fait valider des Binding Corporate Rules (**BCR**) pour des transferts internationaux de données à l'intérieur de son Groupe qui respecte la réglementation (ces documents sont en ligne sur le site https://www.axa.com/fr/a-propos-d-axa/nos-engagements).

Nous restons à votre entière disposition pour toute information complémentaire dont vous souhaiteriez disposer.

Sylvain BIZOUARD
Data Protection Officer
Chief Security Officer
AXA France

Marion CHARLES

Chief IT Security Officer
AXA France